SKI Report 94:2

SAFETY EVALUATION BY LIVING PROBABILISTIC SAFETY ASSESSMENT

PROCEDURES AND APPLICATIONS FOR PLANNING OF OPERATIONAL ACTIVITIES AND ANALYSIS OF OPERATING EXPERIENCE

(NKS/SIK-1(93)16)

Gunnar Johanson and Jan Holmberg (editors)

January 1994

Application:	Long term safety planning	Risk planning of operational activities	Risk analysis of operating experience
Approach:	Risk assessment	Risk monitoring	Risk follow-up
Result:	Identification of risk contributors Comparison of alternative design and procedures	Test planning Maintenance planning Operational decision making	Analysis of operating experience Operational risk experience feedback Verification of PSA models
Risk measure:	Nominal risk Inherent risk	Instantaneous risk	Retrospective risk Probabilistic indicators

ISSN 1104-1374
ISRN SKI-R--94/2--SE

SKI STATENS KÄRNKRAFTINSPEKTION
Swedish Nuclear Power Inspectorate

SKI Report 94:2

SAFETY EVALUATION BY LIVING PROBABILISTIC SAFETY ASSESSMENT

PROCEDURES AND APPLICATIONS FOR PLANNING OF OPERATIONAL ACTIVITIES AND ANALYSIS OF OPERATING EXPERIENCE

(NKS/SIK-1(93)16)

Gunnar Johanson[1] and Jan Holmberg[2] (editors)

1) ES Konsult, Box 12049, 10222 Stockholm, Sweden (since 1995)
2) VTT Automation, Industrial Automation, P.O. Box 1301, FIN-02044, Finland

January 1994

(PDF Reprint November 96)

SUMMARY

Living Probabilistic Safety Assessment (PSA) is a daily safety management system and it is based on a plant-specific PSA and supporting information system. In the living use of PSA, plant status knowledge is used to represent actual plant safety status in monitoring or follow-up perspective. The PSA model must be able to express the risk at a given time and plant configuration. To increase the availability of the basic PSA for the operational safety management, the model as well as the whole PSA programme should be developed to a more dynamic tool. The process, to update the PSA model to represent the current or planned configuration and to use the model to evaluate and direct the changes in the configuration, is called living PSA programme.

The main purposes to develop and increase the usefulness of living PSA are:

Long term safety planning: To continue the risk assessment process started with the basic PSA by extending and improving the basic models and data to provide a general risk evaluation tool for analyzing the safety effects of changes in plant design and procedures.

Risk planning of operational activities: To support the operational management by providing means for searching optimal operational, maintenance and testing strategies from the safety point of view. The results provide support for risk decision making in the short term or in a planning mode. The operational limits and conditions given by Technical Specifications can be analyzed by evaluating the risk effects of alternative requirements in order to balance the requirements with respect to operational flexibility and plant economy. The effect of test interval and possible staggering of redundant tests can be evaluated from the risk point of view by a dynamic and time-dependent plant model.

Risk analysis of operating experience: To provide a general risk evaluation tool for analyzing the safety effects of incidents and plant status changes. The analyses are used to:
- identify possible high risk situations,
- rank the occurred events from safety point of view, and
- get feedback from operational events for the identification of risk contributors.

The development of routines and procedures for living PSA includes transfer of PSA-related information within the organizations. Living PSA application will always require specialists to operate and maintain the model. However, a better operational interface will allow a more efficient use and a broader spectrum of users to carry out the applications. To implement a living PSA programme requires that plant personnel are heavily involved and appreciate the benefits of working according to this procedure. The plant organization will in the end decide for themselves to what extent these methods shall be used in the safety management of the NPP.

Based on the work and the demonstrations carried out it is recommended that a living PSA programme is implemented on a plant specific basis. The implementation can preferably be divided in two steps.

1) Prepare procedures, models, and data to carry out basic risk monitoring applications.

   - Evaluation of test arrangements (test intervals, test staggering and test methods): Following this application also configuration control and short term risk planning will be possible on the same basis.

- Evaluation of allowed outage times and action requirements in failure situations: Following this application also maintenance planning will be possible.

- Analysis of operational experience by risk follow-up, generation of severity ranking and probabilistic safety indicators.

2) Prepare criteria and procedures for risk decision making, i.e. exemptions from limiting conditions for operation stated in Technical Specifications

The early as well as fast identification of discrepancies and deficiencies in plant design and operation is considered essential for safety. The design aspects on plant safety are handled to a large extent by the basic PSA. As a result of a living PSA, the safety aspects on operational, maintenance or testing practices can be evaluated, and modified, and the flexibility in operation may be increased. A feasible risk monitoring system, gradually tailored and implemented for plant specific use by its user organizations, is aimed to support the risk management activities of the utilities, as well as the inspection activities of the authorities.

This report describes the methods, models and applications required to continue the process towards a living use of PSA.

SAMMANFATTNING

Levande probabilistisk (sannolikhetsbaserad) säkerhetsanalys (PSA) är ett system för daglig hantering av säkerhetsfrågor baserat på en anläggningsspecifik PSA och tillhörande informationssystem. Vid en levande användning av PSA utnyttjas den löpande informationen om säkerhetssystemens driftklarhet för att kontinuerligt värdera eller följa upp risken. PSA-modellen måste kunna värdera risken vid en given tidpunkt och konfiguration, d.v.s. driftklarhet av säkerhetrelaterade komponenter. För att möjliggöra detta måste den ursprungliga PSA-modellen och även hela PSA-programmet utvecklas till ett mer dynamiskt verktyg. Denna process att löpande uppdatera PSA-modellen för att representera den nuvarande eller en planerad konfiguration samt att använda modellen till att värdera och styra konfigurationen kallas för ett levande PSA-program.

Det huvudsakliga skälen till att utveckla och öka användbarheten av levande PSA är för:

Långsiktig riskplanering: Att fortsätta den riskvärdering och säkerhetsanalys som startades med den ursprungliga PSAn, genom att utöka och förbättra dess modeller samt data, för att tillhandahålla ett verktyg för analys av säkerhetseffekten vid förändringar i konstruktion eller procedurer.

Riskplanering för drift- och underhållsaktiviteter: Att stödja drift- och underhållsplaneringen genom skapa förutsättningar att söka optimala drift-, underhålls- och teststrategier ur säkerhets-synpunkt. Resultaten skall ge stöd vid beslut i olika driftsituationer eller som ett planeringsverktyg. De driftbegränsningar och villkor som ges i säkerhetstekniska föreskrifter (STF) kan analyseras, och säkerhetseffekten av olika krav kan värderas. Avsikten kan också vara att balansera dessa för att kunna höja flexibiliteten vid drift och förbättra driftekonomin. Effekten av olika testinterval och olika teststrategier kan riskvärderas genom att modellen är mer dynamisk och tidsberoende.

Riskanalys av drifterfarenheter: Att stödja erfarenhetsåterföringen med ett riskvärderingsverktyg för analys av säkerhetseffekten från händelser och förändringar i driftklarhetsstatus för komponenter i anläggningen. Analysen används till:

- Identifiering av driftsituationer med hög risk,
- rangordning av inträffade händelser ur säkerhetsynpunkt och
- ge erfarenhetsåterföring från inträffade händelser för identifiering av dominerade bidrag till härdskaderisken.

Utveckling av rutiner och procedurer för levande PSA inkluderar överföring av PSA-relaterad information inom organisationen. Levande PSA-tillämpningar kommer alltid att kräva specialister för att använda och underhålla modellen. Ett förbättrat användargränssnitt kommer att medföra en mer effektiv användning och ett utökat antal användare. Att införa ett levande PSA-program kräver att anläggningspersonal för drift och underhåll ser värdet i att arbeta enligt denna procedur. Anläggningsorganisationen måste själv besluta i vilken utsträckning dessa metoder skall utnyttjas i säkerhetsarbetet vid verket.

Baserat på det utvecklingsarbete och de praktiska demonstrationer som har utförts rekommenderas att ett levande PSA program införs anläggningsspecifikt. Driftsättningen utförs lämpligast i två steg.

1) Skapa procedurer, modeller och data samt utföra grundläggande risk värderingar.

   - Utvärdering av testarrangemang (testinterval, teststrategier och testmetoder). Med samma underlag kan sedan även styrning av komponenters driftklarhet och löpande riskplanering utföras.

- Utvärdering av driftbegränsningar och tillåtna hindertider vid felsituationer. Med samma underlag kan sedan även underhållsplanering ur risksynpunkt utföras.

- Analys av drifterfarenheter genom riskuppföljning, generering av allvarlighets rangordning efter bidraget till härdskadefrekvensen och sannolikhetsbaserade säkerhetsindikatorer.

2) Skapa sannolikhetsbaserade kriterier och procedurer för beslutsstöd, t.ex. för säkerhetsvärdering av händelser, STF ändringar eller dispenser.

En tidig eller snabb identifiering av fel eller brister i anläggningens konstruktion, drift eller underhåll är väsentligt för säkerhetsarbetet. Säkerhetsaspekterna på konstruktion är i stor utsträckning hanterade i den ursprungliga PSAn. Ett viktigt resultat från levande PSA är att säkerhetsaspekter på drift, underhåll och testarrangemang kan utvärderas och förbättras samt att flexibiliteten i driften kan begrundas. Ett ändamålsenligt riskvärderingssystem, anpassat och drifttaget av anläggningsorganisationen har som mål att stödja det dagliga säkerhetsarbetet på verket, samt även stödja myndighetens tillsyn.

Denna rapport beskriver metoder, modeller och tillämpningar som behövs för att fortsätta arbetet mot en levande användning av PSA.

YHTEENVETO

Elävä todennäköisyyspohjainen turvallisuusanalyysi (PSA) tarkoittaa riskianalyysin käyttöä päivittäisissä ydinvoimalaitoksen turvallisuuden hallintaan liittyvissä kysymyksissä. Se perustuu laitosta kuvaavan riskimalliin ja tietojärjestelmään, jolla riskimallia käsitellään. PSA:n elävässä käytössä mallia käytetään päivittäin laitoksen käyttötilassa tapahtuvien muutosten arviointiin ja suunnitteluun. Jotta se olisi mahdollista, on perus-PSA kehitettävä sellaiseksi, että mallilla pystytään joustavasti arvioimaan laitoksen hetkellistä riskitasoa. Elävää PSA:ta voidaan hyödyntää

• **Riskiperusteisessa pitkän tähtäimen suunnittelussa,** jolloin jatketaan perus-PSA:lla alkanutta turvallisuusanalyysiprosessia parantamalla mallia ja täydentämällä tietokantaa niin, että saadaan menetelmä laitoskonstruktioon tai ohjeisiin tehtävien muutosten arviointiin.

• **Käyttötoimenpiteiden riskiperusteisessa suunnittelussa,** jolloin laitoksen käytön ja kunnossapidon strategioita voidaan optimoida riskiperustaisesti. Analyysin tulokset tukevat lyhyen tähtäimen suunnittelua.

• **Käyttökokemusten riskiperusteisessa arvioinnissa,** jolloin laitoksella sattuneiden tapahtumien turvallisuusmerkitystä analysoidaan. Analyysien avulla voidaan

) tunnistaa tilanteita, joihin on liittynyt merkittäviä riskejä
) vertailla tapahtumia turvallisuusmerkityksen kannalta
) saada käyttökokemuksista palautetta riskitekijöiden tunnistamiseen.

Elävää PSA:ta varten on kehittävä ohjeet, joiden perusteella riskianalyysitoiminta hallitaan organisaatiossa. PSA-asiantuntijoita tarvitaan mallin ylläpitoon ja laskentaan. Tietokonejärjestelmän on kuitenkin vastattava myös varsinaisten hyödyntäjien tarpeita, koska elävän PSA:n toteutuminen ei onnistu, ellei laitoshenkilökunta ole mukana toiminnassa ja ellei se näe toimintaa hyödylliseksi. Laitosorganisaatio päättää aina itse, missä laajuudessa elävä PSA otetaan käyttöön turvallisuuden hallinnassa.

Pohjoismaisessa NKS/SIK-1-tutkimusprojektissa tehtyjen tutkimusten ja demonstraatioiden perusteella suositellaan, että elävä PSA voidaan toteuttaa kahdessa vaiheessa:

1) Kehitetään ohjeet, mallit ja tietokanta dynaamista laskentaa varten, jolloin

) määräisaikaiskoestukseen liittyviä toimintoja voidaan arvioida,
) sallittuja korjausaikoja ja vikatilanteisiin liittyviä käyttöstrategioita voidaan arvioida ja
) käyttökokemuksia voidaan arvioida.

2) Kehitetään päätöksentekokriteerit ja ohjeet riskipäätöksentekoon.

Elävän PSA:n tavoitteena on ennalta ehkäistä vaaratilanteiden syntyminen. Kun perus-PSA:lla voidaan arvioida laitoskonstruktioon liittyviä kysymyksiä, niin elävä PSA mahdollistaa käyttö-, kunnossapito- ja koestustoiminnan vaikutusten arvioinnin. Tämä lisää joustavuutta laitoksen käytössä. Samalla se tukee myös viranomaisen tarkastus- ja valvontatoimintaa.

Tämä raportti kuvaa elävää PSA:ta varten tarvittavat menetelmät, mallit ja elävän PSA:n sovellukset.

FOREWORDS

The development of nuclear safety evaluation has been the object of Nordic research cooperation since 1977. The cooperation in the development of Probabilistic Safety Analysis (PSA) started during the second program (1980 - 85) with NKA/SÄK-1 "PRA Uses and Techniques, a Nordic Perspective". Within the third program NKA/RAS-400 "Risk Analysis and Safety Rationale" (1986 - 90), PSA methodology development was the topic for the project NKA/RAS-450 "Optimization of Technical Specifications by Use of Probabilistic Methods" and NKA/RAS-470 "Dependencies, Human Interaction and Uncertainties in Probabilistic Safety Assessment".

In the current program, the Nordic research project "Safety Evaluation, NKS/SIK-1" (1990-93), the main objective is to define and demonstrate the practical use of Living PSA and Operational Safety Indicators for safety evaluation and for identification of possible improvements in operational safety.

The development and application work has been carried out by a Nordic working group on Living PSA and Safety Indicators. The group consists of experts on operational safety, PSA, reliability assessment and decision support. Representatives from utilities, regulatory authorities, research institutes, vendors and consultants work in these groups. The working groups consist of representatives from Swedish Nuclear Power Inspectorate (SKI), Swedish State Power Board (Vattenfall), Finnish Centre for Radiation and Nuclear Safety (STUK), Teollisuuden Voima Oy (TVO), Risö National Laboratories and Technical Research Centre of Finland (VTT), Avaplan Oy, Relcon AB, IFE Halden, and Studsvik Nuclear have participated. Other Nordic nuclear power utilities Oskarshamnsverkets Kraftgrupp (OKG), Southern Swedish Power Board (Sydkraft) and Imatran Voima Oy (IVO) participate in the working group meetings and in case studies.

PROJECT REPORTING

The NKS/SIK- 1 project reporting are divided in three parts.

I NKS/SIK-1 Project summary report: Safety evaluation by living probabilistic safety assessment and safety indicators, 50 p. (to be published during 1994)
II Safety evaluation by living probabilistic safety assessment (this report), plus NKS/SIK-1 Reports and publications, SKI Technical Report 94:3 (~800 p).
III Safety evaluation by safety indicators, ~100 p., (to be published during 1994).

This report (SKI TR 94:2) has been prepared by a team consisting of:

Gunnar Johanson	IPS AB/Sweden (Consultant representing Swedish Nuclear Power Inspectorate)	Assistant project leader and coordinator for LPSA part. Main author and editor
Jan Holmberg	VTT/Technical Research Centre of Finland	Main author and editor, Decision analysis and Methods development
Kari Laakso	VTT/Technical Research Centre of Finland	Project leader
Johan Sandstedt	Relcon AB/Sweden (Consultant representing the Swedish utility OKG)	LPSA demonstrations and methods
Ulla-Karin Wendt	Vattenfall AB/Sweden (Swedish utility)	LPSA demonstrations and methods
Egil Stokke	IFE Halden/Norway	LPSA system and User Interface
Ilkka Niemelä	STUK - Finnish Centre for Radiation and Nuclear Safety	Demonstrations, User Interface and methods
Tuomas Mankamo	Avaplan Oy/Finland (Consultant)	Demonstrations and methods
Kurt Pörn and Kecheng Shen	Studsvik Ecosafe/Sweden	Uncertainty analysis and decision analysis

Routines and procedures of how to utilize living PSA (LPSA) are demonstrated in the case studies. The demonstrations include applications to exemplify the different development areas. The Oskarshamn 2 PSA has been used as a LPSA demonstration model. To enable the demonstrations and exemplify the capabilities of the LPSA applications the model has been continuously enhanced with respect to LPSA capabilities, completeness and conservatism. This has been possible due to the kind support from the plant owner OKG. The Forsmark 1/2 PSA and TVO I/II PSA have also been used for demonstrations, based on support from the plan owners Vattenfall and Teollisuuden Voima, the demonstrations have been carried out without or with limited model enhancements.

LIST OF ABBREVIATIONS

AGR	advanced gas cooled reactor
AOT	allowed outage time of safety related equipment
ASP	accident sequence precursor
ATV	Arbetsgruppen för Tillförlitlighet, Värmekraft, Reliability data system, Sweden and Finland
BNL	Brookhaven National Laboratory, USA
BWR	boiling water reactor
CCF	common cause failure
CSNI	Committee on the Safety of Nuclear Installations, OECD
EPRI	Electric Power Research Institute, USA
ESSM	Essential Systems Status Monitor, Nuclear Electric
IAEA	International Atomic Energy Agency
IFE	Institutt for energiteknikk, Norway
IPERS	international peer review service of PSA studies, IAEA
IVO	Imatran Voima Oy, Finland
JRC	Joint Research Centre, European Community
LCO	limiting conditions for operation
LER	licensee event report
LMFBR	liquid metal cooled fast breeder reactor
LPSA	living PSA
MGL	Multiple Greek Letter model
NKA/RAS	Nordic research program on risk analysis and safety philosophy, 1985)89
NKS	Nordic nuclear safety research
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission, USA
OECD	Organization for Economic Co-operation and Development
OKG	Oskarshamn Kraftgrupp, Sweden
OSI	operational safety indicators
PI	performance indicator
PSA	probabilistic safety assessment
PWG	principal working group, OECD/CSNI
PWR	pressurized water reactor
RCM	reliability centered maintenance
RHR	residual heat removal
RHRS	residual heat removal system
SAIC	Science Applications International Corporation, USA
SSW	standby service water
SIK	Nordic research program on reactor safety, 1990)93
SKI	Statens kärnkraftinspektion, Swedish Nuclear Power Inspectorate
STI	surveillance testing interval
STUK	Säteilyturvakeskus, The Finnish Centre for Radiation and Nuclear Safety
TS	technical specifications
TVO	Teollisuuden Voima Oy, Industrial power company, Finland
TÜV	Technischer Überwachungs-Verein, Germany
VTT	Valtion teknillinen tutkimuskeskus, Technical Research Centre of Finland

TERMS

Allowed Outage Time. This stipulates the maximum allowed outage time (AOT) for an equipment in a safety system. The unit must usually be placed to a safer operational state, if the operability of the faulty equipment is not reached within its AOT.

Basic Event. A reliability analysis can be carried out down to a component failure mode or human error level where sufficiently reliable experience data can be obtained. The occurrences, included in a reliability model, at the most detailed level are called basic events. The state of *evident* basic events are known with certainty. Examples of evident basic events are maintenances and repairs of the components. The state of *hidden* basic events cannot be known with certainty. Tests and demand situations may timely reveal what the state has been.

Common cause failure. Common cause failures (CCF) are failure causes or mechanisms which results in multiple failures in redundant components. CCF basic events are usually added in the PSA model to cover residual, not explicitly identified dependences between redundant components

Initiating event. An initiating event or initiator is a disturbance in the normal (power) operation which cannot be balanced without an interference of the plant protection and safety systems. Initiating events are usually divided into several categories depending on the required plant responses. Main categories are loss of coolant accidents (LOCA) of various leakage sizes and process transients such as a loss of the main feedwater system, and external events such as loss of off-site power.

Instantaneous risk frequency. The instantaneous risk frequency of PSA corresponds to a PSA model with basic events modelled according to plant status knowledge. The component or system concerned is presented in the model by evident events (true or false) and by hidden events (time-dependent unavailability model). If the evident unavailability caused by maintenance and repair is excluded, then an instantaneous baseline risk frequency is obtained.

Limiting conditions for operation. The limiting conditions (LCO) for operation are rules to be followed in order to maintain the plant operation within the bounds of safety analysis. The LCOs specify requirements on the number of subsystems operable at different operational states and the allowed outage times for equipment. These operational rules shall assure that safety systems are either ready for use or functioning on real demands, i.e. plant transients and accidents.

Minimal cut set. A cut set is a combination basic events, e.g. component failures, leading to system failure. This cut set is called minimal cut set, if the intended system function can be achieved by elimination of a single basic event only.

Nominal risk frequency. The nominal risk frequency of PSA obtained by the use of nominal or time-average failure probabilities for component and system failures as well as for operator errors and by the use of nominal initiating event frequencies. If the evident unavailabilities caused by maintenance and repair are excluded, then a (nominal) baseline risk frequency is obtained. The nominal risk frequency is used in long term risk planning.

Probabilistic safety indicator. The results of a risk follow-up by PSA provides probabilistic safety indicators from the operating experience. Examples of probabilistic safety indicators are average risk frequency during observed period, risk doses, number of incidents exceeding a probability or frequency criterion.

Risk assessment. Risk assessment is the basic evaluation approach with a risk model. The aim of risk assessment is to calculate the nominal risk frequency of the plant and related risk measures. The results can be used to the identification of risk contributors and to long-term risk planning.

Risk dose. Risk dose is the afterwards calculated core damage probability of an incident or the core damage probability over the examined operating period.

Risk follow-up. The aim of risk follow-up is to calculate the risk doses and related risk measures based on the evaluation of operating experience.

Risk measures. Risk measures are means to present the results of various applications of PSA in a form of information, which is suitable for making conclusions. The basic risk measures are nominal, inherent and instantaneous risk frequency. Generated risk measures are used in applications. The most significant application, or rather an objective of PSA, is the risk contributor identification in which risk importance measures are practical. Other applications as well as generated risk measures can be seen as advanced forms of risk contributor identification and risk importance measures, respectively.

Risk monitoring. Risk monitoring has a short-term or an on-line evaluation perspective. The aim is to calculate the instantaneous risk frequency of current or currently planned plant configuration.

Technical Specifications. The technical specifications (TS) are safety rules, approved by the regulatory authority, stipulating the limits and conditions for safe operation of a nuclear power unit.

LIST OF CONTENT

1 INTRODUCTION

The NKS/SIK-1 project is performed within the joint Nordic research program NKS/SIK: Reactor Safety. It is part of the Nordic NKS nuclear safety research program for the period 1990-93. The project is realized in co-operation with Nordic nuclear power utilities, authorities, research institutes and consultants.

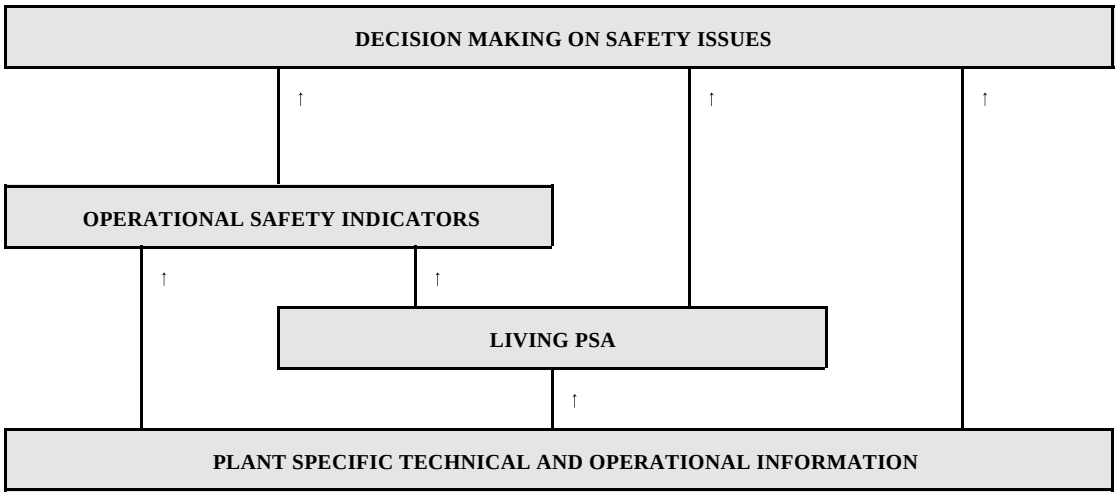
The key idea of this project is that plant state should be monitored and evaluated, and undesired events or accidents will be prevented more efficiently by a combined application of:

- Living probabilistic safety assessment (PSA), and
- Operational safety indicators.

This concept, Figure 1-1, would supplement the use of safety technical specifications by providing improved means for continuous monitoring of the risk level, and for early identification of degrading developments in safety performance of an operating nuclear power plant.

NORDIC RESEARCH PROJECT
NKS/SIK-1

"SAFETY EVALUATION BY USE OF LIVING PSA AND SAFETY INDICATORS"



A Concept of Safety Management Supported by Living PSA and
Operational Safety Indicators.

*Figure **1-2**: Conceptual idea of the use of Operational Safety Indicators and Living PSA.*

1.1 The usefulness of living PSA

The essential objective with the development of a living PSA concept is to bring the use of the plant specific PSA model out to the daily safety work to allow experience feedback of the operational risk and to increase the risk awareness of the intended users. The early and fast identification of discrepancies and deficiencies in plant operation or design is considered essential for safety. Nowadays the design aspects on plant safety are handled to a large extent by the basic PSA. As a result of a living PSA the safety aspects on operational, maintenance or testing practices can be

evaluated and modified and the flexibility in operational safety rules may be increased.

The living PSA concept involves a description of how the original PSA model can be continuously updated according to the actual status of the safety related systems of the plant. It is a daily safety management system, Figure 1-1, and it is based on a plant-specific PSA and supporting information system.

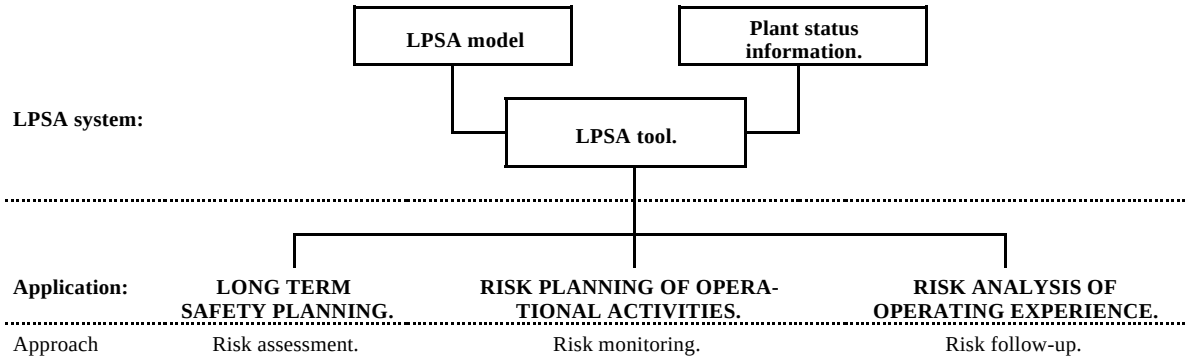


*Figure: **1-2**. The use of living PSA.*

1.1.1 Long term safety planning

> *To continue the risk assessment process started with the basic PSA by extending and improving the basic models and data to provide a general risk evaluation tool for analyzing the safety effects of changes in plant design and procedures.*

For the safety and the design management, the primary purpose of risk assessment is to identify the main risk contributors so that safety improving measures can be identified and prioritized. When the changes in designs or procedures have influence on the safety status, living PSA can provide support for the comparison of the alternatives.

1.1.2 Risk planning of operational activities

> *To support the operational management by providing means for searching optimal operational, maintenance and testing strategies from the safety point of view.*

The purpose of risk monitoring is to evaluate the instantaneous core damage frequency or the probability of reactor core damage during a short time interval given the information about the configuration of the safety-related systems. The results provide support for operational risk decision making in the short term or in a planning mode. Maintenance actions can be prioritized or planned so that the most safety critical systems are repaired or maintained in the first hand and other are postponed.

The operational limits and conditions given by Technical Specifications are analyzed by evaluating the risk effects of alternative requirements. The purpose is to balance the requirements with respect to operational flexibility and plant economy. The high risk situations permitted by Technical Specifications can be identified and replaced by such modes that give minimum risk, and also more flexible

requirements can be justified to replace too stringent ones. Individual requirements can be optimized by e.g. evaluating optimal allowed outage times from risk point of view.

Tests should be planned so that considered failures are detected but introduction of additional failure modes are avoided. The effect of test interval and possible staggering of redundant tests can be evaluated from the risk point of view by time-dependent component failure models.

1.1.3 Risk analysis of operating experience

To provide a general risk evaluation tool for analyzing the safety effects of incidents and plant status changes.

Analyses of operational experience are used to identify possible high risk situations, to rank the occurred events from safety point of view, and to get feedback from operational events for the identification of risk contributors. Exceptional failure combinations, dependencies between failures, repair actions, maintenance or operation modes can be identified. Safety significant events are identified from a large amount of operational data such as licensee event reports (LER), reactor trip reports and component failure reports. The severity is evaluated by calculating the conditional probability of an accident given the event. The safety-significant events are analyzed as deeply as necessary in order to identify the root causes of the events and to evaluate their severity. Ageing analyses are carried out with the aim to identify ageing effects in the safety function, system or component structures.

1.2 Objectives of the project

The main objective of the NKS/SIK-1project [1-1] is to define and demonstrate the practical use of:

- Living probabilistic safety assessment, and
- Operational safety indicators,

for safety evaluation and management and for identification of effective improvements in operational safety. Relating to living PSA the objective is to develop and define the living PSA concept for risk evaluation of:

- temporarily changed operating situations, i.e. failure, maintenance and disturbance situations, and
- permanent changes caused by modifications of designs or procedures.

The project also covers the study of problems related to risk decision making and a formulation of a suitable framework for use of PSA in safety related decision making.

A feasible risk evaluation and monitoring system, to be parallelly and gradually tailored and implemented for plant-specific use by its user organizations, is aimed to support the risk management activities of the utilities, as well as the inspection activities of the authorities.

Practical case studies are performed for specific nuclear power plants in order to:

- support and demonstrate the above developments

- identify related method and model development needs and other problem areas, and

- provide support for safety studies, safety development and safety-related decisions to be made by utilities and authorities.

1.3 Outline of the report

The outcome and experiences of the project related to living PSA are summarized and concluded in this technical report. The chapters in this report are divided and written for different categories of readers, as follows:

- The introduction and status of PSA activities, Chapter 1 and 2, are written for all types of readers and are intended to present an overview of the project and the preconditions for the project when it was started in 1990.

- A living PSA programme, Chapter 3, is written for plant management and is intended to present in general the work and the work format when applying LPSA in safety management.

- A living PSA model, Chapter 4, is written for PSA experts and it presents in detail methods and model features required to carry out the LPSA safety evaluations.

- A living PSA system, Chapter 5, is written for PSA code and system developers and it describes in detail work formats and requirements on codes and procedures.

- Safety evaluation by living PSA, Chapter 6, is written for LPSA users. The different applications are discussed in detail and are exemplified by results from the demonstration studies carried out within the project.

- Conclusions, Chapter 7, summarizes the experience gained from this project.

1.4 Plant and system types studied

The safety management applications described in this report are intended to be applied for nuclear power plants. The main hazard state considered in the application studies has been core damage, this can of course be altered for other states dependent on the safety issue of interest.

Safety functions and systems in Nuclear Power Plants are divided into redundant, and in many cases physically separated, subsystems. A safety function is provided by a system or can as in many cases be carried out by more than one system as a diversified safety function. To design, operate and maintain these functions in an optimal way from a safety point of view is one primary task in safety management and it is in this context the use of living PSA is demonstrated in this report.

1.5 Scope of the Living PSA development within the NKS/SIK-1 project

The steps involved in the development of basic PSA into living PSA and dynamic use of the results is illustrated in Figure 1-3. This project is concentrated on the first step to carry out main living PSA applications and to interpret both static and dynamic results and risk measures. The second and third step indicated in the figure are introduced to present a perspective on the future potential and

development of a risk control/advice system in comparison to the work performed in this project. For the latter steps only limited feasibility studies are performed at this stage.

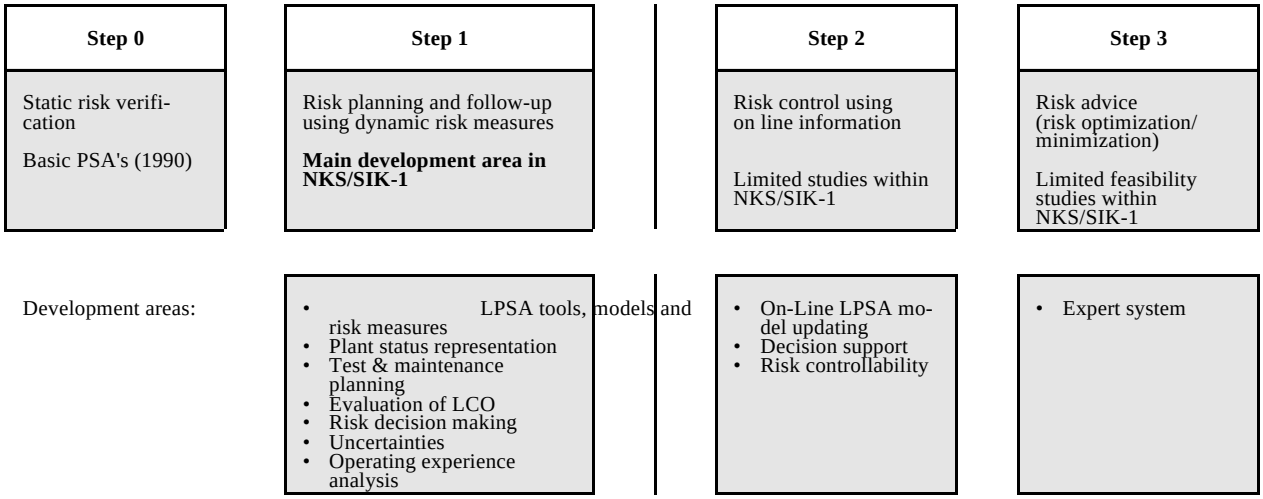


*Figure **1-3**: Development Steps for Living PSA*

1.6 References for section 1

SIK-1 reports

[1-1] Laakso K., Johanson,G., Björe, S., Virolainen, R. & Gunsell, L.. Safety Evaluation by Use of Living PSA and Safety Indicators, Work Plan 1990-1993. NKS/SIK-1(90)8. August 1990.

2 THE STATUS OF LIVING PSA

This chapter describes the status of the Nordic PSA activities based on the results of questionnary [2-1]. In addition, international developments in the field of living PSA systems and applications are presented [2-2], [2-3], [2-4].

2.1 Different phases of a PSA programme

By probabilistic safety assessment (PSA) nuclear power plants are assessed with respect to the likelihood of accidents. PSA provides a structured and logical procedure for identification of credible accident sequences and for assessment of their corresponding likelihood. PSA thus helps to identify weak spots in design and operation and in ranking dominant contributors to reactor core damage in a specific plant.

The overall status of probabilistic safety assessment (PSA) and the experiences of performing and utilizing PSA-studies are quite similar among all the utilities in Sweden and Finland. Three phases can be roughly distinguished in the PSA activities: basic PSA, extended PSA and living PSA (LPSA) [2-5]. The scope of the basic level 1 studies is currently being extended to cover other operational states than the power operation. The utilities are performing the level 2 analyses concentrating in post-accident phenomena in the reactor containment [2-1]. The third phase, the living use of PSA, is practical in parallel with both the first and the second phase. A natural step is to continue towards a living use of the present level 1 models of the plants. Figure 2-1 shows the phases of the PSA programme.

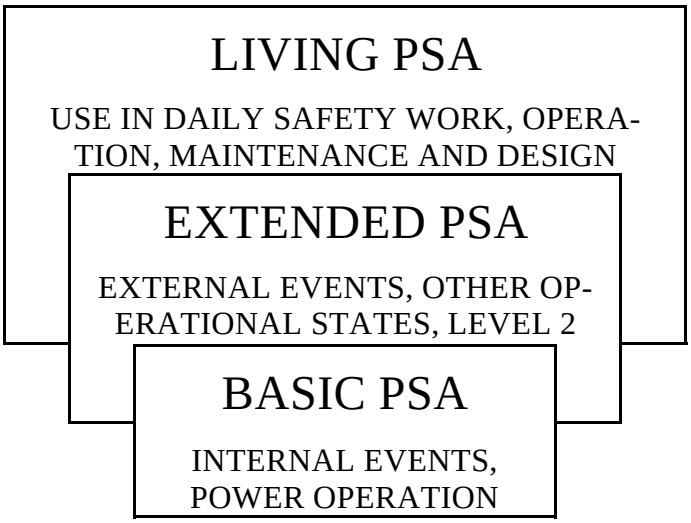


Figure 2-1. Different phases of a PSA programme [2-5].

2.2 The Nordic PSA activities

In order to collect different experiences and views to be used in the planning and execution of the main project a questionnaire concerning safety evaluation was sent to personnel at the Nordic utilities, safety authorities, research institutes and consultants. This section is partly based on the answers and comments concerning PSA and living PSA applications collected in the spring of 1990 from the Swedish and Finnish utilities and authorities within the survey [2-1]. Since then, a clear

step towards living PSA has been taken.

2.2.1 The status of PSA in Sweden and Finland

The Finnish and Swedish nuclear power companies have completed the first phase of wide range plant-specific PSA studies. These so called level 1 analyses have been directed on studying the internal initiating events and accident sequences leading to severe reactor core damages. The PSA-models created, reliability data gathered and the experiences gained from the analysis will be the basis for the living PSA concept. Studies concerning external events are under way.

On an average 4)10 persons are directly working with PSA activities at each power company. At Vattenfall, Sydkraft and IVO these persons are located in the central part of the organization not directly connected to plant operations. At OKG and TVO, the main responsibility is carried by the Reliability Section at the plant.

The status of living PSA is dependent on to what extent PSAs are used. The demands on the present PSAs will increase in consequence with a more advanced use. Also routines and procedures of how to utilize PSA in different situations are necessary to develop. It must be possible and easier to use PSA as an active support in the decision process with acceptable response times. The goal must be to incorporate PSA as a natural part in the decision process. The present status and use of some of the latest PSAs is quite close to a living PSA. However, by now the applications have been performed with the basic PSA and they have been laborious realizations. The models need to be supplemented as well as the computer codes must be improved in order to reach the status of living PSA.

2.2.2 Applications of PSA

PSA is being used in several areas for nuclear power plant safety support. Particularly safety review and prioritization of safety increasing measures. PSA results have supported reevaluation of plant safety and given clear indications and priorities for safety improvements. Other less used areas of application are e.g. changes in equipment surveillance test intervals (STI) and allowable outage times (AOT), and the rules for preventive maintenance in Technical Specifications (TS) for safety related equipment.

The awareness of the PSA activities is high in plant management and safety departments. Operation, maintenance and design departments have a low awareness of PSA-related activities. Persons involved with the PSA activities are familiar with the method. Other people have been occasionally informed about the PSA. PSA issues and reliability engineering methods are included in the internal training of personnel, especially in the training of shift engineers and operating staff.

2.2.3 The problem areas of further utilization of PSA

The maintenance of the PSA-model is in practice a large computer programming project. In order to go from the present situation to a living use of PSA-models, the organization will have to solve a lot of problems concerning the computer environment, codes, applicability of the PSA models and data, maintenance organization etc.

There are completeness problems related to the applications of the present PSA-models and data. The impact of conservative assumptions should be thoroughly analyzed. Modelling of human interaction and common cause failure (CCF) leaves much to be desired, and it is necessarily to

introduce time-dependent component models for a consistent description of temporal developments. There is also need for improvements in the present computer codes for evaluation of PSA models. The codes must become more user-friendly and dynamic, and the response times must be shortened to fulfill for the more demanding requirement posed by a living PSA.

Advocating the use living PSA in decision making should not be done without reference to its limitations, notably the uncertainties are an integral part of any probabilistic assessment. Neither should it be assumed that the concept "risk" has a well-defined meaning to different people or staff groups. Uncertainty analyses (statistical uncertainties) have not been performed for all PSA studies, and there is considerable variation in the application of different types of sensitivity analyses. There are plans for a more intensive utilisation of methods such as Monte Carlo simulation and improved sensitivity analyses to better treat uncertainties and verify conclusions. As of today, the control of conservatism and the impact of a variety of conservative assumptions is not satisfactory. And the treatment of the completeness problem, including the quality of time-dependent and CCF-models must be improved.

It is generally accepted that the present PSA studies provide valuable insight and they have become an essential part of plant safety work. But the growing awareness of the value of PSA should not be allowed to overshadow the fact that its results have to be applied within a strictly defined context. In particular, one should exercise care when using absolute numbers, there is reason to believe that relative values are more appropriate and that PSA results should be used in a comparative manner. This does not preclude the utilisation of reference levels, but it should be borne in mind that there are large uncertainties associated with very small ($\sim 10^{-7}$) probabilities.

The question of how large the risk reduction has to be to warrant a reconstruction or reconfiguration can only be answered through a more detailed analysis where all factors are accounted, including cost-effectiveness of the proposed measures. To establish the best possible decision support there is a strong need for improvement both in models and in the post-processing of PSA results.

Cost-benefit analyses will probably be a part of the decision making process in the future, but today the means for a consistent and efficient assessment of costs related to the proposed corrective measure is not available. Cost cannot be allowed to play a decisive role in questions of safety, if an improvement is identified. Advanced decision support methods are useful if they can simplify or structure the decision process such that decision maker arrives at a reliable conclusion in with less time and effort wasted. But the decision support system must operate in an transparent manner, where the basis for advice and the background information is always made available to the user.

2.3 International living PSA developments

The number of present applications of living PSA is limited, and practical experience concerning the use of PSA as an operational tool has not yet accumulated to the point where a general framework for design and structure has been established. The applications have common denominators in their efforts to quantify risk levels according to projected or assumed plant status, but in actual usage the aims may be quite different. The emphasis is on the research efforts in which the applicability of the PSA technique is tested in a reduced scale. The most advanced developments which aim at using of PSA as a risk monitor, i.e. as an online advisory system supporting the operator in safety-related decision making, comes from United Kingdom, France, USA and Japan.

2.3.1 Nuclear Electric experiences

Nuclear Electric in UK has implemented the ESSM (Essential Systems Status Monitor) system to monitor and predict risk level in the 12 essential post trip cooling systems. The PSA-based system is in use at the two advanced gas cooled reactors (AGR) Heysham 2 and Torness, based on a quite detailed model of failure modes of the post trip cooling systems. The system is in daily use for checking the status of the post trip cooling systems and has proved useful for planning maintenance and testing. ESSM results are checked against technical specification to ensure that safety limits are not violated, within these bounds the system identifies allowed outage states and suggests combinations which give the lowest risk [2-6].

The operational state of Heysham 2 is divided into three unavailability categories. The categories can be defined by probabilistic criteria according to how much the component or system unavailabilities increase the point frequency of the post trip cooling failure, as shown in Table 2.1. The risk increase factor is defined as the ratio of the instantaneous risk frequency and the nominal baseline risk frequency (see Table 4.1).

Table 2.1. Unavailability categories and operating limits with respect to risk increase factors at Heysham 2.

maintenance category	**operating limit**	**risk increase factor**
normal	no limit	)10
urgent	36 hours limit	10)100
infringement conditions	immediate remedial actions	100)

The ESSM system is easy to use and control room operators require only a short period of familiarisation to be able to use the system. Menus guide the user in input and output selection, with results mainly presented in form of tables or historical trend curves. In the status assessment mode the input can be automatic from the plant status monitoring, but in the planning mode the operators would in any case have to supply a certain amount of manual input. The ESSM system is one of the few existing systems in actual use as an on-line tool, the short computing times (3)4 minutes) have no doubt been a decisive factor in this respect.

2.3.2 USA

At several US plants, TS modifications have been accomplished, mostly based on the Electric Power Research Institute (EPRI) sponsored development work and using SOCRATES program [2-7]. Usually, a large number of TS modifications are combined in a package, including changes of both STIs and AOTs. The desired changes for operational flexibility are either motivated by the small risk impact of the individual changes, or by a trade-off between the changes. For the trade-off, the changes decreasing risk have usually been concerned with shortening of test intervals, and this is then used for obtaining longer AOTs.

The most recent EPRI sponsored project [2-8] defines and evaluates more closely the following three approaches:

) negligible risk increase,
) risk tradeoff,

) TS action alternatives.

The third approach develops alternate actions to follow that will allow plant operation to continue by compensatory measures directed at reducing the risk increase. Typical compensatory actions may include assuring redundant operation paths, starting up standby trains into running reserve or aligning unit-to-unit cross-ties.

Another recent bigger venture was concerned with TS modifications for the South Texas Project plant [2-9]. The two plant units belong to the new PWR generation with three electrically independent and physically separate safety trains. However, the current TS are generally based on the standard Westinghouse TS which were developed for two-train designs. The proposed changes primarily consist of extending

) AOTs for single train failure from 3 days to 10 days
) STIs from monthly to quarterly testing

In addition to trade-off among part of the modifications, the proposed AOT and STI extensions were defended by considering an impact of 10% or less in the average core damage frequency acceptable (applied to each single AOT change disjointly). The proposal has been under consideration and review at the USNRC for about two years, and provides useful insights about the risk-based TS modification process.

At the regulatory side, the TS improvement program was established by the USNRC in 1984 to completely rewrite and streamline the TS as well as to make line item improvements to existing TS. To support this effort, a comprehensive examination was performed of all surveillance requirements to identify those that should be improved [2-10]. The study resulted in numerous detailed recommendations, and generally concluded that while testing is essential to verify equipment and system operability, safety can be improved, equipment degradation decreased, and unnecessary personnel burden relaxed by selectively reducing the amount of testing at power. The combination of reliability concepts and preventive maintenance in a reliability centered maintenance program, together with focused testing based on the reliability characteristics of the system or component would be an effective method.

USNRC sponsored research includes following recent studies of special interest:

) Evaluation of STIs including adverse risk impacts of test-caused trips and equipment wear-out [2-11].
) Development and application of degradation modeling to define maintenance practices [2-12].
) Technical Specification action statements requiring shutdown: risk comparison approach with application to the RHR/SSW systems of a BWR [2-13].

The first and second study expand the conventional methods for STI and PM evaluation. The third study is similar in approach to TVO/RHRS study [2-14], as being directed to consider LCO shutdown risk for a consistent assignment of AOTs and action statements.

Most nuclear power plants in the USA are required to have level 1 PSA completed in the near future, meaning that an important prerequisite for living PSA will exist. In most cases the impetus to perform a PSA has come from licensing authorities, but a few power companies have established their own PSA programme independent of regulatory requirements.

2.3.3 France

In France level 1 studies for their 900 and 1300 MWe series reactors are completed. An interesting feature is their fairly detailed treatment of other than full power operating conditions [2-15]. A risk criterion limiting the integrated risk over AOT below 1 E-7 (single occurrence risk), was established already about ten years ago. This limit corresponds to a relative criterion of about 1)10 % acceptable for a failure situation with respect to the annual core damage probability, when considered against the background that the usual average CDF is about or below 1 E-5 1/a, in power operation state. Recently, the plant shutdown risk is also taken into consideration for defining AOTs [2-16].

2.3.4 Germany

Technischer Überwachungs-Verein (TÜV) Norddeutschland has developed AOT guidelines, which combine deterministic approach with reliability considerations at the safety function level [2-17]. The plant level balance is aimed to be achieved by tuning the AOTs among systems according to the demand frequency of different safety functions.

2.3.5 Japan

In Japan the current development of the living PSA system LIPSAS has as objectives to generate a framework for updating of PSA models, risk level monitoring and operator support in accident management situations [2-18]. Defining an optimum AOT, by using different criteria, and taking into account plant shutdown risk if the AOT is exceeded, was examined with application to RHR system at an LMFBR plant [2-19]. Compare with the further discussion of the AOT criteria in Section 6.2.4 and of the computer code in Section 5.4.1.

2.3.6 Other countries

In addition to the Nordic countries and the examples given above, there are several other countries where projects bordering on a living PSA concept are in progress. Ontario Hydro in Canada operates 20 CANDU reactors, for each station there is a living PSA programme based on level 3 PSA. The development of the new CANDU 6 Mark 1 is supported by PSA evaluations of design changes [2-20]. In Italy [2-21], Spain [2-22] and Switzerland [2-23], the regulatory bodies and utilities are enganged in living PSA activities.

2.3.7 International cooperation

The International Atomic Energy Agency (IAEA) Technical Committee Meeting on "Use of PSA to evaluate technical specifications" in 1990 recommended that a report be prepared detailing relevant methods and providing case studies on the topics [2-24]. The prepared document addresses the rationale for optimizing TS, discusses optimization methods and approaches, summarizes recent applications of the methodology and fully describes two distinctive case studies [2-25]. The working draft of the document was reviewed in another Technical Committee Meeting on "Advances in Reliability Analysis and PSA" in 1992, when also several recent applications were presented and discussed (proceedings will be published by the IAEA).

The OECD CSNI/Principal Working Group no. 5 initiated in 1992 a special task on "Risk-Based Management of Safety System Reliability" with a scope ranging from the developments of real time risk monitor and on-line configuration control system to PSA-based improvements of traditional TS

and configuration management. The task is aimed at a "state-of the art" report in 1994 including:

- status and achievements by the leading examples,
- estimates of investments required to implement various schemes given a suitable PSA to start with,
- potential benefits and uses of the schemes,
- conclusions on overall effectiveness of the different schemes for PSA-based risk management of safety system reliability.

The task has been started with a review of recent developments and applications.

2.4 References for the section 2

SIK-1 reports

[2-1] Holmberg, J., Laakso, K., Lehtinen, E., Johanson, G. and Björe, S., Preproject report: Nordic survey on safety evaluation by use of living PSA and safety indicators (NKS/SIK-1). SKI technical report 91:3, Swedish Nuclear Power Inspectorate, Stockholm, 1991. 22 p. + app. 21 p.

[2-2] Holmberg, J., Laakso, K., Lehtinen, E., Johanson G. and Björe, S. International survey of living-PSA and safety indicators. VTT Research Notes 1326, Technical Research Centre of Finland, Espoo 1992. 52 p. + app. 22 p.

[2-3] Stokke, E. Operational interface for LPSA. Report NKS/SIK-1(91)33, IFE/Halden, Halden, 1993. 57 p. (draft)

[2-4] Holmberg, J. A Limited Survey on the ASP Methodology. Report VTT/SÄH 18/91, RISKI(91)10, NKS/SIK-1(91)40, Technical Research Centre of Finland, Espoo 1991. 11 p.

Other references

[2-5] Hirschberg, S., Applications and implications of the living PSA concept. In Proc. of the 2nd TÜV-Workshop on Living PSA application, Hamburg, 7)8 May 1990, ed. H.-P. Balfanz, TÜV-Norddeutschland e.V., Hamburg, 1990. 23 p.

[2-6] Horne, B. The use of probabilistic safety analysis methods for planning the maintenance and testing unavailabilities of essential plant at Heysham 2 AGR power station. Proc. of the IAEA technical committee meeting on the use of PSA to evaluate NPP's technical specifications, Vienna, June 18)22, 1990. Vienna 1990, International Atomic Energy Agency. 8 p. + app. 11 p.

[2-7] Wagner, D.P., Minton, L.A. & Gaertner, J.P., Risk-based analysis methods and applications to nuclear power plant technical specifications. CSNI-Unipede Specialist Meeting on Improving Technical Specifications for NPPs. Madrid, 7-11 September 1987.

[2-8] Risk-Based Technical Specification Program. Prepared by G.R. Andre (Westinghouse), and L. Lee, T.L. Leserman and R.L. Thierry (Pacific Gas and Electric Co.), Report EPRI TR-101894, January 1993.

[2-9] Fleming, K.N. & Murphy, R.P., Lessons learned in applying PSA methods to TS optimization. IAEA Technical Committee Meeting on Advances in Reliability Analysis and

PSA, Budapest, 7-11 September 1992. Proceedings.

[2-10] Lobel, R. and Tjader, T.R. Improvements to Technical Specifications Surveillance Requirements. Report NUREG-1366, U.S. Nuclear Regulatory Commission, Washington D.C., 1992.

[2-11] Quantitative evaluation of Surveillance Test Intervals including test-caused risks. Prepared by Kim, I.S., Martorell, S., Vesely, W.E. & Samanta, P.K. for USNRC, BNL & SAIC, Report NUREG/CR-5775, February 1992.

[2-12] Development and application of degradation modeling to define maintenance practices. Prepared by Stock, S., Vesely, W.E. & Samanta, P.K. for USNRC, BNL & SAIC, November 1992.

[2-13] Technical Specification action statements requiring shutdown: a risk perspective with application to the RHR/SSW systems of a BWR. Prepared by Mankamo, T., Kim, I.S. & Samanta, P.K. for USNRC, report NUREG/CR-5995, Brookhaven National Laboratory, September 1993.

[2-14] Continued plant operation versus shutdown in failure situations of standby safety systems, application of risk analysis methods for the evaluation and balancing of allowed outage times for the residual heat removal systems at TVO I/II plant. Technical report, prepared by Mankamo, T. and Kosonen, M., 30 August 1992. Working draft for a TECDOC, IAEA-J4-CS53/92, 1992.

[2-15] Villemeur, A., Berger, J.P., Dubreuil-Chambardel, A. and Moroni, J.M. Living probabilistic safety assessment of a French 1300 MWe PWR nuclear power plant unit: Methodology, results and teachings. In Proc. of the 2nd TÜV-Workshop on Living PSA application, Hamburg, 7)8 May 1990, ed. H.-P. Balfanz, TÜV-Norddeutschland e.V., Hamburg, 1990. 10 p.

[2-16] Deriot, S., Impact of shutdown risk on risk-based assessment of Technical Specifications. IAEA Technical Committee Meeting on Advances in Reliability Analysis and PSA, Budapest, 7-11 September 1992. Proceedings.

[2-17] Theiss, K., Approaches for ascertainment of allowable outage times (AOTs). IAEA Technical Committee Meeting on The Use of PSA to Evaluate NPP's Technical specifications, Vienna, 18-22 June 1990.

[2-18] Nakai, R. Application of a living PSA system to LMFBR. Proc. of the 3rd Workshop on Living-PSA-Application, Hamburg, May 11)12, 1992, ed. H.-P. Balfanz, TÜV-Nordeutschland. 16 p.

[2-19] Hioki, K. & Kani, Y.,Risk based evaluation of technical specifications for a decay heat removal system of an LMFBR plant. IAEA Technical Committee Meeting on The Use of PSA to Evaluate NPP's Technical specifications, Vienna, 18-22 June 1990.

[2-20] Dick, B.N. and Lawrence, P.N. Use of PSA to evaluate operating strategy compliancy with operating policies and principles requirements. In Use of probabilistic safety analysis to evaluate nuclear power plant technical specifications, report IAEA-TECDOC-599 of a Technical Committee Meeting, Vienna, June 18)22, 1990. International Atomic Energy Agency, Vienna, 1990. Pp. 89)95.

[2-21] Bassanelli, A., Traini, E., Caporali, R. and Cozzone, M. The living PSA as an effective tool to support the design development of new generation NPPs. Proc. of the 3rd Workshop on Living-PSA-Application, Hamburg, May 11)12, 1992, ed. H.-P. Balfanz, TÜV-Nordeutschland.

[2-22] Gómez, J.A., García, M., Azcárate, M.C., Juncosa, P. and Gutiérrez, E. Approach of living PSA system in basis of the IIE and UITESA experience. Proc. of the 3rd Workshop on Living-PSA-Application, Hamburg, May 11)12, 1992, ed. H.-P. Balfanz, TÜV-Nordeutschland. 14 p.

[2-23] Schmocker, U., Chakraborty, S., Deutschmann, H., Fenske, R., Isaak, H.P., Khatib-Rahbar, M., Cazzoli, E.G., Hanan, N. Approach to regulatory review of Swiss probabilistic safety assessments. In Use of Probabilistic Safety Assessment for Operational Safety, PSA '91. Proc. of an International Symposium, Vienna, June 3)7, 1991. International Atomic Energy Agency, Vienna, 1992. Paper IAEA-SM-321/10, pp. 125)133.

[2-24] IAEA Technical Committee Meeting on The Use of PSA to Evaluate NPP's Technical specifications, Vienna, 18-22 June 1990. IAEA-TECDOC-599, April 1991.

[2-25] Risk-based application of NPP Technical Specification improvements. Working draft for a TECDOC, IAEA-J4-CS53/92, 1992.

3 A LIVING PSA PROGRAMME

This chapter describes in brief terms the definition of a concept for applying living PSA for safety management. The process of how to achieve a consistent use of living PSA applications is described in detail in the following chapters 4, 5 and 6. This chapter is intentionally written with an overlap to the following chapters (4, 5 and 6) to allow the reader a complete overview of how to apply the LPSA programme.

The Nordic status and experience of PSA [3-1] have been examined. The risk monitoring and follow-up have been tested using, Forsmark 1/2 PSA [3-2], Oskarshamn 2 PSA [3-3], [3-4], [3-5] & [3-6], and TVO I/II PSA [3-7]. Within this project a specification for a living PSA system has been generated [3-8]. More safe and economical operational strategies have been studied for test and preventive maintenance arrangements as well as in the case of failures in safety systems [3-3].

3.1 A concept for Living PSA in safety management

The first step of a typical PSA programme is the performance of a level 1 study concentrating on internal events and accident sequences leading to core damage, called *basic* PSA. The basic PSA model is static, and it is made for the evaluation of the time-average core damage probability of the plant. To increase the availability of the basic PSA for the operational safety management, the model as well as the whole PSA programme should be developed to a more dynamic tool. The process, to update the PSA model to represent the current or planned configuration and to use the model to evaluate and direct the changes in the configuration, is called *living* PSA programme [3-9].

The first version of a plant-specific, basic PSA is usually not adequate to all those possibilities we can see for PSA. For instance, the basic PSA model and data does not quite support flexible evaluations of the plant safety level, few PSA computer codes are user-friendly and fast enough, and there are seldom procedures as well as understanding to use and maintain PSA in the daily safety management. A living PSA is a PSA which has been integrated into the operational safety management.

An important part of the living PSA concept is how the evaluation results are interpreted for the decision making of safety related issues. In this context, we have to define risk measures used to present the results of the applications. The fundamental aspect of a living PSA result is that it expresses the core damage risk given a certain time and plant status. This structure changes in different operational modes as well as the basic event probabilities vary according to the knowledge of the component statuses. A living PSA model should be able to follow the changes.

The living PSA concept involves a description of how the original PSA model can be used in a more dynamic sense, continuously updated according to the actual status of the safety related systems of the plant. The main purposes to develop a living PSA are to provide a risk evaluation tool for analyzing the safety effects of changes in plant design, procedures and Technical Specifications, and to support the maintenance planning and operational management by providing a tool for searching optimal operational strategies, maintenance and testing from the safety point of view.

A living PSA programme will, following this concept, become a daily safety management system based on a plant-specific PSA and supporting information system, Figure 3-1.

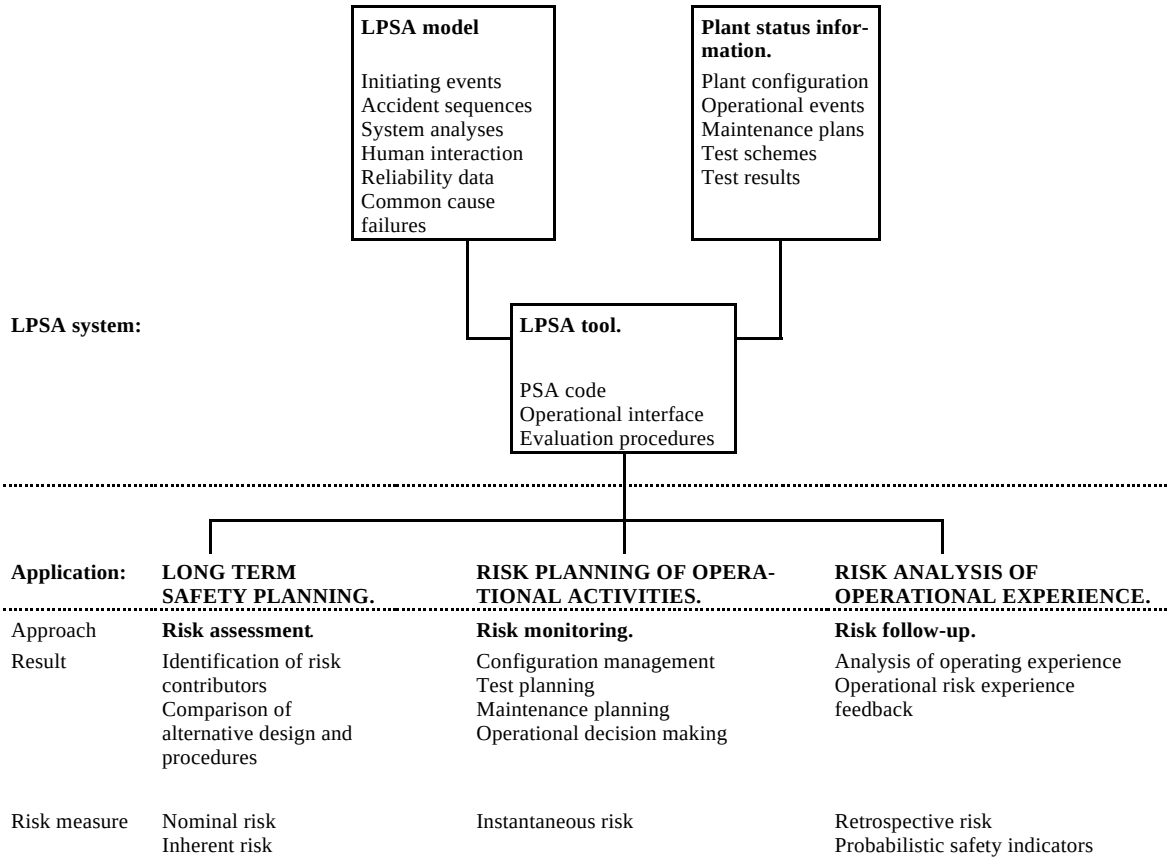


*Figure: **3-1**. The living PSA concept.*

3.2 Three different approaches to use a living PSA

The living PSA applications can be divided into the three application approach categories: 1 - risk assessment, 2 - risk monitoring, and 3 - risk follow-up.

3.2.1 Risk assessment

The risk assessment application is close to the idea of the basic PSA, i.e. the evaluation of the average risk caused by the operation of the plant. The primary purpose of the risk assessment is to verify the average risk level of the plant and to identify the major risk contributors. The results of the assessment are applicable for the long term planning in order to improve the identified weaknesses of the plant.

Long term plannings include static evaluations and comparisons of risk effects of changes in the plant design, maintenance or test arrangements, procedures and Technical Specifications. The aim of these studies is to optimize the plant operation, maintenance and design with respect to the risk minimization and operational flexibility. Living PSA can also provide a controlled way of trading excessive safety margin for the operational or maintenance flexibility in specific cases.

The present applications of the Nordic PSA studies are good examples of the risk assessment application area. Experiences have been gained from a wide range of safety management activities in Finland [3-10],[3-11], Sweden [3-12], and in the research field [3-13].

3.2.2 Risk monitoring

The idea of the risk monitoring applications is to calculate the instantaneous risk experienced during the operation of the plant. Differing from the risk assessment, in which an average plant configuration is applied, the risk monitoring applies the plant configuration observed at that moment.

The risk monitoring applications can be performed in an on-line, off-line or planning mode. The on-line risk monitoring is carried out by the operators of the plant who have the up-to-date information of the plant status. The off-line risk monitoring is performed based on operational experiences. In the planning mode, hypothetical configurations are evaluated beforehand in order to identify safety jeopardizing configurations.

The risk monitoring applications would mean that the operating or maintenance planning personnel uses living PSA as an advisory tool to supplement the Technical Specifications by evaluating the near or sudden changes in the plant operation and maintenance. This is carried out by controlling the risk level of operational alternatives and decisions, and by identifying means to control high variations of the risk. The results of the monitoring are applicable for the short term planning in order to select the operational or maintenance strategies in a given or planned situation.

So far, only few examples exist of risk monitoring applied as an on-line system. The most advanced system is perhaps the Essential Systems Status Monitor developed by Nuclear Electric for the Heysham 2 plant where the operators of the plant control the risk level by updating the PSA according to the events at the plant [3-14]. In Sweden and Finland, the goal for the near future is to be able to apply PSA for short term planning.

3.2.3 Risk follow-up

The idea of the risk follow-up applications is to calculate the retrospective risk i.e. the evaluation of the risk experienced during operation of the plant. The purpose of the risk follow-up is to evaluate the severity of the incidents from the safety point of view. Another aim is to search for suitable and effective improvements in the present technical and organizational performance of the plant. The analysis of the operating experiences also supports the verification as well as the completion of the PSA models and data.

The risk follow-up has been the main application area in the SIK-1 project. The risk follow-up is considered the first step in the development of the living PSA system because the living PSA model requirements are similar to the risk monitoring applications.

3.3 Requirement and capabilities for safety management applications

A living PSA system is an information structure based on the plant-specific PSA model and the computerized tool needed to manage the LPSA activities. The PSA model of the plant is constituted of basic events. Examples of basic events are component or system failures, and operator errors. The risk model represents which combinations of the basic events can lead to the accident.

The living PSA system constitutes the link between the PSA model, the plant status information and

living PSA application results. Further, the extensive information contained in a plant specific PSA model must be made accessible to all potential users involved in safety management. This is the primary objective in developing a living PSA system to manage the models and to provide an operational interface for living PSA and the evaluation procedures involved in the living PSA applications.

Within this project a specification for a living PSA system is generated. This includes specifications of further development of the codes used and also feasibility studies of integrating the PSA model into the plant information system [3-8]. An even more important question is the PSA staff organization and manpower effort to carry out the necessary tasks, this section will concentrate on the latter.

3.3.1 Model requirements and capabilities

Uses of LPSA for different applications requires that it has features necessary for each specific application. Reviews undertaken, i.e. IAEA/IPERS, show that the PSAs being completed not always can be effectively used in many of the intended applications [3-15]. This brings up the question of requirements, IAEA [3-16], with respect to scope, degree of detail in the modeling, capabilities to perform the necessary calculation, quality and type of data used, and acceptable assumptions in the treatment of central PSA or LPSA topics.

Both this report and the IAEA Report serve multiple purposes that to a large extent are identical:

- It identifies the immediate application areas of PSA.
- It provides guidance to PSA developers who can either develop or extend their PSA for the intended uses.
- It will assure greater consistency both in the scope and content of the PSA and in their uses.
- It will promote PSA applications in enhancing safety in nuclear power plants.

In addition this report describes the approach, methodology, model requirement and data requirement necessary to meet and to carry out the applications. Demonstration studies performed within NKS/SIK-1 have provided applicational experience and are used to identify areas where the basic PSAs must be improved. This experience are documented in the following chapters and will not be discussed here.

3.3.2 System requirements and capabilities

An LPSA programme requires a system to operate and maintain the LPSA model. This system includes procedures for input/output, procedures for model maintenance, the PSA code and the operational interface.

An LPSA programme will require resources to operate and maintain the model. In the organization there must be one or two persons that are responsible for the base model. Procedures for protecting the base model are needed, as well as procedures to make sure that everyone is using the correct model. The long term management of a plant model involves a large number of decisions regarding various aspects on the model and the model capabilities.

Resources spent on the initial issue of a plant-specific PSA are approximately 5)10 manyears and 0.5)1 manyear per year for updating the PSA thereafter. This has been estimated as a reasonable effort based on the experience with the existing PSAs [3-1]. An important part is also the scope

extensions (external events, other operational states, level 2 etc) that require additional manpower effort of approximately 1)3 manyears per extension. The manpower resources for this effort is strongly dependent on the level of ambition and plant generation, e.g. a modern plant is much less sensitive to external events and also easy to analyze due to consistent separation in the design.

On an average 4)10 persons are directly working with PSA activities at each Nordic power company to establish and maintain the basic PSAs. The LPSA activities, to monitor and follow-up the risk, will require a staff of this size on a long term basis. LPSA application analysis performed with a living PSA system covers a large scale of tasks from reading documentation to analysis of status changes or modifications in operational procedures of the plant. The LPSA activities require a close relationship to plant operation and maintenance compared to the basic PSA applications that to a much larger extent are directed towards plant safety management, designers and authorities.

3.4 Applying LPSA in safety management

The living PSA applications can be divided into specific areas which better reflect the usage of the results. Table 3-1 shows the application areas and the users. In addition to these users, the reliability engineers and code developers are always needed to maintain the system. Living PSA has also the function as a communication tool between the authorities and the utilities [3-17]. In Finland, the utilities and authorities do not share only the same PSA models but also the computer code which enables safety evaluations from the same basis [3-18].

3.4.1 Long term risk planning

1. Safety goal evaluation.

In safety goal evaluation (plant risk assessment) the results are used in an absolute manner. The nominal core damage frequency is compared with a national or international criterion (the utility may have criteria of its own). The criterion is considered more a target because results of PSA are sensitive to the approach used in the risk assessment. Especially, the level of completeness of PSA affects the result a lot.

2. Identification of the risk contributors.

For the safety and design management, the primary purpose of risk assessment is to identify the main risk contributors so that safety improving measures can be identified and prioritized. The results are used in a relative manner. The risk importance measures of the basic events, e.g. fractional contributions, are the first hand results in the identification of the risk contributors [3-19], [3-20].

3. Comparison of alternative designs and procedures.

When the changes in designs or procedures have influence on the safety status, LPSA can provide support for the comparison of the alternatives. The uncertainties and economical aspects should also be taken into consideration. The responsibility of these applications are carried by the plant design or the safety management, depending on the plant life cycle phase.

*Table **3-1**: Application areas of living PSA and their users*

Application	EA[1)]	Users: Safety managament	Operational management	Maintenance planning	Designers	Authorities
Long term safety planning.						
Safety goal evaluation, Plant risk assessment.	ra	x			x	x
Risk contributor identifi-cation.	ra	x			x	x
Comparisons of design and procedure changes.	ra	x	x		x	x
Optimization of limiting conditions for operation.	ra/rm	x	x			x
Operator training	ra		x			
Accident management	ra	x	x		x	x
Risk planning of operational activities.						
Planning of preventive maintenance	ra/rm			x		
Planning of corrective maintenance	rm			x		
Surveillance tests planning.	rm	x	x			
Incident management	rm	x	x	x		
Exemptions from Technical Specificatons.	rm	x	x			x
Risk analysis of operational experience.						
Off-line risk monitoring. Probabilistic indicator analysis.	rm	x				
Risk follow-up. Retrospective risk analysis and indicators	rf	x	x			x
Incident analysis	rf	x	x			x
Generic precursor studies	rf	x	x			x
Ageing analysis	rf		x	x		x

1) Evaluation approach: ra = risk assessment, rm = risk monitoring, rf = risk follow-up

4. Optimization of limiting conditions fo operation.

The operational limits and conditions given by Technical Specifications are analyzed by evaluating the risk effects of alternative requirements. Planning of test strategies is also related to this activity. The purpose is to balance the requirements with respect to operational flexibility and plant economy. The high risk situations permitted by Technical Specifications are identified and replaced by such modes that give minimum risk, as well as the too stringent requirements are substituted by more flexible ones.

5. Operator training.

The results of the identification of the risk contributors can be utilized in planning which accident sequences should be emphasized in the operator training. Vice versa, the operator training can be used to verify the realism of the human interaction models in the considered accident sequences.

6. Accident management planning.

Accident management planning is more related to level-2 and level-3 PSA applications. Generally, the identified risk contributors, dominant accident sequences, recovery and success paths, as well as end states can support the planning of the accident management program.

3.4.2 Risk planning of operational activities

1. Planning of preventive maintenance.

The maintenance office evaluates the risk effects of the preventive maintenance program. The isolation of systems or components important for safety temporarily increases the risk level. The duration of the maintenance work and the combination of isolated or unavailable systems are controlled. Risk increase factor, safety margins and safety margin degradations indicate the effects of scheduled maintenance actions [3-21]. The benefits of performing additional tests can be considered, too.

2. Planning of corrective maintenance.

In contrast to down time caused by preventive maintenance, the down time caused by corrective maintenance takes place randomly. Based on operating experience, the frequency of the events can be predicted and, subsequently, the lifetime contribution can be controlled by adjusting the allowed outage time. The lifetime contribution is controlled similarly as with preventive maintenance.

3. Planning of surveillance tests and their schemes.

The risk monitoring produces an instantaneous risk frequency curve which follows the changes in the plant configuration. Due to time-dependent probability of hidden failures of standby safety systems the risk curve has a saw-teeth shape. The surveillance test of a standby component or system either drops or increases the instantaneous risk frequency, because certain hidden failures can be detected in the tests. An evident unavailability, such as preventive maintenance of the system, on the other hand, increases immediately the risk frequency. The operational management can this way analyze the risks and benefits of the test strategies, Figure 3-2, [3-3]. The tests should be planned so that considered failures are detected but introduction of additional failure modes are avoided, [3-22]. The effect of test interval and possible staggering of redundant tests can be evaluated from

the reliability point of view by time-dependent component failure models [3-6] .

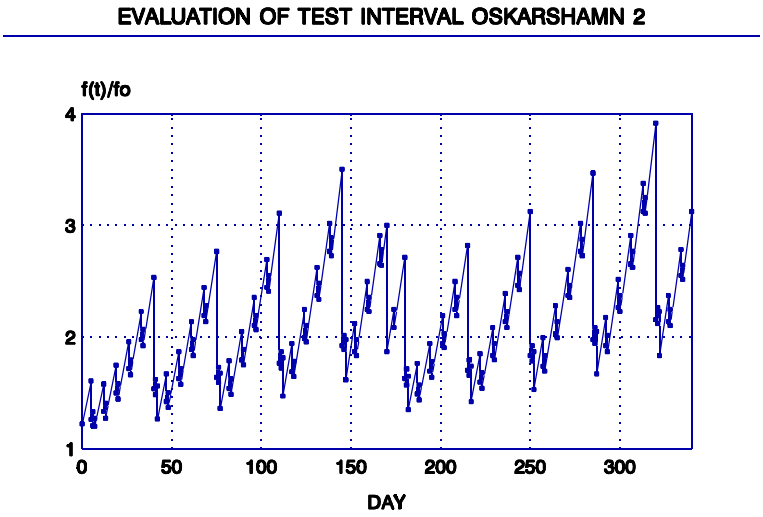


*Figure **3-2**: Risk variation due to an actual test scheme in Oskarshamn 2 NPP.*

4. Incident management.

The purpose of on-line risk monitoring is to evaluate the instantaneous risk frequency or the probability of core damage during a short time interval given the information about the plant configuration. The incident management deals with failure situations at the plant where prompt decisions are needed. The severity is controlled by on-line monitoring. The results provide support for operational risk decision making in short term. The maintenance actions can be prioritized so that the most critical systems are repaired or maintained first, or some specific maintenance isolation are postponed. Success path importance, e.g. risk decrease factors, can be used to rank the actions. A test importance type of measure can be used to decide whether some action is worth performing. Safety margins and degradations describe also the severity of the situation. Test information importance can be used to decide whether the test provides relevant information from the safety point of view. The evaluations are related to considerations of exemption from Tech. Spec. and maintenance planning.

5. Exemptions from Technical Specifications.

An exemption from the Technical Specifications has usually an influence on the plant safety. The risk quantity caused by the exemption is compared with risks of other operational alternatives. The application is similar to the configuration control and optimization of allowed outage times.

3.4.3 Risk analysis of operating experience

1. Probabilistic indicator analysis and retrospective risk follow-up.

The result of risk follow-up applications is a historical risk frequency curve from which we can generate probabilistic safety indicators. The main indicators are

) instantaneous frequency peaks of the curve,

) the core damage probabilities over the peaks, and
) the average frequency during the observation period.

The results can be used to identify possible high risk situations to rank the occurred events from safety point of view, Table 3-2, and thus to get feedback both for the identification of risk contributors and for the verification of PSA-models [3-4].

The results are also input for more advanced risk follow-up applications, to calculate the retrospective risk. In addition to operational experiences analyzed in the off-line risk monitoring, the retrospective risk follow-up considers the hidden events as accurately as possibly given the available information. Exceptional failure combinations, dependencies between failures, repair actions, maintenance or operation modes can be identified.

*Table **3-2**: Risk follow-up at Oskarshamn 2 - 1987, the Core Damage Probability and risk contribution for each component failure and initiating event that occurred during 1987.*

Component failure/Initiating event	Date	Risk dose[1], P_{dose}	Contribution (% of P_d)
Transient with loss of feed water system.	870713	3.2E-6	65
Gas turbine 649G13 unavailable.	870904 - 870925	9.1E-7	18
Transformer 649T13 unavailable.	870925 - 870930	2.2E-7	4
Transient with loss of power conversion system.	870224	1.5E-7	3
Transient with all safety systems available.	870731	7.1E-8	1
Transient with all safety systems available.	871009	6.8E-8	1
Diesel generator 661DG212 unavailable.	871208 (16h)	6.7E-8	1
Transient with all safety systems available.	870715	6.0E-8	1
Transient with all safety systems available.	871227	5.4E-8	1
Diesel generator 661DG212 unavailable.	870121 (10h)	4.9E-8	1
Unsalted water pump 733P23 unavailable.	871130 - 871203	4.8E-8	1
Diesel generator 661DG212 unavailable.	870204 (3h)	1.6E-8	<1
Bus bar 641SG6 unavailable.	870319 (6h)	9.0E-9	<1
Rotating converter 666G222 unavailable.	870714 (16h)	8.1E-9	<1
Service water pump 713P1 unavailable.	871009 (8h)	3.9E-9	<1
Total risk dose due to unavailabilities in safety systems, $P_{d,u}$	8701-8712	1.5E-6	31% (of P_d)
Total risk dose due to initiating events, $P_{d,i}$	8701-8712	3.4E-6	69% (of P_d)
Total risk dose, P_d	8701-8712	4.9E-6	100% (120% of P_n)
Nominal risk dose, P_n (PSA estimate)	1 average year	4.1E-6	

1) See chapter 6.5 for definition.

2. Incident analysis.

The safety-significant events are analyzed as deeply as necessary in order to identify the root causes of the events and to evaluate their severity. The function of LPSA is the severity evaluation, in this

context.

3. Generic precursor studies (Event evaluation).

The accident sequence precursor (ASP) studies performed in USA and Germany are examples of extensive operating experience analysis using an event evaluation approach [3-23],[3-24]. There are two type of plant events that can be regarded as precursors:

) initiating events possibly followed by failures in the safety systems, and
) unavailabilities in the safety systems.

The event evaluations identify significant events from a large amount of operational data such as licensee event reports (LER) and component failure reports. The severity is evaluated by calculating the conditional probability of an accident given the plant event. The accident sequence precursor (ASP) studies provide two type of results:

) generic precursor frequencies, and
) safety margins during individual plant events.

4. Ageing analysis.

Ageing analysis aims at identifying ageing effects in the system or component structures or functions. From the reliability point of view, indications on forthcoming incidents and changes in failure frequencies are monitored so that the planned plant lifetime can be reached, and if possible extended. The ageing components can be ranked according to their criticality for the plant safety and availability which enables the planning of the maintenance and surveillance programs to take into account the ageing effects. The probabilistic safety indicators are used as measures. The measure can be e.g. an ageing parameter in a component failure rate model [3-25] which can be affected by changing the maintenance program [3-26].

3.4.4 Regulatory and inspection activities

Regulatory and inspection activities relate to all of the above mentioned applications of PSA. The applications connected to requirements in the Technical Specifications are of course important to review and approve. In the case of exemptions from TS, specific case studies can use the same approach to provide basis to support decision making. Inspection guidance can be obtained by using basic results from the risk assessment such as dominant risk contributors.

3.5 References for section 3

SIK-1 reports

[3-1] Holmberg, J., Laakso, K., Lehtinen, E., Johanson, G. and Björe, S., Preproject report: Nordic survey on safety evaluation by use of living PSA and safety indicators (NKS/SIK-1). SKI technical report 91:3, Swedish Nuclear Power Inspectorate, Stockholm, 1991. 22 p. + app. 21 p.

[3-2] Erhardsson, U.-K. and Flodin, Y., Momentaneous risk level. PM-project for living PSA. Report PK-79/81, NKS/SIK-1(91)30, Vattenfall, Vällingby, October 1991. (In Swedish)

[3-3] Sandstedt, J., Demonstration studies on living-PSA. SKI Technical Report 93:33 (NKS/SIK-1(92)27 Relcon AB), Swedisch Nuclear Power Inspectorate, Stockholm , August 1993.

[3-4] Holmberg, J., Johanson, G., Sandstedt, J. The Generation of Probabilistic Safety Indicators from The Risk Follow-Up Results. 3rd Workshop on Living PSA applications, Hamburg, May 11-12, 1992.

[3-5] Sandstedt, J., Time dependent modelling LPSA-O2. Presented in the IAEA technical committee meeting on Guidelines on probabilistic safety assessment (PSA) requirements for use in safety management, Stockholm, 16)20 September 1991, Report Relcon-13/91, NKS/SIK-1(91)31, Relcon AB, Sundbyberg, September 1991.

[3-6] Sandstedt, J., Pilot study: Analysis of prescribed testintervals, Oskarshamn 2. NKS/SIK-1(92)XX, Relcon AB, Sundbyberg, August 1993.

[3-7] Holmberg, J., Pulkkinen, U. and Mankamo, T., Risk follow-up by PSA) Experience from the Finnish pilot study. Presented in the IAEA technical committee meeting on Guidelines on probabilistic safety assessment (PSA) requirements for use in safety management, Stockholm, 16)20 September 1991, Report VTT/SÄH 16/91, NKS/SIK-1(91)35, Technical Research Centre of Finland, Espoo, September 1991.

[3-8] E. Stokke, Operational interface for living PSA, Report NKS/SIK-1(91)33, IFE/Halden, Halden, 1992 (draft).

Other references

[3-9] Bonaca, M.V. (ed.) Living probabilistic safety assessment for nuclear power plant management. Paris 1992, OECD/Nuclear Energy Agency, OECD Publications, 81 p.

[3-10] Himanen, R. and Toivola, A., PRA program on NPP TVO. In *Probabilistic safety assessment and management*, Proc. of the international conference on probabilistic safety assessment and management (PSAM), Beverly Hills, 4)7 February 1991, ed. G. Apostolakis, Elsevier Science Publishing Co., Inc., New York, 1991. Pp. 1001)1006.

[3-11] Mohsen, B. and Vaurio, J.K., PSA as a safety improvement tool for Loviisa NPs. In *Probabilistic safety assessment and management*, Proc. of the international conference on probabilistic safety assessment and management (PSAM), Beverly Hills, 4)7 February 1991, ed. G. Apostolakis, Elsevier Science Publishing Co., Inc., New York, 1991. Pp. 1007)1011.

[3-12] Hammar, L. and Liwång, B., The use of PSA techniques in regulatory and safety work in Sweden. In Proc. of the CSNI workshop on PSA applications and limitations, Santa Fe, September 4)6, 1990, ed. T. Molina, Report NUREG/CP-0115, SAND90-2797, Sandia National Laboratories, Albuquerque, 1991.

[3-13] Bengtsson, G. (editor), Risk analysis and safety rationale. Final report of a joint Nordic research program in nuclear safety. NORD 1989:91, Nordic liaison committee for atomic energy, Stockholm, December 1989.

[3-14] Horne, B. The use of probabilistic safety analysis methods for planning the maintenance and testing unavailabilities of essential plant at Heysham 2 AGR power station. Proc. of

the IAEA technical committee meeting on the use of PSA to evaluate NPP's technical specifications, Vienna, June 18)22, 1990. Vienna 1990, International Atomic Energy Agency. 8 p. + app. 11 p.

[3-15] Hirschberg, S., Experience from International Peer Reviews of Probabilistic Safety Assessment. Procedings of International Symposium on the Use of Probabilistic Safety Assessment for Operational Safety, PSA´91, held in Vienna 3-7 June 1991. Paper IAEA-SM-321/53. IAEA Vienna.

[3-16] Hirschberg, S., Johanson, G. and Samanta, P.K., Requirement and Capabilities of PSA for Safety Management Applications. Draft report IAEA , Vienna, 1992.

[3-17] Hammar, L., Carlsson, L., Karlsson, C. and Johanson, G., The regulatory use of PSA in Sweden. Presented in the IAEA technical committee meeting on Guidelines on probabilistic safety assessment (PSA) requirements for use in safety management, Stockholm, 16)20 September 1991, Report SKI/UA-16/91, Swedish Nuclear Power Inspectorate, Stockholm, September 1991.

[3-18] Virolainen, R., Living PSA) A communication tool between regulator and utilities. In Proc. of the 2nd TÜV-Workshop on Living PSA application, Hamburg, 7)8 May 1990, ed. H.-P. Balfanz, TÜV-Norddeutschland e.V., Hamburg, 1990.

[3-19] Vesely, W.E., Davis, T.C., Denning, R.S., Saltos, N. Measures of risk importance and their applications. Report NUREG/CR-3385, Battelle Columbus Laboratories, Columbus, 1983.

[3-20] Schmidt, E.R. et.al. Importance measures for use in PRAs and risk management. Proceedings: International topical meeting on probabilistic safety methods and applications. Report EPRI NP-3912-SR, Vol. 2: Sessions 9)16, Electric Power Research Institute, Palo Alto, 1985, Paper No. 83.

[3-21] Samantha, P.K. Modeling of risk impact and benefit of maintenance. Brookhaven National Laboratory, New York. 1991.

[3-22] Kim, I.S, Martorell, S., Vesely, W.E., Samantha, P.K. Quantitative evaluation of surveillance test intervals including test-caused risk. Prepared for U.S. Nuclear Regulatory Commission. NUREG/CR-5775. Brookhaven National Laboratory, February 1992.

[3-23] Minarick, J.W. The US NRC accident sequence precursor program: Present methods and findings. Reliability Engineering & System Safety 27(1990)1, pp. 23)52.

[3-24] Hoertner, H., Kafka, P. & Reichart, G. The German precursor study) methodology and insights. Reliability Engineering & System Safety 27(1990)1, pp. 53)76.

[3-25] Bier, V.M., Issues in the Estimation of Aging in Event Frequencies. To be in the Proc. of the International Symposium on the Use of Probabilistic Safety Assessment for Operational Safety, PSA '91, Vienna, 3)7 June, 1991. International Atomic Energy Agency, Vienna. Paper IAEA-SM-321/29.

[3-26] Vesely, W.E., Calculation of the Core Damage Frequency Increase due to Aging under a Given Maintenance Program. To be in the Proc. of the International Symposium on the

Use of Probabilistic Safety Assessment for Operational Safety, PSA '91, Vienna, 3)7 June, 1991. International Atomic Energy Agency, Vienna. Paper IAEA-SM-321/28.

4 LIVING PSA MODEL

This chapter presents the features needed to make a PSA model feasible for various applications. The model should be flexible enough to be able to represent changes in the conditions of safety systems of the plant [4-1]. A living PSA model must treat time dependences in a much more complete way than a conventional PSA model [4-2], [4-3]. Completeness and realism of the model and data are very important, much more so than in basic PSA [4-4]. A problem area in this development of a living PSA model is the common cause failure (CCF) model [4-5], [4-6].

In the context of living PSA with its frequent, time-dependent risk monitoring and risk follow-up studies, there may be too little time to carry out evaluations with the whole model, instead of which simplified or shortened calculations are made. For instance, the performing a conventional Monte Carlo uncertainty analysis would be too time-consuming. In case of integrated uncertainty analysis, much of the uncertainty analysis can be prepared through precalculations of necessary, total basic event probabilities [4-7].

4.1 Definition of risk frequencies

The definitions are presented here in the case where the risk is expressed in terms of risk frequency, i.e., frequency of accident, or probability of accident per unit of time. Risk frequency is denoted by *f*. Usually, the risk frequency is expressed in units 1/year as a mean frequency over a given time period. The risk frequency can be interpreted also as expected number of accidents over a given time period per time period.

The content of "accident" is specific for the application. In level 1 PSA of a nuclear power plant, a reactor core damage event is the accident considered. Respectively, the risk frequency is called core damage frequency.

Generally, the risk frequency can obtain any positive value. A zero risk frequency is interpreted as an impossibility of the occurrence of the accident. In practice, the core damage frequency is $1 \cdot 10^{-6}$)$1 \cdot 10^{-4}$ per reactor-year. System and component failure frequencies tend to be significantly higher.

The basic risk measures express the plant risk frequency given certain conditions of safety systems. The basic risk measures discussed are

- nominal risk frequency,
- instantaneous risk frequency, and
- inherent risk frequency.

The basic risk measures are the results of the main living PSA approaches (see chapter 3), namely

- risk assessment,
- risk monitoring, and
- risk follow-up.

The nominal risk frequency is normally used in risk assessment, and the instantaneous risk frequency is used in risk monitoring as well as in risk follow-up. For each approach, an inherent risk frequency can be defined so that results can be presented in a relative manner. Table 4-1 summarizes the definitions of the measures. According to the need, we can define application specific measures which are called generated risk measures. Respectively, the features of the main living PSA approaches are summarized in Table 4-2.

Table 4-1. Basic risk measures.

Risk measure	Notation	Description
Nominal risk frequency	f_n	The risk frequency obtained by the use of nominal or time-average failure probabilities for component and system failures as well as for operator errors and by the use of nominal initiating event frequencies. If the evident unavailability caused by maintenance and repair is excluded, then a (nominal) *baseline* risk frequency is obtained.
Instantaneous risk frequency	$f(t)$	The risk frequency of the current conditions of the safety systems. The component or system concerned is presented in the model by evident events (operating q=0, failed q=1) and by hidden events ($q(t)$ = unavailability model). If the evident unavailability caused by maintenance and repair is excluded, then an instantaneous *baseline* risk frequency is obtained.
Inherent risk frequency	f_0	The risk frequency of the conditions where no component is unavailable due to maintenance or repair events, and all standby components have been recently tested without any failure indications. Inherent risk frequency represents the *lowest theoretically achievable* risk frequency with current design.

4.1.1 Nominal risk frequency

The nominal risk frequency f_n is the top result of a basic PSA. It is obtained using nominal values for the basic event probabilities. Component unavailabilities are estimated from operating experience or from generic data sources. Tests and corrective as well as preventive maintenance actions are performed according to the rules in Technical Specifications. The nominal risk frequency is meant to be an approximation of the average risk frequency of the plant

$$f_n \approx f_{ave} = \frac{1}{T}\int_0^T f(t)\,dt. \qquad (4\text{-}1)$$

where T is for instance one operating year.

If the evident unavailability caused by maintenance and repair is excluded, then a (nominal) *baseline* risk frequency is obtained [4-8].

4.1.2 Instantaneous risk frequency

From the living PSA point of view, the instantaneous risk frequency is the basic risk measure. It is a function of time and conditions of the safety systems $f(x(t))$. We normally denote it just as a variable of time $f(t)$ and call it instantaneous risk frequency, but sometimes also as a variable of the condition $f(x)$ depending on which aspect is emphasized.

Table 4-2. The model features of the living PSA approaches.

Model feature	Risk assessment	Risk monitoring	Risk follow-up
Results	Nominal risk frequency	Instantaneous risk frequency	Retrospective risk frequency, indicators
Potential use of generated results	Long term planning Risk contributor identification	Short term planning Operational risk decision making	Analysis of operating experience Risk contributor identification Risk experience feedback
Criteria	Nominal based Risk contributors	Peak based Allowed duration for given configuration	Average based Number of events significant for safety
Conditions [1]	Average, power operation	Monitored or postulated, power operation	Historical power operation, may include initiators
Initiating events	Nominal frequencies	Nominal frequencies	Nominal frequencies for full-power periods, P=1 for occurred initiators [2]
Basic events	Nominal unavailabilities	As monitored	As monitored or retrospective
Evident events		0 or 1	0 or 1, possibility of recovering
Hidden events		$q+\lambda t$ or q [3]	$q+\lambda t$ or q_{00} for successful [4] 1 or conditional prob. for unsuccessful [5]
Human errors		As basic events	As basic events, recovery possibilities

[1] Only power operation PSA model available
[2] Occurred initiators calculated in probability dimension
[3] $q+\lambda t$-model is used for time-dependent component unavailability model
[4] Standby component functions in test or demand
[5] Standby component fails in test or demand

In the evaluation of the instantaneous risk frequency, basic events are modelled according to knowledge about the conditions of the safety systems. In practical terms, the component or system concerned is presented in the model by evident events (operating q=0, failed q=1) or by hidden events ($q(t)$=unavailability model). If the evident unavailability caused by maintenance and repair is excluded, then an instantaneous *baseline* risk frequency is obtained

The evaluation of the instantaneous risk frequency as a function of time is a demanding task, and it requires an accurate reliability model and an efficient computer code. For instance, FRANTIC code has been developed for system level time-dependent analyses [4-9]. In living PSA, similar analyses are performed at the nuclear power plant level by a time-dependent PSA model, and actual event data. The overall contribution of test and maintenance strategies cannot be examined without plant level analyses which might bring out other risk contributors than the nominal risk assessments [4-10].

4.1.3 Inherent risk frequency

Inherent risk frequency f_0 is used in the result presentation and decision making. It is obtained from the nominal risk frequency by setting the evident maintenance and repair events to 0, and hidden component events to as if just repaired or replaced. Otherwise nominal probabilities are used. A

standard operational alignment of the systems, or if there exist alternative alignments, the alignment most frequently used corresponds to the inherent conditions.

The inherent frequency represents the *lowest theoretically achievable* risk frequency, which is hypothetical because standby components can never be tested simultaneously. There will always remain failure modes which cannot be "tested" or "repaired" away, such as operator errors, so that inherent risk frequency is not zero.

Inherent conditions can be defined at any model level from the plant, safety function and system level down to specific component models. The advantage of the inherent frequency with respect to the nominal frequency is that the evident, and to some extent temporary, unavailability contribution caused by maintenance and repair actions is removed from the result. Therefore it has a closer relationship to the definition of the instantaneous risk frequency than the nominal frequency has.

It should be noted that the inherent risk frequency is a predicted risk level which can be reached by testing the components and restoring the unavailable equipments. In the risk follow-up perspective, where the situation is examined retrospectively, we have more information about the component operabilities. In principle, a lower risk level can be reached due to finding out that certain hidden failure modes could not have existed.

4.2 LPSA model features

4.2.1 Representation of the plant safety status

The plant safety status depends on the conditions of the systems and components of the plant. Some systems and components are in operation, some are in standby mode, some are repaired, some are maintained etc. The model should reflect our knowledge about which condition each system and component is in, and how this affects the plant risk level.

From the plant safety status point of view, we distinguish between various types of basic events. The main division is between the initiating events and basic events. The PSA model can be considered a fault tree model with the top event "core damage". The top event is caused by an initiating event AND subsequent failure of the safety systems i.e. the plant response. If there are more than one initiating event class, the top event is an OR-gate which branches to the initiating event classes. Figure 4-1 outlines the top structure of a "PSA fault tree".

The dimension of the initiating event is frequency (1/time unit), and the dimensions of the safety system failures are probabilities per demand. Thus the top event has a frequency dimension which we call risk frequency. As a reliability function, it can be expressed

$$f(t) = \sum_i \lambda_i P\{\Phi_i(t)=1\}, \qquad (4\text{-}2)$$

where λ_i:s are the initiating event frequencies and $P\{\Phi_i(t)=1\}$ is the probability of the plant response failure given the initiating event i at time t.

The safety function failure probability is calculated by a reliability model constituted of basic events such as component failures and unavailabilities as well as human errors [4-11]. The model represents which combinations of the basic events can lead to the accident. It should be noted that the basic event probability is a conditional probability: the probability that the basic event is true given the initiating event.

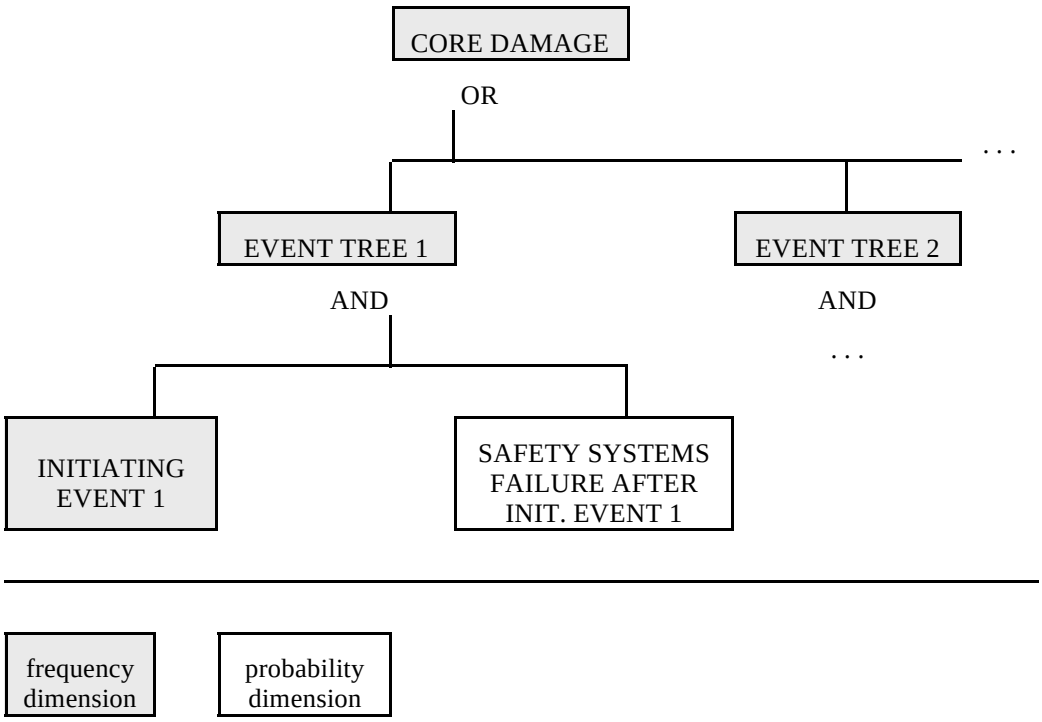


Figure 4-1. Top structure of PSA in a fault tree format.

From the observer point of view, basic event states can be divided to *evident* and *hidden* (latent) events. Evident events are such that the observer knows with certainty whether the event is true or not. Other events remain hidden.

In the basic PSA, this division does not appear so clearly because nominal unavailability may include both type of events. The distinction is important for a living PSA model. All observations such as maintenance or repair should be easily updated in the model to reflect the changed plant configuration. The modification of the static component and system models to dynamic ones is perhaps the main effort to be carried out in the development of basic PSA for living use. Table 4-3 categorizes the usual basic event types for evident and hidden ones.

Let $X(t)$ be the binary variable denoting the state of the component at the time moment t as follows

$$X(t) = \begin{cases} 0, \text{ component is functioning,} \\ 1, \text{ component is failed.} \end{cases} \tag{4-3}$$

The probability of the basic event being true is denoted by

$$q(t) = P\{X(t)=1\}. \tag{4-4}$$

In the evaluation of the nominal risk frequency, we use the average unavailability

$$q_{ave} = \frac{\text{time of being unavailable}}{\text{observation time}}. \tag{4-5}$$

Table 4-3. Classification of the basic events to evident and hidden events.

Basic event type	**Observability**
Component[1] unavailable due to maintenance	Evident
Component unavailable due to repair	Evident
Standby component failure	Hidden
Demand time failure	Hidden
Test and maintenance error (human error type 1)[2]	Hidden
Human error in accident response (type 3)5)[2]	Hidden

[1] component is interpreted in this table as a system or equipment, too
[2] see chapter 4.2.5 for human error type classification

In the evaluation of the instantaneous risk frequency, we use for the evident events the observed value

$$q(t) = 0, \text{ or } q(t) = 1. \tag{4-6}$$

In the evaluation of the inherent risk frequency, $X(t)$ is usually 0 for the evident events yielding $q(t)=0$.

Failures of standby components and human errors are typical hidden events. We do not know their status beforehand. In many cases, however, tests provide some information which improves the probability estimation of $q(t)$. The hidden events can be divided into time-dependent and time-independent failure modes.The time-independent (non-detectable) events, such as operator action errors after an initiator, have a constant failure probability in all evaluations

$$q(t) = q. \tag{4-7}$$

The time-dependent events can be modelled in several ways. The common "$q+\lambda t$"-model will be introduced in chapter 4.2.3. In the evaluation of the nominal risk, the limiting average unavailability is used

$$q_{ave} = \lim_{t\to\infty} \frac{1}{t} \int_0^t q(s)\,ds = \frac{1}{t_r} \int_0^{t_r} q(s)\,ds, \tag{4-8}$$

where t_r is (known) time between two renewal points of the unavailability model, such as a surveillance test or maintenance performed as in the planned test and maintenance strategy.

In instantaneous risk frequency evaluations, value of $q(t)$ depends on the time-dependent model and available information. According to our definition, the inherent risk represents the lowest theoretically achievable risk frequency which is fulfilled for time-dependent events just immediately after the renewal point (t=0) such as test, repair, restoring. The inherent basic event unavailability is denoted by $q(0)$.

4.2.2 Initiating events

An initiating event is a fault, failure or other occurrence leading to a need for subcriticality and removal of decay heat by the plant safety systems. The initiating events are modelled with an occurrence frequency (1/a or 1/h). The parameters describing the average frequency are usually regarded as constants; ageing or trend models may be used also [4-12].

Considered time periods can be divided into power operation periods and shutdown periods. For risk assessment and monitoring approaches, the power configuration is the initial state for the evaluations. From the risk follow-up point of view, initiators may be included in the observation period. Table 4-4 summarizes the value of initiating event frequencies in the applications.

Table 4-4. Use of the initiating event frequencies in living PSA approaches.

Evaluation period	**Risk assessment**	**Risk monitoring**	**Risk follow-up**
Power operation period	nominal	nominal	nominal
Initiators	[1]	[1]	1, for the initiator [2] 0, for the other ones [2]

[1] not applicable
[2] probability dimension

If we are calculating the risk frequency of the plant in a power operation state, the nominal values are applied to the initiating event frequencies. In the risk assessment and monitoring approaches, there should not be any interpretational problems, but risk follow-up deserves some explanation. In principle, we could think that we have knowledge about the occurrence of the initiating events but this perspective would always yield a historical risk frequency $f(t)=0$ unless a core damage actually have occurred. The generated results are, in this perspective, trivial. If follow-up is limited to the safety system events, meaningful measures can be obtained because the results can be represented as probabilities of plant response failure given an initiating event i at that moment, $P\{\Phi_i(t)=1\}$ (see equation (4-2)).

In the risk follow-up, the instantaneous risk frequency cannot be assessed for an initiator. We can, however, calculate a conditional core damage probability given the initiator, i.e., $P\{\Phi_i(t)=1 \mid$ "observed safety function performance"$\}$. For the occurred initiating event, the probability of the initiating event is set to 1 and the probabilities of other initiators are 0. One problem is that to what extent the information about successful and unsuccessful safety function responses is used. Again, in principle, a successful plant response would imply $P\{\Phi_i(t)=1 \mid$ "no core damage"$\}=0$. However, if the successful system operations are ignored so that nominal probabilities are used for the probability of successful operation, the probability of plant response failure is greater than 0. Failed or unavailable functions and components are, on the other hand, modelled as failed with certainty. This approach can be called "failure memory only".

4.2.3 System and component models

From risk monitoring and follow-up point of view, the most interesting basic event model is related to failures of periodically tested or maintained standby components. The model should account for that some failures cannot be detected in tests although they would later cause an unwanted failure at a real demand. A general model, covering all combinations of time-dependent and time-independent failure modes, detectabilities with respect to both modes, etc. is difficult to create, and even more difficult to apply. As a candidate model for the living PSA purposes, the model presented in reference [4-13] and used in the Nordic reliability data book [4-14] is chosen with minor modifications. Figure 4-2 illustrates a corresponding fault tree. It should be noted that the basic events in this model are *not* independent but rather exclusive events.

The basic standby component model, "$q+\lambda t$"-model, is applied to the calculation of the time-dependent component unavailability

$$q(t) \approx q_0 + \lambda_s (t - TL) + \lambda_d \cdot TM, \qquad (4\text{-}9)$$

where q_0 is the time-independent component failure probability, λ_s the standby failure rate, TL the last test moment, λ_d the operation time failure rate, and TM the average demand time. More generally, TL represents any last time point when a failed state could have been detected. In addition to a surveillance test, it can be end of maintenance or repair, demand situation, etc. These time points are *renewal* points in the reliability history of the stand-by component.

The equation yields the basic event probability for risk monitoring applications. If a failure is detected or the component is maintained, the basic event must be replaced by an evident basic event with an unavailability of 1.

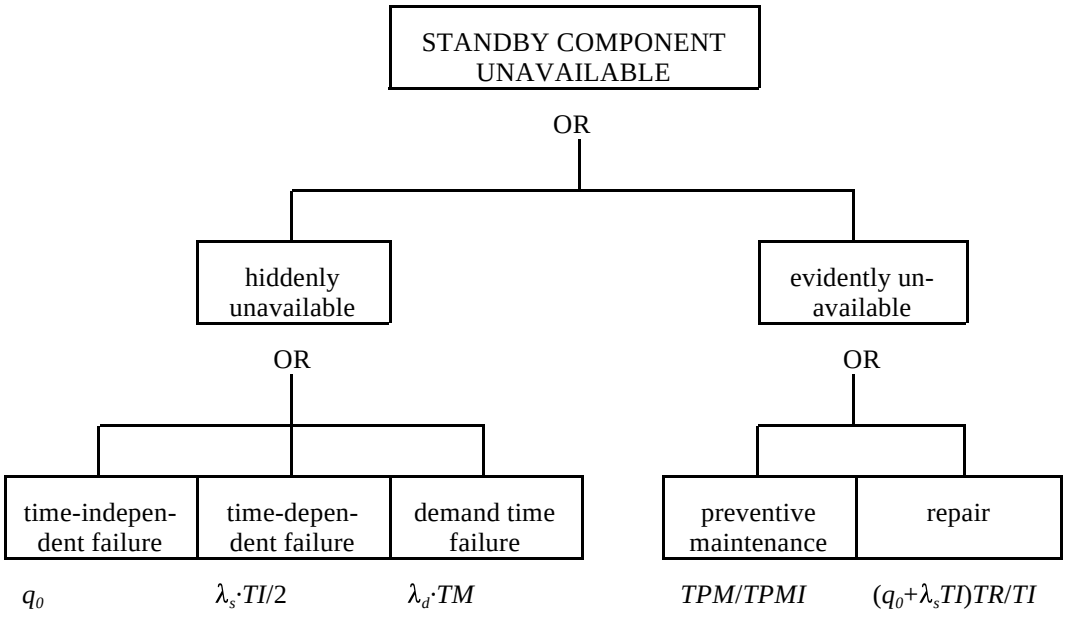


Figure 4-2. A standby component unavailability model.

In risk assessment, the average value is used. The average unavailability must, however, include the evident periods, i.e. the repair and maintenance periods, so that

$$q_{ave} \approx q_0 + \frac{1}{2}\lambda_s \cdot TI + (q_0 + \lambda_s \cdot TI)\frac{TR}{TI} + \lambda_d \cdot TM + \frac{TPM}{TPMI}, \qquad (4\text{-}10)$$

where *TI* is the test interval, *TR* is the average repair time, *TPM* the average (scheduled) preventive maintenance time, and *TPMI* the average preventive maintenance interval [4-14]. The possibility to restore the component while in repair or in maintenance is not credited in this equation. The unavailability during testing is ignored, too, or it can be included explicitly if necessary.

In risk follow-up, we have to distinguish between *successful* and *unsuccessful* components. A successful component is a component that has been proved to be in a state where it can perform its intended function. The state has been detected in a recent renewal point such as a test. A test can, however, be incomplete to detect all failure modes, so that the component may fail in a true demand. If the component fails in a test or demand, it is called an unsuccessful component. An unsuccessful component has become latently unavailable at some time during the preceding test interval.

Successful components

Successful components can be treated in two ways:

1) the standby component unavailability model (equation (4-9)) is used, or

2) non-detectable unavailability of the component is used.

The first approach is called the *risk follow-up with failure memory only*, because it does not take credit for successful events. This approach is used to evaluate conditional core damage probabilities of occurred initiators. The second approach is called the *risk follow-up with total memory*. Non-detectable unavailability of the component depends on the test effectiveness.

The failure data presented in the Nordic reliability data book [4-14] are based on failure experience from surveillance testing. This implies that only the component baseline risk contributor without test effectiveness considerations is available in data. A simplified assumption is made that the test conditions are equal to the demand requirements) the test is perfect.

If the test effectiveness is included, the time-dependent component unavailability model must be changed. More parameters are needed. The additional parameters can be expressed by introducing different probabilities for "failure on demand" (q_0) and "failure on demand but not on test" (q_{00}). Another way to model the test effectiveness is to multiply the failure probability by a test effectiveness parameter (η).

In connection to a renewal point, the component may remain failed so that test does not detect the failed state but the component would fail when demanded again. The probability for this failure is q_{00} or $(1\text{-}\eta)q_0$, where η is the test effectiveness

$$\eta = \frac{q_0 - q_{00}}{q_0}. \qquad (4\text{-}11)$$

In connection to a renewal point, the component may remain failed so that both test and demand detect the failed state. The probability for this failure is q_0-q_{00} or ηq_0. Thus total failure probability for the baseline contribution is q_0. In this definition, the q_{00}-term is presented as time-independent.

In principle, the test effectiveness considerations should be extended to the time-dependent failure contribution, as in the following equation

$$\begin{aligned} q(t) &= P\{X(t)=1 \mid TL\} \\ &\approx P\{\text{non-detectable failure in last renewal point}\} + \\ &\quad P\{\text{non-detectable failure before last test}\} + \\ &\quad P\{\text{remains failed in last test}\} + P\{\text{failure before } t\} \\ &\approx q_{00} + 1 - e^{-\lambda_{s0} TL} + q_0 - q_{00} + 1 - e^{-\lambda_s (t-TL)} \\ &\approx q_0 + \lambda_{s0} TL + \lambda_s (t - TL) \\ &= q_0 + \lambda_s (t - \eta_l TL), \end{aligned} \qquad (4\text{-}12)$$

where η_l is the test-effectiveness of the time-dependent part, and the last restoration of the component took place at t=0. Similarly, we define that λ_s includes both failure rate of test detectable failures and non-detectable failures. If η_l=1, i.e., the test detects all time-dependent failures.

The approximation is valid if q_{00}, $\lambda_{s0}t$, q_0 and $\lambda_s t$ are small so that the probability of union of events can be expressed as sum of the probabilities of the events. Figure 4-3 shows the saw-teeth increasing unavailability function when the condition is examined only by surveillance tests, but not by true demands.

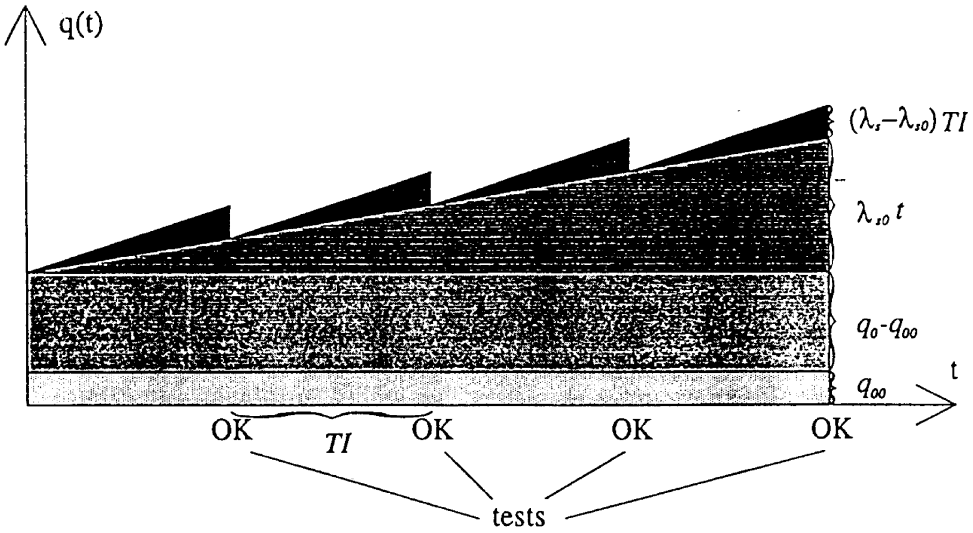


Figure 4-3. The instantaneous component unavailability by risk monitoring.

Unsuccessful components

The unsuccessful component is known to have failed at some time between the two detection moments. There are several approaches to represent when the failure actually occurred. The two perhaps simplest ways to do it are:

1) A latent unavailability, $q(t)=1$ since the latest successful test.

2) A linear probability for the failure to occur at any time in the interval from the latest successful test to the detection of the failure

$$q(t) = \frac{1-(1-q_0)e^{-\lambda_s(t-TL)}}{1-(1-q_0)e^{-\lambda_s TI}} \approx \frac{q_0+\lambda_s(t-TL)}{q_0+\lambda_s TI}. \qquad (4\text{-}13)$$

The first approach is the most conservative way to assess the component unavailability. The second approach is an attempt to make the model less conservative by applying the conditional probability expression for the failure time. The treatment of standby basic events in the main living PSA approaches is summarized in Table 4-5.

Table 4-5. Summary of the treatment of standby component basic events.

	Risk assessment	**Risk monitoring**	**Risk follow-up**
Successful equipment	$q_{ave}=q_0 + 0.5\lambda_s TI + (q_0+\lambda_s TI)TR/TI + \lambda_d TM + TPM/TPMI$	$q(t)=q_0+1-\exp\{-\lambda_s(t-TL)\}+\lambda_d TM$	a) with failure memory only $q(t)=q_0+1-\exp\{-\lambda_s(t-TL)\}+\lambda_d TM$, b) with total memory $q(t)=q_{00}$
Unsuccessful equipment	As successful, no credit for restoring given	Hidden event until detection $q(t)=q_0+1-\exp\{-\lambda_s(t-TL)\}+\lambda_d TM$ Evident event during corrective actions: $q(t)=1$ Restoring possibilities	Hidden event until detection a) latent unavailability $q(t)=1$, or b) linear unavailability $q(t)=(q_0+\lambda_s(t-TL))/(q_0+\lambda_s TI)$ Evident event during corrective actions: $q(t)=1$ Restoring possibilities

4.2.4 Common cause failures

The modelling of underlying, non-identified dependence mechanisms between redundant safety system trains is usually done by common cause failure (CCF) models. In basic PSA, CCFs represent events which make several safety systems simultaneously unavailable [4-15]. Time-dependence introduced with living PSA sets new requirements on CCF models. Stand-by system unavailabilities are dependent on test arrangements. The problem is how to avoid conservatism and to allow non-

symmetric test arrangements as well as how to treat events with one redundancy evidently or latently unavailable.

A time-dependent CCF model, analogous to the single failure time-dependent model, can be created by accounting the dependence on the test time points, as possible points, where latent faults can be detected and removed, or new faults can be introduced. In a shock model of CCFs [4-5], following assumptions are made:

1. Latent faults can occur at a random time point while components are in a standby mode.

2. If several components are affected by the same latent failure mechanism while on standby, the components enter failure state at the same time point.

3. Faults introduced by testing or other component activation, fail the component shortly after being restored into standby. This failure state can arise systematically through the whole group at time points determined by tests or other activations.

4. Faults are detected in the next test with likelihood 1, and subsequently perfectly repaired.

The assumptions lead to a linear time-dependent model for shared cause events

$$P\{C_{A_1 \ldots A_k}(t) = 1\} \approx q_0^{k|n} + \lambda_s^{k|n}(t - TL_{A_1 \ldots A_k}), \qquad (4\text{-}14)$$

where $A_1 \ldots A_k$ is a specific subgroup of k out of n components and $TL_{A1 \ldots Ak}$ is the last point when some of the components have been tested. The component group failure parameters, $q_0^{k|n}$, $\lambda_s^{k|n}$, can be then developed by parametric models such as SHACAM (shared cause model) [4-16].

When failures are detected or components are otherwise unavailable, the CCF probabilities must be recalculated by conditioning the shared cause events with respect to the detected situation. In practice, it is, however, reasonable to apply specific time-dependent CCF-models only in systems of interest and otherwise apply time-average unavailabilities as in the diesel-generator study [4-5].

In the living PSA model for OKG 2 [4-4], a modified version of the Multiple Greek Letter (MGL) model [4-17] has been used. This modification is called "the minimum-value variation" [4-6], and it works in the following way. Each CCF group involves two or more components. Of all the components in a particular CCF group, the one with the lowest independent failure probability is used as a basis for calculation of the probability for the respective CCF event (see example Figure 4-4). An exception to this rule is the situation where a failure exists, or may have existed (in risk follow-up) among the components involved in the CCF group. If this is the case, it is the probability of the existing failure that is the basis for the CCF probability. For example, if one component is known to be failed (probability = 1) the probability of a second component failure is β until the state of those other components have been verified.

Further analysis is needed before any recommendations related to this problem can be given. A wish would be that the used model would be based on observed common cause failures and that it would account variations in system success criteria, testing rules and test intervals.

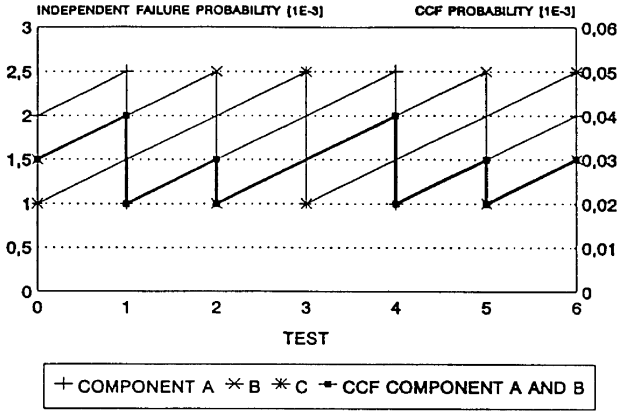


Figure 4-4 Behaviour of the minimum-value variation in CCF modelling.

4.2.5 Human errors

Human errors are included in the plant model to represent various type of human interactions during the course of events. The human interaction can be categorised into five different types relating to component unavailabilities and initiating events [4-18]:

1. Before an initiating event, plant personnel can affect the system or component unavailability.

2. Human actions leading to an initiating event.

3. Errors of omission; after an initiating event, plant personnel fails to initiate the required action.

4. Errors of commission; after an initiating event, plant personnel fails to follow procedures.

5. Recovery actions; after an initiating event, plant personnel, by improvising, recovers the situation.

Type 1 interactions are evident, such as tests and maintenances, but they may cause hidden failures. The components are restored in an unavailable state. The hidden failures can be usually detected in following interactions. Type 2 interactions should be included in the initiating event frequencies. Type 3, 4 and 5 interactions are part of accident sequences. Therefore they are hidden.

4.3 Data

4.3.1 Failure data

Failure data include various basic event parameters. A basic requirement is that the data should be plant-specific, and one part of the living PSA concept is that failure data is regularly updated and verified. Table 4-6 shows the sources of failure data.

Table 4-6. Sources of basic event parameters.

Parameter	Operating experience	Generic data bases	Deterministic analyses	Operating procedures (Tech. Spec.)	Expert judgement
per demand failure probabilities	x	x			
failure rates	x	x			
repair times	x	x			
CCF-parameters	x	x			x
demand times	x		x	x	
test intervals				x	
maintenance intervals				x	
test effectiveness parameters	x				x
uncertainty parameters	x	x			x

To increase the credibility of the results of living PSA, the estimation of the failure data should be validated. This often requires rather extensive and deep data analyses such as performed for diesel-generators [4-19] and motor operated valves [4-20], [4-3]. The analyses clarifies the problems affecting validity, such as [4-3]:

1) Problems in testing:
   test conditions are different from real demands, test may cover only part of the component, test covers only part of the possible failures, not all failures are removed, new failures may be introduced.

2) Problems in failure reporting:
   coverage of reporting, correctness of reports, information reported.

3) Problems in preparation of quantitative failure data:
   definition of component boundaries, grouping of components, number of demands, statistical treatment.

4) Problems in reliability modelling:
   ageing and test ineffectiveness may have been disregarded, assumption on degree of time-dependence, estimation of time-independent part.

4.3.2 Operational data

Operational data are needed both in risk monitoring and follow-up approaches. In risk monitoring, operational data include information about states of the components and systems. Based on the operational data, evident basic events can be set to false or true. Depending on the realization of the living PSA system, the models are updated by responsible persons according to the procedures. In an on-line system, the operators of the plant keep the models up-to-date all the time. If the use of PSA is less frequent, the information is gathered every time when a PSA evaluation has to be made. The main pieces of information needed are:

- operational mode of the plant (power operation, hot standby, cold standby, etc.),

- operational mode of the main systems (operation, standby, amount of trains in operation, isolated),
- operational mode of individual components (running, standby, open, closed, in maintenance, repair or test),
- records of last surveillance tests.

In risk follow-up approach, the operational data can be gathered from several sources depending on the reporting practices of the plant, such as:

- licensee event reports,
- monthly reports,
- daily reports,
- test lists,
- failure reports
- scram reports.

4.4 Uncertainties

Just as in the case of risk assessment, there are different kinds of uncertainties to take into account in the context of living PSA. To begin with the most difficult one, we are always uncertain about the degree of completeness or coverage of the phenomena to be modelled. Another source of uncertainty, also difficult to cope with, is the degree of relevance or validity of the model used. Thirdly, the kind of uncertainty we will concentrate on in this section is the so called *parametric uncertainty*, an uncertainty concerning the values of the multitude of parameters that are used in the comprehensive PSA-models.

Successively, along with the development of the PSA-work in general the uncertainty of both completeness and modelling will reduce. But how to get measures of these uncertainties, of the former at least, is even hard to imagine. The conventional method by which the modelling uncertainty hitherto has been handled, is sensitivity analysis. By choosing alternative models just for the phenomena we are most uncertain about, we get a range of values for the key input variable (decision variable). Recently, a Bayesian reasoning has been suggested also for the treatment of modelling uncertainty [4-21], where the various model alternatives are assigned a priori probabilities which are then updated with regard to the fitness of the models.

4.4.1 Parametric uncertainty in living PSA

The risk assessment can be divided, as explained in section 4.2.1, into two essentially different parts:

1) the assessment of the initiating events and
2) the assessment of the safety system failure probabilities.

The dimension of the first part is frequency or intensity (1/time unit), while the dimension of the system failures are probabilities per demand. The basic event probabilities of the fault tree models are estimated on the basis of various component unavailability models. The parameters of these models are used as carriers of the information from available operating experience. Our knowledge or uncertainty about these parameters is called *parametric uncertainty*. How this uncertainty is utilized in the estimation of the safety system failure probability and the risk frequency is the central object of the parametric uncertainty analysis.

The most common approach in this uncertainty analysis is "uncertainty propagation", e.g., by the use of Monte Carlo simulation. Another view on parametric uncertainty is taken in the recently suggested "integrated uncertainty analysis" [4-7].

4.4.2 Uncertainty propagation

In a conventional, point value PSA the basic event probabilities q_j are conditional probabilities of the type q_j=P{$E_j|\lambda_j$}, where the parameter(s) λ_j is assumed to be known. Then the analysis also results in a conditional risk frequency $f|\lambda$, conditioned by known values of all basic event parameters λ involved.

Further, in conventional uncertainty analysis each basic event parameter λ_j is treated as a stochastic variable, which is propagated through the plant model to provide an uncertainty distribution for the risk frequency, the top level parameter. The usual way for this propagation is Monte Carlo simulation, which means that the risk frequency $f|\lambda$ is calculated repeatedly for sampled λ-values. Experiences gained of this type of analysis show that the mean value of such a top level distribution is normally a factor of 3 to 4 higher than the point value of $f|\lambda$ [4-22].

4.4.3 Integrated uncertainty analysis

In the recently proposed approach of integrated uncertainty analysis (IUA) [4-7], one avoids the use of uncertainty of probabilities. According to the Bayesian methodology, the purpose of fictive model parameters is to be used for the estimation of the probabilities of observable events. Thus, e.g., the total (unconditional) component failure probability q_j is calculated according to the law of total probability

$$q_j = \int q_j|\lambda_j \cdot p(\lambda_j)\, d\lambda_j, \qquad (4\text{-}15)$$

where $q_j|\lambda_j$ denotes the component unavailability model with known parameter(s) and $p(\lambda_j)$ stands for the uncertainty concerning the parameter(s) λ_j. Thereby, the parametric uncertainties are utilized on the level they belong to, namely the calculation of the basic event probabilities.

The integrated uncertainty analysis is a consistent approach. It deviates from the conventional approach only in that the conditional probabilities $q_j|\lambda_j$ are substituted by the total probabilities like that of the previous equation. When these total probabilities are calculated, all details that are known in the specific situation can be accounted in the unavailability model. For example, in risk monitoring and risk follow-up, the times elapsed since the latest tests are quantities of great interest.

By integrated uncertainty analysis, all knowledge about model parameters (not only some point values) is directly used resulting in a unique safety function failure probability. Thereby, we need not worry about the discrepancy between the results of point value analysis and uncertainty analysis. Integrated uncertainty analysis results in a risk frequency distribution that is directly applicable in decision analysis. Specific problem areas, like the modelling of CCF-uncertainty and state-of-knowledge dependences, are easier to handle, because multi-dimensional distributions are integrated on the basic event level.

In the context of living PSA with its frequent, time-dependent risk monitoring and risk follow-up studies, the carry-out of conventional Monte Carlo uncertainty analysis would be too time-consuming. In case of integrated uncertainty analysis, much of the uncertainty analysis can be prepared through precalculations of necessary, total basic event probabilities.

4.5 Limitations

Even though an extensive work has been made to improve the fault tree and event tree models to make them more complete and to remove conservatism, there are still many remaining deficiencies and uncertainties.

4.5.1 Incompleteness

The incompleteness problem arises because a manageable model cannot encompass all conceivable events and sequences, i.e. the entire risk is not covered by the model. Incompletenesses may not only result in an erroneous absolute risk level, it may also result in wrong relative importance for individual failures. This may in turn lead to wrong decisions based on the living PSA application results. It is therefore important to remove as much as possible of all incompletenesses.

One very important incompleteness can be that the PSA model includes only a sub-set of all possible initiating events. A number of incompleteness issues arises also around component failure modes: Some failure modes are missing, possible dependencies are not modelled, the test effectiveness is not 100 % as assumed, etc.

4.5.2 Conservatism

In many cases, PSA models are made with conservatisms built into the model and data. The reason is usually to simplify the model while at the same time making estimates on the conservative side. The success criteria used for the different safety functions in the event trees are in many cases conservative. In some cases, credit is not taken for safety functions or support functions. Another example is that recoveries are not taken into account properly. This is acceptable in situations where the main purpose of the calculations is to verify a certain absolute risk level. In many living PSA applications, however, the conservatisms may lead to wrong relative importance and wrong decisions, and thereby in the end leading to non-conservative actions.

4.5.3 Common cause failures (CCF)

Time-dependent system unavailabilities and common cause failures are not fully modelled in conventional PSAs. The stand-by system unavailabilities are dependent on test arrangements. The problem is to avoid conservatism and to allow non-symmetric test arrangements as well as how to treat events with one or more redundancy evidently unavailable. A time-dependent CCF model, analogical to the single failure time-dependent model, can be created by taking into account the dependency on the test time points, as possible points, where latent faults can be detected and removed, or new faults can be introduced. Further analysis is needed before any recommendations related to this problem can be given.

4.5.4 Testing and test effectiveness

The failure data presented in the Nordic reliability data book are based on failure experience generated from testing. This implies that only the component risk contributor without test effectiveness considerations is available in the data. In practice, a simplified assumption is made that the test conditions are equal to the demand requirements) the test is perfect. If the test effectiveness is taken into account, the time-dependent component unavailability model must be changed; more parameters are needed. There is also a lack of data regarding test effectiveness.

4.5.5 Practical time constraints

In the context of living PSA with its frequent, time-dependent risk monitoring and risk follow-up studies, there may be too little time to carry out evaluations with the whole model, instead of which simplified or shortened calculations are made. One way to reduce the calculation time is to use a precalculated minimal cut set list, and only update basic event probabilities. Naturally, the changes among evident events may cause the result to be strongly biased. The time limit is also one motivation for the use of integrated uncertainty analysis, because the time-consuming Monte Carlo simulation is avoided. See chapter 5 for constraints of the evaluation tools.

4.5.6 Simplified approach for time-dependent evaluations

Many computer programs used in PSA analysis apply only nominal unavailabilities to basic events. What is required for the practical implementation is a routine that reads an event file and finds out the time points where computations are needed. At each time point, new probabilities are calculated for the cut set components, just before and after the moments. As a result, a risk log with time points and corresponding risk frequencies is obtained.

In risk monitoring, nominal values are used for hidden events. The contribution of the maintenance and repair action caused unavailabilities should be removed. For evident unavailability periods, q=1 is used. The time-dependence comes into view in the risk follow-up. When a failure of a standby component is detected, a latent unavailability $q(t)$=1 since the last test is used. In the failure memory only approach, successful periods are evaluated as in risk monitoring, namely using nominal unavailabilities. In the total memory approach, q_{00} value is applied instead. Table 4-7 lists the equations for "exact" and simplified approaches.

Table 4-7. Unavailability equations for "exact" and simplified risk follow-up approaches.

		Test result
Approach	**Successful**	**Unsuccessful**
Off-line monitoring	$q_0+\lambda_s(t\text{-}TL)+\lambda_d TM$	$q_0+\lambda_s(t\text{-}TL)+\lambda_d TM$
simplified	q_n	q_n
With total memory	$q_{00}+\lambda_d TM$	$(q_0+\lambda_s[t\text{-}TL+(TI\text{-}t+TL)\lambda_d TM])/(q_0+\lambda_s TI)$
simplified	$q_{00}+\lambda_d TM$	1
With failure memory only	$q_0+\lambda_s(t\text{-}TL)+\lambda_d TM$	$(q_0+\lambda_s[t\text{-}TL+(TI\text{-}t+TL)\lambda_d TM])/(q_0+\lambda_s TI)$
simplified	q_n	1

4.6 References for section 4

SIK-1 reports

[4-1] Holmberg, J., Johanson, G. and Niemelä, I. Risk measures in living probabilistic safety assessment. VTT Publications 146, Technical Research Centre of Finland, Espoo, 1993, 59 p. + app. 10 p.

[4-2] Johanson, G. Survey on time dependencies in LPSA models. Report NKS/SIK-1(91)6, Swedish Nuclear Power Inspectorate, Stockholm, 1991, 14 p.

[4-3] Knochenhauer, M. & Johanson, G. Derivation of time dependent component unavailability models and application to Nordic PSA:s. To be presented in PSAM II conference, San Diego, March 20)24, 1994. Report NKS/SIK-1(93)31, 1993. 6 p.

[4-4] Sandstedt, J. Demonstration case studies on living PSA. Report NKS/SIK-1(92)27, Relcon AB, Sundbyberg, 1993, 25 p.

[4-5] Mankamo, T. A time-dependent model of dependent failures) Application to a pairwise symmetric structure of four components. Espoo 1992, Avaplan Oy, Report manuscript NKS/SIK-1(92)13. 31 p. (draft)

[4-6] Erhardsson, U-K. Test av några tidsberoende CCF-modeller. Vällingby 1990, Swedish State Power Board, Report PK-168/90. 4 p. + app. 6 p. (in Swedish)

[4-7] Pörn, K. and Shen, K. Integrated Uncertainty Analysis in PSA. Report Studsvik/NS-91/71, NKS/SIK-1(91)23, Studsvik, Studsvik AB, 1991.

Other references

[4-8] Optimization of technical specifications by use of probabilistic methods) A Nordic perspective. Final report of the NKA project RAS-450, ed. by K. Laakso. 1990, Nordic liaison committee for atomic energy, NORD 1990:33. 156 p.

[4-9] Vesely, W.E., Goldberg, F.F., Powers, J.T. FRANTIC II) A Computer Code for Time-Dependent Unavailability Analysis. Upton 1981, Brookhaven National Laboratories, Report NUREG/CR-1924, BNL-NUREG-51355. 98 p.

[4-10] Andsten, R.S. & Vaurio, J.K. Sensitivity, Uncertainty, and Importance Analysis of a Risk Assessment. Nuclear Technology 98(1992) 160)170.

[4-11] Henley, E.J. & Kumamoto, H. Reliability Engineering and Risk Assessment. Prentice Hall, London, 1980.

[4-12] Pörn, K., Blomquist, R. and Shen, K. I-Boken, version 1. Inledande händelser i svenska kärnkraftverk. Report STUDSVIK/NS-93/17, SKI/TR 019/93, Nyköping, Studsvik AB. 208 p. + app. 13 p. (in Swedish)

[4-13] Mankamo, T. Pulkkinen, U. Test interval optimization of stand-by equipment. VTT Research Notes 892, Espoo 1988, Technical Research Centre of Finland. 22 p.

[4-14] T-book. Reliability Data of Components in Nordic Nuclear Power Plants. 3rd edition. Prepared by the ATV Office and Studsvik AB. Vällingby 1992, The ATV Office, Vattenfall AB. 235 p.

[4-15] Procedures for treating common cause failures in safety and reliability studies. Report NUREG/CR-4780, EPRI NP-5613, Vol. 2, Electric Power Research Institute, Palo Alto 1988, 130 p.

[4-16] Mankamo, T. SHACAM, Shared Cause Model) A Review of Multiple Greek Letter Method and a Modified Extension of the Beta-Factor Method. Espoo 1985, Avaplan Oy. 34 p.

[4-17] Fleming, K.N., Mosleh, A. & Deremer, R.K. A systematic procedure for the incorporation of common cause events into risk and reliability models. Nuclear Engineering & Design 93(1986) 245–273.

[4-18] Hannaman, G.W. & Spurgin, A.J. Systematic Human Action Reliability Procedure (SHARP). Palo Alto 1984, Electric Power Research Institute, Report EPRI NP-3583. 126 p.

[4-19] Mankamo, T. Test strategies for standby diesel generators. SKI research program "Defence against CCF", pilot study for diesel generators. 1993. (draft)

[4-20] Laakso, K. (ed.) Optimization of technical specifications by use of probabilistic methods. A Nordic perspective. Final report of the NKA-project 450. Report NORD 1990:33, 1990.

[4-21] Pulkkinen, U. Bayesian Uncertainty Analyses of Probabilistic Risk Models. In Proc. of the PSA '89 – International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, April 2–7, 1989.

[4-22] Hirschberg, S. (ed.) Dependencies, Human Interactions and Uncertainties in Probabilistic Safety Assessment. Final report of the NKA project RAS-470, NORD 1990:57, 1990.

5 A LIVING PSA SYSTEM

5.1 Introduction

The living PSA system described in this report is based on experience collected from different countries and studies of various systems described in the literature [5-1],[5-2]. The principles for the design of a living PSA operational interface is the outcome of development work carried out within the NKS/SIK-1 project, [5-3].

5.1.1 Objectives with the system

The living PSA concept has its focus on the realism of the analysis applied to current situations at the plant. Basically the question is how the PSA model can be updated to reflect a changing plant and adapted to the needs of continuous safety assessment. To establish a living PSA model is a practical possibility today. Judging from existing applications, it is more a question of resources than development of technical solutions. However, the practical implementation requires development of the existing PSA codes to minimize calculation times and to perform cutset based reevaluations.

With an access to an updatable model providing a realistic representation of plant safety status one has in principle available an in-depth safety analysis in a computerized form. This fact opens the possibility for a much broader utilization of PSA in safety related decisions. This can be achieved by constructing a living PSA system, encompassing the model and underlying analyses, making them more accessible for utilization in plant design and procedure evaluation, operational planning and experience feedback. The kernel of the living PSA system is the model, but in addition a software environment is created with the following aims in mind:

- Support the user in extracting all relevant information from living PSA.
- Integrate living PSA with existing plant information systems.
- Relate living PSA results to deterministic criteria.

Such wider scopes of application must however be introduced only after careful consideration of all aspects to ensure that living PSA results are correctly understood and used. This requires a thorough evaluation of areas where living PSA can contribute to enhanced safety and efficient operations, with particular emphasis on how living PSA results should be introduced to staff with limited knowledge of PSA. The risk measures which are the results of the evaluations, e.g. the core damage frequency, are outputs of the system [5-4].

Part of the purpose of the SIK-1 project is to outline a living PSA interface specification which would support the related code developments in the Nordic countries [5-5],[5-6]. A principal requirement on a PSA software tool is to allow flexible means to manage the model, data and information needed for the evaluation of the PSA and safety management. The basic calculation function is to generate minimal cut sets and to calculate the accident frequency. In addition to this, a number of other requirements can be raised to improve the use of the PSA results and insights.

An important aspect is the calculation time to allow reevaluation of the models given certain specific conditions. The software system must support flexible specification of components, trains or systems, i.e. out of service or reconfigured, in order to update the plant risk status information.

5.1.2 Basic requirements

A living PSA system must be logical, easy to use, efficient, capable to handle a detailed model. By definition, a living PSA is intended to be used on a day-to-day basis. Due to this there are some underlying requirements in all living PSA systems that stem from the basic living PSA requirement. The PSA model must at be kept up-to-date. This means that it must be possible to update the PSA model and results in a simple manner.

Logicality: The living PSA tool and model must form a consistent, compact and logical set of information from top to bottom (relational, hierarchical structure). From this structure the user should be able to find the desired place in a logical way. All connections between entities must be clear (e.g. the user must be able to find out where a certain data set is used). This property must remain even after large number of updates. There should be enough background information for the user to understand the logic of the model and the program. There should be as small number of repeated entities as possible. A reference mechanism ensures that a change in one place is imported to all relevant places.

Ease of use: A living PSA tool is user-friendly and convenient to use, so as not to waste time with the program and its limitations, but to direct the efforts to the PSA model itself. There must be flexible functions to find out and edit information in the model. The model editor should have extensive error-checking and recovery functions. The program should have enough supporting functions or connections, to other programs (e.g. it should be possible to start a text editor or a spreadsheet program from the living PSA program).

It must be convenient and fast to make back-up copies of the model. At any time the PSA should be immediately executable, so that the execution and results are independent of the user (unless the user wishes to do something 'special'). An important feature is that the program itself is able to keep accounts of changes that have not yet been recomputed. The program should possible take care of updating information depending on other information (e.g. updating results when data have been changed). It could e.g. issue a warning that the results are out-of-date.

Efficiency: The recalculation must be quick enough for a daily living PSA work. It may be desirable to have two sets of truncation values, one for quick computations and the other for more exact computations. The program should be able to produce the desired results without manual intervention once started (immediately executable PSA).

In order to guide the user to use the model and program efficiently, the tool should provide the user with hierarchical information on calculated results. E.g. at the highest level the user should see the core damage frequency and the most important initiating events and/or sequences. The next level should present the most important sequences and basic events. The tool should guide the user through the model, starting from a general overview, to the most important details.

Model requirements: Basic requirements on the PSA model are scope, completeness and realism. In general the SIK-1 project deals with level-1 PSA which also indicates the scope according to e.g. IAEA PSA Guidelines [5-7]. Other demands on the scope of PSA raise requirements on completeness and realism which are in many cases central for the validity of the PSA application. The nominal risk model cannot be used for the short-term risk monitoring and risk control applications, and an investigation of the need for the development of a time-dependent model for the instantaneous risk or core damage frequency calculations has been deemed necessary. In the living PSA model, components which are known to be unavailable or available are set to failed or

working with the probability of unity. The model should not contain any events used in the nominal risk model to average unavailability contributions, e.g. from test and repair, but time-dependent component unavailability models should be used [5-8]. A significant deficiency of the time-dependent models is the treatment of the common cause failures. Common cause failures are a problem area already for the basic PSA [5-9], but the time-dependence aspect brings out a new, not yet studied, problem.

Data requirements: It is natural to apply plant specific failure and event data when available. Besides failures and events, many other types of data exist for which generic data cannot be accepted, such as test and maintenance procedures and related plant configurations. Time-dependent models require specific failure data analyses so that time-independent and time-dependent failure mechanisms can be identified. The Nordic reliability data book, T-book, provides a simplified model that can be used as a basis for time-dependent modelling [5-10].

5.2 Features of a living PSA tool

Living PSA tools are computer codes for managing the models, data and information needed in the nuclear power plant's safety management and evaluation by means of PSA. Special features of Living PSA tools are the user friendly interface, fast computation routines and the capacity of storing and manipulating large amount of various kind of information. These features are needed so that PSA would become an every-day safety management tool in nuclear power plants. In this section a description of an *ideal* living PSA tool is provided. The presented features have been picked out from existing tools which are briefly described in a survey carried out to provide an international overview [5-1].

The concept of a living PSA requires a flexible plant model that can be updated in parallel with plant modifications or reconfigurations. It has been assumed that in the future there could be demands that the full scale plant model must be updated in very short time intervals. The user group will expand and will in the future not be restricted to PSA specialists only.

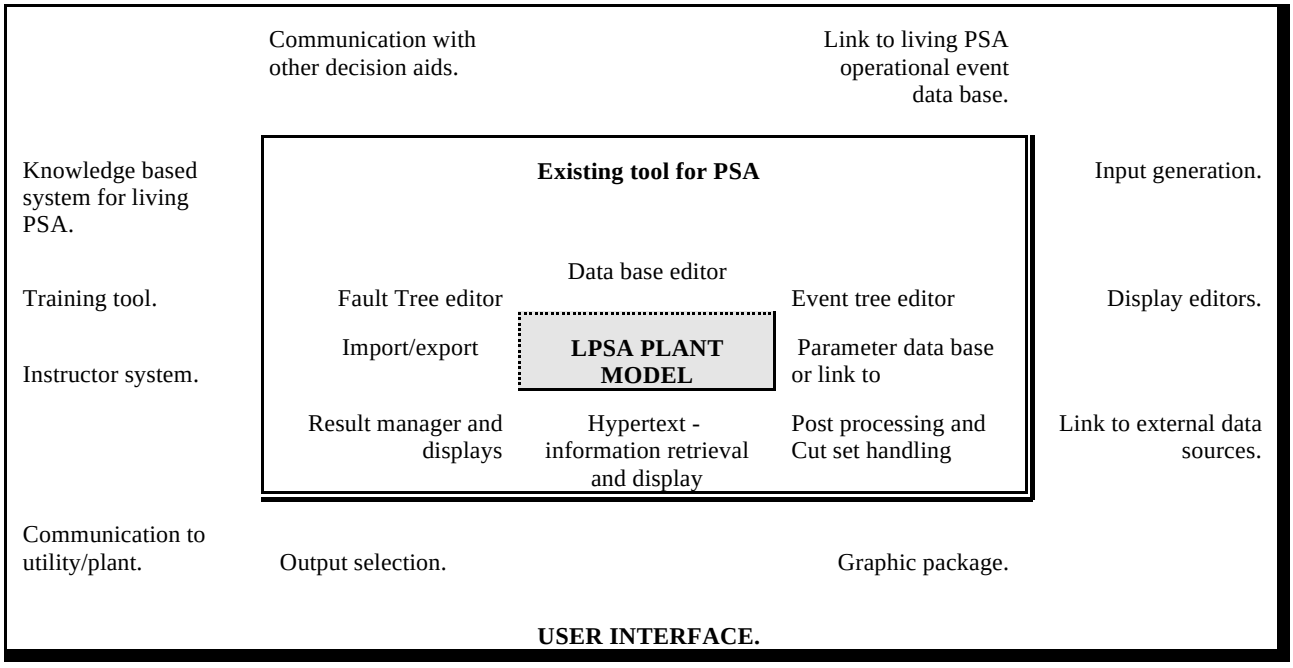


*Figure **5-1**: Living PSA operational interface.*

The structure of a living PSA system designed according to the principles is illustrated in Figure 5-1. At the center of the system is the living PSA plant model with the existing communication facilities, embedded in an environment created for easier access and extended communication with other information sources.

5.2.1 Present systems for applying living PSA

The number of present application of living PSA is limited, and practical experience concerning use of PSA as an operational tool has not yet accumulated to the point where a general framework for design and structure has been established. The applications do have common denominators in their efforts to quantify risk levels according to projected or existing plant status, but in actual usage the aims may be quite different. The emphasis is on the research efforts in which the applicability of the PSA technique is tested in a reduced scale. The most advanced developments aimed at using PSA as a risk monitor, i.e. as an on-line advisory system supporting the operator in safety-related decision making, comes from United Kingdom, Germany, USA and Japan, see also chapter 2.3.

Nuclear Electric in UK has implemented the ESSM (Essential Systems Status Monitor) system to monitor and predict risk level in the 12 essential post trip cooling systems. The PSA-based system is in operation since 1988 at the two advanced gas cooled reactors (AGR) at Heysham 2 and a similar system is in operation at Torness [5-11]. The system is in daily use for checking the status of the post trip cooling systems and has proved to be very useful for planning maintenance and testing, Figure 5-2 . ESSM results are checked against technical specifications to ensure that safety

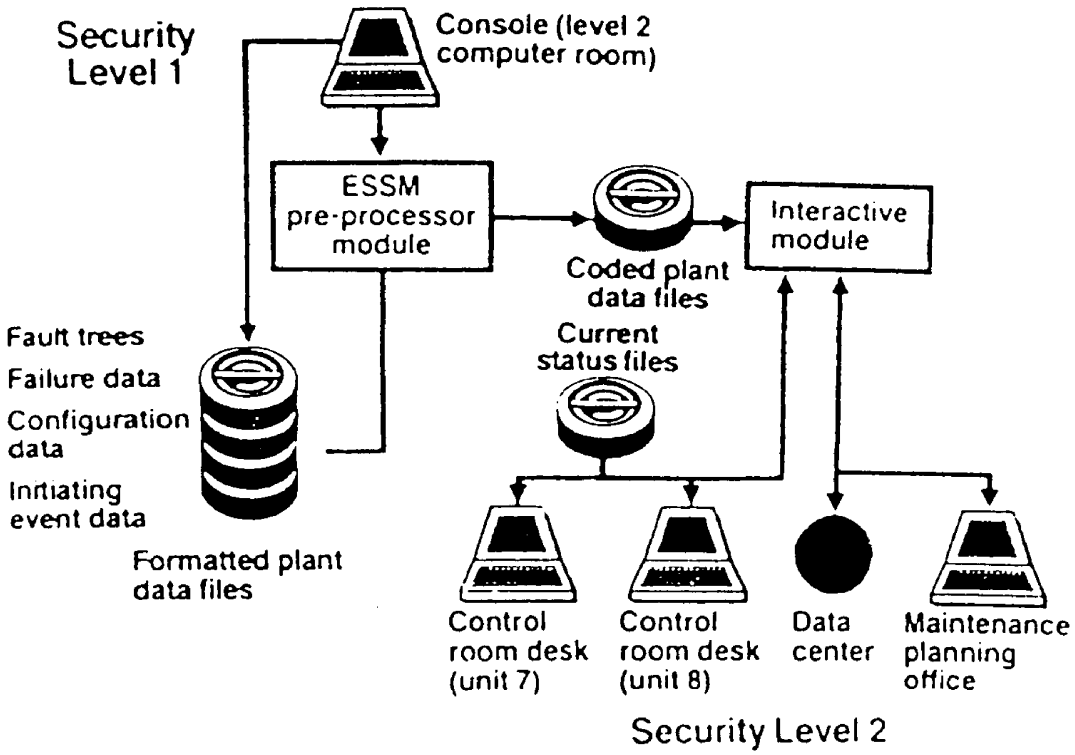


*Figure **5-2** ESSM computer system.*

limits are not violated. Within these bounds the system identifies allowed outage states and suggests combinations which give the lowest risk.

The German SAIS (Safety Analysis and Information System) applies PSA logical models as part of a more comprehensive plant information and analysis system. The development of the system is undertaken by TÜV-Norddeutschland in cooperation with the Technical University of Berlin and sponsored by the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety [5-12]. The SAIS system incorporates living PSA features and adds a wider scope of application in a plant-wide information and safety analysis system. This concept could be representative of the future information system where the PSA model is part of a comprehensive safety assessment system. The design of the user interface in SAIS takes into account that PSA offers valuable insight in plant safety which should be made available to plant staff in general.

The STARS (Software Tool for Analysis of Reliability and Safety) project aims at developing an integrated set of software tools that can be used for plant safety and reliability analysis. Partners in the joint venture are JRC (Ispra, Italy), Risø (Denmark), VTT (Finland) and TECSA SpA (Levate, Italy) and various industrial companies affiliated to the project [5-13]. Primarily STARS is intended for safety and reliability studies, but it has potential for use as an on-line decision support system for safety management, maintenance planning and optimization.

LIPSAS (Living PSA System) has been developed by Power Reactor and Nuclear Fuel Development in Japan based on the PSA for the liquid metal fast breeder reactor at Monju [5-14] . The intention is to use LIPSAS for development of operating procedures, including emergency operating procedures, and as a decision support system in operational safety management, Figure 5-3.

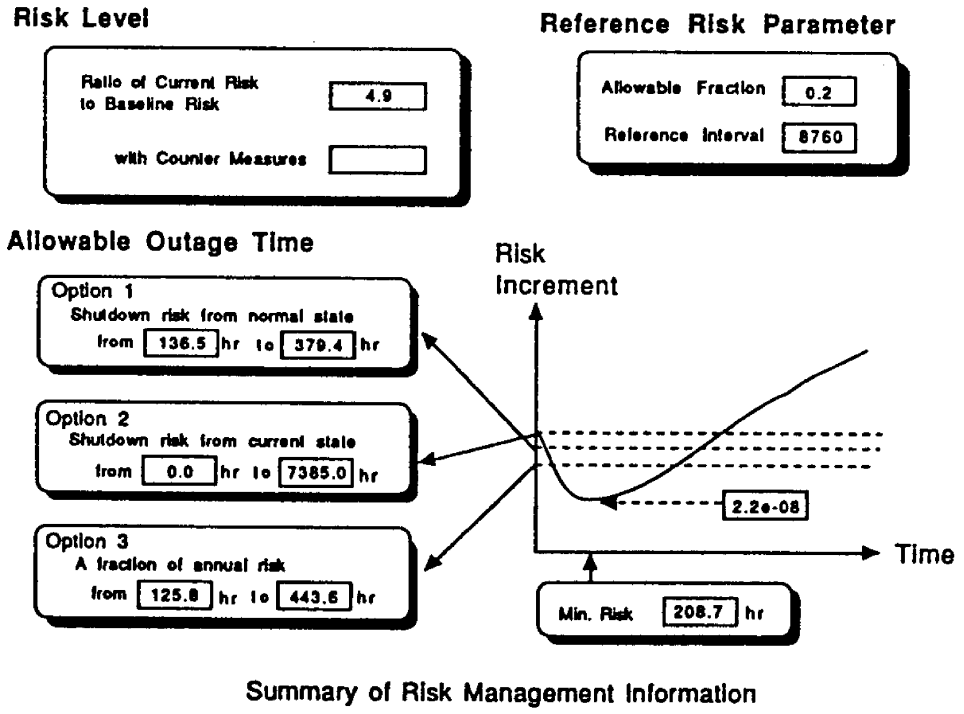


*Figure **5-3** Example of result presentation in LIPSAS user interface.*

5.2.2 Functional overview

One principal aim with the software is that it shall contain a complete set of tools for conducting and maintaining a level 1 PSA for a nuclear power plant. Special attention is sometimes paid to requirements for so called "living PSA" activities, e.g. accessible data base, quick re-calculations and easily made updates of models and data. In the following section the basic functions are summarized.

The plant model manager is the core of the tool. It takes care of the editing and analysis function of the plant model (fault trees & event trees). The capacity of the plant model manager is the most restricting parameter of the living PSA tool. The plant model manager can be described in five parts:

1) construction,
2) evaluation,
3) post processing,
4) result management,
5) plant model service function

Plant model construction: The model construction consists of tabular and graphical editors for fault trees and event trees. A hypertext plant and model documentation system is a preferable function. Qualitative analysis functions such as failure mode effect and criticality analysis (FMEA) coupled to the fault tree analysis function, functions for identification and generation of hazardous events and event sequences as well as for the identification of common cause failures should be available, too. Assessment of consequences of identified hazards and vulnerability analysis is an optional function.

Failure data analysis function and failure data assignment are needed for the evaluation and management of basic event parameters. Initiating event data analysis function is helpful in classification and evaluation of occurred initiators.

Plant model evaluation: This part of the model manager shall carry out the qualitative and quantitative minimal cut set (MCS) analysis. The cut sets are determined and the top event unavailability or frequency is calculated. A living PSA tool should support time dependent analysis. A standard part of the evaluation is the calculation of various importance measures for individuals or groups of model data or events i.e. importance analysis. The sensitivity analysis is the next step from the importance analysis in which the sensitivity of the model with respect to boundary conditions or assumptions in plant model, plant data or plant event response is verified.

The risk increase factors produced from the nominal risk assessment are limited to represent the nominal plant state and may not be reliable for low probability events due to truncation effects. Consequently, a living PSA tool must enhance risk quantifications for given train or system unavailability situations, eventually with situation specific realignment of the remaining operational path. This means that after eventual model modification in the logic and data a comprehensive minimal cut-set search, reminimization and a comprehensive reevaluation are needed.

The parametric uncertainty analysis provides means for investigation of effect of the parametric uncertainties in the top results. Various methods (Monte-Carlo, Latin Hypercube or Integrated methods) can be applied. This function requires that so called uncertainty parameters have been assessed for the basic event parameters.

Plant model post processing and evaluations: This function includes cut set editor for extending and analyzing results, e.g. recovery analysis. An attribute analysis enables to temporarily modify plant

models in order to adapt to specific analysis needs, e.g. analysis of fire and flooding, by assigning attributes to gates and basic events.

The user interface should support flexible specification of components that are out of service. Updated plant risk status can be generated based on this new information. Also the specification of plant alignment and operational strategies, e.g. extra tests, and generation of updated plant risk status information based on this new information should be included. A high level of interactivity can be realized by advanced user interfaces based on window techniques and using CAD approaches. Future technology may provide expert system facilities for the emulation of the reasoning process and heuristic of safety and reliability analysis allowing the construction of more detailed and reproducible models with less effort.

A life cycle cost (LCC) analysis function and cause consequence analysis function are optional features.

Plant model result management: This function takes care of storage and documentation of analysis results and analysis specifications. Minimal cut set, point estimate and uncertainty distribution can be stored in the data base for each analyzed top event or sequence. All analysis specifications e.g. the type of analysis and analysis set up parameters, the cut off values etc. are useful information, too. It is important that the information retrieval from the PSA data base is efficient. A user shall quickly and easily be able to locate and combine information of interest, and to present this information on the screen or on printed/plotted reports.

Plant model service function: Various service functions are needed for the management of projects and jobs. Typical service functions are word processing, spreadsheet, database and setup programs. They can be provided by other codes, but the integration of the service function to the code package increases the applicability of the tool.

5.2.3 Information and Data

All event trees, fault trees, basic events, analysis results etc. for a particular project (e.g. nuclear power plant PSA) are maintained in an integrated project data base, with flexible ways of adding information to further enhance the documentation. This is to facilitate updating, model and data management, traceability and quality control.

Basic Information stored in a living PSA data base: Basic information stored in a living PSA data base consists of the basic data used to construct and quantify the basic model, Table 5-1. A PSA project data base includes a complete integrated model with basic data for all parts of the model and also data for specific quantifications and results obtained. This basic data must be stored in order to guarantee that any results obtained can be reproduced.

Pre-processed Information and rankings stored in a living PSA data base: With pre-processed information and rankings stored in a living PSA data base, Table 5-2, we here refer to specific quantifications and results obtained that a user can quickly and easily be able to locate, combine and present.

The main results from a living PSA system include minimal cut sets, mean and instantaneous core damage frequencies, importance measures (see chapter 6.3.2), sensitivity analyses and uncertainty analysis. There should be one set of results immediately available without any extra computation. The program should be able to draw attention to the results that have changed after last recalculation. It should also be possible to make a cross comparison between results from a 'base' model and from

the changed model. The documentation system should be active also when viewing the results (e.g. to find out what an FMEA form says about a certain failure). The program must be able to present summary results, detailed results and a variety in between. The outputs should contain enough information to identify the computation fully, so that there is no possibility to mix the outputs. There should be flexible way to produce outputs also from the information system.

5.2.4 Principles for a living PSA user interface

A comprehensive and flexible plant model is the key component if PSA is to become a practical decision support system in plant operation. The corresponding requirements to model and tool development have been discussed in previous sections. Assuming that a model with the defined

*Table **5-1**. Basic information stored in a living PSA data base.*

Model element	Information
Accident sequence analysis	Top event (consequence, sequence, function etc.) - description and data
Event tree analysis	Description and data, initiating events, functional events and hazard states
Fault tree analysis	Logic, gate and basic event descriptions
Basic event data	Definitions, boundaries and parameters
Parameter data	Parameter specifications, source data specifications or failure data analysis
Attribute specifications	Group definitions (for importance and sensitivity analysis)
House event specifications	Boundary condition specifications
Operational data	Test schemes, alignment etc.
Library of plant data	Safety reports, System descriptions, P&ID´s, Layouts, Component information (location, type, failure mode, manufacturer), Technical Specifications, etc..

qualities is available for a future living PSA system the next step is to clarify its utilization in plant management and operation. This is a task different from the model development as such and it has to take into account the applicability of PSA results in different areas, the background of living PSA system users and how to integrate living PSA with the existing plant information systems.

To make full use of the living PSA model potential without stepping over the limits of safe application of PSA results demands that the living PSA system must be seen in context with safety principles, operational requirements and user preferences. To achieve this the principles for living

PSA use must have their counterparts in a practical environment designed for efficient utilization of the living PSA system. This environment must facilitate access to the living PSA model, establish links to other information sources and provide a man-machine interface adaptable to different user needs.

The living PSA operational interface should create a software and hardware structure encompassing the living PSA model and must be designed for extracting maximum benefit from use of the model and the underlying analyses.

*Table **5-2**. Pre-processed Information and rankings stored in a living PSA data base.*

Processed data	Information
Nominal results. The basic risk assessment representing an average plant state.	Precalculated results and importance of dominators and contributors. Descriptions of dominant accident sequences. Top event results (consequence, sequence, function, system, etc.). Sensitivity and uncertainty analysis results.
Failure propagation data, dependencies	FMEA based on fault tree logic. Component and support system interface information.
Rankings	Importance rankings such as risk reduction and risk achievement for scenarios, functions, systems, components, failure modes, etc. Ranking of sensitivity and uncertainty issues.
Instantaneous results. Risk monitoring evaluations.	Results generated following operational records or results generated following postulated or planned scenarios.
Operational data	Operational data or plans for test and maintenance activities. Operational event data for transients, component unavailabilities, e.t.c.. Event conditional data, information that is relevant when a component (specified by the user) is out of service.
Conditional rankings	Ranking of the operational situations and the most important failure scenarios. Ranking of components according to their relative contribution the instantaneous core damage frequency. Conditional ranking in failure situations, i.e. ranking of the failed equipment according to the benefit of restoring each to service.
Retrospective results. Risk follow-up evaluation of the retrospective risk and probabilistic indicators	Results generated following operational records taking into account the complete, retrospective, knowledge of successful and unsuccessful plant functions.
Operational data	Retrospective operational event data for transients, component unavailabilities, e.t.c.. Event conditional data.
Conditional rankings	Retrospective ranking of the operational situations and the most significant events. Presentation of risk based indicators and trends.

Any existing PSA has a user communication for manipulating the model, input definitions and for selection of desired output. The variation in scope and range of applicability is considerable, but in general the user communication is constructed for people with deep or fairly deep PSA knowledge. For these users there is no urgent need for an extended operational interface as long as PSA is used to solve traditional tasks, say core damage frequency estimates or risk importance measures for well defined plant states.

For present PSA applications the time available for input preparation, calculation and evaluation of results is in most cases long compared to the envisaged response of a living PSA system. The total interaction time is a decisive factor in the discussion of design principles for a living PSA operational interface. This is the time required to access the living PSA system, prepare input, complete the calculations and present the results in a predefined form. To be really useful in operational situations one has to aim for a system which can produce reliable results within minutes rather than hours or days.

A thorough analysis of which activity areas and staff may derive benefits from utilization of a living PSA system is outside the scope of this work, but considering the information contained in a PSA and its supporting documentation there could be a variety of potential users. Apart from safety authorities, that central utility staff as well as plant personnel in safety, planning, retrofitting, maintenance and even operation may find a living PSA system useful. Thus the design of an operational interface should take into account that users have widely different backgrounds and qualifications, but this should not deny them access to PSA results. Consequently one should design the interface flexible and adaptable to different user groups. The restrictions on how PSA are to be applied must of course be decided on beforehand to exclude inappropriate use.

Based on the viewpoints presented above there emerges a framework of principles for the design of a living PSA operational interface:

- Operation of the system should not require data expertise or extensive knowledge in PSA methodology.

- Preparation of input must be made easy and fast, predefined and/or automated generation where possible.

- Selection of calculations to be performed and result presentation must be flexible and cover a wide range of applications.

- Initiating and executing model calculations shall require very few operations when input and output options are defined.

- Where appropriate living PSA results must be seen in context with other relevant information and limiting conditions. The living PSA system must communicate with plant and utility information sources/data bases.

- Wherever possible the system should be equipped with an extensive set of interactive programs for extracting and processing information contained in the living PSA model and documentation. In practice this means creating a software system which acts as a user oriented environment built around the living PSA model.

The general principles for design of a living PSA operational interface are in many aspects the same as those applied to other computerized decision aids, but there are some which are particular to a

living PSA system. One has to pay special attention to the dangers connected with a 'black box' approach where the living PSA system is conceived as an advise production machine without any qualification as to the validity of said advise. The numerous projected applications of PSA information and advise puts strong emphasis on the need for quality control and comparison with advise derived through other means and from other sources.

5.3 System input/output

Collection and screening of relevant operational experience and development of systematic methods for making observations are important aspects. The model management can be divided into two main tasks:

- Long-term updating of the base model
- Analysis with temporary changes in plant status or operational procedures.

Procedures for above tasks are needed for quality assurance and for coherent use of the PSA by different persons throughout the lifetime of the PSA-system.

5.3.1 Long term updating of PSA model

In the organization there must be one or two persons that are responsible for the basic model. Procedures for protecting the basic model are needed, as well as procedures to make sure that everyone is using the correct model. The long term management of a plant model involves a large number of decisions regarding various aspects of the model and the model capabilities. A living PSA programme will require resources to operate and maintain the model. Procedures can of course be established for these activities but since there is a large spectrum of different issues to address in a procedure we only list the main questions that should be included here:

- to decide when to update model and/or documentation (depends also on the regulatory body)
- to decide which information to include
- to decide the level of detail
- to decide which methods and persons are used when transforming the plant to PSA modelling language (FMEA, cause-consequence analysis etc.)
- to revise plant reliability data analysis
- to document assumptions/simplifications in the model
- to document deficiencies of the model and/or documentation for the model developers
- to make back-up copies
- to control access rights to the PSA system
- to keep record on the contents of the PSA model
- to give feedback for the plant personnel
- to document deficiencies of the PSA tool and to give feedback to the system developer.
- training of the PSA personnel
- training plant personnel to use PSA tool and/or results

5.3.2 Application

The living PSA activities require a close relationship to plant operation and maintenance compared to the basic PSA applications, that to a much larger extent are directed towards plant safety management, designers and authorities.

The analyses performed with a living PSA system cover a large scale from reading documentation to analysis of major modifications of the plant. There must be a covering record of the contents of the PSA system so that each user knows which information is currently included. In the following, a course of a new application is described, Figure 5-4. A new application can be just to make a log over a day or a period of operation or analysis of a postulated case for planning purposes or risk evaluation in general.

The first phase is to determine which changes (if any) are the reason for reevaluation. The reevaluation may be due to equipment outage or what-if questions. Depending on the situation there may be more or less items to be changed than there were originally defined in the previous phase. The reason for less items could be e.g. that from previous results the importance of an item is negligible. The reason for more items could be e.g. the requirements of the Tech Specs, changed success criteria in the situation, dependencies (e.g. fire), etc. To generate status information requires a lot of background information and is demanding for the information system.

The required information specify changes from the basic information in Table 5-1. The results of this step should be constantly collected and documented as information that is relevant when a component is out of service. The required changes in status information will be described as new event status values and modifications in the fault trees and event trees. The model requirements of the status information are translated to the modelling language of the PSA system. The status changes are implemented into the PSA model as temporary changes.

If the program is fast enough, it may be worthwhile to make the changes one at a time starting from the most important (if known) one and to recompute the results in between. In the case the application in question is to log the operational experience the temporary changes can be saved and the application can stop here, otherwise the relevant results are computed or reevaluated. It must be verified that mission times, truncation values etc. are valid for the changed situation. The main output of this phase is the numerical results.

The results are evaluated against the changed model. The information system is used to explain the results. The starting situation, all changes and the reason for the changes are documented together

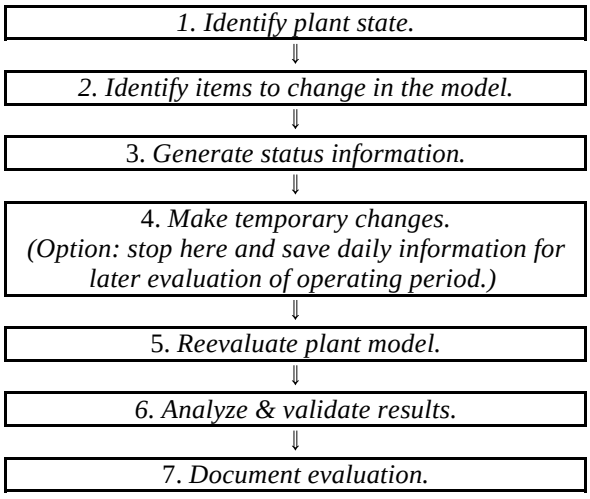


*Figure **5-4**. Steps in a new application*

with the results. It is especially important to gather information that is relevant when a component is out of service and to add this information to the model documentation.

In addition to the static input such as infrequently updated reliability parameters, the user must provide temporary inputs depending on the application. For instance, in the configuration control type of applications, the user specifies unavailable components and system configurations. In the risk monitoring and follow-up, this information is obtained from the plant operating history. On the other hand, if the user is performing short-term planning, the information is based on planned or hypothetical configurations [5-15].

5.3.3 Quantitative output and presentation

The quantitative output from the living PSA system is a set of risk measures to be used to support the decision making. The basic risk measures are the nominal risk and inherent risk frequency evaluated in the risk assessment, and the instantaneous risk evaluated in the risk monitoring and follow-up as defined in chapter 4.2.

A crucial information when using quantitative results in decision making is their sensitivity to assumptions in the model. If a number (importance) is sensitive to uncertain parameters, uncertainty distribution should be included. Such parameters could be e.g. test efficiency, CCF parameters, success criteria, human interaction probabilities.

5.3.4 Qualitative output and information retrieval

Qualitative information is needed for the documentation of the living PSA model, and for the explanation of the quantitative results. The first objective can be satisfied with the documentation procedures connected to the PSA model development, whereas the latter objective can only be fulfilled if qualitative information is an integrated part of the living PSA system. If the analyst is familiar with the structure of the PSA model documentation this information is accessible and quick to use. The drawbacks are slow updating and sometimes difficulties in finding certain specific information. A living PSA system should include a documentation system that can be accessed within the living PSA system.

Qualitative information in a living PSA system is needed for three purposes:

1. Documentation of the living PSA model
2. Explanation of quantitative results
3. Generation of qualitative information

Points 1 and 2 can be satisfied with paper documents, whereas point 3 can be achieved only when the qualitative information is integrated in the living PSA model.

Model documentation: Model documentation is needed for the analyst to understand the living PSA model, its assumptions and its limitations. It is essential when changing the living PSA model, especially when introducing failed components (Tech Specs may prohibit use or repair of other systems due to component failure). It is important that the documentation preserves all information for a new analyst to trace and reproduce the results.

- why is this data used here?
- why is this fault tree branch connected here?
- why is this function excluded from the model?

- what do the Tech Specs say of this failure?

The living PSA model editor and the documentation system should be interconnected in such a way that user can search for information related to his current work in the editor.

Explanation of quantitative results: A living PSA system should not only generate numerical results, it should also explain them. Largely the ability to explain results depends on the properties of the living PSA model editor and result generator. The questions can be raised when quantitative results are analyzed (e.g. why this is a minimal cut set?, why does this failure have this effect?, why is this importance measure as it is?). It requires certain capabilities, that is not often seen in any available software, such as:

- trace the propagation of a minimal cut set until the top event
- find conditions preventing a set of events to propagate
- find common events in event tree branch points
- find dependencies (e.g. components fed by same cable)
- display supporting information in the outputs (basic event comments, location of equipment, FMEA forms etc.)
- compare results from two different computations

Generation of qualitative information: This is partly achieved in many programs through different listings, e.g. list of trees for each component, data listings etc. However, the user should be able to see this information in the model editor and in the output generator. The relevant questions that can be treated or answered within a living PSA tool are e.g. which components are affected by a fire in this room, which cut sets could have a CCF due to component type failure mode. The plant information included in area event analysis and dependency analysis allows to produce room cut sets instead of equipment cut sets using data available in the model. The information required for this purpose is:

- gate and event comment
- component information: location, type, failure mode, manufacturer, etc.
- routines to collect and display information from the documentation system, e.g. FMEA forms by component name

5.3.5 Resources for management of the system

Resources spent on the initial issue of a plant-specific PSA are approximately 5)10 manyears and 0.5)1 manyear per year for updating the PSA thereafter. This has been estimated as a reasonable effort based on the experience with the existing PSAs [5-1] . An important part is also the scope expansions (external events, other operational states, level 2 etc.) that require additional manpower effort of approximately 1)3 manyears per expansion. The manpower resources for this effort is strongly dependent on the level of ambition and plant generation, e.g. a modern plant is much less sensitive to external events and also easy to analyze due to consistent separation in the design.

On an average 4)10 persons are directly working with PSA activities at each Nordic power company to establish and maintain the basic PSAs. The living PSA activities, to monitor and follow-up the risk, will require a staff of this size on a long term basis.

5.4 Broadening the use of a living PSA system

The SIK-1 project has defined and demonstrated the practical use of living PSA for safety evaluation based on mainly off-line application of living PSA with the purpose to identify possible improvements in operational safety. Subjects discussed are dealing with the practical implementation and use of PSA to make proper safety related decisions and evaluations. In view of the capabilities of living PSA, a discussion about broadening the use of living PSA from NKS/SIK-1 point of view may be appropriate.

5.4.1 On-line operational activities

The purpose of on-line risk monitoring is to evaluate the instantaneous risk frequency given the information about the plant configuration to provide support for operational risk decision making in the short term. This must in some cases be performed on an on-line basis to gain the maximum benefit from the applications. Today simplified PSA models are applied in operational planning and maintenance. It will still take some time before a full scale plant model can be used on-line, meaning that it can give nearly continuous assessment of plant status and risk level.

Coupling of the PSA model to the plant data acquisition computer with continuous status updating is not an unsurmountable problem, but for the PSA model to correctly handle all different status changes it has to be extremely flexible and complete.

The rationale behind development and implementation of an on-line PSA applications would be that it improves the safety at the plant. This is difficult to prove before one has gained experience and as yet there is very little to build on in that respect. The arguments for an on-line system are that the extensive analysis precipitated in a full scale PSA can provide useful advice in short-term decisions. The arguments against on-line living PSA arise one two levels: Safety and cost-benefit. If it cannot be proven or made highly plausible that an on-line system will enhance safety of the plant there is no real incentive to develop the system. A cost benefit analysis of an on-line system has to take a number of factors into account. If the technical problems associated with the generation of an updatable model are solved it should not take large resources to maintain and support the model. But a substantial initial investment could be required, and unless this can be defended either in terms of enhanced safety, improved operation or benefits related to licensing requirements one should not expect the utilities to priorities the development of an on-line system.

Before using different on-line (time dependent) risk measures, an uncertainty analysis should be done in order to compare, how large the changes in risk measures are in relation to their impact on the nominal risk frequency uncertainty. Only then meaningful changes can be identified.

Following examples of on-line applications that can be carried out are:

Status monitoring: The status monitoring provides support for operational risk decision making in short term. Safety margins and degradations describe the severity of the situation. Test information importance can be used to decide whether the test provides relevant information from the safety point of view. The evaluations are related to considerations of exemptions from Tech. Spec. and maintenance planning.

Planning of preventive maintenance: The isolation of safety important systems or components temporarily increases the risk level. The duration of the maintenance work and the combination of isolated or unavailable systems are controlled. Risk increase factor, safety margins and safety margin degradations indicate the effects of scheduled maintenance actions[5-16] [5-17]. The benefits of

performing additional tests can be considered, too. The evaluations are similar to the AOT optimization related Tech. Spec. optimization.

It is impossible to figure out and evaluate all possible combinations of allowed component outages on beforehand. Therefore there is an on-line aspect tied to this type of application. The use of the instantaneous risk frequency model and operational data from actual experiences (when no Technical Specification violations have occurred) gives an empirical view on this issue.

Incident management: The incident management is a typical on-line risk monitoring application and deals with severe situations at the plant where rapid decisions are needed. The severity is controlled by on-line monitoring. The maintenance actions can be prioritized so that the most critical systems are repaired or maintained first, or some specific maintenance isolation are postponed. Success path importance, e.g. risk decrease factors, can be used to rank the actions. A test importance type of measure can be used to decide whether some action is worth performing.

Operational risk monitoring applications, that do not require on-line application, are e.g. planning of surveillance tests and their schemes and optimization of Technical Specifications.

5.4.2 Integration with other information systems

The advantage of more rapid updating and combination of information should be exploited, and this is best achieved by connecting the living PSA system with other information sources and support systems. The plant status is automatically updated via the plant computers, present and planned maintenance from a maintenance data base, communications with computerized, technical specifications, manuals and operational procedures. This will make the living PSA system more efficient as decision support. In this context, a living PSA is comparable to a computer based operational support system. It is possible that there will in fact be PSA based operational support system in the future along the lines of ESSM in Great Britain and SAIS in Germany. At present the concept of operator support system based on a full scale PSA is not well developed although there is a number of proposals outlining the structure and functioning of such a system, [5-3].

5.4.3 Expert system techniques

The extensive analysis of plant configuration and transient response supporting a PSA model represents a very large amount of engineering knowledge. The PSA model can be looked upon as a knowledge base which is organized according to principles suited for probabilistic assessment. Since the frequency for one, or several, undesired hazard states, e.g core damage, is the final measure, the PSA model may be too strongly associated with only the core damage frequency (or the hazard states in question), and there is less emphasis on the considerable amount of information relating to plant configuration and its inherent safety structure. The hazard states, end states, in an event tree are not all serious damage states, and at early stages in the event trees there are several possible paths leading to different end states. The likelihood of reaching the least serious end states can be increased by operator actions or possible reconfigurations.

Expert systems techniques can be applied to assist the user in his analysis of the situation and the selection of appropriate actions to bring the plant to a safe state as efficiently as possible. The event tree identifies which system or function is essential as the next line of defence, and it is important to have information on the status of the system supporting the required safety function. This can be achieved by combining component status identification with assessment of the importance of components.

5.4.4 Living PSA as a training tool

As a training tool living PSA would be useful in several aspects. It would offer a practical introduction to PSA for plant staff that has little or very little experience with PSA, and enhance the general level of understanding of the capabilities of PSA. Equally important, it would introduce plant personnel to the reasoning behind probabilistic safety analysis and the methodology employed in safety assessment.

5.5 References for section 5

SIK-1 reports

[5-1] Holmberg, J., Laakso, K., Lehtinen, E., Johanson, G. and Björe, S., Preproject report: Nordic survey on safety evaluation by use of living PSA and safety indicators (NKS/SIK-1). SKI technical report 91:3, Swedish Nuclear Power Inspectorate, Stockholm, 1991. 22 p. + app. 21 p.

[5-2] Holmberg, J., Laakso, K., Lehtinen, E., Johanson G. and Björe, S. International survey of living-PSA and safety indicators. VTT Research Notes 1326, Technical Research Centre of Finland, Espoo 1992. 52 p. + app. 22 p.

[5-3] Stokke, E. Operational interface for living PSA. Report NKS/SIK-1(91)33, IFE/Halden, 1992.

[5-4] Holmberg, J., Johanson, G. and Niemelä, I., Risk measures in living Probabilistic Safety Assessment applications. VTT publication 146. Technical Research Centre of Finland. Espoo 1993.

Other references

[5-5] Niemelä, I., Properties of Finnish STUK PSA-code. In Proc. of the 2nd TÜV-Workshop on Living PSA application, Hamburg, 7)8 May 1990, ed. H.-P. Balfanz, TÜV-Norddeutschland e.V., Hamburg, 1990.

[5-6] Berg, U., Realization of true living PSA: A challenging software development task. In Proc. of the 2nd TÜV-Workshop on Living PSA application, Hamburg, 7)8 May 1990, ed. H.-P. Balfanz, TÜV-Norddeutschland e.V., Hamburg, 1990.

[5-7] Procedures for conducting probabilistic safety assessment of nuclear power plants. IAEA Safety Series report. International Atomic Energy Agency, Vienna, to be published 1992.

[5-8] Simola, K., Pulkkinen, U. and Huovinen, T., Analysis of time dependencies in probabilistic safety assessments. In Proc. of the Scandinavian reliability engineers symposium: Reliability in power, process control and transport, Västerås, 10)12 October, 1988, Society of Reliability Engineers, Scandinavian Chapter, 1988.

[5-9] Hirschberg, S., Björe, S. and Jacobsson, P., Retrospective quantitative analysis of common cause failures and human interactions in Swedish PSA studies. In Proc. of the international topical meeting on probability, reliability, and safety assessment) PSA '89, Pittsburgh, 2)7 April 1989, American Nuclear Society, Inc., La Grange Park, 1989. Pp. 258)269.

[5-10] Bento, J.-P., Björe, S., Ericsson, G., Hasler, A., Lyden, C.-D., Wallin, L., Pörn, K. and Åkerlund, O., Reliability data book for components in Swedish nuclear power plants. RKS 85-25, Swedish Nuclear Power Inspectorate, Stockholm, May 1985.

[5-11] Horne, B. The use of probabilistic safety analysis methods for planning the maintenance and testing unavailabilities of essential plant at Heysham 2 AGR power station. Proc. of the IAEA technical committee meeting on the use of PSA to evaluate NPP's technical specifications, Vienna, June 18)22, 1990. Vienna 1990, International Atomic Energy Agency. 8 p. + app. 11 p.

[5-12] Balfanz, H.-P. and Musekamp, W. Experiences from the Development and Application of the Computer Code System "Safety Analysis and Information System" SAIS. Paper presented in 3rd TÜV-Workshop on Living-PSA-Application, Hamburg, May 11)12, 1992. 10 p., app. 9 p.

[5-13] Besi, A. and Poucet, A. A Knowledge-Based System for Living PSA. Paper presented in 3rd TÜV-Workshop on Living-PSA-Application, Hamburg, May 11)12, 1992. 12 p.

[5-14] Nakai, R. Application of a living PSA system to LMFBR. Paper presented in 3rd TÜV-Workshop on Living-PSA-Application, Hamburg, May 11)12, 1992. 16 p.

[5-15] Samantha, P.K., Vesely, W.E. and Kim, I.S., Study of risk-based configuration control. Report NUREG/CR-5641, BNL-NUREG-52261, Brookhaven National Laboratory, Upton, August 1991.

[5-16] Samantha, P.K. Modeling of risk impact and benefit of maintenance. Brookhaven National Laboratory, New York. 1991.

[5-17] Kim, I.S, Martorell, S., Vesely, W.E., Samantha, P.K. Risk effectiveness evaluations of surveillance testing. Draft report for U.S. Nuclear Regulatory Commission. Brookhaven National Laboratory, Upton. 1990.

6 SAFETY EVALUATION BY LIVING PSA

6.1 Introduction

The safety evaluation by living PSA can be divided into three application categories:

1) long term safety planning,
2) risk planning of operational activities and
3) risk analysis of operational experience [6-1].

In addition, regulatory activities can be distinguished, although they can be categorized into the application areas mentioned above.

Figure 6-1 illustrates the interaction of the applications towards the final objective of living PSA improved operational safety and availability [6-2]. The basic PSA is firstly performed by which long term actions can be planned. A development of a dynamic, living PSA is needed for operational planning and analysis of operational experience. These two application areas use the same operational data, but the in operational planning the usage is to support short term actions while in analysis of operational experience the purpose is to get feedback to risk contributor identification.

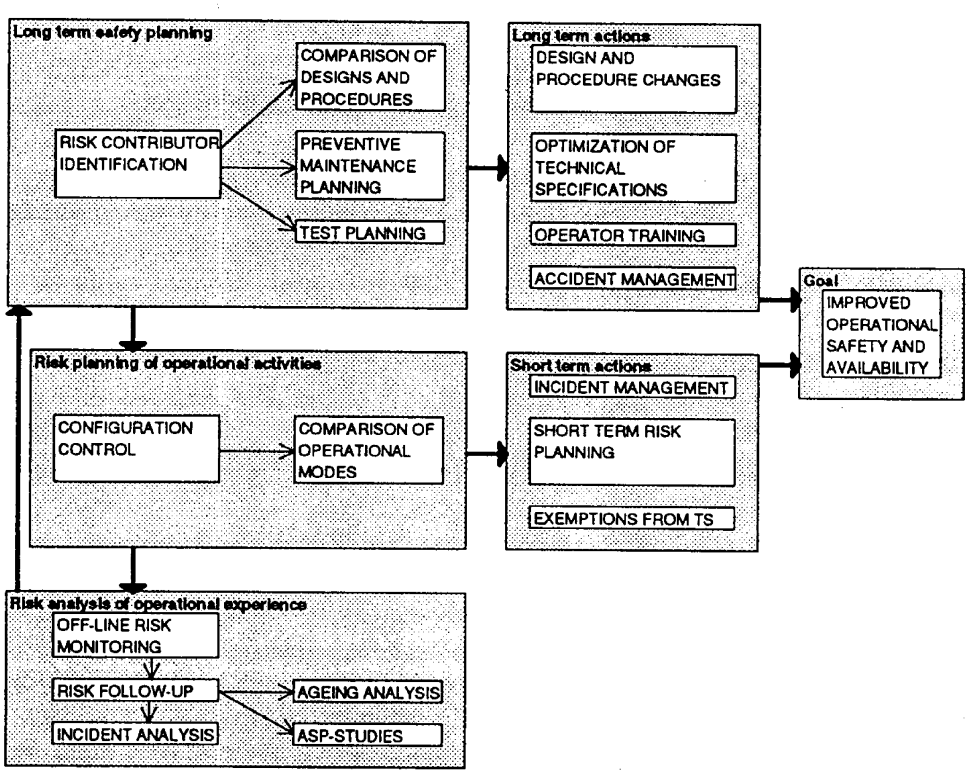


Figure 6-1. Interaction of living PSA applications.

This chapter presents the case studies performed in the NKS/SIK-1 project. Based on the case studies, evaluation procedures for various application areas, such as optimization of limiting conditions of operation [6-3], are outlined. The living PSA model made for Oskarshamn 2 BWR unit will be used as an example model to demonstrate the evaluation of risk measures in various

applications [6-4]. The role of decision making and decision analysis is discussed, and the benchmark study on risk decision making is described [6-5], [6-6], [6-7].

6.2 Nordic case studies

In the Nordic NKS/SIK-1 project, parts of the living PSA concept have been experimented in various applications by participating utilities, authorities, researchers and consultants. The risk follow-up of the operational experience has been performed for real examples in Swedish and Finnish nuclear power plants. By this approach, events significant for safety, to be examined more in detail, can be identified. Direct feedback to verify and revise the PSA is also obtained. More safe and economical operational strategies have been studied, too, for test and preventive maintenance arrangements as well as in the case of failures in safety systems. Occurred incidents have been analysed more specifically by PSA. The relationship between PSA results and safety indicators has been presented as well as the use of decision models has been experimented. Table 6-1 shows which application areas the case studies cover.

As a first task in the case studies, the plant-specific PSA models were modified and enhanced to living application purposes. The treatment of common cause failure aspects was found problematic. The completeness and realism of the model and data are very important, much more so than in basic PSA. This is due to the fact that living PSA model should cover, and be quantitatively accurate in many different situations (e.g. when failures have occurred), and not only on average. Also, conservatism in the model may lead to wrong and possibly non-conservative decisions.

6.2.1 Living PSA demonstrations for Oskarshamn 2 (RELCON/OKG)

Under contract with the Swedish Nuclear Power Inspectorate (SKI) and OKG (the utility), a plant-specific living PSA model for the Oskarshamn 2 BWR (boiling water reactor) has been developed using the existing level 1 PSA as a basis [6-4]. This living PSA model has been used in conducting several application studies. The model has been used in several different applications:

1) risk follow-up with the operating year 1987 as an example (see chapter 6.5.2),
2) evaluation of allowed outage times (AOT) and comparison with existing limiting conditions of operation (see chapter 6.4.2),
3) evaluation of test intervals and comparison with existing Technical Specifications (see chapter 6.4.3) [6-8], and
4) demonstration of the relationship between PSA results and safety indicators [6-9]

.The extent of the living PSA model is roughly the same as for the normal PSA model. The system level modelling is somewhat more comprehensive than in a regular PSA model. The main reason for this is to remove unnecessary conservatism due to model simplifications, and thereby creating a more realistic model also for cases where components are already out of service. Each system is modelled by a single system fault tree. These "generic" system fault trees include "house events", which can be used to modify the fault tree logic for different situations. These house events are, e.g., used to activate variations of the system fault tree to be used for different initiating events. They are also used to "switch in" and "switch out" components or trains in a system to model different system conditions, pipe alignments etc. In the plant which has been studied there are a number of systems which are included in the PSA model and for which there are different possible conditions. E.g.,there are systems with two redundant trains and normally one train is in operation and one is in stand-by. The component models in the example PSA model takes into account the effect of various types of events and actions such as tests, actual demands, failures and maintenance. The advantage with the time-dependent modelling is that the effect of tests can be evaluated in any given situation.

Table 6-1. Case studies in SIK-1 project.

	CASE STUDIES							
Application area	OKG living PSA	Forsmark 1 risk follow-up	TVO risk follow-up	shut-down risk	pressure relief transient	external pipe break	diesel generator CCF	decis-ion analysis
Safety goal evaluation								
Risk contributor identification	x	x	x					
Comparisons of design and procedure changes				x		x	x	
Optimization of limiting conditions for operation	x			x				
Operator training								
Accident management								
Planning of preventive maintenance			(x)					
Planning of corrective maintenance	x			x				x
Test planning	x		(x)		x		x	
Incident management								
Exemptions from the Technical Specifications								x
Off-line risk monitoring	x	x	x					
Risk follow-up	x	x	x					
Incident analysis		x			x	x		
Accident precursor studies								
Ageing analysis								

6.2.2 Risk follow-up of Forsmark 1 unit (VATTENFALL)

Vattenfall analysed events at Forsmark 1 unit during the operation period from the 1989 revision to 1990 revision outage [6-10]. The objective of the study was to identify, demonstrate and report, the potential problems and limitations in the use of mainly existing PSA-models for risk follow-up of occurred down times of equipment in safety systems and plant disturbances. This task included:

- collection of fault, maintenance and event data,

- risk evaluation, using improved PSA,
- compilation and presentation of results.

The classification and evaluation of event descriptions, obtained from various sources, took most of the time. In the evaluation of the instantaneous risk frequency, both "risk follow-up with total memory" and "risk follow-up with failure memory only" approaches were used. The risk follow-up curve is shown in Figure 6-2.

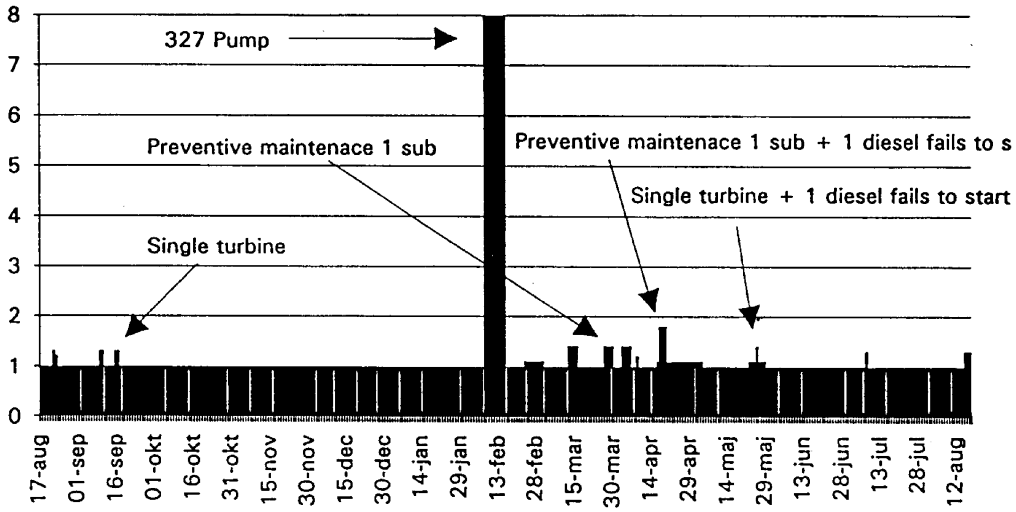


Figure 6-2. The risk-follow-up of one operating year at Forsmark 1 unit.

As in the Oskarshamn study, the treatment of common cause failure (CCF) events was found problematic when one train is unavailable. A distinction was made between the unavailibilities due to maintenance and due to repair. In the used Multiple Greek Letter CCF-model the ratios between failure probabilities of various multiplicity is expressed by parameters (Greek letters) (see chapter 4.2.4) Therefore the probability of a CCF event depends on the single event probability. For a failed component, the single event probability is set to 1. Consequently, the probabilities of CCF events will increase. If the component is maintained then the CCF probabilities will not be changed.

While doing the "total memory" follow-up another problem occurred. Since there where no existing data on test effectiveness, how should the failure probability between two successful tests be estimated? To evaluate the differences between "total memory" and "failure memory only", a generic value of failure probability in between successful test was set to 10% of the single failure probability. The difference of the results from the two types of follow-up studies, "total memory" and "failure memory only", was very small. One explanation of this could be that the Forsmark 1 PSA is dominated by CCF events. For a plant of less redundancy the result could be different.

Methodological conclusions from this study were:

- With some improvements in the existing PSA-model, a risk follow-up could be used to evaluate the risk level during a period of time.
- How to deal with the failure probability of a component between two successful test is still an unsolved problem, until the test effectiveness is known.
- How to deal with CCF, both when components in the group fail and when they succeed in tests is also an unsolved problem.

6.2.3 Pilot study on risk follow-up by PSA (VTT/Avaplan/TVO)

Technical Research Centre of Finland, Teollisuuden Voima Oy (TVO) and Avaplan Oy have performed a pilot study on risk assessment of operating history by probabilistic safety assessment (PSA) [6-11]. The main objective of the pilot study was to develop and test a method for the risk follow-up by PSA models and data. A secondary objective was to demonstrate the usefulness of risk-based operating history assessments. Third objective was to get feedback from operating experiences. The PSA-based approach is a method to assess quantitatively the severity of occurred incidents or other events. Thus the aim was to look for applicable indicators, so called probabilistic safety indicators, which could compactly describe and indicate possible trends and levels in the safety performance of the plant. This objective was left on discussion level.

The analysis was limited to cover the events related to:

- safety relief valves,
- shutdown service water and
- shutdown secondary cooling.

The plant operational data were gathered from the January and February in 1991. The operational state of both units (TVO I and II) was power operation. The information sources were: failure reports, daily reports, monthly reports, and test lists. The number of events amounted to 28 but only 19 of them affected the PSA calculations. The relevant events could be grouped into preventive maintenance packages (diesel-packages), periodic tests of the shutdown cooling systems, safety relief valve tests and chemical cleaning of a heat exchanger in the shutdown secondary cooling system.

The risk curves were evaluated in two ways:

1. as off-line risk monitoring, and
2. as risk follow-up with total memory (see chapter 4 for the definitions).

The realistic modelling of CCF-failures is the actual problem in the time-dependent risk assessment. This exercise shows that time-dependent extensions of CCF quantifications needed for the risk follow-up considerations are not trivial. Problems are not so much connected to CCF modelling features but instead to sparse data reflecting the rare nature of identified CCF events, which makes it difficult to verify time-dependent behaviour of CCF mechanisms. As an example, it could be asked what type and degree of CCF-modes are possible when one train is unavailable due to the maintenance. The CCF-problem was not only related to quadruple redundant systems, but also to the treatment of high-redundant systems such as the safety relief valves. In the TVO PSA, the safety relief valve function quantifications were done by using common load model for representing mean unavailabilities. Actual time-dependence was taken into account to some extent when determining CCF parameters corresponding to mean unavailability interpretation, but mostly pessimistic estimates were used. In this pilot study, the common load model was extended to describe the time-dependent failure mechanism by applying the linear $q_0+\lambda_s t$-model to common load model probability parameters with assessed proportions between time-independent and time-dependent parts [6-12].

We looked over three types of indicators. The first indicator is the variation of core damage frequency, particularly its maximum values and the number of times it exceeded some criteria level. At TVO II, the maximum core damage frequency was 7.6 E-5 1/a by risk monitoring and 5.9 E-

5 1/a by risk follow-up. At TVO I any variation at the core damage frequency can hardly be recognized. The second indicator is based on the integration of the core damage frequencies over the periods with significantly increased risk level. This indicator can be used to rank the events. The probability of core melt during the three diesel-packages was (according to risk monitoring) about 3 E-6 which is 10 % of nominal core melt probability per year. Relatively, the diesel-packages are considerable risk contributors. The third indicator is the average core damage frequency during the two months. Off-line risk monitoring gives the frequencies 3.3 E-5 1/a for TVO I and 4.2 E-5 1/a for TVO II. Risk follow-up with total memory, on the other hand, gives the frequencies 2.7 E-5 1/a for TVO I and 3.4 E-5 for TVO II. These numbers are very close to the nominal core damage frequency (3.3 E-5 1/a).

The results show that the increase of the risk frequency level is small during test intervals. According to the exercise model, the preventive maintenance package raises the risk level two and a half times higher from the normal level. It particularly increases the contribution of small LOCA accident sequences. It should be noted that the use of reduced PSA model (2000 most important minimal cut sets) as a base model might lead to incorrect conclusions of the effect of the maintenance outage. Some minimal cut sets, which could be important for this situation, are omitted due to the initial cut off from the calculation model. Anyhow, an important lesson is to pay attention to minimal cut set lists, too, because the risk profile might change strongly due to unavailability of safety important components. The nominal, risk monitoring and risk follow-up with total memory frequency curves are in Figure 6-3.

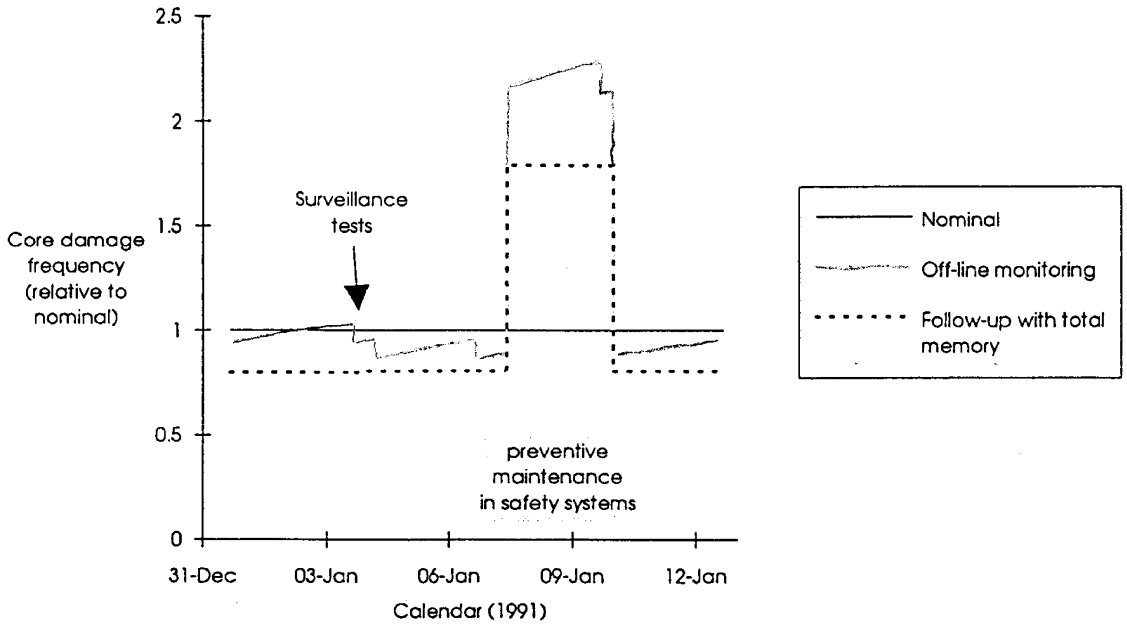


Figure 6-3. The risk follow-up at TVO II.

The exercise considerations have reflections also to the test arrangement issue. Presently, there the safety relief valves are tested once during the power operation period. Without the test, the nominal risk frequency would increase about 4 % according to the data and assumptions used in this study. However, there are many qualitative features related to development of possible CCF mechanisms, which are not properly covered in this kind of simple model consideration, but which should be carefully addressed before eventually deciding upon a relaxation of the safety relief valve-test frequency.

The difference of the off-line risk monitoring and risk follow-up with total memory approach is in the treatment of standby components. The off-line risk monitoring calculation is easier to implement and easier to interpret. The risk follow-up with total memory needs further analysis on the test effectiveness but it provides more information in utilization of operating experience and verification of PSA models and data.

The present PSAs are already feasible for the evaluation of the experienced risks due to observed unavailabilities in safety systems. A more accurate modelling which would take into account the possible hidden unavailabilities is difficult to perform. The foreign experiences indicate, however, that the risk follow-up will be one of the most important application areas of living PSA. The safety management gains benefit by improving knowledge of the severity of the events, and the PSA people by verifying or improving the quality of the PSA models and data.

6.2.4 Plant shutdown risk in failure situations of a safety system (Avaplan/TVO)

The earlier TVO/Avaplan risk analysis performed in the NKA/RAS-450 project, for development of AOT rules in technical specifications, is reported and documented in a comprehensive way including [6-13]:

- Evaluation at plant level as a complement to the earlier study at safety function level, and, extended reporting and documentation of modelling and quantification aspects.

The technical report was prepared and discussed within spring 1991 within SIK-1, and it contributed as an IAEA pilot study on risk based development of technical specifications.

6.2.5 Pressure relief transient (Avaplan/TVO)

The detection of a Common Cause Failure (CCF) in the electromagnetic pilot valves in the safety relief system at the TVO plant in 1985, provides an interesting case study object, as the detection of the latent CCF mechanism was connected to an actual demand transient [6-14]. In the case study, the emphasis is in CCF modeling and quantification of high redundancy systems, conditional with respect to the knowledge about the status of the components, specially in situations where a part of the redundant components are affected.

The developed approach utilizes a new concept of *CCF scenario* in order to describe the origin, development, detection and removal of a CCF mechanism. It extends in a significant manner the earlier shock-type CCF assumptions towards modelling the CCF mechanism as a timedependent failure-renewal process. The *impact vector* is used to describe the degree in which the redundant components are affected by the CCF mechanism, being defined as:

$$\text{Altogether } j \text{ components are failed at time } t\}, \text{ with } \sum_{j=0}^{n} \nu_j(t) = \quad (6\text{-}1)$$

$\nu_j(t) = 0$, for $j>0$, if all components are intact,

$\nu_k(t) = 0$, for $k \neq j$, if precisely j components are failed and oth

The conventional impact vector approach is extended to include the time variable in order to describe the CCF mechanism as a time-dependent process. This new approach allows far more realistic consideration of important CCF defenses such as component-to-component variability and detection as well as removal paths.

The study aided to develop a method to place CCF incidents into a proper perspective. In fact, in the considered practical case, the system level impact of the CCF mechanism was strong, but not substantial at the plant level, which confirms the safety classification of the case into IAEA's Incident Class 2. The developed methodology allows evaluation of remaining safety margin, as well as influence of periodic test arrangement (most important preventive measure and defense against developing CCFs) and role of countermeasures in a problem situation.

6.2.6 Analysis of an external pipe break (VTT/TVO)

A methodology to analyse incidents by the help of PSA was developed. The methodology is a combination of qualitative root cause analysis and a quantitative analysis of an event sequence. As an example, the external pipe break occurred at TVO I unit during the initial operating phase was analysed. The incident appeared to have little significance for safety. The reasons for that are that the leakage size was rather small, it can be isolated in many ways, and the operators can balance the situation by other means [6-15].

In the light of the experience gained, a rough quantitative analysis of incident contributors and the interpretation of its results seems to be an appropriate way to link incident investigation with PSA. An incident analysis requires that the information concerning the case has been recorded through documentation or interviews within a reasonable time after the incident.

The investigation showed that it should be possible to model incidents in the probabilistic sense. A quantitative evaluation can give a fruitful view on the safety significance of the incident. However, the results of such an analysis always have to be interpreted with care.

6.2.7 A time-dependent model for a pairwise symmetric system of four diesel generators (Avaplan/TVO)

The primary incentive and background to the development of a timedependent CCF model for standby components was the risk-based study for allowed outage times at the TVO I/II plant [6-16]. This study was concerned with failure situations of four redundant trains in the residual heat removal (RHR) systems. In order to consistently predict and compare the risks of operational alternatives in a failure situation, it was essential to realistically take into account the information available for the operator about the safety system components, specially:

1) status at the point of an operational decision, such as failed, operating or standby state,
2) prior history, such as time points of the last tests of the components, which are in standby state.

Item 2 is specially crucial for a situation where in a group of identical redundant, one part of the components is detected failed, while the other part is in standby state and the presence of a CCF (affecting also the components in standby) can not be excluded by the information about the earlier test outcomes. This practical problem was elaborated further as an example case throughout the study.

The RHR trains at the TVO I/II do not represent a fully symmetric group of four (which contrasts with the usual assumption of homogeneity in CCF modeling), but instead they should be considered as a pairwise symmetric group, where each pair of trains share a common sea water channel and also common piping in the secondary cooling circuit. This is also reflected to the group of four diesel-generators (DG), because they are cooled by the RHR trains. Besides, the DGs have a pairwise staggered test scheme. In order to properly take this asymmetry into account, a pairwise symmetric

extension of CCF model is used, and the specialized parametrization, developed on the analogy of conditional CCF probability, proved convenient for this purpose.

For the inclusion of time-dependence, the linear model for shared cause events was used (see chapter 4.2.4). The properties of the model are exemplified considering the situation specific unavailability of four diesel generators, given that two are detected failed in a periodic test, and evaluating the impact performing or not performing an additional test of the other two diesel generators.

6.3 Long term safety planning

6.3.1 Safety goal evaluation

Plant risk assessment is basic application in which the primary result is the nominal risk frequency f_n describing the overall risk level of the plant. The designers, authorities and the plant safety management use the result to control whether the plant design and the safety status are at an acceptable level or whether some safety improving measures should be taken.

To obtain the risk of the operation of the plant, f_n is multiplied by the expected plant lifetime. The total risk is the probability of core damage during the remaining plant life time, t_l,

$$P_{tot} \approx t_l \cdot f_n, \qquad (6\text{-}2)$$

The result can be used both for generic and plant specific purposes. In a generic purpose, by which we mean plant to plant comparisons or comparisons of nuclear industry risks to other risks in the society, the result is used as an absolute number. This is not so popular because risk assessments of different objects are seldom comparable with each other.

The evaluation of the inherent risk frequency f_0 is part of the plant risk assessment. The result describes the risk level without the effect of test intervals and preventive maintenance actions. To decrease the inherent risk frequency, the plant design should be changed.

Table 6-2 shows the basic risk measures of the example plant. The results should be then compared with defined safety goals.

Table 6-2. Safety goal evaluation by the example PSA.

Risk measure		
Nominal risk frequency	f_n	4.1 E-6 1/a
Inherent risk frequency	f_0	1.8 E-6 1/a
Plant lifetime	t_l	40 a
Total risk	P_{tot}	1.6 E-4

6.3.2 Risk contributor identification

For the safety management, the primary purpose is to identify the main risk contributors so that safety improving measures can be identified and prioritized. In the same manner, the authorities can use PSA to focus the inspection resources on most important areas for safety. The results are used in a relative manner. The importance of a basic event or a group of basic events for the final result, e.g. the instantaneous or nominal risk frequency, can be presented by risk importance measures. The basic setting in the importance measure evaluation is that the considered basic event has a nominal probability p ($0 < p < 1$) which contributes to the (nominal) risk frequency. If the basic event probability is set to 0 or 1 another risk frequency level is obtained. The importance measures describe the changes in a relative manner [6-17], [6-18], [6-19].

Risk increase factor A_x is the factor by which the risk frequency increases when a basic event or basic event group is failed or unavailable

$$A_x = \frac{f(X=1)}{f}, \tag{6-3}$$

where $f(X=1)$ and f refer to the evaluations of risk frequency with the variated assumption the component is failed ($X=1$) and it is in a nominal state, respectively.

Risk decrease factor D_x describes the factor by which the risk frequency decreases if a basic event or basic event group would not fail

$$D_x = \frac{f}{f(X=0)}. \tag{6-4}$$

Fractional contribution C_x is defined to be the relative contribution of the basic event or basic event group to the risk frequency

$$C_x = \frac{f - f(X=0)}{f} = 1 - \frac{1}{D_x}. \tag{6-5}$$

Risk increase and decrease factors are always greater than one for relevant basic events. Fractional contribution is between 0 and 1. The significance of the basic event increases along with increasing importance measures.

The risk importance measures described above are defined for the basic events. The fractional contribution and risk decrease factors can be used to rank also initiating events, but the increase factor cannot be applied to events of frequency dimension. Instead, the importance of the initiating events can be compared with the conditional core damage probabilities given an initiating event i, $P\{\Phi_i=1\}$. Relations are presented in Figure 6-4 [6-20].

The risk importance measures, e.g. fractional contributions, are the first hand results in the identification of risk contributors and improvement possibilities. For an operational plant, two general objectives of using importance measures are safety assurance and risk reduction [6-21]. The use of various importance measures for the risk contributor identification is shown e.g. in [6-22].

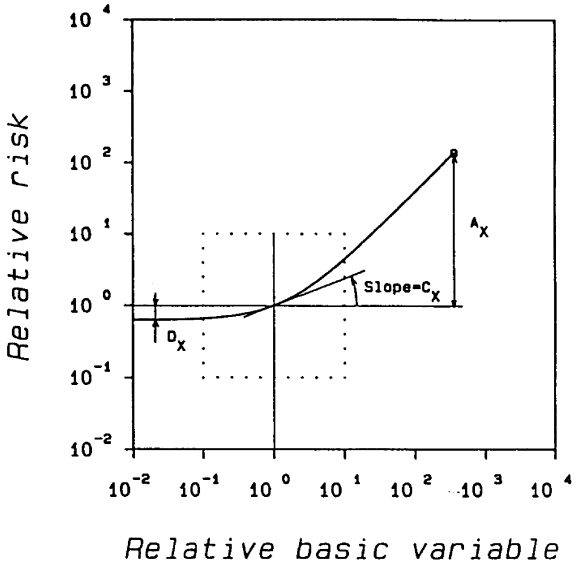


Figure 6-4. Relationship between risk importance measures and sensitivity curve [20].

6.3.3 Comparison of design and procedure changes

When the changes in designs or procedures have influence on safety status, PSA can provide support for the comparison of the alternatives. The relative change in the nominal risk frequency f_n of the alternatives usually forms the basis for the decision making. The uncertainties and economical aspects should be considered, too. The responsibility of these applications is carried by designers or the safety management, depending on the plant life cycle phase.

6.3.4 Optimization of limiting conditions for operations

The operational limits and conditions given by the Technical Specifications are analysed by evaluating the risk effects of alternative requirements. The purpose is to balance the requirements with respect to operational flexibility and plant economy. The high risk situations permitted by Technical Specifications are identified and replaced by such modes that give minimum risk, as well as too stringent requirements are substituted by more flexible ones. This section discusses the overall principles in the optimization of maintenance, repair and testing.

The optimization of test intervals aims at controlling the risk impact of the latent development and occurrence of failures in standby safety systems in the most acceptable way. The optimization of Technical Specifications should firstly follow qualitative criteria [6-3]. The general criteria for tests is that tests shall be planned so that considered failures are detected and introduction of additional failures is avoided. Test methods shall be planned by taking into account the known component standby failure mechanisms.

The optimization of allowed outage times aims at controlling the risk impact of failure situations in the most acceptable way. AOT is the maximum allowed time for a component to be inoperable in a given plant state. If the operability cannot be reached within AOT, the plant must be placed to a safer state, usually in a shutdown state. Qualitative criteria for planning of limiting conditions

of operation are formulated in Table 6-3. The criteria can be compared to quantitative used at Heysham 2 plant (Table 2.1).

Table 6-3. Qualitative criteria for limiting conditions of operation.

) complete loss of a safety function shall require an immediate remedial actions, e.g. a shutdown (within 24 h)
) single or multiple failures in a safety system and 100 % capacity remaining shall require an immediate repair within a **short** time frame (e.g. 1)3 days)
) single failure in a safety system and 100)200 % capacity remaining shall require a repair within a **medium** time frame (e.g. one week)
) single failure in a safety system and 200 % or more capacity remaining shall require a repair within a **long** time frame (e.g. one month)
) redundant components shall be tested if a failure is detected

Quantitative, probabilistic criteria are applied in checking and in special adjustment of the rules and in short term operational planning when unplanned or unexpected plant conditions of safety systems take place. The quantitative criteria can be defined in a risk frequency or probability dimension and they can be stated in an absolute or relative form. Further, we distinguish between long term contribution and individually occurring situations.

The long term contribution of the rules can be analysed by the results of risk assessment. The nominal risk frequency of plant is composed of three types of unavailabilities, the contributions of which can be measured as follows in Table 6-4. Since Technical Specifications affect the two last type of unavailabilities, an overall test procedure and preventive maintenance policy contribution can be expressed by

$$TS_c = \frac{f_n - f_0}{f_n}. \qquad (6\text{-}6)$$

This measure is sensitive to assumptions made in time-dependent component models. Thus it also characterizes applied PSA modelling practices, and it can be used to compare various PSAs. For the example plant, the overall test procedure and preventive maintenance policy contribution is TS_c=0.56.

Table 6-4. Main overall risk contributions.

Unavailability cause	**Risk frequency**	**Fractional contribution**
Time-independent hidden failures	f_0	f_0/f_n
Time-dependent hidden failures, detectable in surveillance tests and demands	f_b-f_0 [1]	$(f_b$-$f_0)/f_n$
Evident downtime due to preventive and corrective maintenance	f_n-f_b	$(f_n$-$f_b)/f_n$

[1] f_b = nominal baseline risk frequency

The risk impact of an individual AOT can be controlled by setting limits for

1) the increase in the instantaneous risk frequency,
2) the additional cumulative risk over the allowed outage time or expected repair time,
3) the increase in the nominal risk frequency.

The increase in the instantaneous risk frequency depends on how critical the component is for safety functions. The cumulative risk over down time depends further on the repair time (the uncertainty in the repair time is discussed in section 6.4.2). The increase in the nominal risk frequency depends on the occurrence rate of the events considered. The various approaches to control the risk, and to justify the shut down are summarized in Table 6-5.

Table 6-5. Quantitative criteria for AOT.

Risk impact	**Risk measure**	**Alternative decision rules to shut down or to evaluate AOT**
Instantaneous risk frequency	$f(x)$	$f(x) > f_{acc}$ $f(x)-f_0 > \Delta f_{acc}$ $f(x) > A_{acc} f_0$
Cumulative risk over the down time	$f(x)\tau_x$ [1]	$\tau_x > P_{acc}/f(x)$ $\tau_x > \Delta P_{acc}/(f(x)-f_0)$ $\tau_x > P_{sd}/f(x)$ [2]
Long term risk	$f(x)\tau_x\lambda_x$ [3]	$\tau_x > C_{acc}/(f(x)\lambda_x)$

[1] τ_x is the down time
[2] $P_{sd}(x)$ is the shutdown risk in the configuration x
[3] λ_x is the occurrence frequency

The risk-based evaluation of AOT needs criteria for allowed risk impacts. Firstly, the level of acceptable instantaneous risk frequency or risk increase factor should be defined. If this criterion is met then the cumulative risk over the down time should be compared with a probability criterion or to the risk of a shutdown. Thirdly, the fractional contribution to the long term risk should considered. More about the risk-based approach can be found in a report being prepared by the International Atomic Energy Agency [6-23], and in [6-24], [6-25]. The subject is further discussed in section 6.4.

6.3.5 Operator training

The results of the identification of the risk contributors can be utilized in planning which accident sequences should be emphasized in the operator training. Vice versa, the operator training can be used to verify the realism of human interaction models in the considered accident sequences. Also the conditional core damage probabilities point out in which initiators the plant response including operator actions is important [6-22].

6.3.6 Accident management

Accident management planning is more related to the level 2 and 3 applications which are omitted in this context. Generally, the identified risk contributors, dominant accident sequences, recovery and success paths, as well as end states can support the planning of the accident management program. The conditional core damage probabilities given the initiating event provide information about the importance of the mitigating actions.

6.4 Risk planning of operational activities

Risk planning of operational activities is an intermediate form of risk assessment and monitoring. It is a daily or weekly activity performed by the operational management and maintenance office. Operational and maintenance strategies for the near future are planned. Risk importance measures are used for safety assurance. Test importance can be used to decide whether a test provides relevant information from the safety point of view. The evaluations are related to considerations of exemptions from the Technical Specifications and maintenance planning. Short term planning as well as a few other application areas are close to the concept "risk based configuration control" introduced in [6-26].

6.4.1 Planning of preventive maintenance

The maintenance office evaluates the risk effects of the preventive maintenance program. The isolation of systems or components important for safety increase the risk level temporarily. The duration of the maintenance work and the combination of isolated or unavailable systems are controlled. The two quantities to be controlled are the lifetime contribution of a maintenance program and temporary contribution of single outage situation as explained in section 6.3.4.

The preventive maintenance effectiveness can be, in principle, assessed by comparing the benefits of the maintenance with the risk impacts [12, 24]. The risk contribution caused by maintenance is the increase in the nominal risk frequency (for power state) due to unavailable components. The risk contribution decrease due to better functioning equipment is more difficult to estimate, and it requires detailed analyses on maintenance effectiveness. The maintenance effectiveness is related to ageing of the components. A simple model of presenting the degradation, failure and maintenance states as a Markov model has been studied in [6-25]. The maintenance effectiveness from the component point of view is defined as the probability of detecting degradation before a failure.

6.4.2 Planning of corrective maintenance

In contrast to down times caused by preventive maintenance, the down time caused by corrective maintenance takes place randomly. Based on operating experience, the frequency of the events can be predicted and, subsequently, the lifetime contribution can be controlled by adjusting the allowed down time for maintenance.

The lifetime contribution is controlled similarly as with preventive maintenance. Here, we consider the problem of controlling the contribution of a single down time. Let $g(t)$ be the repair time density with mean τ_x. Then the repair is allowed, if

$$\int_0^{\infty} [\int_0^{s} (f(t) - f_b)\, dt]\, g(s)\, ds \;\le\; A_{acc}. \tag{6-7}$$

Assuming a constant instantaneous risk frequency over the down time, we obtain the condition for the allowed repair

$$(f(x) - f_b) \int_0^{\infty} s \cdot g(s)\, ds \;=\; (f(x) - f_b) \cdot \tau_x \;\le\; A_{acc}. \tag{6-8}$$

If this is not acceptable, then the shutdown risk should be compared with the risk of staying in the power operation state. If the relative criterion A_{acc} is substituted by the shutdown accident probability $P_{sd}\{x\}$, a condition for the allowed repair is obtained. $P_{sd}\{x\}$ should include also risks of being in a shutdown state as well as the risks at power-up. If the following inequality holds,

$$\int_0^{\infty} [\int_0^{s} f(x(t))\, dt]\, g(s)\, ds \;\le\; P_{sd}\{x\}, \tag{6-9}$$

or for a fixed repair time τ_x

$$\int_0^{\tau_x} f(x(t))\, dt \;\le\; P_{sd}\{x\}, \tag{6-10}$$

or for a constant risk frequency increase

$$f(x) \cdot \tau_x \;\le\; P_{sd}\{x\}, \tag{6-11}$$

then the component can be repaired without a shutdown. By solving τ_x in the equations, allowed outage times can be defined, respectively.

Allowed outage times can be considered also in a following way. First, a certain risk frequency level is considered normally acceptable f_{acc}. It can be determined relative to nominal or inherent risk frequency. The risk increase over this limit is compared with the shutdown risk. Then the allowed outage time is evaluated as follows

$$\tau_x \;\le\; \frac{P_{sd}\{x\}}{f(x) - f_{acc}}. \tag{6-12}$$

In the example PSA application, an instantaneous risk frequency of order $f_{acc}=4*f_0$ was considered acceptable. Table 6-6 presents a comparison between calculated AOT and the AOT according to the present LCOs for four different components. The AOTs according to present limiting conditions for the operation are shorter than the calculated AOTs, except for the gas turbine.

Table 6-6. Comparison of risk-based and current allowed outage times.

Component failure	AOT (days), PSA	AOT (days) TS
Core cooling pump	6	2
Gas turbine	8.3	30
Diesel generator	4	2
Battery-backed bus-	14	1

There may often be other operational alternatives to faster reduce the instantaneous risk than the component repair. These alternatives should, of course, be accounted in the optimization of the operational strategy. A comprehensive study on this type of decision making situation has been made for the residual heat removal system failures [6-27].

The AOT optimization task is different if the impact to the long term average risk is aimed to be minimized by taking into account that the operating rules demand to shut down plant if the component has not been restored in time. The objective function with respect to the AOT can be formulated as follows

$$\begin{aligned} \min_{\tau_x} \Delta_b P\{x,\tau_x\} &= \int_0^{\infty} \Delta_b P\{\text{core damage} | TR=t, \tau_x\} g(t)\, dt \\ &= \int_0^{\tau_x} [\int_0^t f(x(s)) - f_b)\, ds]\, g(t)\, dt + \int_{\tau_x}^{\infty} g(t)\, dt \cdot P_{sd}\{x\}. \end{aligned} \tag{6-13}$$

The probability $\Delta P\{x,\tau\}$ is the additional contribution to the baseline probability due to chosen τ_x. Modifications of this problem as well as the criteria setting have been discussed in [6-28].

Sometimes, a decision has to be made whether to allow the component be unavailable until the next planned shutdown, provided that a cold shutdown state is required for the repair work. Let τ_{sd} be time to the shutdown, and c be an overall (not system condition dependent) probabilistic criterion for the allowed increased contribution to the core damage probability before planned shutdown. A time limit can be evaluated then by the equation

$$\tau = \frac{c \cdot f_n \cdot \tau_{sd}}{f_n(X=1) - f_n} = \frac{c}{A_x - 1} \cdot \tau_{sd}, \tag{6-14}$$

where A_x is the risk increase factor, and τ_{sd} is the maximum allowed operation time in a given condition of safety systems. If $\tau_{sd} > \tau$, i.e., if $c < A_x - 1$, then the plant must be shut down earlier than planned.

6.4.3 Test planning

The operational management analyses risks and benefits of test strategies. Tests should be planned so that considered failures are detected but an introduction of additional failure modes are avoided. The effect of test interval and possible staggering of redundant tests can be evaluated from the reliability point of view by time-dependent component failure models [6-29].

The effectiveness of a surveillance test depends on the risk contribution which is caused by the test R_C and the risk contribution detected by the test R_D. The risk contribution caused by the test is, for instance, the probability to cause a plant transient in connection to a test. It can be estimated from the operating experience. The risk contribution of the test is the risk increase due to time-dependent failure mechanism [6-30].

One application conducted with the example PSA was to evaluate the test intervals that are specified in the plant's Technical Specifications and the reconfiguration intervals according to the plant operating procedures [6-8]. The analysis of test intervals consisted of two prestudies in which

a) relative test intervals were examined, and
b) timing of tests was analysed.

The main purpose of the evaluations was to find test series which decrease the number of tests and reconfigurations without affecting the average risk. The selected test series were analysed in the third phase.

In the analysis of relative test intervals, an upper bound of risk level in normal power operation (with no existing failures and no ongoing maintenance) is decided. This risk level is selected in such a way that the average risk becomes approximately equal to the average risk when tests are performed according to the present Technical Specifications. In the studied plant the core damage frequency varies between $1.2*f_0$ and $4*f_0$ if tests and reconfigurations are performed according to Technical Specifications. If the upper bound of core damage frequency is set to $2.7*f_0$, and the procedure described above is followed, the resulting average risk becomes the same as in the case when tests and reconfigurations are made according to Technical Specifications. The procedure that was used in this application involves the following steps:

1. Starting in the beginning of an operating year (after refuelling), the core damage frequency is calculated each day until it reaches the predetermined upper bound (it increases due to the time-dependent part of the unavailability for stand-by components.
2. At this time-point, find the test or reconfiguration that has the highest risk reduction worth, and perform this test.

Steps 1 and 2 are repeated through the entire operating year. When following this procedure, the total number of tests and reconfigurations made during an operating year is 67. This can be compared with the 117 tests and reconfigurations that need to be made according to Technical Specifications. The number of tests has thus decreased by 43 %, but the average risk is maintained at the same level. It is also possible to change the procedure in different ways, such as:

- Acceptance of an increasing average risk over the operating year, to get more even distribution of tests over time.
- Fixed (not varying) test and reconfiguration intervals (in long term planning).
- One or more test- and reconfiguration intervals are fixed at a certain length regardless of evaluation results (long term planning).

In the analysis of timing of tests, the aim was to identify tests which degrade the effectiveness of each others from the risk point of view. The degree of degradation effect depends on how much the tests appear in same minimal cut sets. In order to avoid the degradation effect, such tests should be placed as far away as possible from each others. The analysis covered possible combinations of seven tests included in the PSA model. The degree of test independence was calculated in a following way:

1. For each combination of test (A and B), four conditions were evaluated:

   K1: The risk level before tests,
   K2: The risk level after test A,
   K3: The risk level after test B,
   K4: The risk level after tests A and B.

2. When tests A and B are performed as first tests, the risk reductions are K1-K2 and K1-K3, respectively. When they are performed as second tests, the risk reductions are K3-K4 and K2-K4, respectively.

3. The relative effects of performing a test as a second test with respect to as a first test is

   for test A: (K3-K4)/(K1-K2),
   for test B: (K2-K4)/(K1-K3).

   If the number is less than 1, the two tests appear in same minimal cut sets, and they should not be performed simultaneously, from the risk point of view.

A matrix shown in Table 6-7 was used to planning of effective test series.

Table 6-7. Relative remaining effect of performing a test as a second tests [6-8].

	Second test						
First test	323	327	649G13	649G23	661DG211	661DG212	314
low pressure injection system (323)	)	58	100	100	100	100	39
high pressure injection system (327)	46	)	97	96	99	98	65
gas turbine (649G13)	99	97	)	45	51	51	100
gas turbine (649G23)	99	95	45	)	51	51	100
diesel generator (661DG211)	100	98	53	53	)	23	100
diesel generator (661DG212)	100	98	53	53	23	)	100
pressure relief system (314)	57	86	100	100	100	100	)

Table 6-8 presents the number of tests of selected test series compared with the number of tests according to Technical Specifications for a number of different components and systems. Alternatives 1)3 are chosen based on the analysis of test intervals. The relative test intervals are as close as possible to the optimal test series. The number of tests of alternatives 4 and 5 are same as in Technical Specifications but timing of tests is optimal in test series 4 and the worst possible in test series 5.

Table 6-8. Analysis of selected test series [6-8].

System	Tech. Spec.	Analysed test series 1	2	3	4	5
Depressurization system	1	12	16	24	10	10
Core cooling system	10	6	8	12	10	10
Auxiliary feedwater system	10	6	8	12	24	24
Gas turbine 1	24	6	8	12	24	24
Gas turbine 2	24	12	16	24	24	24
Diesel generator 1	24	12	16	24	24	24
Diesel generator 2	24	2	3	5	1	1
Total number of tests	117	56	75	113	117	117
f_{ave}/f_0	2.13	2.77	2.24	1.78	2.10	2.82

6.4.4 Incident management

Compared to above applications of short term risk planning, incident management deals with severe situations at the plant where quick decisions are needed. The severity is controlled by configuration control measures. The maintenance actions can be prioritized so that the most critical systems are repaired or maintained first, or some specific maintenance isolation are postponed.

A measure of the most critical errors with respect to an aggravation of the current situation is obtained directly from the risk increase factor. If the likelihood of the event is considered, the fractional contribution is a more descriptive measure. Success path importance should give a priority of available success paths out of the current situation. It is obtained by risk decrease factor from the instantaneous risk frequency.

If the risk level of the plant increases temporarily, there might arise a need to check the statuses of the standby components by additional tests. A test of the component x can either increase the risk to level $f(t;x=1)$ or decrease it to level $f(t;q_x(0))$ (x recently tested). If the test is perfect, then the probability of detected failure is $q(t\text{-}TL)$. Often, the possibility of a common cause failure must be accounted, which makes the evaluations somewhat more complicated.

The importance of an additional test can thus be considered from two aspects. If the risk level is already unacceptably high, a successful test result may justify that special safety level reducing actions are not necessary. If a potentiality to an unacceptable risk level has increased due to the preceding events, a detection of a failed component would support the decision on immediate safety reducing actions. Therefore both the risk increase and decrease factor can give guidance to select an appropriate test.

6.4.5 Exemptions from the Technical Specifications

The exemptions from the Technical Specifications have usually an influence on the plant safety. Both the instantaneous risk frequency and probability of the core damage during the proposed exemption period should be evaluated and controlled. The resulted quantity is compared with risks of other operational alternatives, as well as with the nominal or inherent level. The measures are similar to the configuration control and optimization of allowed outage times. The benchmark study on decision analysis presented in chapter 6.6.2 discusses how to formulate decision criteria for the treatment of exemptions.

6.5 Risk analysis of operational experience

6.5.1 Off-line monitoring

Off-line risk monitoring is the simplest form of risk follow-up. Configuration control is repeated with collected event data. The result is a risk frequency curve from which we can generate probabilistic safety indicators. The main indicators are

- instantaneous frequency peaks of the curve, the core damage probabilities over the peaks, and
- the average frequency during the observation period.

The results can be used to identify possible high risk situations, to rank the occurred events from safety point of view, and thus to get feedback both for the identification of risk contributors and for the verification of PSA models. One purpose is also to select events which are then examined more detailed by other risk follow-up approaches.

The conditional *risk dose* of an event is the probability of core damage during the event

$$P_{dose}\{x_i\} \approx \int_{\Delta t_i} f(x_i(t))\,dt. \tag{6-15}$$

In the evaluation of occurred initiating events, a "failure memory only" approach has to be applied, because in an actual demand the whole plant response is "tested". A total memory approach would yield a probability of 0 unless an accident have happened. To avoid trivial results, accident sequence precursor studies treat initiating events in a following way. The associated event tree is used for screening considered event sequences. For failed branches, a probability of 1 or equal to the likelihood of the recovery is used. For successful or unobserved branches, estimated (nominal) probabilities are used [6-31].

The risk dose can also be expressed as an increase relative to the inherent risk frequency

$$\Delta P_{dose} = \int_{\Delta t_i} (f(x_i(t)) - f_0)\,dt, \tag{6-16}$$

or as a *dose factor* relative to the nominal risk during one year

$$C_{dose}(x_i) = \frac{P_{dose}\{x_i\}}{f_n \cdot 1\ a}. \tag{6-17}$$

6.5.2 Risk follow-up

In addition to operational experience analysed by the off-line risk monitoring, risk follow-up considers the hidden events as accurately as possibly given the available information. Exceptional failure combinations, dependences between failures, repair actions, maintenance or operation modes can be identified. Risk importance measures can be used to select which indicators, both risk-based and conventional, are worth monitoring. Even a risk-based indicator system similar to conventional safety indicator systems could be developed. Risk-based indicators can be defined, calculated and monitored for various safety barriers [6-32]. Specifically, indicators are measures generated from an observation of the behaviour of some measure during a time period, such as average, count, trend measure etc. The average observed frequency is

$$f_{ave} = \frac{1}{\Delta t} \int_{\Delta t} f(t)\, dt, \tag{6-18}$$

where Δt is the length of the observation period. The average risk frequency is compared with the nominal frequency, because in the long run, if correctly calculated and defined, these two quantities should not deviate much from each other.

The yearly *cumulative risk dose* is

$$P_{cum} = \sum_i P_{dose}\{x_i\}, \tag{6-19}$$

where the summation is taken over the significant events. The risk dose is composed either:

- of unavailabilities in safety systems, the dose of which is denoted by $P_{dose,u}$, or
- of initiating events, the dose of which is denoted by $P_{dose,i}$.

Principally, these two doses may not be summed up to an overall risk dose because they are based on different type of conditioning of the operating history.

Indicators are needed as simple feedback numbers of a very complex system. If we have defined probabilistic criteria for significant events the number of significant events can be counted. The criterion can be absolute, or relative with respect to the inherent or the nominal risk frequency. It can be expressed both in a probability form and in a frequency form. An absolute frequency based indicator is

$$I_f = \frac{\#\{\, x_i : f(x_i) > f_{sig} \}}{\text{observation time}}, \tag{6-20}$$

where # denotes the cardinality of the set of events during which the instantaneous risk exceeds the criterion f_{sig}. A relative indicator with respect to the inherent frequency is

$$I_{A_0} = \frac{\#\{\, x_i : A_0(x_i) > A_{sig} \}}{\text{observation time}}, \tag{6-21}$$

which is the number of events increasing the risk level more than for instance 10 times higher than the inherent frequency. If the significance of the event is measured in the probability dimension, the indicator is obtained from the expression

$$I_P = \frac{\#\{ x_i : \int f(x_i(t))dt > P_{sig} \}}{\text{observation time}}, \qquad (6\text{-}22)$$

where the integration is taken over the time of the event, such as safety system unavailability. P_{sig} can be related to e.g. nominal probability of core damage during one year.

The main types of follow-up results, from which trends can be observed, are:

1) A set of time points, e.g. the time history of when safety significant events have occurred.
2) A set of time points and related probabilities, e.g. the time history of risk peaks.
3) A set of time periods of unavailabilities of systems or components.
4) A set of time periods of a component or a system being in certain status, e.g. stand-by, operation, repaired, maintained (a more detailed classification than in 3)
5) Probability curves in time, e.g. instantaneous risk frequency history or component unavailability history.

The types 2 and 5 are clearly probabilistic, but also the other ones can be such if probabilistic models are applied to the classification of the events. The type 5 result can be considered the basic result from which other types of histories can be conducted using e.g. a criterion for safety significant events to select the risk peaks.

In the simplest form, the trends are identified from the indicator plots. Statistical tests are used to verify trend behaviours. The indicators are connected to decision making by defining warning limits that alarm if the followed quantity has deteriorated too much. A study on safety system function trends, which covers these aspects of an indicator analysis, has been carried out in USA [6-33]. In this study, many of the indicators were based on sliding averages which is a common technique in the indicator analyses.

The data sources used in the example application were:

1. Licensee Event Reports (LERs)
2. Disturbance Records
3. Test Records
4. Plant Operating Procedures

Two types of analyses were made in the risk follow-up study, depending on the type of situation that was analyzed. One type of analysis was to calculate the core damage frequency in power operation, and the other type is to calculate the core damage probability given occurrence of a component failure or an initiating event. The core damage frequency is calculated by using a top event Spectrum which analyses all core damage sequences in all event trees. The core damage probability given that an initiating event already has occurred is calculated by analyzing all core damage sequences in the event tree for this initiating event. The probability for this initiating event is first set to 1. The top event definition is the same as described above, but in this case it is specified that only one particular event tree is to be included in the analysis. The experience feedback from the evaluation of this period could be that the gas turbines should be always tested after completed maintenance. The redundant gas turbine should be tested directly when a gas turbine has been found to be failed, as well. If these rules had been followed, the risk increase would have been only 30% of the increase that actually occurred. The results are summarized in Table 6-9.

Table 6-9. The risk follow-up in year 1987 with the example PSA.

Indicator	
max $f(t)$, A_n, A_0	2.1 E-5 1/a, 5.1, 11.6
f_{ave}	4.9 E-6 1/a
max P_{dose} [1]	3.2 E-6
P_{cum}, $P_{d,u}$, $P_{d,i}$	4.9 E-6, 1.5 E-6, 3.4 E-6
I_P [2]	4.0 1/a
I_t [3]	0.085

[1] transient with loss of feedwater system
[2] P_{sig} = 1 E-7
[3] f_{sig} = 1 E-5 1/a

6.5.3 Incident analysis

In the incident analysis, events significant for safety are analysed as deeply as necessary in order to evaluate their severity and to identify root causes of the events. The function of living PSA is the severity evaluation, in this context. On the other hand, recommended safety improvements can be evaluated by PSA, as done in the analysis of disturbances in Swedish boiling water units [6-34].

6.5.4 Accident sequence precursor studies

The accident sequence precursor (ASP) studies provide two types of results:

1) generic precursor frequencies, and
2) safety margins during individual precursors.

The generic precursor frequency can be used to verify the PSA models. It can be seen also as a competitive approach to PSA to be used for risk assessment of an operating plant. In the society aspect, ASP-studies can be used to assess the risk of considered industry [6-31], [6-35]. The ASP-studies applies the conditional and cumulative risk doses (see sections 6.5.1 and 6.5.2) as risk measures.

6.5.5 Ageing analysis

Ageing analysis aims at identifying ageing effects in the system or component structures or functions. From the reliability point of view, indications on forthcoming incidents and changes in failure frequencies are monitored so that the planned plant lifetime can be reached, and if possible extended. Safety indicators which have been developed, e.g., in the second part of the NKS/SIK-1 project [6-36] are generally methods to observe and analyse trends. By risk follow-up, probabilistic safety indicators can be generated to rank ageing components according to their criticality for the plant safety and availability. It enables the planning of the maintenance and surveillance programs to account the ageing effects. The measure can be e.g. an ageing parameter in a component failure rate model [6-37] which can be affected by changing the maintenance program [6-38]. Besides ageing factors, the component failure rates are affected by risk decreasing factors such as the replacement schemes and learning improved maintenance.

6.6 Other level 1 PSA activities

The applications mentioned above are more or less living type of applications which are based on a well performed basic PSA. The first hand basic PSA covers analyses of internal initiating events and possibly some of the most important external events. Basic PSA can be applied already to living PSA purposes but PSA can and should be extended to other safety issues, too. Examples of auxiliary PSA activities are analyses of external initiators as well as low-power analysis to complete the basic PSA, and design phase analyses for licensing and designing supporting purposes.

6.7 Decision analysis

The decision analysis is a co-operation between the decision maker, the decision analyst and the experts. The decision maker is a single person or a group of persons who have to solve a decision problem. The role of decision analyst is to familiarize the decision maker and the expert with the decision analytic method applied and to make sure that all necessary information is available. The experts are used to give information about the specific problems. The main phases of the decision analytic process are

1) the structuring of the problem,
2) the construction of the preference model and
3) sensitivity studies.

During the structuring of the problem, the problem is characterized, and decision alternatives as well as objectives are identified. The background material is collected and some additional analyses may have to be performed. Uncertain factors are identified as well as dependences between the elements of the problem. The structuring is the most valuable part of the analysis.

As a result of the structuring, the elements of the preference model are obtained. The preference model is used to prioritize the decision alternatives. The structuring of the model as well as the quantification methods depend on the approach. The decision maker must understand the used method and the relationship between the answers and results. A computer code helps the structuring and manipulation of the preference model.

Sensitivity studies include the treatment of the problem with the model. The purpose is to study the sensitivity of the results when inputs are variated. It can be useful to find the turnover points where preference order given by the basic inputs is changed. Thus, the critical assessments can be identified.

6.7.1 Types of decision criteria

Decision making criteria are rules or objectives followed in a decision making process. Core damage probability is only one aspect to be considered in safety related problems. Potential consequences must be included, too. To estimate the consequences of a core damage accident, level 2 and 3 analyses are needed. On the other hand, more immediate economical consequences are often the primary interest of the utility; the chosen decision alternative must be cost-effective.

In this section, we restrict the discussion in the use of probabilistic criteria as decision aids. As such, they lead to a slightly artificial use of the results so that no definite rules can be given to establish and use probabilistic criteria. The general use is namely to compare the risk frequency with a probabilistic safety criterion for accepting a certain plant modification or condition. However,

probabilistic safety criteria implicitly include the monetary aspect, because risk is accepted due to the economical benefits obtained in a form of power production [6-6]. The acceptability can be based on:

- criteria which focus on minimizing the risk (frequency) increase,
- criteria which define acceptable risk (frequency), or
- criteria which define a negligible risk (frequency) [6-39].

In the sense of acceptability, the risk frequency can be treated in various ways, such as

- an absolute value,
- a relative change with respect to the reference level,
- an absolute difference from the reference level, or
- in a trade-off manner [6-40].

Ultimately, the absolute value is the correct quantity to be considered. It is also the only quantity when the results are compared with other risk studies. However, PSA is incomplete and involves uncertainties. Therefore, it might be misleading to compare results of one PSA with PSAs of other plants, or to results of other risk analyses. The use of relative measures and criteria may be sufficient for plant-specific applications.

Below, we discuss how the types of probabilistic criteria appear in various approaches. In general, a distinction can be made between risk assessment and risk monitoring as well as risk follow-up approach, i.e. between the nominal risk frequency and the instantaneous frequency evaluations. The criteria can be extended to lower level so that even a hierarchy of configuration control criteria is obtained [6-26].

In the nuclear regulation level, the nominal risk frequency is compared with a national or international criterion (the utility may have criteria of its own). The criterion is considered more a target because results of PSA are sensitive to the approach used in the risk assessment. Especially, the level of completeness of PSA affects the result a lot. Internationally, a risk frequency criterion of 10^{-5} a^{-1} has often been suggested for the core damage accident and 10^{-6} a^{-1} for the large off-site release, e.g. in a report prepared by the International Atomic Energy Agency [6-41].

The requirement of a balanced risk profile of the plant is an example of a relative criterion. The criteria can be extended to a lower level to hold for systems, components, basic events etc. so that we could have a hierarchy of probabilistic safety criteria from the offsite release level down to the component failure level [6-42]. It should be noted that the risk balanced design requirement suffers from the differences in the modelling practices unless PSA-technique is standardized. A violation of the risk balance could be presumed to lead to more accurate modelling of the high risk contributors in the first place, and then to plant modifications.

The main methods to control instantaneous risk frequency are

- peak risk frequency control,
- allowed outage time control, and
- average risk frequency control.

The peak value control is not very sensible unless it is coupled with the duration of the event. However, there exist proposals for highest acceptable frequencies the exceeding of which is not tolerated at any circumstances. For instance, at Heysham 2 nuclear power plant the monitored

frequency is compared with the nominal baseline value so that a frequency increase of factor 100 would cause immediate remedial action e.g. a plant shutdown. There are also similar but smaller criteria to limit the allowed operation at a high risk level at Heysham 2 [6-43].

Another type of the peak value control is used in risk follow-up, in particular in the accident sequence precursor studies. The number of exceeding of a certain high risk level is tracked. A violation of this criterion leads to safety improvements at the plant. The allowed outage time control is based on controlling time allowed for certain risk frequency level. The average risk frequency control is related to risk follow-up. Average frequency can be compared with the nominal, inherent or baseline risk frequency. At Heysham 2, the overall safety guideline includes a principle that the annual risk frequency should be kept lower than twice the nominal baseline risk frequency [6-43].

6.7.2 Benchmark study

A piloting benchmark study was made on a decision making case of an exemption from Technical Specifications. In the benchmark study, Technical Research Centre of Finland (VTT) [6-5] and Studsvik [6-6] simulated the decision making of the safety authorities by applying decision models as an aid.

The benchmark case is following. At a Swedish boiling water reactor, in the main feedwater system, one of the inner isolation valves of the containment gave an indication of failure to close in a periodical valve closing test. According to the Technical Specifications, either the plant must be shut down or the power must be reduced to 65 %, while one pipe line is kept closed by the outer isolation valve. The experience of indication failures in other valve indications of the same type made the power company to suspect that the failure was in the indication, and not in the operation of the check valve. To avoid the requirement stated by Technical Specifications, the power company applied an exemption from the rules to continue the power operation during the remaining seven weeks to the next annual refuelling outage.

The task of the case study was to simulate the decision making situation both from the power company and from the safety authority side. The decision analysis was made simultaneously and independently by VTT and Studsvik. Both teams were allowed to choose the decision analysis approach freely. The teams selected rather different methods. The approach used by VTT is an example of how the decision analysis could be carried out when there is time to discuss the objectives, attributes, value assessments, etc. A decision model was constructed for the prioritization of the decision alternatives. The model construction involved three phases so that the detailness of the model was gradually increased. First, the decision alternatives were identified, and an objectives hierarchy was formed (see Figure 6-5). Then the analytic hierarchy process (AHP) was applied. Finally, a multi-attribute value function was defined to rank the alternatives

The Studsvik approach is characterized by that efforts were concentrated on the safety functions, rather than the overall core damage event. Further, the decision situation was analysed both from the authority and the power company point of view. The power company's decision situation has been analysed taking into account the economic risks. In both cases, a single-attribute utility function was applied.

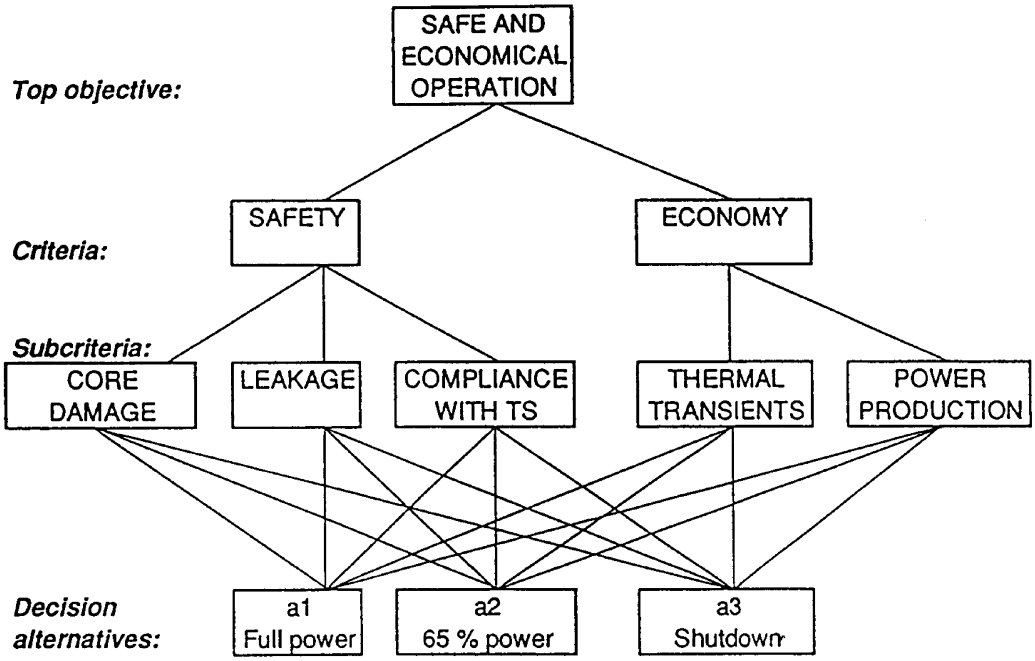


Figure 6-5. The objectives hierarchy.

The preference order according to the VTT decision model was:

1. to continue the operation at full power (decision 100 %),
2. to shut down the reactor, and inspect the check valve (0 %),
3. to continue the operation at the reduced power level 65 % and to have the outer isolation valve closed (65 %).

The three decision models gave slightly different arguments for the preference orders. The attribute of leakage probability had a strong influence on the order. Without the leakage considerations, there would be little doubt on the superiority of the decision alternative 1.

The authority model of Studsvik suggests that, with reasonable probability criterion for the operability of the check valve (R_0), the authority should reject the application for continued operation of the check valve, i.e., the whole plant or the feedwater train should be closed. The analysis of power company's decision situation suggests the same preference as VTT above. However, it should be noted that the seemingly small difference between the expected utilities of d_1 and d_2 may be considered insignificant.

The both teams pointed out that the significant probability of no closing indication when the valve succeeds to close. Therefore, efforts should be directed to the study of such failures to improve the indication reliability.

6.7.3 Decision analysis procedure

A decision analysis procedure has been outlined [6-7]. The practical performance of the phases of the analysis depends on the analysts and decision makers involved. In a team work, a discipline is needed for carrying out various phases of the problem solving. The order of the phases must be

agreed upon, regular meetings must be arranged, and a standard for the evaluation method must be created. When the use of the decision models becomes a routine, many of the steps can be borrowed from earlier decision analyses. The basic conditions required by the decision model, however, should be kept in mind and verified. The procedure is in Figure 6-6.

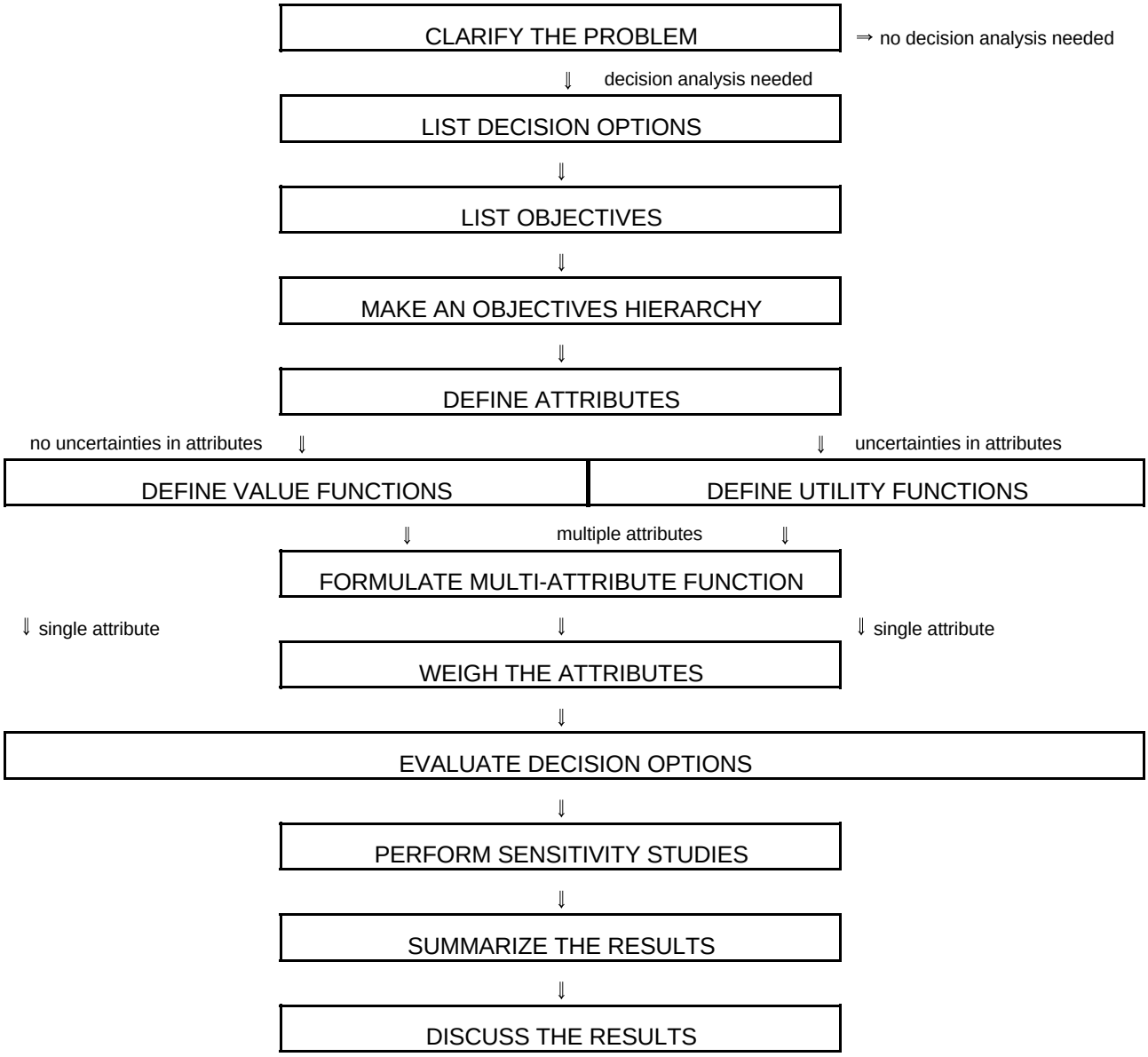


Figure 6-6. A scheme for a decision analysis.

There should be a computerized decision support system in the management of the analysis process. Such a system can be used to document the findings made in the course of the analysis as well as it would provide tools to work with decision models.

6.7.4 Practical needs for decision analysis

The large range of safety related decision situations at a nuclear power plant can be classified according to several aspects. From the decision analysis approaches point of view, we divide them into long-term decision situations and short-term decision situations.

Long-term decisions are typically related to changes in the plant design, in operating procedures, in maintenance instructions and in the Technical Specifications. A decision analysis could provide a method to manage this type of problem solving process. Various activities required for the problem solution can be organized according to the decision analysis scheme.

The short-term problems belong to situations where time for decision making extends from one hour to a few days. Such situations are the incident as well as accident management, and planning of daily operational and maintenance tasks. In short-term problems, the major part of the decision analysis has to be prepared in advance. A rule based approach could be a framework for making judgements on the decision alternatives. Concerning safety, it would mean probabilistic safety criterion, e.g., maximum allowed core damage frequency or increase in the core damage frequency.

6.7.5 Conclusions

The benefit of a decision analysis is that facts and decision alternatives of the case will be identified and they will be listed for an open discussion. There are several levels of decision models to be chosen. Decision supporting calculations can be developed to a sophisticated model by assessing a hierarchy of objectives, introducing value functions and, finally, using utility functions. The more advanced model is chosen, the clearer the objectives, criteria, attributes, etc. need to be defined. The models usually require that criteria are put in a quantitative form, and therefore some qualitative aspects might be forgotten. A use of a sophisticated model demands also time.

In the benchmark study, some insights have been gained into the area of decision analysis. Subjective knowledge, available information (in forms of raw or treated data, for example) and risk aversion (personal attitude) are the cornerstones in a decision analysis process. A good decision requires sound knowledge and experience of the object, carefully collected and rigorously analysed data and risk-taking attitude of the individuals involved. In connection with a PSA study, it is realized that a decision under uncertainty should not be based solely on probabilities, particularly when the event in question is a rare one and its probability of occurrence is estimated by means of different kinds of approximations. PSA, at least level 1 PSA, can only support partly the decision making process. The probabilities generated by a PSA should be used together with results of the other analyses or direct engineering judgement to support a decision.

A systematic decision analysis is particularly useful if the choice of the decision is not clear. A decision model allows e.g. to perform sensitivity studies which may guide to the preference order. The definition of the decision making criteria could be reconsidered, if the alternatives are very equal. The establishment of the decision making criteria is, in fact, the main part of the decision analysis. The rest is just technical analysis or numerical exercise.

6.8 References for section 6

SIK-1 reports

[6-1] Johanson, G. and Holmberg, J. The use of living PSA in safety management, a procedure developed in the Nordic project "Safety Evaluation, NKS/SIK-1". In proc. of Probabilistic Safety Assessment International Topical Meeting, PSA '93, Clearwater Beach, Florida, January 27)29, 1993.

[6-2] Holmberg, J., Johanson, G. and Niemelä, I. Risk measures in living probabilistic safety assessment. VTT Publications 146, Technical Research Centre of Finland, Espoo, 1993.

[6-3] Johanson, G., Berglund, L., Holmberg, J. and Karlsson, C. Regulatory decision making: Test of qualitative and quantitative decision criteria for improvements in Technical Specifications. In Proc. of IAEA Technical Committee Meeting on "Procedures for use of PSA for optimizing nuclear power plant operational limits and conditions", Barcelona, September 20)23, 1993, (IAEA-J4-TC-855), report NKS/SIK-1(93)30, RISKI(93)17, 12 p.

[6-4] Sandstedt, J., Demonstration studies on living-PSA. Report NKS/SIK-1(92)27, Relcon AB, Sundbyberg, 1992.

[6-5] Holmberg, J. and Pulkkinen, U. Decision Analysis on an Exemption from the Technical Specifications. Report VTT/SÄH 4/92, RISKI(92)1, NKS/SIK-1(92)8, Technical Research Centre of Finland, Espoo, 1992. 19 p. + app. 16 p.

[6-6] Pörn, K. and Shen K. Decision Making under Uncertainty) A Pilot Study on Exemption from Technical Specifications. Report STUDSVIK/NS-91/90, NKS/SIK-1(91)29, Studsvik AB, Studsvik, 1992. 46 p.

[6-7] Holmberg, J., Pulkkinen, U., Pörn, K. and Shen, K. Risk Decision Making in Operational Safety Management) Experience from the Nordic Benchmark Study. Report STUDSVIK/ES-93/37, NKS/SIK-1(92)17, RISKI(93)1, Studsvik EcoSafe, Nyköping, 19 p. + app. 6 p.

[6-8] Sandstedt, J. Förstudie. Analys av föreskrivna testintervall Oskarshamn 2. Report RELCON-12/93, NKS/SIK-1(93)26, Relcon AB, Sundbyberg, 1993. (in Swedish)

[6-9] Sandstedt, J. Importance and sensitivity analysis of O2 indicators. Sundbyberg 1993, Relcon AB, Report RELCON 13/92, NKS/SIK-1(92)49.

[6-10] Erhardsson, U.-K., Flodin, Y., Momentaneous risk. R&D-project for living PSA. Report PK-79/91, NKS/SIK-1(91)30. Swedish State Power Board, Stockholm, 1991. (in Swedish)

[6-11] Holmberg, J., Pulkkinen, U., Laakso, K., Mankamo, T., The risk follow-up by PSA) report of the Finnish pilot study. Report VTT/SÄH 14/91, RISKI(91)2, NKS/SIK-1(91)27, Technical Research Centre of Finland, Espoo, 1992.

[6-12] Mankamo, T., TVO I/II SRV CCF quantifications. Timedependent models/Risk monitor exercise. Report NKS/SIK-1(91)48, Work notes, Avaplan Oy, Espoo, 1991. 8 p. + app. 15 p.

[6-13] Mankamo, T. and Kosonen, M. Continued plant operation versus shutdown in failure situations of standby safety systems application of risk analysis methods for the evaluation

and balancing of allowed outage times for the residual heat removal systems at TVO I/II plant. Espoo, 1992, Avaplan Oy. Report NKS/SIK-1(91)4, RISKI(91)16. 100 p.

[6-14] Mankamo, T. A pressure relief transient with pilot valve function affected by a latent CCF mechanism. Work report NKS/SIK-1(92)35, Avaplan Oy, Espoo, 1993, 31 p. (draft)

[6-15] Holmberg, J. and Pyy, P. Analysis of an external pipe break. Report NKS/SIK-1(93)17, RISKI(93)12, Technical Research Centre of Finland, Espoo, 1993 (draft).

[6-16] Mankamo, T. A timedependent model of dependent failures) Application to a pairwise symmetric structure of four components. Report NKS/SIK-1(92)13, Avaplan Oy, Espoo, 1992 (draft).

Other references

[6-17] Vesely, W.E., Davis, T.C., Denning, R.S. & Saltos, N. Measures of risk importance and their applications. Columbus 1983, Battelle Columbus Laboratories, Report NUREG/CR-3385. 84 p.

[6-18] Schmidt, E.R. et al. Importance measures for use in PRAs and risk management. Proceedings: International topical meeting on probabilistic safety methods and applications. Palo Alto 1985, Electric Power Research Institute, Report EPRI NP-3912-SR, Vol. 2: Sessions 9)16, Paper No. 83.

[6-19] Andsten, R. & Vaurio, J. Reliability importance measures and their calculation. Helsinki 1989, Imatran Voima Oy, Research Reports IVO-A-01/89. 42 p.

[6-20] Mankamo, T., Pörn, K. & Holmberg, J. Uses of risk importance measures. Technical Report. Espoo 1991, Technical Research Centre of Finland, Research Notes 1245, 36 p. + app. 8 p.

[6-21] Vesely, W.E. & Davis, T.D. Evaluations and Utilizations of Risk Importances. Washington D.C. 1985, U.S. Nuclear Regulatory Commission, Report NUREG/CR-4377.

[6-22] Andsten, R. and Vaurio, J.K. Sensitivity, uncertainty, and importance analysis of a risk assessment. Nuclear Technology 98(1992) 160)170.

[6-23] Risk-based application of nuclear power plant technical specification improvements. Working material of a IAEA consultants meeting, Vienna, August 31)September 4, 1992. Vienna 1992, International Atomic Energy Agency, Report IAEA-J4-CS53/92. (draft)

[6-24] Laakso, K. (ed.) Optimization of technical specifications by use of probabilistic methods) A Nordic perspective. Final report of the NKA project RAS-450. 1990, Nordic liaison committee for atomic energy, NORD 1990:33. 156 p.

[6-25] Samantha, P.K., Vesely, W.E., Hsu, F. & Subundhi, M. Degradation Modeling with Application to Aging and Maintenance Effectiveness Evaluations. Upton 1991, Brookhaven National Laboratories, Report NUREG/CR-5612, BNL-NUREG-52252.

[6-26] Samantha, P.K., Vesely, W.E. & Kim, I.S. Study of Operational Risk Based Configuration Control. Upton 1991, Brookhaven National Laboratory, Report NUREG/CR-5641, BNL-NUREG-52261. 78 p. + app. 59 p.

[6-27] Mankamo, T. Operational Decision Alternatives in Failure Situations of Standby Safety Systems Development of Probabilistic Approach and PC Program TeReLCO. Reliability Engineering & System Safety 36(1992) 29)34.

[6-28] Kani, Y., Hioki, K., Sakuma, T., Nakai, R. & Aizawa, K. Application of Probabilistic Techniques to Technical Specifications of an LMFBR Plant. In Proc. of the Int. Topical Meeting on Probability, Reliability, and Safety Assessment, PSA '89, Pittsburgh, April 2)7, 1989. La Grange Park 1989, American Nuclear Society. Pp. 810)819.

[6-29] Engqvist, A. & Mankamo, T. Test Scheme Rearrangement for Diesel Generators at Forsmark 1/2. In Proceedings of the International topical meeting on probability, reliability, and safety assessment PSA '89, Pittsburgh, April 2)7, 1989. La Grange Park, 1989, American Nuclear Society. Pp. 337)343.

[6-30] Kim, I.S., Martorell, S., Vesely, W.E. & Samantha, P.K. Quantitative Evaluation of Surveillance Test Intervals Including Test Caused Risks. Upton 1992, Brookhaven National Laboratory, Report NUREG/CR-5775, BNL-NUREG-52296.

[6-31] J.W. Minarick, The US NRC accident sequence precursor program: Present methods and findings. *Reliability Engineering & System Safety* 27(1990)1 23)52.

[6-32] Risk-based indicators. Working material of an IAEA consultants meeting, Vienna, October 5)9, 1992. Vienna 1992, International Atomic Energy Agency, Report IAEA-JA-CS55/92. 28 p. + app. 23 p.

[6-33] Boccio, J.L., Vesely, W.E., Azarm, M.A., Carbonaro, J.F., Usher, J.L. & Oden, N. Validation of Risk-Based Performance Indicators: Safety System Function Trends. Upton 1989, Brookhaven National Laboratories, Report NUREG/CR-5323, BNL-NUREG-52186.

[6-34] Laakso, K. A systematic analysis of plant disturbance experience in Swedish nuclear power units. Presented at the NEA Symposium on Reducing Reactor Scram Frequency, April 14)18, 1986, Tokyo. 16 p.

[6-35] H. Hoertner, P. Kafka and G. Reichart, The German precursor study) methodology and insights. *Reliability Engineering & System Safety* 27(1990)1 53)76.

[6-36] Laakso, K., Agner, A., Hoffström, A., Lehtinen, E. & Nyman, R. Operational safety indicators for effective experience feedback. A part of the NKS/SIK-1 project reporting. Espoo 1993, Technical Research Centre of Finland. Report NKS/SIK-1(93)25. (draft)

[6-37] Bier, V.M. Issues in the Estimation of Aging in Event Frequencies. In Use of Probabilistic Safety Assessment for Operational Safety, PSA '91, Proceedings of an International Symposium, Vienna, June 3)7, 1991. Vienna 1992, International Atomic Energy Agency, paper IAEA-SM-321/29. Pp. 337)347.

[6-38] Vesely, W.E. & Hassan, M.H. Calculation of the Core Damage Frequency Increase due to Aging under a Given Maintenance Program. In *Use of Probabilistic Safety Assessment for Operational Safety, PSA '91*, Proceedings of an International Symposium, Vienna, June 3)7, 1991. Vienna 1992, International Atomic Energy Agency, paper IAEA-SM-321/28. Pp. 327)335.

[6-39] Vesely, W.E. & Samantha, P.K. Risk Criteria Considerations in Evaluating Risks for Technical Specification Modifications. Upton 1989, Brookhaven National Laboratory.

(draft)

[6-40] Knochenhauer, M. & Hirschberg, S. Probabilistically based decision support. Reliability Engineering and System Safety 36(1992) 23)28.

[6-41] Basic safety principles for nuclear power. A report by the international safety advisory group. Vienna 1988, International Atomic Energy Agency, Safety Series no. 75-INSAG-3. 74 p.

[6-42] Guidelines on the role of probabilistic safety assessment and probabilistic safety criteria in nuclear power plant safety. IAEA Safety series report (Draft 4). Vienna 1989. International Atomic Energy Agency. 31 p.

[6-43] Horne, B. The use of probabilistic safety analysis methods for planning the maintenance and testing unavailabilities of essential plant at Heysham 2 AGR power station. Proc. of the IAEA technical committee meeting on the use of PSA to evaluate NPP's technical specifications, Vienna, June 18)22, 1990. Vienna 1990, International Atomic Energy Agency. 8 p. + app. 11 p.

7 CONCLUSIONS

7.1 Preconditions and remarks

The survey carried out as an initial step of the project found that the overall status of PSA and experiences of performing and utilizing PSA-studies are quite similar among all the utilities in Sweden and Finland. The Finnish and Swedish nuclear utilities have completed the first phase of a wide range of plant-specific PSA studies, 1991. These so called level 1 analyses have been directed on studying the internal initiating events and accident sequences leading to severe reactor core damages. The scope of the basic level 1 studies is currently being expanded to cover other operational states than the power operation. The utilities are planning to perform the level 2 analyses concentrating in post-accident phenomena in the reactor containment.

A natural step is to continue towards a living use of the present level 1 models of the plants. Persons involved in the PSA activities at the utilities as well as at the regulatory bodies are convinced about the usefulness of these activities. The major needs in the present realizations of PSAs to be living ones are:

- Establish routines and procedures of how to utilize PSA,
- Enhance model completeness and reduce conservatism in assumptions, and
- Develop user friendly and fast computer codes.

The following PSA application areas got most support by the persons interviewed:

- Comparison of alternative design and procedure changes,
- Maintenance planning,
- Optimization of the Technical Specifications and control of risks of exemptions from the Technical Specifications, and
- Surveillance tests and their schemes.

The most important methodological problem areas when carrying out PSAs are how to control the incompleteness and conservatism in the models. A general opinion is that the status of present models is not sufficient. The PSAs should be more complete, and the use of conservative assumptions reduces the usefulness and acceptance of the results from the PSAs.

In an international perspective the number of present applications of living PSA is small, and practical experience concerning the use of PSA as an operational tool has not yet accumulated to the point where a general framework for design and structure has been established. The applications have common denominators in their efforts to quantify risk levels according to projected or assumed plant status, but in actual usage the aims may be quite different. The emphasis is on research efforts in which the applicability of the PSA technique is tested in a reduced scale.

7.2 A Living PSA programme

Definition, what is Living PSA

Living PSA is a daily safety management system and it is based on a plant-specific PSA and supporting information system. In the living use of PSA plant status knowledge is used to represent actual plant safety status in monitoring or follow-up perspective. The PSA model must be able to express the risk given a time and plant configuration. To increase the availability of the basic PSA for the operational safety management, the model as well as the whole PSA programme should be

developed to a more dynamic tool. The process, to update the PSA model to represent the current or planned configuration and to use the model to evaluate and direct the changes in the configuration, is called a living PSA programme.

Usefulness

The main purposes to develop and increase the usefulness of Living PSA are summarized in Table 7-1.

Long term safety planning: To continue the risk assessment process started with the basic PSA by expanding and improving the basic models and data to provide a general risk evaluation tool for analyzing the safety effects of changes in plant design and procedures.

Risk planning of operational activities: To support the operational management by providing means for searching optimal operational, maintenance and testing strategies from the safety point of view. The results shall provide support for risk decision making in the short term or in a planning mode.

Risk analysis of operating experience: To provide a general risk evaluation tool for analyzing the safety effects of incidents and plant status changes. The analyses are used to identify possible high risk situations, rank the occurred events from safety point of view and get feedback from operational events for the identification of risk contributors.

Table 7-1: Application of living PSA.

Application:	Long term safety planning.	Risk planning of operational activities.	Risk analysis of operating experience.
Approach:	Risk assessment.	Risk monitoring.	Risk follow-up.
Result:	Identification of risk contributors. Comparison of alternative design and procedures.	Test planning. Maintenance planning. Operational decision making.	Analysis of operating experience. Operational risk experience feedback. Verification of PSA models.
Risk measure:	Nominal risk. Inherent risk.	Instantaneous risk.	Retrospective risk. Probabilistic indicators.

Application and model development

Within the NKS/SIK-1 project demonstration studies have been carried out, parts of the living PSA concept have been tried out through various applications. Applicational experience has been generated both to identify problem areas for model and method development and for demonstration of the usefulness of the results.

The main elements in the model development are:

1- to define risk measures and suggested uses of them in various living PSA applications for the operational safety management, and
2- to describe specific model features required for living PSA applications.

The living PSA applications can be divided into the three application approach categories: 1 - risk assessment, 2 - risk monitoring, and 3 - risk follow-up. To distinguish between these application categories and define the approach and purposes for them is one important result of this work. The different types of results obtained from the applications are exemplified by the case studies.

In a living PSA model all observations such as preventive maintenance or repair of safety related equipment should be easily updated in the model to reflect the changes in plant configuration. The modification of the static component and system models to dynamic ones is perhaps the main effort to be carried out in the development of the basic PSA for living use.

7.3 Demonstrations of living PSA/Case studies

Routines and procedures of how to utilize living PSA (LPSA) are demonstrated in the case studies. The demonstrations include applications such as planning of surveillance tests and their schemes, maintenance planning, optimization of limiting conditions for operation and risk control of exemptions from the Technical Specifications.

Results

Oskarshamn 2 LPSA.

- A surveillance test series could be planned from the risk point of view in which the same risk level can be maintained although 43 % less tests are performed. Figure 7-1 shows the original test scheme. By shortening the interval for risk efficient tests (and prolong others) and by optimized timing, by staggering, an improved test scheme was generated from a probabilistic viewpoint.
- The risk follow-up of one year (1987) lead to recommendations to always test gas turbine after maintenance and to always test redundant gas turbine when one gas turbine has been detected unavailable. If these rules had been followed, the risk increase during the examined year would have been only 30% of the increase actually occurred.
- The risk based allowed outage times appeared to be many times longer than according to present Technical Specifications except for gas turbines. In the analysis of operational alternatives when a gas turbine failure occurs, allowed outage times could be prolonged further, a factor 3, by testing a redundant gas turbine.
- An example application on short term, event conditional, test planning showed how the allowed outage time of a gas turbine could be prolonged further, a factor 2, due to testing of diesels generators according to event conditional estimates of the risk importance.
- The relationship between LPSA risk follow-up results and event based safety indicators has been presented.
- Group importance ranking for event evaluation and for ranking of observed trends, i.e. ageing have been defined.

Forsmark 1/2 PSA.

- The risk follow-up application performed for Forsmark 1 provided results that did not correspond with the operators opinion of the severity of the occurred events. Through the discussions that followed the actions and events that occurred were better understood and the risk awareness increased. Direct feedback to verify and revise the PSA was also obtained. The ranking of the

severity of events was facilitated and could be improved. Risk increase due to preventive maintenance 40%, an interfacing system LOCA event gave a risk dose of nine normal operating years.

TVO I/II PSA.

- The risk follow-up with TVO I/II PSA showed the high importance of preventive maintenance activities. Afterwards the maintenance strategy has been changed so that the high pressure and low pressure injection system trains are not simultaneously unavailable.
- In the analysis of a pressure relief transient at TVO, the timing of the growth of the common cause failure phenomena was modelled by a new approach. Time dependent aspects on testing and failure dependence was shown and changes in test procedures could be suggested accordingly.
- In the analysis of an external pipe break at TVO, a qualitative root cause analysis demonstrated how an operating procedure error eventually causing the incident could exist and how it could be avoided.
- In the shutdown risk analysis for TVO I/II, allowed outage times for single and multiple failures in a 4x100% redundant residual heat removal system were examined. The AOTs for single and double failures were justified. For triple or quadruple failure, a 3 day AOT was suggested instead of cold shutdown within 24 h. The operational risk at continued operation with a triple or quadruple failure was considerably lower than with the shutdown alternative.

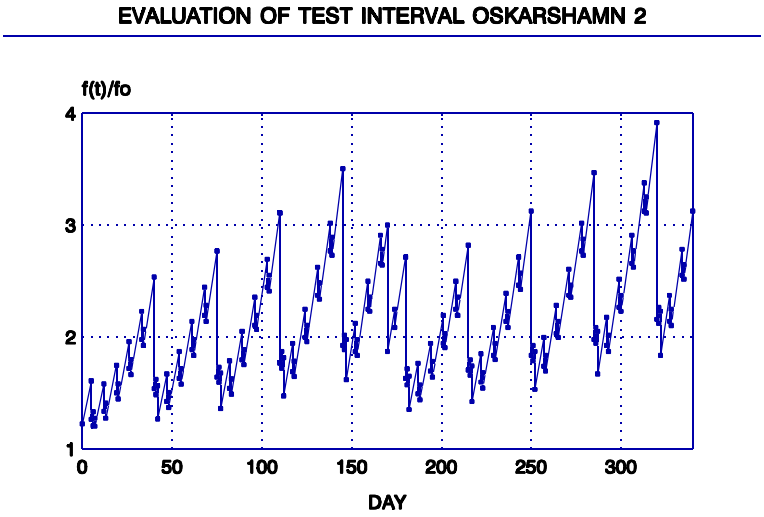


Figure 7-1: Risk variation due to an actual test scheme in Oskarshamn 2 NPP..

Diesel Generator study.

- Time-dependent common cause failure models have been developed to compare operational strategies when failures in a diesel generator are detected. To complete the repair before carrying out the test of redundant component is preferred.

Oskarshamn 3.

- Decision analysis: Procedures and approach demonstrated for an exemption from Technical Specifications. The procedure includes a combined use of probabilistic estimates, engineering judgement and other analyses (deterministic).

Limitations in models and methods

Incompleteness/conservatism: The incompleteness problem has to do with missing elements (component failure modes, initiating events and plant functions) in the model, i.e. the entire risk is not covered by the model. In many cases, PSA models are made with conservatism built into the model and data. The reason is usually to simplify the model while at the same time making estimates on the conservative side. Conservatism is acceptable in situations where the main purpose of the calculations is to verify a certain absolute risk level. In many living PSA applications, however, the conservatism may lead to wrong relative importance and wrong decisions, and thereby in the end leading to non-conservative actions. The solution to this problem can only be found in a long term usage of the plant model. Experience from the development of the basic PSA´s demonstrate how the models are gradually improved. The next step is to use the PSA for risk analysis of operating experience, risk follow-up, on a long term basis. This activity will provide experience regarding the capability of the model and provide modelling feedback that will gradually reduce the impact of these problems.

Validation of results: A qualitative validation will always be necessary due to the limitations in the quantitative results caused by incompleteness and conservatism.

Common cause failures (CCF): Time-dependent system unavailabilities and common cause failures are not fully modelled in conventional PSAs. The stand-by system unavailabilities are dependent on test arrangements. The problem is to avoid conservatism and to allow non-symmetric test arrangements as well as how to treat events with one or more redundancy evidently unavailable. Further experience, from data analysis, will show if the models suggested in this project are valid. It is now assumed that common cause failure phenomena have the same time-dependency as single failures.

Testing and test effectiveness of standby components: The failure data presented in the Nordic reliability data book are based on failure experience generated from testing. This implies that only the component risk contributor without test effectiveness considerations is available in the data. In practice, a simplified assumption is made that the test conditions are equal to the real demand requirements) the test is perfect. There is no data available to enable implementation of the suggested standby component model taking the ineffectiveness of tests into account.

Practical time constraints: In the context of living PSA with its frequent, time-dependent risk monitoring and risk follow-up studies, there may be too little time to carry out evaluations with the whole model, instead of which simplified or shortened calculations are made. One way to reduce the calculation time is to use precalculated minimal cut set list, and only update basic event probabilities. Naturally, the changes among evident events may cause the results to be strongly biased. The time limit is also one motivation for the use of integrated uncertainty analysis, because the time-consuming Monte Carlo simulation is avoided.

Simplified approach for time-dependent evaluations: Many computer programs used in PSA analysis apply only nominal unavailabilities to basic events. A simplified approach for time-dependent evaluations applied in this case has been developed.

Integrated uncertainty analysis: Integrated uncertainty analysis results in a risk frequency distribution that is directly applicable in decision analysis. Specific problem areas, like the modelling of CCF-uncertainty and state-of-knowledge dependence, are easier to handle, because multi-dimensional distributions are integrated on the basic event level. However, the approach requires code developments to calculate the total (unconditional) component failure probability for the basic events.

7.4 Recommendations for development of safety management

PSA should be better integrated with other safety management methods. Operational or design alternatives can be compared in a more understandable way, and a more effective support can be gained to react to gradual or sudden changes in the operational safety status of the plant.

Staffing and cost benefit of living PSA

On an average 4)10 persons are directly working with PSA activities at Nordic utilities (2-7 units) to establish and maintain the basic PSAs. The LPSA activities, to monitor and follow-up the risk, will require a staff of this size on a long term basis. The LPSA activities require a close relationship to plant operation and maintenance compared to the basic PSA applications, that to a much larger extent are directed towards plant safety management, designers and authorities.

To enable a discussion of the cost benefit of the recommendations and the LPSA activities, the different elements in this comparison are summarized in Table 7-2. This valuation must be made by the plant personnel together with the decision whether or not to implement these activities in the daily safety management.

Implementation and use

The development of routines and procedures for living PSA includes transfer of PSA-related information within the organizations. Living PSA application will always require specialists to operate and maintain the model. However, a better operational interface will allow a more efficient use and a broader spectrum of users to carry out the applications. To implement a living PSA programme requires that plant personnel is heavily involved and appreciates the benefits of working according to this procedure. The plant organization will in the end decide for themselves to what extent these methods shall be used in the safety management of the nuclear power plant.

Table 7-2: Cost benefit of LPSA

Cost	Benefit
Basic PSA: 5-10 manyears Expansions of PSA: 1-3 manyears per expansion (6-9 manyears, the level of ambition differs due to plant generation)	Identification of risk contributors
Maintenance of plant model (PSA or LPSA): 0.5-1 manyear per year and unit LPSA appl.: 0.5-1 manyear per year and unit	Increased flexibility in testing, maintenance and limiting conditions for operation. Increased risk awareness. Improved experience feedback
Upper estimate ≃ 20[1)] manyears plus 2 manyears/year.	*"If you think safety is expensive try an accident."*

1) In Sweden: The initial investment, the basic PSA, of 10 manyears was required as a part of the first round of periodic safety review, ASAR-80. The expansions, ≃10 manyears, is required as a part of the second periodic safety review, ASAR-90. In Finland: The situation is approximately the same, the work is not carried out within the framework of a periodic safety review programme.

Based on the work and the demonstrations carried out it is recommended that a Living PSA programme is implemented on a plant specific basis. The implementation can be divided in two steps:

1) Prepare procedures, models, and data to carry out

- Risk evaluation of test intervals: Following this application also configuration control and short term risk planning will be possible on the same basis.
- Risk evaluation of allowed outage times: Following this application also maintenance planning will be possible.
- Analysis of operating experience by risk follow-up, generation of severity ranking and probabilistic safety indicators.

2) Prepare criteria and procedures for risk decision making, i.e. exemptions from LCOs in Technical Specifications

Decision making and regulatory aspects

A proper use of the applications requires that decision making criteria are established. Probability and frequency criteria are not sufficient in complex decision making situations. They might, however, give guidance or first indication about the acceptability of the decision alternative. The decision making procedure shall include and allow a combined use of probabilistic estimates, deterministic analyses and engineering judgement.

The recommendation to prepare decision criteria are in the first place directed towards the regulatory side, but must be prepared and implemented in agreement with the industry. Regulatory and inspection activities relate to all applications of PSA. The applications connected to requirements in the Technical Specifications are important to review and approve. In the case of exemptions from Technical Specifications, specific case studies provide basis to accept or reject the exemption. Inspection guidance can be obtained by using basic results from the risk assessment such as dominant risk contributors.

7.5 Future developments and broadening the use of living PSA

Operational interface

The overall structure of a living PSA operational interface is presented. The central module can be any PSA software. The emphasis is on the development of additional user functions and means for linking PSA software with external data bases or plant computers. This includes integration with other information systems. At present the concept of operator support system based on a full scale PSA is not well developed although there is a number of proposals outlining the structure and functioning of such a system.

Living PSA as a training tool would offer a practical introduction to PSA for plant staff that has little or very little experience with PSA, and it would enhance the general level of understanding of the capabilities of probabilistic safety in relation to deterministic safety.

On-line operational activities

The purpose of on-line risk monitoring is to evaluate the instantaneous risk frequency given the information about the configuration of safety related systems to support for operational risk decision

making in the short term. This must in some cases be performed on an on-line basis to gain the maximum benefit from the applications. Today simplified PSA models are applied in planning of operational and maintenance activities. It will still take some time before a full scale plant model can be used on-line, meaning that it can give nearly continuous assessment of plant status and risk level. In view of expert system techniques the PSA model can be looked upon as a knowledge base which is organized according to principles suited for probabilistic assessment. Expert systems techniques can be applied to assist the user in the analysis of the situation and the selection of appropriate actions to bring the plant to a safe state as efficiently as possible.

7.6 Consensus

The early as well as fast identification of discrepancies and deficiencies in plant design and operation is considered essential for safety. The design aspects on plant safety are handled to a large extent by the basic PSA. As a result of a living PSA, the safety aspects on operational, maintenance or testing practices can be evaluated, and modified, and the flexibility in operation may be justified. A feasible risk monitoring system, gradually tailored and implemented for plant specific use by its user organizations, is aimed to support the risk management activities of the utilities, as well as the inspection activities of the authorities. This project describes the methods, models and applications required to continue the process towards a living use of PSA. We recommend to implement a LPSA programme and to start to produce dynamic applications based on off-line risk monitoring and risk follow-up.

NKS/SIK-1 REPORTS AND PUBLICATIONS ON LPSA DEVELOPMENT

SKI Technical Report 94:3 present the supporting documentation for this report (SKI TR 94:2). Below are the titles included in 94:3 listed. The reports listed in *italic* typeface are not included, they have been published elsewere or been written for other purposes.

Enclosure number in TR 94:3

1 NKS/SIK-1(90)5. Mankamo, T., Pörn., K. & Holmberg, J. Uses of risk important measures. Espoo 1991, Technical Research Centre of Finland. VTT Research Notes 1245. 36 p. + app. 8 p.

2 NKS/SIK-1(90)8. Laakso, K., Johanson, G., Björe, S., Virolainen, R. & Gunsell, L. Safety evaluation by use of living PSA and safety indicators. Work plan 1990)1993. Espoo 1990. 21 p.

3 NKS/SIK(90)10. Holmberg, J., Laakso, K., Lehtinen, E., Johanson, G. & Björe, S. International survey of living PSA and safety indicators. Espoo 1992, Technical Research Centre of Finland, VTT Research Notes 1326. Report RISKI(90)2. 51 p. + app.

NKS/SIK-1(90)11. Mankamo, T. & Kosonen, M. Operational decision alternatives in failure situations of standby safety systems. Proceedings of the IAEA Technical Committee Meeting on the Use of Probabilistic Safety Assessment to Evaluate Nuclear Power Plant's Technical Specifications, Vienna, June 18-22, 1990. IAEA-TECDOC-599. Report RISKI(91)15. 20 p.

4 NKS/SIK-1(90)13. Holmberg, J., Laakso, K., Lehtinen, E., Johanson, G. & Björe, S. Nordic survey on safety evaluation by use of living PSA and safety indicators (NKS/SIK-1). Stockholm 1991, Statens Kärnkraftinspektion. SKI technical report 91:3, 28 p. + app. 16 p.

5 NKS/SIK-1(91)4. Mankamo, T. & Kosonen, M. Continued plant operation versus shutdown in failure situations of standby safety systems - application of risk analysis methods for the evaluation and balancing of allowed outage times for the residual heat removal systems at TVO I/II plant. Espoo 1992, Avaplan Oy. Report RISKI(91)16. 100 p.

6 NKS/SIK-1(91)6. Johanson, G. Survey of time dependences in LPSA models. Stockholm, 1991, Statens Kärnkraftinspektion. 14 p.

7 NKS/SIK-1(91)7. Johanson, G., Gunsell, L., Laakso, K. & Hellström, P. Safety evaluation by use of living PSA and safety indicators. Current status and future development of models and tools within the Nordic project "Safety Evaluation, NKS/SIK-1". In: Use of probabilistic safety assessment for operational safety, Proc. of an international symporium, Vienna, 3-7 June, 1991. Vienna, 1992, International Atomic Energy Agency, Pp. 659)676.

8 NKS/SIK-1(91)23. Pörn, K. & Shen, K. Integrated uncertainty analysis in PSA. Nyköping: Studsvik Ecosafe Ab, 1991. Report STUDSVIK/NS-91/71. 37 p.

9 NKS/SIK-1(91)27. Holmberg, J., Pulkkinen, U., Laakso, K. & Mankamo, T. The risk follow-up by PSA) report of the Finnish pilot study. Espoo 1992, Avaplan Oy. Report VTT/SÄH 14/91, RISKI(91)4. 18 p. + app. 2 p.

10 NKS/SIK-1(91)29. Pörn, K. & Shen, K. Decision making under uncertainty) A pilot sturdy

on exemption from technical specification. Nyköping 1992, Studsvik Ecosafe Ab. STUDSVIK/NS-91/90. 30 p. + app. 15 p.

11 NKS/SIK-1(91)30. Erhardsson (Wendt), U.-K. & Flodin, Y. Momentan risknivå. Fud-projekt inom levande PSA. (Instantaneous risk level). Vällingby 1991, Vattenfall Ab. 20 p. (In Swedish)

11b PK-168/90. Erhardsson (Wendt), U-K. Test av några olika tidsberoende CCF modeller. Vällingby, Nov. 1990.

12 NKS/SIK-1(91)33. Stokke, E. Operational interface for LPSA. Halden 1993, IFE Halden. (draft)

13 NKS/SIK-1(91)35. Holmberg, J., Pulkkinen, U. & Mankamo, T. Risk follow-up by PSA. In: Proc. of the IAEA Technical Committee Meeting on Guidelines on Probabilistic Safety Assessment (PSA) Requirements for Use in Safety Management, Stockholm 16)20 September 1991. Report VTT/SÄH 16/91, RISKI(91)9. 13 p. + app. 2 p.

14 NKS/SIK-1(91)38. Holmberg, J., Johanson, G. & Niemelä, I. Risk measures in living probabilistic safety assessment. Espoo 1993, Technical Research Centre of Finland. VTT publications 146, 59 p. + app. 8 p.

15 NKS/SIK-1(91)40. Holmberg, J. A limited survey on the ASP methodology. Espoo 1991, Technical Research Centre of Finland. Report VTT/SÄH 18/91, RISKI(91)40. 11 p.

16 NKS/SIK-1(91)48. Mankamo, T. Timedependent models/risk monitor exercise. TVO I/II SRV CCF Quantifications. Espoo 1993, Avaplan Oy. Work notes. 25 p. (draft)

17 NKS/SIK-1(92)2. Holmberg, J. & Johanson, G. Definition of a concept for safety evaluation by use of living PSA) the Nordic project "safety evaluation, NKS/SIK-1". In: Petersen, K. & Rasmussen, B. (ed.) Safety and reliability '92. Proc. of the European safety and reliability conference '92 (ESRC '92), Copenhagen, June 10)12, 1992. London 1992, Elsevier. Pp. 995)1006.

18 NKS/SIK-1(92)3. Mankamo, T. Extended common load model. A tool for dependent failure modelling in highly redundant structures. Espoo 1990, Avaplan Oy. Publication manuscript. 26 p.

19 NKS/SIK-1(92)7. Holmberg, J., Johanson, G. & Sandstedt, J. The generation of probabilistic safety indicators from the risk follow-up results. In: Balfanz, H.-P. (ed.) Proc. of the 3rd workshop on living-PSA-application, Hamburg, May 11)12, 1992. TÜV-Norddeutschland, Hamburg, 1992. 15 p.

20 NKS/SIK-1(92)8. Holmberg, J. & Pulkkinen, U. Decision analysis on an exemption from the technical specification. Espoo 1992, Technical Research Centre of Finland. Report VTT/SÄH 4/92, RISKI(92)1. 19 p. + app. 16 p.

21 NKS/SIK-1(92)12. Pörn, K. & Shen, K. On the integrated uncertainty analysis in probabilistic safety assessment. Nyköping 1992, Studsvik Ab. 13 p.

22 NKS/SIK-1(92)13. Mankamo, T. A timedependent model of dependent failures)

Application to a pairwise symmetric structure of four components. Espoo 1994, Avaplan Oy. 31 p.

23 NKS/SIK-1(92)15. Johanson, G., Holmberg, J. & Sandstedt, J. Living PSA application for a Swedish BWR. In: Kafka, P. & Wolf, J. (ed.) safety and reliability assessment - an integral approach proc. of the European Safety and Reliability Conference, München, May 10-12, 1993. Elsevier, Amsterdam. Pp. 455-465.

24 NKS/SIK-1(92)17. Holmberg, J., Pulkkinen, U., Pörn, K. & Shen, K. Risk decision making in operational safety management - experience from the Nordic benchmark study. Nyköping 1993, Studsvik EcoSafe. Report STUDSVIK/ES-93/37, RISKI(93)1. 19 p. + app. 6 p.

25 NKS/SIK-1(92)20. Johanson, G. & Holmberg, J. The use of living PSA in safety management, a procedure developed in the Nordic project "Safety Evaluation, NKS/SIK-1". In: Proc. of the Probabilistic Safety Assessment International Topical Meeting in Florida, January 27-29, 1993. 11 p.

26 NKS/SIK-1(92)22. Sandstedt, J. & Berg, U. Living PSA applications for a Swedish BWR with the aid of Risk Spectrum. In: Balfanz, H.-P. (ed.) Proc. of the 3rd workshop on living-PSA-application, Hamburg, May 11-12,1992. Hamburg 1992, TÜV-Norddeutschland. 25 p.

27 NKS/SIK-1(92)27. Sandstedt, J. Demonstration studies on living PSA. Sundbyberg 1992, Relcon Ab. 24 p.

28 NKS/SIK-1(92)35. Mankamo, T. A pressure relief transient with pilot valve function affected by a latent CCF mechanism. Espoo 1994, Avaplan Oy. 34 p.

NKS/SIK-1(92)39. See (92)15.

29 NKS/SIK-1(92)49. Sandstedt, J. Betydelseanalys och känlighetsanalys av O2-indikatorer FAS 1 och 2. Stockholm 1993, SKI. Ski/RA report - 4/93. (In Swedish)

30 NKS/SIK-1(93)3. Holmberg, J., Lehtinen, E. & Laakso, K. Safety management supported by living probabilistic safety assessment (PSA) operational safety indicators. Presented in Workshop on Integrated Risk Management for Large Industrial Complexes and Energy Production Systems, Moscow, February 22)26, 1993. Espoo 1993, Technical Research Centre of Finland. Report RISKI(93)2. 16 p.

31 NKS/SIK-1(93)4. Mankamo, T. A risk-based approach to AOTs. Espoo 1993, Avaplan Oy. 6 p. (draft, missing)

NKS/SIK-1(93)5. Holmberg, J. Operating experience feedback in probabilistic safety assessment. Espoo 1993, Helsinki University of Technology. Licentiate thesis. 99 p.

NKS/SIK-1(93)13. Lehtinen, E., Holmberg, J. & Laakso, K. Integrated use of probabilistic safety indicators to support operational safety management. Paper submitted to the IFAC symposium Safeprocess '94, Espoo, June 13-15, 1994. Report RISKI(93)11. 2 p.

32 NKS/SIK-1(93)17. Holmberg, J. & Pyy, P. Analysis of an external pipe break. Espoo 1993, Technical Research Centre of Finland. Report RISKI(93)11. (Abstrakt only)

33 NKS/SIK-1(93)21. Holmberg, J., Pulkkinen, U., Pörn, K. & Shen, K. Risk decision making in operational safety management) experience from the Nordic benchmark study. Espoo 1993, Technical Research Centre of Finland. Report RISKI(93)14. 19 p. (Submitted for Risk Analysis)

34 NKS/SIK-1(93)26. Sandstedt, J. Pilot study. Analysis of Prescribed Test Intervals, Oskarshamn 2. Sundbyberg, Relcon AB, Relcon Report 15/93, August 1993.

The Report also exist in Swedish:
Relcon -12/93. Förstudie. Analys av föreskrivna testinterval Oskarshamn 2. Sundbyberg, Augusti 1993, Relcon AB. 32 p.

35 NKS/SIK-1(93)30. Johanson, G., Berglund, L., Holmberg, J. and Karlsson, C. Regulatory decision making: Test of qualitative and quantitative decision criteria for improvements in Technical Specifications. In Proc. of IAEA Technical Committee Meeting on "Procedures for use of PSA for optimizing nuclear power plant operational limits and conditions", Barcelona, September 20)23, 1993, (IAEA-J4-TC-855). Report RISKI(93)17. 12 p.

36 NKS/SIK-1(93)31. Knochenhauer, M. and Johanson, G. Derivation of time dependent component unavailability models and application to Nordic PSA:s. To be presented in PSAM II conference, San Diego, March 20)24, 1994. 1993. 6 p.