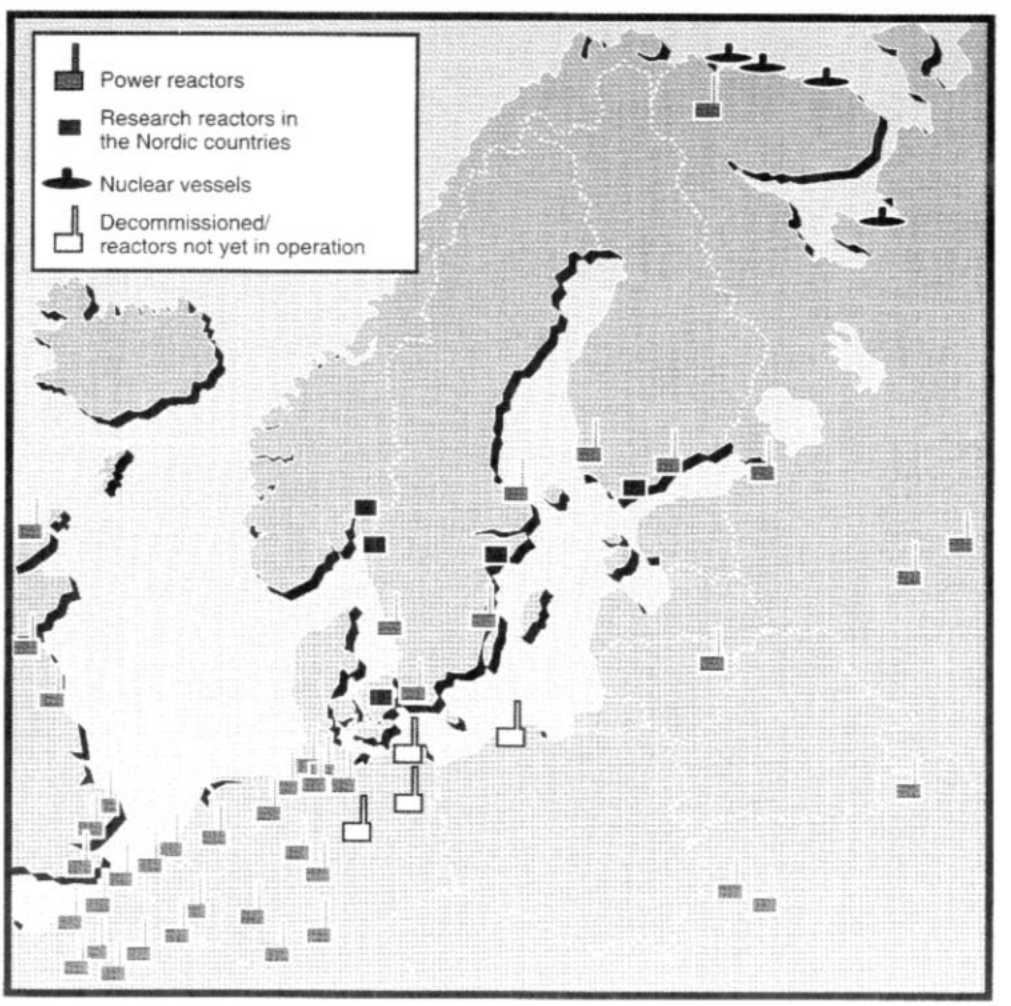
Nuclear Safety

Nordic Studies in Reactor Safety

TemaNord
1994:544



Nordic Studies in Reactor Safety

Nordic Studies in Reactor Safety

Final report of the
Nordic Nuclear Safety Research Programe SIK

Edited by
Bengt Pershagen
December 1993

TemaNord 1994:544

Nordic Studies in Reactor Safety

TemaNord 1994:544

ISBN 92 9120 461 1
ISSN 0908-6692
Printing and distribution: Nordic Council of Ministers, Copenhagen
Printed on Paper Approved by the Nordic Environmental Labelling
Information about the NKS reports can be obtained from:

NKS
P.O.Box 49
DK-4000 Roskilde
Telefax (+45) 46 32 22 06

The Nordic Council of Ministers
was established in 1971. It submits proposals on co-operation between the governments of the five Nordic countries to the Nordic Council, implements the Council's recommendations and reports on results, while directing the work carried out in the targeted areas. The Prime Ministers of the five Nordic countries assume overall responsibility for the co-operation measures, which are co-ordinated by the ministers for co-operation and the Nordic Co-operation Committee. The composition of the Council of Ministers varies, depending on the nature of the issue to be treated.

The Nordic Council
was formed in 1952 to promote co-operation between the parliaments and governments of Denmark, Iceland, Norway and Sweden. Finland joined in 1955. At the sessions held by the Council, representatives from the Faroe Islands and Greenland form part of the Danish delegation, while Åland is represented on the Finnish delegation. The Council consists of 87 elected members - all of whom are members of parliament. The Nordic Council takes initiatives, acts in a consultative capacity and monitors co-operation measures. The Council operates via its institutions: the Plenary Assembly, the Presidium, and standing committees.

Foreword

The report summarizes the achievements of a joint Nordic research programme in reactor safety. The programme, known under the acronym SIK, was carried out during 1990-1993 and includes three separate projects in the areas of safety evaluation, severe accidents, and safety features of reactors in neighbouring countries.

The research work has been carried out in collaboration between Nordic nuclear utilities, safety authorities, research institutes and consultants. The total volume of effort was approximately 380 person months. The total funding amounted to about DKK 26 million.

Each of the three projects was managed by a project leader. Effective operation of the whole programme was ensured by a programme coordinator. A reference group with representatives of the participating countries followed the work and suggested directions of research.

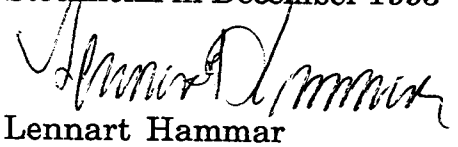
The report has been edited on the basis of the technical task reports. Suggestions and comments were given by the programme coordinator, the project leaders, and members of the reference group. The report has been reviewed and approved for publication by the reference group.

The report addresses both the interested layman and the specialist. It tries to explain why the research was undertaken, how it was carried out and what was achieved. It can be considered as a reference document which sets the SIK programme into context and highlights its results.

An overview of programme and its results is presented in the Summary (also available in Danish and Finnish). Conclusions of each of the three projects are given at the end of each Chapter describing the individual projects. Overall conclusions with regard to essential questions pertinent to reactor safety management are found in the final Chapter 6. For the benefit of the non-specialist, a summary of reactor safety fundamentals, and a glossary of terms and abbreviations are appended.

The SIK programme has largely contributed to improving and sharing knowledge and understanding of reactor safety matters in all Nordic countries and to strengthening the professional contacts. The devotion and efforts of all participants who so successfully contributed to this end are gratefully acknowledged.

Stockholm in December 1993



Lennart Hammar
Chairman of the SIK Reference Group

Abstract

The SIK programme in reactor safety is part of a major joint Nordic research effort in nuclear safety. The report summarizes the achievements of the SIK programme, which was carried out during 1990-1993 in collaboration between Nordic nuclear utilities, safety authorities, and research institutes. Three main projects were successfully completed dealing with:

(1) development and application of a living PSA concept for monitoring the risk of core damage, and of safety indicators for early warning of possible safety problems;

(2) review and intercomparison of severe accident codes, case studies of potential core melt accidents in Nordic reactors, development of chemical models for the MAAP code, and outline of a system for computerized accident management support;

(3) compilation of information about design and safety features of neighbouring reactors in Germany, Lithuania and Russia, and of naval reactors and nuclear submarines.

The report reviews the state-of-the-art in each subject matter as an introduction to the individual project summaries. The main findings of each project are highlighted. The report also contains an overview of reactor safety research in the Nordic countries and a summary of fundamental reactor safety principles.

Key words Living PSA, risk monitoring, risk follow-up, risk measures, safety indicators, incident and trend analysis, risk based decision making, severe accident analysis, severe accident codes, chemical models for MAAP, aerosol models, accident mitigation, accident management, VVER reactors, RBMK reactors, naval reactors.

Summary

The safety of nuclear reactors depends on the inherent characteristics of the reactor type, and on the engineered safety features and safe operation of the particular reactor. Safe operation implies that the reactor power is always under control and the core well cooled, and that radioactive substances are confined. If these conditions are not met, the core may be damaged and radionuclides be released to the environment.

The risk of core damage is evaluated by probabilistic safety analysis (PSA). The PSA methodology has been applied and extended since the mid-1970s. The progression of core damage and the behaviour of the molten core in the reactor vessel and containment is studied by deterministic analysis. Comprehensive severe accident research started after the Three Mile Island accident in 1979. The Chernobyl accident in 1986 revealed a considerable lack of information in the Nordic countries and elsewhere in the West about the design and safety features of Russian reactors.

Probabilistic safety assessment, severe accident analysis, and safety design features of neighbouring, notably Russian, reactors, were the main areas of interest for joint Nordic research when the SIK programme was initiated in 1990. The programme was structured in three separate projects covering each area of interest.

Living PSA

Probabilistic safety assessment has been used for risk evaluation of Nordic reactors since the early 1980s. The risk is expressed as the estimated frequency of potential core damage, i.e. the probability of core melt per reactor operating year.

The strength of PSA is that a large amount of data can be handled in a systematic way and integrated into a quantitative estimate of risk. Risk values must be treated with caution, however, because of the inevitable limitations of the PSA methodology. While safety, therefore, cannot be assessed solely by PSA, basic PSA has proved to be a very effective means of identifying weaknesses and evaluating improvements in the safety design and operational procedures.

Basic PSA uses average values for the unavailability of safety-related components and systems to estimate a nominal risk. In reality, a component or system may fail when needed or be inoperable due to maintenance. The term "living PSA" has been coined to characterize the extended PSA which attempts to take this variability into account. The result will be an instantaneous risk value and a time-dependent risk curve. In general, living PSA refers to the process of maintaining a continuously updated plant-specific PSA model for everyday use in the safety work at the plant and by the authorities.

In the SIK-1 project, a living PSA concept has been specified. Application areas and risk measures were defined. Pilot studies were carried out on Nordic reactors. Some results of the pilot studies have already been of direct practical importance. The risk significance of occurred operational events during selected periods of time in Nordic boiling water reactors was clearly demonstrated. It was also shown that living PSA can be used to improve some of the existing rules for safe operation.

The ultimate goal of living PSA is to provide a tool for supporting day-to-day safety management at the nuclear power plants. The studies indicate that the proposed approach is feasible for this purpose. Additional efforts are needed, however, to improve the flexibility of certain models, to test further applications, and to implement the tools at the individual nuclear power plants.

Safety indicators

Living PSA will be used as a complement to other means of safety assessment, such as safety indicators. Safety indicators reflect the safety performance of the plant in a condensed way. They are intended to provide early warning of potential problems, but also to evaluate improvements in plant operation and safety performance.

A system of safety indicators has been proposed. The system aims at preserving the integrity of the barriers for radionuclide release, i.e. the fuel cladding, the pressure boundary of the primary reactor system, and the reactor containment. Some of the indicators are already in use at the nuclear power plants.

The indicators use data processed from the vast amount of information about operation and maintenance collected at the plants. Methods for screening the information systems by computerized search patterns were developed and tested. Several safety and maintenance indicators were validated and suggested for use.

Risk based decision making

Safety depends to a large extent on the evaluation of the risks involved in the design, operation and maintenance of the plant, and on subsequent decisions by reactor operators and safety authorities. Decision analysis can give some guidance and support in the often very complex decision situations as a complement to other analyses and engineering judgement.

A pilot study was undertaken for a real case on exemption from the technical specifications for safe operation in a Swedish boiling water reactor. Two independent approaches were used for simulating the decision situation. The studies gave valuable insights in structuring and weighting the decision objectives and criteria. A new method of uncertainty analysis in PSA was applied in one of the pilot studies.

Severe accident codes

The course of potential severe accidents is predicted by means of computer codes which describe the genesis of core damage and the behaviour of the molten core in the reactor vessel and containment. A two-stage approach is used where simplified codes are used for survey calculations, and detailed codes are used for independent verification of parts of the process. The commonly used tool for survey calculations in the Nordic countries is the MAAP code, developed in the USA and adapted to Nordic conditions.

In SIK-2 , two detailed severe accident codes, SCDAP/RELAP and MELCOR, were taken into active use. The codes are being developed in the USA and have been made available through the participation of Finland and Sweden in an international cooperative programme, operated by the U.S.Nuclear Regulatory Commission.

Predictions of accident progression in the reactor vessel have been compared for the detailed codes and MAAP. The comparison showed qualitative agreement but significant quantitative differences on important items. Some improvements of the codes were suggested. Substantial improvement could only be obtained through well characterized experiments.

It is concluded that the general understanding of basic phenomena has increased considerably during recent years. MAAP is considered useful as a tool for assessing containment integrity and measures for accident mitigation. The predictions of MAAP as well as of other severe accident codes must, however, be treated with caution and interpreted with expertise.

Chemical and aerosol modelling

The modelling of chemical phenomena and processes in MAAP is based on pre-determined assumptions for the species occurring under accident conditions. In a subtask of SIK-2, improved models for treating chemical behaviour in MAAP have been developed and tested. The tests showed considerable differences in the transport of radiologically important species in the reactor vessel and containment, depending on the model assumptions.

Under accident conditions, some of the chemical species, part of which are radioactive, appear as aerosols in the atmosphere of the reactor vessel and containment. A review of aerosol models and codes was undertaken. The review indicated that basic aerosol phenomena are well understood and modelled, but that the treatment of aerosol behaviour in complex geometries and the interaction of chemical and aerosol phenomena can be improved.

Accident management support

Accident management is the term used to characterize human action and procedures for accident mitigation. Preventive accident management aims at restoring core cooling at an early stage to avoid further progression of an incipient accident. Mitigative accident management is directed to reducing the offsite consequences of a severe accident, once it has occurred.

While it is recognized that all potential accident situations cannot be anticipated, some general principles and rules for accident management can be formulated. A project has been initiated to develop a computerized accident management system for operator support. A prototype concept has been defined, and some simulator software has been implemented.

Reactors in neighbouring countries

Information has been compiled on the design and safety features of 14 reactors close to the borders of the Nordic countries. Eight of them are located in Russia, two in Lithuania, and four in Germany.

Four of the Russian reactors are pressurized water reactors, type VVER, at the Kola nuclear power plant about 120 km from the border of Finland and 220 km from Norway, and four are Chernobyl-type boiling water cooled graphite reactors, RBMK, at Sosnovy Bor near St. Petersburg, about 100 km from from Finland.

Two reactors of each type are first generation plants and two of each type are second generation plants. The first generation reactors have clearly inferior safety characteristics as compared to Western standards. The second generation reactors have better safety features, in some respects comparable to those in the West.

The two reactors at Ignalina, Lithuania (450 km from the Swedish island of Gotland) are later generation RBMKs. After Chernobyl, safety-enhancing measures were implemented, as in all RBMKs. Safety is still being improved, like in all the Russian reactors mentioned.

The German reactors included in the data compilation are located in the lower region of the river Elbe near Hamburg, about 100 km from the border of Denmark. Two units are boiling water reactors and two are pressurized water reactors. Their safety design corresponds to the best of Western standards.

Naval reactors

Nuclear icebreakers and submarines are known to operate in the seas near to the Nordic countries. Information has therefore been collected on the design and safety features of naval reactors. Published information on submarine incidents and accidents is reviewed and commented.

Conclusions

Methods of probabilistic safety analysis have been extended to include the evaluation of operational safety. Living PSA allows more effective feedback of operational experience as well as improvement of the rules and procedures for safe operation. Living PSA tools and safety indicators can provide valuable support for safety management and decision making on safety issues concerning reactor operation and maintenance. Additional efforts are required to further improve these aids and to implement them at the nuclear power plants.

The understanding of basic phenomena in severe core damage and subsequent processes in the reactor vessel and containment has improved considerably over the last decade. The computer codes presently used in Finland and Sweden can predict the general progression of severe accidents sufficiently well. The objective of current research is to study selected phenomena in more detail. Continued research and follow-up of international progress in the area is needed in the Nordic countries.

The compilation of data on the design and safety features of reactors in neighbouring countries provides adequate overall information for the Nordic safety authorities at the present time. Periodic updating is required to take into account design changes and safety improvements of Russian reactors, in particular.

Sammenfatning

Kernereaktorers sikkerhed beror på reaktortypens naturlige egenskaber, reaktorens sikkerhedsmæssige udformning og på en sikker drift af reaktoren. Sikker drift indebærer, at reaktoreffekten til stadighed er under kontrol, at kernen er vel afkølet, og at radioaktive stoffer holdes indesluttet. Hvis disse betingelser ikke er opfyldt, kan kernen tage skade og radioaktive stoffer blive frigjort til omgivelserne.

Sandsynligheden for ulykker beregnes med probabilistisk sikkerheds-analyse (PSA). PSA-metoden er anvendt og videreudviklet siden midten af 1970'erne. Forløbet af et kernehavari og den smeltede kernes opførsel i reaktorens primærsystem og dens indeslutning studeres ved deterministisk analyse. Efter Three Mile Island ulykken i 1979 begyndte man at foretage omfattende undersøgelser af alvorlige ulykker. Katastrofen i Tjernobyl i 1986 afslørede en betydelig mangel på information i de nordiske lande og andre steder i den vestlige verden om de russiske reaktorers konstruktion og sikkerhedssystemer.

Probabilistisk sikkerhedsvurdering, analysemetoder for kernehavari og sikkerhedsforhold ved reaktorer nær de nordiske lande - især russiske - var de vigtigste emner for det fællesnordiske SIK-forskningsprogram, der begyndte i 1990. Programmet blev opdelt i tre hovedprojekter, et for hvert emneområde.

Levende PSA

Probabilistisk sikkerhedsanalyse har været anvendt til sikkerheds-vurdering af nordiske reaktorer siden begyndelsen af 1980'erne. Risikoen udtrykkes som en vurderet kernehavarifrekvens dvs. sandsynligheden for kernehavari per driftsår.

Fordelen ved PSA er, at en stor mængde data kan håndteres systematisk og sammenfattes i en kvantitativ vurdering af risikoen. Absolutte risikoværdier må dog behandles med forsigtighed på grund af de uundgåelige begrænsninger i PSA-metodikken. Selvom en sikkerheds-vurdering derfor ikke kan baseres alene på PSA, så har PSA vist sig meget effektiv, når det drejer sig om at opdage svage punkter og vurdere forbedringer i sikkerhedsforhold og driftsprocedurer. Generelt er levende PSA blevet betegnelsen for den proces, som indebærer opretholdelse og kontinuert opdatering af en anlægsspecifik PSA model og anvendelsen af den i det daglige sikkerhedsarbejde både ved anlægget og hos sikkerheds-myndighederne.

Grundlæggende PSA anvender middelværdier for svigt af sikkerheds-relaterede komponenter og systemer til at vurdere en nominel risiko. I virkeligheden kan en komponent enten svigte, når der er brug for den,

eller den kan være uanvendelig på grund af vedligeholdelsesarbejde. Begrebet "levende PSA" er formuleret for at betegne den PSA, som forsøger at tage hensyn til disse forhold. Resultatet vil fremstå som en momentan risiko og en tidsafhængig risikokurve.

I SIK-1 er der udarbejdet et koncept for levende PSA. Anvendelsesområder og risikomål er defineret. Pilotundersøgelser er udført på nordiske reaktorer. Visse resultater af disse pilotundersøgelser har allerede haft direkte praktisk betydning. Den risikomæssige betydning af drifts-hændelser ved nordiske kogendevandsreaktorer i udvalgte tidsperioder blev klart demonstreret. Det er også blevet vist, at levende PSA kan benyttes til at forbedre eksisterende forskrifter for sikker drift.

Det endelige formål med levende PSA er at understøtte den daglige sikkerhedsmanagement ved kernekraftværker. De gennemførte under-søgelser tyder på, at dette er muligt. Det er dog nødvendigt med yderligere arbejde for at forbedre fleksibiliteten i visse modeller, at prøve andre anvendelser og at introducere metoden til praktisk brug ved de enkelte kernekraftværker.

Sikkerhedsindikatorer

Levende PSA vil blive brugt som supplement til andre former for sikkerhedsvurdering som f.eks. sikkerhedsindikatorer. Sikkerheds-indikatorer afspejler i koncentreret form anlæggets sikkerhedsmæssige kvalitet. Det er meningen, de skal give et tidligt forvarsel om potentielle problemer, men de skal også bringes til at vurdere forbedringer af sikkerheden under driften.

Der er foreslået et system af sikkerhedsindikatorer. Systemet tager sigte på at bevare barriererne mod udslip af radioaktive stoffer dvs. brændslets indkapsling, reaktorens primærsystem og indeslutningen.

Indikatorerne udnytter bearbejdede data fra den omfattende information om drift og vedligeholdelse, der er samlet ved kraftværkerne. Der er udviklet og afprøvet datamatiske metoder til afsøgning af informations-systemerne. Et antal indikatorer er foreslået.

Risikobaseret beslutningstagning

Sikkerhed beror i væsentlig grad på vurdering af risici i forbindelse med konstruktion, drift og vedligehold af anlægget og på driftspersonalets og sikkerhedsmyndighedernes efterfølgende beslutninger. Beslutningsteori kan give en vis vejledning og støtte i de ofte meget komplekse beslutningssituationer.

Der er gennemført en undersøgelse af en virkelig situation, hvor man fraveg de eksisterende sikkerhedsforskrifter for drift af en svensk kogendevandsreaktor. Der benyttedes to forskellige metoder til at simulere

beslutningssituationen. Undersøgelserne gav værdifuld indsigt i, hvordan man kan strukturere mål og kriterier for beslutningen.

Beslutningstagning i sikkerhedsspørgsmål ledsages ofte af usikkerhed. En ny metode til usikkerhedsanalyse i PSA blev udviklet og benyttet i den ene af de nævnte undersøgelser.

Dataprogram til analyse af alvorlige uheld

Forløbet af et eventuelt alvorligt kernehavari beregnes med edb-programmer, der beskriver kernenedsmeltningen og den smeltede kernes opførsel i reaktortank og indeslutning. Der benyttes en totrins metode, hvor forenklede programmer benyttes til at give et overblik over situationen, mens mere detaljerede programmer bruges til uafhængig verifikation af dele af processen. Det program, der normalt anvendes i de nordiske lande til oversigtsberegninger, er MAAP, som er udviklet i USA og tilpasset til nordiske forhold.

I SIK-2 er to nye detaljerede edb-programmer, SCDAP/RELAP og MELCOR, taget i brug. Programmerne er udviklet i USA og er til rådighed i Finland og Sverige som følge af internationalt samarbejde under ledelse af den amerikanske sikkerhedsmyndighed.

Der er gennemført en sammenligning af beregninger af uheldsforløbet foretaget med de detaljerede koder og med MAAP. Sammenligningen viser kvalitativ overensstemmelse, men væsentlige kvantitative forskelle på vigtige punkter. Der er foreslået visse modifikationer af programmerne. Væsentlige forbedringer vil kun kunne opnås ved at sammenholde beregninger med vel karakteriserede eksperimenter.

Det kan konstateres, at den generelle forståelse af de grundlæggende fænomener anses for at være tilstrækkelig til sit formål, nemlig at vurdere reaktorindeslutningens integritet samt effekten af modforholdsregler. Resultaterne af beregninger med MAAP såvel som med andre programmer til uheldsberegninger må imidlertid behandles med varsomhed og tolkes med indsigt.

Kemiske og fysiske beregningsmodeller

Kemiske fænomener og processer behandles i MAAP ud fra forud fastlagte antagelser om de stoffer, der optræder under uheld. I et delprojekt under SIK-2 udvikledes og afprøvedes forbedrede modeller for den kemiske opførsel. Afprøvningen viste betydelig forskel ved transporten af radiologisk vigtige stoffer i reaktortanken og indeslutningen afhængigt af hvilke antagelser, der var gjort i de grundlæggende modeller.

Under uheldsforløb vil nogle af de kemiske stoffer, hvoraf en del er radioaktive, forekomme som aerosoler i reaktortankens og indeslutningens atmosfære. I et af delprojekterne undersøgtes modeller og koder til

beskrivelse af aerosoltransport. Konklusionen var, at de grundlæggende fænomener er velkendte og godt modellerede, men at kendskabet til aerosolers opførsel i komplicerede geometrier samt vekselvirkning imellem kemiske og fysiske fænomener kan forbedres.

Bistand til havarihåndtering

Havarihåndtering er et udtryk, der benyttes til at betegne menneskelige indgreb og procedurer til at begrænse ulykker. Forebyggende havarihåndtering søger på et tidligt tidspunkt at genoprette kølingen af kernen for at forhindre, at ulykken udvikler sig til noget mere alvorligt. Konsekvenslindrende havarihåndtering har til formål at mindske virkningerne på omgivelserne, når et alvorligt havari allerede er indtruffet.

Selvom man ikke kan forudse alle potentielle uheldsforløb, kan man formulere almindelige principper og regler for havarihåndtering. Under SIK-2 er der påbegyndt et delprojekt, der går ud på at udvikle et datamatisk system til havarihåndtering som støtte for driftspersonalet i uheldssituationer. Et forslag til prototype er blevet udarbejdet, og nogle simuleringsprogrammer er taget i brug. Hidtidige erfaringer tyder på, at projektet vil kunne gennemføres.

Reaktorer i nabolande

Der er samlet information om reaktorudformning og sikkerhedssystemer for 14 reaktorer beliggende i nærheden af de nordiske lande. Otte reaktorer ligger i Rusland, to i Litauen og fire i Tyskland.

Fire af de russiske reaktorer er trykvandsreaktorer af VVER typen i kernekraftværket i Kola ca. 120 km fra den finske grænse og 220 km fra Norge. De fire andre er kogendevandsreaktorer af typen RBMK i Sosnovy Bor nær St. Petersborg, ca. 100 km fra Finland. De er af samme type som den havarerede reaktor i Tjernobyl.

To reaktorer af hver type er af ældre model, og de øvrige to er anden generations reaktorer. De ældre reaktorer har tydeligvis dårligere sikkerhedsegenskaber, end hvad der er standard i den vestlige verden. Anden generations reaktorerne har bedre sikkerhedssystemer, der i visse henseender er sammenlignelige med dem i vesten.

De to reaktorer i Ignalina i Litauen (450 km fra Gotland) er RBMK reaktorer af anden generation. Efter ulykken i Tjernobyl er der ligesom i andre RBMK reaktorer indført sikkerhedsforbedrende foranstaltninger. Sikkerheden forbedres til stadighed ligesom i de andre omtalte russiske reaktorer.

De tyske reaktorer, der indgår i datasamlingen, ligger alle nær Hamborg ved Elbens nedre løb ca. 100 km fra den danske grænse. To er kogende-

vandsreaktorer, og to er trykvandsreaktorer. Sikkerhedsforholdene svarer til vestlig standard, når den er bedst.

Skibsreaktorer

Det er velkendt, at nukleart drevne isbrydere og undervandsbåde opererer i farvande nær de nordiske lande. Derfor er der også indsamlet tilgængelig information om konstruktion og sikkerhedsforhold ved skibsreaktorer. Offentliggjort information om havarier på nukleart drevne undervandsbåde er gennemgået og kommenteret.

Konklusioner

Metodikken ved probabilistisk sikkerhedsanalyse er udvidet til at omfatte vurdering af sikkerhed ved drift og vedligehold. Levende PSA muliggør en mere effektiv indsamling af driftserfaringer og forbedring af forskrifterne for sikker drift. Levende PSA og sikkerhedsindikatorer vil kunne give en væsentlig hjælp til sikkerhedsvurdering og beslutningstagning i sikkerhedsspørgsmål, når det gælder drift og vedligeholdelse af reaktorer. Det er imidlertid nødvendigt med yderligere arbejde for at videreudvikle disse hjælpemidler og tage dem i anvendelse ved kernekraftværkerne.

Der er opnået væsentligt bedre kendskab til de grundlæggende fænomener og processer ved alvorlige ulykker og deres videre forløb i reaktortank og indeslutning. De beregningsprogrammer, der nu findes i Sverige og Finland anses for tilstrækkelige til at dække de nuværende behov. Dette betyder dog ikke, at fortsat forskning er overflødig. Der findes fortsat problemområder, som bør studeres nærmere. Der synes således også i fremtiden at være behov for en nordisk opfølgning af internationale fremskridt.

Den indsamlede information om sikkerhedsforholdene ved reaktorer i lande, der grænser op til de nordiske lande, dækker det øjeblikkelige behov hos de nordiske sikkerhedsmyndigheder. Informationen må imidlertid jævnligt opdateres så der tages hensyn til løbende og planlagte ændringer og til forholdsregler, der sigter imod en forbedring af sikkerheden i specielt de russiske reaktorer.

Yhteenveto

Ydinvoimalaitoksen turvallisuus perustuu laitostyypin perusominaisuuksiin, laitoksen teknisiin turvallisuusratkaisuihin ja käytön turvallisuuteen. Turvallinen käyttö vaatii, että reaktorin teho on hallinnassa, sydän pysyy jäähdytettynä ja fissiotuotteet pysyvät polttoainesauvojen sisäpuolella. Jos nämä ehdot eivät täyty, on vaarana sydämen vaurioituminen ja radioaktiivisten aineiden leviäminen ympäristöön.

Reaktorisydämen vaurioitumistodennäköisyys arvioidaan todennäköisyyspohjaisella turvallisuusanalysillä (PSA). PSA-tekniikkaa on kehitetty ja sovellettu 1970-luvun puolivälistä lähtien. Sydämen vaurioitumisen eteneminen ja sulaneen sydämen käyttäytyminen lasketaan deterministisin menetelmin. Näiden niin sanottujen vakavien reaktorionnettomuuksien laajamittainen tutkimus aloitettiin vuoden 1979 TMI-2-onnettomuuden jälkeen. Tshernobylin onnettomuus vuonna 1986 paljasti, että Pohjoismaissa ja muissa länsimaissa vain vähän tietoa tämän reaktorityypin ominaisuuksista ja turvajärjestelmistä.

Todennäköisyyspohjainen turvallisuusanalyysi, vakavien onnettomuuksien laskentamenetelmät ja lähialueiden reaktorien turvallisuusominaisuudet olivat tärkeimmät yhteisen tutkimuksen kiinnostuksen kohteet, kun SIK-tutkimusohjelma käynnistettiin vuonna 1990. Ohjelma jaettiin kolmeen pääprojektiin, yksi jokaiselle tutkimuskohteelle.

Elävä PSA

Todennäköisyyspohjaista turvallisuusanalyysiä on hyödynnetty pohjoismaisten ydinvoimalaitosten turvallisuustarkasteluissa 1980-luvun alkupuolelta lähtien. PSA:n etu on, että suuri määrä tietoa voidaan käsitellä systemaattisesti, ja että onnettomuusriski voidaan arvioida kvantitatiivisesti. Absoluuttisiin riskiarvioihin tulee kuitenkin suhtautua varauksselliseti, mikä johtuu PSA-menetelmien rajoituksista. Vaikka laitoksen turvallisuusarviota ei voida täysin perustaa PSA-tuloksiin, on PSA osoittautunut hyvin tehokkaaksi etsittäessä laitosten heikkoja kohtia ja vertailtaessa erilaisia turvallisuutta parantavia toimintoja.

Arvioiden pohjana on laitoksen keskimääräisen sydänvauriotaajuuden ilmaiseva PSA, jossa lähtötietoina on käytetty turvallisuuteen liittyvien järjestelmien ja laitteiden keskimääräisiä epäkäytettävyysarvoja. Laite voi myös olla pois käytöstä huoltotöiden johdosta. Käsite "elävä PSA, Living PSA, LPSA" on otettu käyttöön tarkoittamaan PSA:n laajennusta, jossa paremmin otetaan huomioon erilaiset epäkäytettävyystilanteet. Tuloksena on ajan tasalla oleva ja ajasta riippuva riskiarvio. Yleisenä käsitteenä elävä PSA tarkoittaa prosessia, jossa laitoskohtaista PSA-mallia pidetään yllä ja päivitetään jatkuvasti osana laitoksen ja viranomaisten jokapäivästä turvallisuustoimintaa.

SIK-1 projektissa on tutkittu LPSA-käsitettä laatimalla uusia menetelmiä ja soveltamalla niitä. Sovellustyö on vaatinut muutoksia järjestelmien ja komponenttien epäkäytettävyysmalleihin. Projektissa on myös määritelty mahdollisia sovellusalueita ja riskimittareita. Menetelmiä on sovellettu pohjoismaisten ydinvoimalaitosten tarpeisiin.

Joitakin tuloksia on jo voitu hyödyntää käytännössä. Pohjoismaisilla kiehutusvesireaktoreilla tapahtuneiden tilanteiden riskimerkitystä on selvitetty. On myös osoitettu, että LPSA-menetelmiä voidaan käyttää täydentämään laitoksen käyttöohjeita.

Lopullinen päämäärä LPSA-työlle on tukea ydinvoimalaitosten jokapäiväistä turvallisuustoimintaa. SIK-1 projektissa tehdyt tutkimukset ovat osoittaneet tämän mahdolliseksi. Lisätyötä tarvitaan mallien joustavuuden parantamiseksi ja mallien testauksen laajentamiseksi, ennen kuin ne voidaan ottaa jokapäiväiseen käyttöön voimalaitoksilla.

Turvallisuusindikaattorit

LPSA:n lisäksi voidaan laitoksen turvallisuusarvioita täydentää käyttämällä ns. turvallisuusindikaattoreja. Turvallisuusindikaattorit ilmaisevat tiiviissä muodossa laitoksen tilan. Niiden odotetaan antavan etukäteisvaroituksen mahdollisista ongelmista. Toisaalta niillä voidaan seurata käytön aikaisen turvallisuuden paranemista.

SIK-1 projektissa on esitetty perusteet indikaattorijärjestelmälle. Järjestelmän perustana on seurata laitoksen päästöjä ehkäiseviä esteitä: polttoainetta, reaktoripiiriä ja suojarakennusta.

Indikaattorit hyödyntävät laitoksen tiedonkeruujärjestelmistä saatavaa informaatiota, josta poimitaan tarvittava tieto ja muokataan se indikaattoreille sopivaksi. Tähän tarkoitukseen on projektissa kehitetty ja testattu tietokonepohjaisia menetelmiä. Joitakin indikaattoreita on ehdotettu sovellettavaksi käytäntöön.

Riskipohjainen päätöksenteko

Turvallisuus perustuu olellisesti laitoksen ominaisuuksien, käytön ja kunnossapidon pohjalta tehtäviin riskiarvioihin ja näiden perusteella tehtäviin laitoshenkilökunnan ja turvallisuusviranomaisten päätöksiin. Päätöksentekoteoria voi antaa tukea ja ohjeita käytännössä usein monimutkaisiin päätöksentekotilanteisiin.

Päätöksentekoteoriaa on sovellettu tekemällä esitutkimus, jossa esimerkkitapauksena oli turvallisuusteknisistä käyttöehdoista poikkeaminen ruotsalaisella kiehutusvesilaitoksella. Päätöksentekotilanteen mallintamiseen käytettiin kahta toisistaan riippumatonta lähestymistapaa. Tutkimuksella saatiin arvokasta kokemusta päätöksenteon päämäärien ja kriteerien ryhmittelemiseksi. Se johti kuitenkin osittain ristiriitaisiin tuloksiin ja osoitti jatkotutkimukset tarpeellisiksi.

Päätöksentekoon liittyy usein epävarmuuksia. PSA:n epävarmuusanalyysille on kehitetty uusi menetelmä, ja sitä on sovellettu esitutkimuksen yhteydessä.

Vakavien reaktorionnettomuuksien etenemistä laskevat tietokoneohjelmat

Mahdollisten vakavien onnettomuuksien kulku lasketaan tietokoneohjelmilla, jotka kuvaavat sydämen vaurioitumisen ja sulan sydänmateriaalin käyttäytymisen paineastiassa ja suojarakennuksessa. Laskennassa on käytetty kaksivaiheista lähestymistapaa, missä onnettomuuden yleinen kulku lasketaan helppokäyttöisillä, yksinkertaisemmilla ohjelmilla ja yksityiskohtaisia ohjelmia käytetään osaprosessien selvittämiseen. Pohjoismaissa tavallisimmin käytetty työkalu onnettomuuden yleisen kulun laskentaan on MAAP-ohjelma, joka on kehitetty Yhdysvalloissa ja muunnettu pohjoismaisille ydinvoimalaitoksille soveltuvaksi.

SIK-2 projektissa on otettu käyttöön ja testattu kaksi uutta vakavien onnettomuuksien laskentaohjelmistoa: MELCOR ja SCDAP/RELAP5. Ohjelmat on kehitetty Yhdysvalloissa USNRC:n rahoituksella ja ne on saatu käyttöön Suomessa ja Ruotsissa osallistumalla USNRC:n koordinoimaan kansainväliseen CSARP-tutkimusohjelmaan.

Ohjelmien laskemaa onnettomuuden etenemistä ABB Atomin kiehutusvesireaktorin valikoiduille onnettomuustilanteille on verrattu MAAP-ohjelman tuloksiin. Ohjelmat antoivat yhteneviä ennusteita onnettomuuden yleispiirteistä, mutta erosivat joissakin tärkeissä yksityiskohdissa. Tämän perusteella on ohjelmiin suositettu parannuksia. Joidenkin kysymysten osalta on parannuksia mahdollista saavuttaa vain tekemällä hyvin karakterisoitua kokeellista tutkimusta.

Yhteenvetona voidaan todeta, että viime vuosina on tietämys perusilmiöistä kasvanut merkittävästi. MAAP-ohjelmaa pidetään riittävän tarkkana sen alkuperäiseen käyttötarkoitukseen. On kuitenkin todettava, että kaikkien tietokoneohjelmien ennusteisiin liittyy epävarmuuksia, joten niiden antamia tuloksia on tulkittava varovaisesti muuhun asintuntemukseen tukeutuen.

Kemiallisten ja aerosoli-ilmiöiden mallinnus

Kemiallisten ilmiöiden kuvaus MAAP-ohjelmassa perustuu etukäteisarvioon onnettomuuden aikana syntyvistä yhdisteistä. SIK-2 projektin osatehtävänä oli kehittää parannettuja kemiallisten reaktioiden malleja MAAP-ohjelmaan ja testata niitä. Vertailulaskut osoittivat, että eri alkuoletuksilla saatiin tulokseksi huomattavia eroja radiologisesti merkittävien aineiden kulkeutumisessa paineastiassa ja suojarakennuksessa.

Useimmat onnettomuustilanteissa vapautuvat kemialliset aineet muodostavat aerosoleja jäähdytysjärjestelmän ja suojarakennuksen ilmatilaan. SIK-2 projektissa arvioitiin eri aerosolimalleja ja niiden laskentaan kehitettyjä tietokoneohjelmia. Arvio osoitti, että aerosolien käyttäytymisen perusilmiöt ovat hyvin tunnettuja ja mallinnettuja. Parannuksia tarvitaan kuvaamaan aerosolien käyttäytymistä monimutkaisissa geometrioissa sekä aerosolien fysikaalisten ja kemiallisten ilmiöiden yhteisvaikutusten mallintamiseen.

Onnettomuustilanteiden tukivälineet

Onnettomuuden hallinnalla tarkoitetaan toimintaa, jolla on tarkoituksena lieventää ja rajoittaa onnettomuuden seurauksia. Onnettomuuden ehkäisyllä pyritään palauttamaan sydämen jäähdytys mahdollisimman aikaisessa vaiheessa, jotta merkittäviltä sydänvaurioilta vältyttäisiin. Seurausten lieventämisellä pyritään estämään tai vähentämään jo tapahtuneen onnettomuuden aiheuttamaa haittaa ympäristölle.

Vaikka kaikkia mahdollisia onnettomuustilanteita ei pystytä ennakoimaan, voidaan onnettomuuden hallinnalle kehittää yleisiä toimintaohjeita. Tutkimusohjelmassa on käynnistetty projekti, jossa kehitetään operaattorien tueksi tietokonepohjaista onnettomuuden hallinnan apuvälinettä. Järjestelmän prototyyppi on määritelty, ja osa simulointiohjelmistosta on otettu käyttöön. Ennakkoarviot viittaavat siihen, että lähestymistapa on toteuttamiskelpoinen.

Lähialueiden reaktorit

SIK-3 projektissa on kerätty sunnittelu- ja turvallisuuspiirteitä koskevia tietoja 14 Pohjoismaiden lähellä sijaitsevasta reaktorista. Näistä kahdeksan sijaitsee Venäjällä, kaksi Liettuassa ja neljä Saksassa.

Venäläisistä reaktoreista neljä on VVER-tyyppisiä painevesireaktoreita. Ne sijaitsevat Kuolassa, noin 120 km Suomen ja 220 km Norjan rajalta. Neljä on RBMK-tyyppisiä grafiittimoderoituja kiehutusvesireaktoreja Sosnovy Borissa, noin 100 km Suomen rannikolta.

Molemmista reaktorityypeistä kaksi on vanhempaa ja kaksi uudempaa mallia. Vanhempien reaktorien tekniset turvallisuusratkaisut eivät selvästikään vastaa länsimaisia kriteerejä. Uudempien tyyppien turvallisuus on parempi, joissakin suhteissa niiden turvallisuusjärjestelmät vastaavat länsimaisia.

Liettuan (450 km Gotlannista) kaksi Ignalinan reaktoria ovat toisen sukupolven RBMK-laitoksia. Tshernobylin onnettomuuden jälkeen niihin on lisätty, kuten kaikkiin muihinkin RBMK-reaktoreihin, turvallisuutta lisääviä ratkaisuja. Turvallisuusparannukset ovat edelleen käynnissä. Sama koskee myös kaikkia mainittuja venäläisiä laitoksia.

Mukaan otetut saksalaiset reaktorit sijaitsevat Elben alajuoksulla Hampurin lähellä, noin 100 km Tanskan rajalta. Niistä kaksi on kiehutusvesi- ja kaksi painevesireaktoreja. Niiden turvallisuus vastaa tavanomaisia länsimaisia standardeja.

Laivareaktorit

Ydinkäyttöiset jäänsärkijät ja sukellusveneet toimivat Pohjolan lähivesillä. Tämän johdosta kerättiin tietoja myös laivareaktorien turvallisuuspiirteistä. Lisäksi arvioitiin julkistettuja ydinkäyttöisten alusten onnettomuuksia.

Johtopäätöksiä

Todennäköisyyspohjaisen turvallisuusanalyysin menetelmiä on laajennettu käyttöturvallisuuden arviointiin. Elävän PSA:n avulla on mahdollista hyödyntää käyttökokemukset tehokkaasti sekä parantaa turvallisen käytön toimintaehtoja ja määräyksiä. LPSA-työkalut ja turvallisuusindikaattorit tulevat tukemaan merkittävästi ydinvoimalaitosten käytön ja kunnossapidon turvallisuushallintaa ja päätöksentekoa. Lisätyötä tarvitaan, jotta niitä voidaan parantaa otettavaksi käyttöön laitosten jokapäiväisessä toiminnassa.

Tieto vakavien sydänvaurioiden ilmiöistä ja niiden seurauksista jäähdytyspiirissä ja suojarakennuksessa on kasvanut huomattavasti viime vuosikymmenen aikana. Vakavien onnettomuuksien laskentaan Suomessa ja Ruotsissa käytettävät tietokoneohjelmat pystyvät ennustamaan onnettomuuksien yleisen kulun riittävällä tarkkuudella. Uuden tutkimuksen tarkoituksena on selvittää yksittäisiä ongelma-alueita entistä tarkemmin. Siksi jatkuva omaehtoinen tutkimus ja kansainvälisen kehityksen seuranta on Pohjoismaissa vastakin tarpeen.

Tietojen keruu lähialueiden reaktorien suunnittelu- ja turvallisuuspiirteistä on tuottanut riittävästi tietoa pohjoismaisten ydinturvallisuusviranomaisten nykytarpeisiin. Tietoja on päivitettävä ajoittain, jotta erityisesti venäläisillä laitoksilla tulevaisuudessa tapahtuvat laitosmuutokset ja turvallisuusparannukset voidaan ottaa huomioon.

NORDIC STUDIES IN REACTOR SAFETY

List of contents **Page**

NORDIC STUDIES IN REACTOR SAFETY

1 The SIK programme

An intensified cooperation in nuclear safety started sixteen years ago among the five Nordic countries: Denmark, Finland, Iceland, Norway and Sweden. While only Finland and Sweden have nuclear power plants in operation, there are many reactors in neighbouring countries. It was recognized to be of common interest not only to have unified views on the safety of the Nordic nuclear plants but also to maintain a high level of knowledge and preparedness in nuclear safety matters in all the Nordic countries, in order to facilitate the discussion of issues of common concern over the borders.

The fourth four-year Nordic research programme in nuclear safety during the period 1990-1993 was structured in four areas:

- Emergency preparedness
- Waste and decommissioning
- Radioecology
- Reactor safety

This report summarizes the achievements in the area of reactor safety. The research programme, which is known under the acronym SIK, can in large part be seen as a continuation of earlier Nordic research programmes in the areas of activity release in the reactor containment, and risk analysis and safety philosophy.

The objectives of the SIK programme were formulated as follows:

- contribute to a common basis for the assessment of reactor safety issues and for the exchange of information between the Nordic countries;
- follow and evaluate international research activities in the fields of safety analysis and severe accidents;
- define and demonstrate the practical use of advanced methods for safety evaluation;
- maintain and further improve the expertise on severe accident phenomena and calculational tools;
- collect and evaluate information on the safety design of reactors in neighbouring countries.

The SIK programme was divided into three separate projects:

SIK-1 Safety Evaluation by Use Living PSA and Safety Indicators

SIK-2 Severe Accident Research

SIK-3 Design and Safety Features of Nuclear Reactors in Neighbouring Countries.

SIK-1 is concerned with the probabilistic analysis of potential accidents and with methods for early warning of possible safety problems, as a means of monitoring and reducing the risk of severe core damage.

SIK-2 deals with the deterministic analysis of the progression and mitigation of severe accidents, as a means of assessing and minimizing the release of radioactive substances to the environment.

SIK-3 attempts to collect information on the safety design of foreign reactors for evaluation and information preparedness, should an incident or accident occur close to the borders of the Nordic countries.

The report starts with a brief overview of reactor safety research in the Nordic countries. In subsequent chapters, the state-of-the-art in each subject matter is highlighted as an introduction to the individual project summaries. The main findings of each project are emphasized. The report ends with overall conclusions and recommendations. Appendices on project organisation, reactor safety principles, and terms and abbreviations are attached.

For detailed information, reference is made to the final reports of the individual projects [1, 2, 3] and other NKS/SIK technical reports, listed at the end of the report.

2 Nordic reactor safety research

2.1 The Nordic scene

Nuclear power has demonstrated that it can supply large amounts of electricity efficiently and economically. In the beginning of 1993, 330 651 MW of nuclear power were installed in 424 reactors in 29 countries all over the world. They generated nearly 17 % of the world's electricity in 1992. The cumulated operating experience is approaching 6500 reactor years.

Only two of the Nordic countries have nuclear power plants in operation, Table 1. Finland has four plants with a total net capacity of 2310 MW, which in 1992 generated 18.2 TWh or 29 % of the country's electricity consumption. The corresponding figures for Sweden are 9916 MW, 60,8 TWh[1] and 44 %. All are light water reactors, eleven of which boiling water reactors (BWRs) of ABB Atoms design, and five are pressurized water reactors (PWRs).

Table 1 Nordic nuclear power plants

COUNTRY Plant	Type	Owner	NSSS Supplier	Power Gross/net MWel	Commercial operation
FINLAND					
Loviisa 1	PWR	IVO[1)]	Atomenergoexport	465/445	1977
Loviisa 2	PWR	IVO	Atomenergoexport	465/445	1981
TVO-I	BWR	TVO[2)]	Asea Atom[3)]	735/710	1979
TVO-II	BWR	TVO	Asea Atom	735/710	1982
SWEDEN					
Barsebäck 1	BWR	Sydkraft	Asea Atom	615/600	1975
Barsebäck 2	BWR	Sydkraft	Asea Atom	615/600	1977
Forsmark 1	BWR	FKA[4)]	Asea Atom	1006/968	1981
Forsmark 2	BWR	FKA	Asea Atom	1006/969	1981
Forsmark 3	BWR	FKA	Asea Atom	1197/1155	1985
Oskarshamn I	BWR	OKG[5)]	Asea Atom	462/442	1972
Oskarshamn II	BWR	OKG	Asea Atom	630/605	1975
Oskarshamn III	BWR	OKG	Asea Atom	1205/1160	1985
Ringhals 1	BWR	Vattenfall	Asea Atom	825/795	1976
Ringhals 2	PWR	Vattenfall	Westinghouse	905/875	1975
Ringhals 3	PWR	Vattenfall	Westinghouse	960/915	1981
Ringhals 4	PWR	Vattenfall	Westinghouse	960/915	1983

1) Imatran Voima Oy
2) Teollisuuden Voima Oy
3) Now ABB Atom
4) Forsmarks Kraftgrupp Aktiebolag
5) Oskarshamns Kraftgrupp Aktiebolag

[1] The nuclear electricity production was 17 % less than previous year (1991) due to the forced shutdown of five reactors from 17 September 1992.

Denmark and Norway have no nuclear power, but both have research reactors in operation and foreign nuclear power plants close to their borders, see Figure 2. Foreign plants of particular concern are the Russian-built reactors at Kola (two units of the older type VVER 440/230 and two of a newer type, distance to the borders of Norway and Finland 220 and 120 km), at Sosnovy Bor near St Petersburg (two units of an older and two of a newer RBMK type, distance to the border of Finland 100 km), and at Ignalina, Lithuania (two newer RBMK units, 450 km from the Swedish island of Gotland).

The nuclear utilities are directly responsible for the safe operation of the nuclear power plants. The nuclear safety activities are regulated and supervised by government authorities: STUK (Finnish Centre for Radiation and Nuclear Safety) in Finland, and SKI (Swedish Nuclear Power Inspectorate) and SSI (National Institute of Radiation Protection) in Sweden. The corresponding organizations in Denmark are the Danish Emergency Management Agency and the National Institute for Radiation Hygiene, and in Norway the Norwegian Radiation Protection Authority.

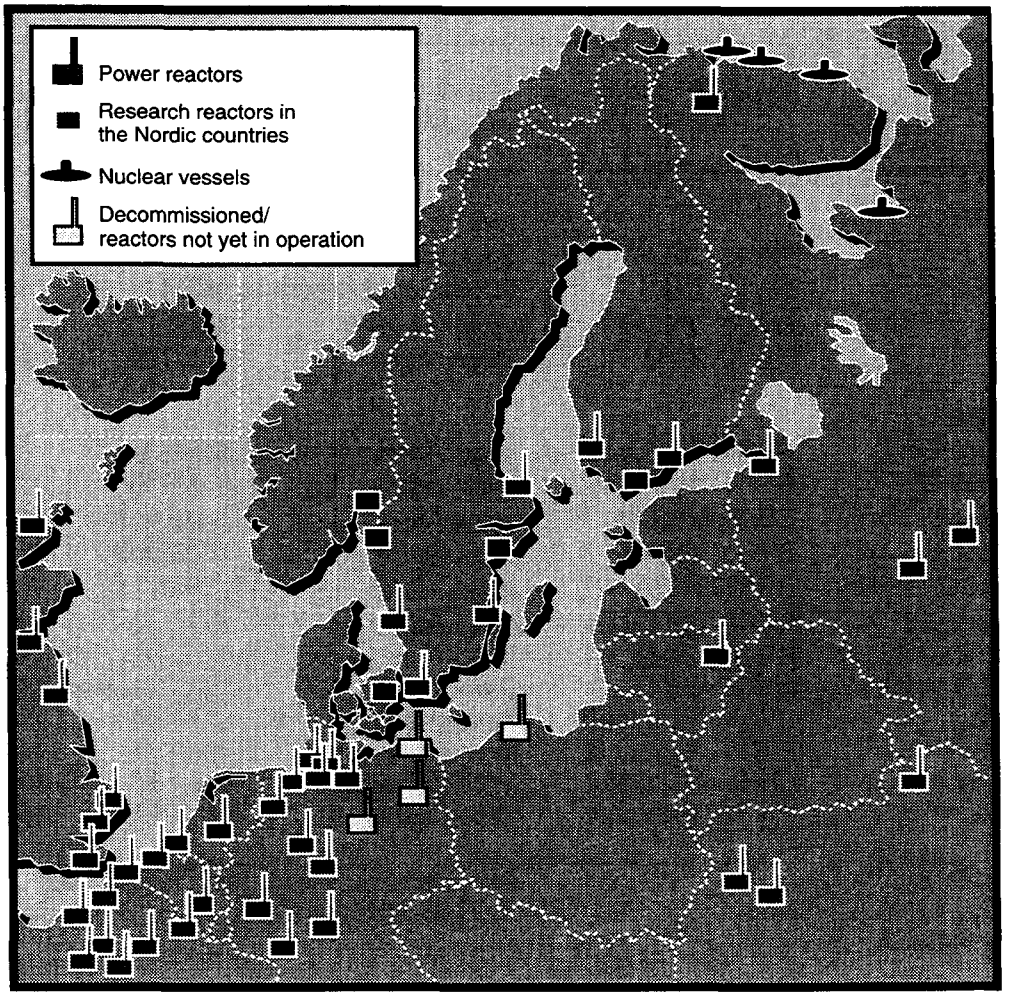


Figure 2 Nuclear reactors in the Nordic and neighbouring countries

2.2 *Denmark*

There is no coordinated research programme in reactor safety in Denmark. Separate studies are carried out at the Risø National Laboratory. The Danish Nuclear Inspectorate together with Risø and the Department of Reactor Physics of the Technical University of Denmark are participating in a "knowledge-preparedness group", which has collected information on the safety of nuclear installations in neighbouring countries and on advanced reactors.

2.3 *Finland*

Most of the Finnish reactor safety research financed by public means is currently performed in two national programmes for 1990-1994:

- Systems behaviour and operational safety
- Structural safety of nuclear power plants

The programmes are mainly financed by the Ministry of Trade and Industry. Other major contributors are the Technical Research Centre of Finland (VTT) and the Finnish Centre for Radiation and Nuclear Safety (STUK). The nuclear utilities participate in the funding in addition to carrying out several self-financed research projects. The total budget for the 1990-1994 period is FIM 120-130 million for the programme on systems behaviour and operational safety, and FIM 65-70 million for the programme on structural safety. Most of the publicly financed research takes place at VTT, but other research institutes, universities and STUK are also involved.

The research programme on *systems behaviour and operational aspects of safety* focuses on transient and accident management, development of nuclear plant analysers and probabilistic safety analysis. Studies of nuclear fuel and reactor core concentrate on fuel high burnup behaviour, VVER fuel experiments, and reactor core behaviour in complex reactivity transients.

Experimental work on thermal hydraulics has focused on VVER reactor geometry. A series of experimental facilities with increasing scale and complexity has been built and operated since the mid-1970s. The latest PACTEL facility models the Loviisa plant in a volumetric scale of 1:305 preserving full height. Validation of accident analysis codes has been carried out by participation in a large number of international standard problems. The severe accident research work has largely relied on international cooperation for acquisition of computer codes and for obtaining relevant experimental data. Major emphasis has been put on verifying the suitability of the computer codes for Finnish nuclear power plants.

The novel APROS (Advanced Process Simulator) process simulator environment has been used for developing comprehensive and detailed nuclear plant analysers for efficient safety analysis. Other applications of the APROS system include enhancing the training of technical and operational staff, support of the process and automation design, and evaluation of new nuclear and conventional thermal power plant design.

The research programme on *structural safety of nuclear power plants* concentrates on factors affecting the mechanical properties of reactor pressure boundary materials. Such areas include irradiation embrittlement and recovery of reactor pressure vessel materials, methods for determining neutron fluence, material degradation rates and mechanisms, and monitoring of water chemistry during reactor operation.

Much effort has been devoted to monitoring the pressure vessel of the Loviisa unit 1. Hot cell testing of irradiated surveillance samples has provided a large material property data base which is continually being expanded. More accurate non-destructive testing methods and procedures have been developed, in particular for applications in which traditional NDE methods are not well suited.

The safety authority STUK has a research programme, partly related to the national programme. The most important research areas are reactor physics and dynamics analysis, fire safety, licensing of software-based reactor protection systems, and irradiation embrittlement of Loviisa 1 reactor pressure vessel.

The work in the PSA area has been mainly done and financed the IVO and TVO utilities. STUK has developed a fast PSA code for communication with the utilities. TVO has actively participated in the development and testing of the code.

2.4 *Norway*

The reactor safety research in Norway is connected to the OECD Halden Project, operated by Institutt for energiteknikk, the national research institute for energy and nuclear research. The Halden Project is a collaborative venture of national safety authorities, research institutes, utilities and manufacturing industries in 14 OECD countries.

The technical programme focuses on two main areas: fuel and materials testing, and information technology. The thermal and mechanical properties of reactor fuel are studied during irradiation tests under a wide range of operating conditions. Current research addresses separate effects as well as the integral behaviour of high-burnup fuel. The corrosion properties of different alloys are studied under controlled water chemistry and thermohydraulic conditions.

A central part of the development work in the area of information technology is the application of full-scale process simulators for nuclear power plants, coupled to an advanced experimental control room. Special emphasis is being placed on the design and testing of the man-machine

interface. An integrated supervisory and control system has been implemented. Various advanced alarm methods are studied. Diagnostic and advisory systems utilizing knowledge-based technology are being developed.

2.5 *Sweden*

A large part of the reactor safety research is carried out under the direction of SKI and is financed by annual fees from the nuclear utilities. The budget for fiscal year 1992/93 was SEK 65 million. Most of the research is carried out by universities, research institutes and consulting firms, often in international cooperation.

Research in the area of *man-technology-organisation* was initiated in the mid-1980s. Studies have been carried out for example for control room evaluation, operator procedures, operator training, and emergency preparedness.

The *materials* research is concentrated on three main areas: (i) corrosion and its dependence on water chemistry, irradiation and aging, (ii) fracture mechanics, notably crack formation and crack propagation in stress corrosion, and (iii) methods for non-destrutive testing.

The research on *reactor fuel* is to a large extent carried out in international cooperation in the OECD Halden project and is mainly directed to the irradiation behaviour of the fuel and its interaction with the can as well as to corrosion issues.

The emphasis in *thermohydraulics* research has shifted from large-scale experiments and code development to validation of more realistic models and application studies, including the analysis of other operating conditions than normal full-power operation, e.g. shutdown states and power transients with operator intervention, and to the analysis of reactor instabilities.

The *severe accident* research has been carried out in a series of projects in close cooperation between the authorities and the utilities. It has included participation in international research programmes on degraded fuel and core melt behaviour and the release and transport of radionuclides. Analytic capabilities have been acquired and applied to the design of systems and procedures for accident mitigation.

The research in *safety analysis* is based on the use of probabilistic safety analysis (PSA). Methods have been developed for the estimation of core damage frequencies (PSA level 1) and applied in the recurrent safety reviews of the nuclear power plants, prescribed by the authorities. The methods are further developed to include PSA level 2 and external events.

The nuclear utilities have substantial research programmes under their own management and funding. The total cost of safety-related research is estimated at SEK 50 million per year. The research is mainly directed to operational safety and fuel research, partly in cooperation between the utilities and with other national and international organizations.

The utilities jointly own the Nuclear Training and Safety Center (KSU). The main activities of KSU include the feedback of operating experience, operator training and education. Information on operational events in reactors all over the world is systematically collected, evaluated and disseminated. KSU also operates full-scope simulators for both boiling and pressurized water reactors for training.

3 Living PSA and safety indicators (SIK-1)

3.1 Operational safety

3.1.1 Rules and procedures

The *technical specifications* (TS) for safe plant operation consist of operating rules and limits for assuring safety during operation. They allow a certain flexibility for the operator to achieve optimum plant conditions, notably a high plant availability. The TS are formulated by the licensee and submitted to the licensing authority for approval before operation is permitted. The TS include:

- Bounding values for essential safety-related parameters. If the bounding limits are exceeded, a special investigation and report to the safety authorities is required before operation is resumed.

- Conditions for plant operation with regard to the functional preparedness of standby systems and components. If the conditions cannot be fulfilled, restrictions of operation are imposed and restoring measures required in each particular case.

- Type and frequency of testing and inspection of components and systems. If the prescribed testing is not carried out or if negative results are obtained, the component or system is considered to be out of service, resulting in restrictions of operation.

- Rules to be followed during normal operation as well as in abnormal situations and during maintenance outage.

- Requirements on the documentation and reporting of operational events and design modifications.

The TS are based mainly on deterministic analyses and technical judgment. They are updated to take into account new experience and plant modification. A general rule stipulates that the plant should be retained in or brought to a safe condition in any unclear situation which cannot be immediately diagnosed.

Detailed plant operation and maintenance activities are governed by written instructions and work orders. A duty engineer is always in service at each plant for advising the control room crew on safety matters. The duty engineer takes on special responsibilities in case of emergency.

The technical specifications include instructions for plant operation during accidents within the design bases. The procedures are trained and retrained on full-scale plant simulators. The rules are traditionally event-oriented which means that they are based on the diagnosis and predicted progression of the design basis accidents.

After the accident at Three Mile Island, guiding instructions have been developed also for accidents beyond (the) design (bases), i.e unexpected events that the safety systems fail to or are not designed to control. These *emergency operating procedures* are usually symptom-oriented and aim at securing the basic safety functions of controlling the power, maintaining adequate core cooling, and minimizing radioactive releases.

The emergency operating procedures are essentially rules for *preventive accident management*. The objective is to maintain a coolable core configuration, thereby avoiding severe core degradation, which can lead to loss of reactor pressure vessel integrity. The procedures are based on best-estimate predictions of beyond-design events and can to a certain extent be trained on full-scale simulators.

If core melting cannot be prevented, accident management measures are directed to maintaining the integrity of the reactor containment in order to minimize radioactive releases to the environment. This is known as *mitigative accident management* and may include action for cooling the core melt outside the reactor pressure vessel, for hydrogen control in the containment, and for filtered containment venting

3.1.2 Performance and safety indicators

The performance of a nuclear power plant is continuously monitored and displayed in the control room. According to the technical specifications, all safety-related events must be communicated to the supervisory authority. All outages must be reported and the reason for the outage stated, e.g. automatic reactor shutdown (scram) or turbine trip. Plant-specific information on safety-related events is stored and processed in computerized data bases and exchanged among nuclear utilities and safety authorities in international networks.

General information of plant performance is also collected and disseminated internationally. Uniform definitions of *performance indicators* have been adopted. They are used for monitoring the progress in maintaining a high level of safety and a high reliability of energy production, by minimizing outage times, reducing unplanned scrams, and reducing the unavailability of safety system components.

Although the performance indicators are considered to have a positive correlation with safety performance, they are not suitable for the daily management of operational safety. For this purpose more detailed *safety indicators* are needed. They should give the operator and technical support staff as well as the safety authorities early warning of impending safety problems, for example by keeping track of the reliability of safety functions, the effectiveness of maintenance activities as well as of human and organisational performance.

Significant progress has been made in recent years in establishing internationally accepted plant performance indicators. The World Association of Nuclear Operators (WANO) has adopted a set of ten

overall performance indicators which are used since 1990 by nuclear plant operators worldwide. One of the indicators is safety system performance.

The purpose of the safety system performance indicator is to monitor the readiness of important safety systems to respond to off-normal events and accidents. Three safety systems each for PWRs and BWRs are selected to be monitored. The performance indicator is calculated separately for each of the three PWR systems and each of the three BWR systems.

The performance indicator is defined for each system as the sum of the unavailabilities, due to all causes, of the components in the system during a time period, divided by the number of trains in the system.

Some concern has been raised about covering the many aspects of plant safety by the WANO indicators. Accordingly, efforts are being made to find indicators that are better suited for safety management. NRC has developed a logic model which encompasses some of the key contributors to plant safety. The safety indicators are structured to cover not only safety system unavailablities but also plant disturbances and human and organizational performance.

The IAEA has been involved in the development of safety indicators for use within its OSART (Operational SAfety Review Teams) programme. The IAEA has also sponsored workshops to outline approaches for the quantitative assessment of operational safety performance. One of the recommended approaches was to use methods that directly measure risk, such as indicators based on PSA techniques. It was also concluded that safety indicators should be developed which provide early warning of declining safety.

It is generally agreed that performance and safety indicators are important tools for use by plant and regulatory staff in maintaining a high level of safety and making decisions on possible actions for safety improvement.

3.2 PSA methods development and application

PSA has become a standard technique to further improve the safety of nuclear power plants. At present more than 200 PSAs have been carried out. The studies usually focus on the identification of risk contributors and the assessment of plant modification and backfitting options. Other applications, such as those supporting plant operation by living PSA, are rapidly growing.

Individual PSA studies differ in scope and structure. Comparative studies have shown significant differences in models and assumptions. This requires that absolute values of integral PSA estimates, such as core damage frequencies, be treated with caution.

3.2.1 Methodology

The PSA methodology, Figure 3, is well developed although problems and limitations still exist. Some of them are intrinsic, while others are matters of practice and can be reduced or resolved by further research and experience. The problems include incompleteness, lack of consistency, inadequate data bases, difficulties in modelling human and organisational behaviour, and certain less obvious dependences [4].

Incompleteness results from the impossibility of identifying, modelling and quantifying all potential accident sequences. It can be reduced by experience and careful review but never completely eliminated. While new accident sequences are still being identified, it is unlikely that significant sequences are overlooked, due to the systematic way in which current analyses are made.

Basic information on the frequency of initiating events and the reliability of components and humans will always be more or less uncertain, although data are continuously improving by experience and measurement [5]. The uncertainties propagate through the fault tree and contribute to the uncertainty of the end result.

Plant systems are designed and operating rules formulated with the abilities and limitations of humans in mind. Nevertheless, experience has shown that human error is a significant contributor to the initiation and propagation of incidents and accidents. On the other hand, human initiative and action is of decisive importance for recovery actions in accident situations.

Available data for predicting human action apply only to well-structured tasks. Obviously, all human behaviour cannot possibly be accounted for in PSA, such as knowledge-based behaviour. This an important reason why overall safety cannot be judged solely by PSA.

The determination of system requirements, notably the minimum configuration of systems for the successful performance of a particular safety function, as well as the interdependence between front-line and support systems is of particular concern in PSA. Dependent failures or common cause failures (CCF) tend to increase the frequency of multiple, simultaneous failures. Redundant systems are particularly susceptible to CCF. A typical common cause initiator (CCI) is loss of power. Other important CCIs are caused by internal fires and floodings. An example of a less predictable CCI is component ageing. Many models have been suggested for the treatment of CCF, and the area is still in development.

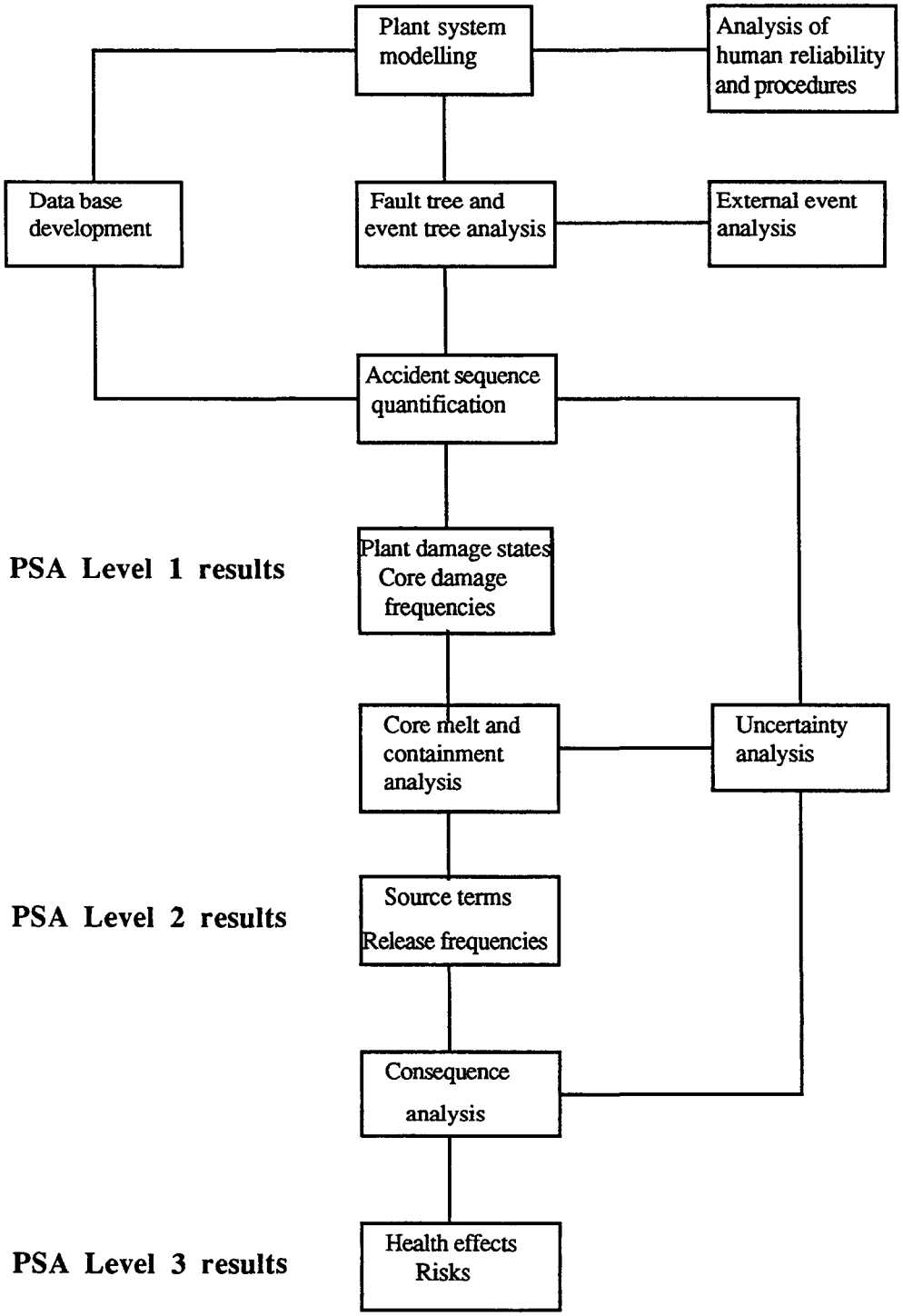


Figure 3 Probabilistic safety assessement procedure

Most of the current PSA studies are on level 1. Although PSA level 2 addresses the important aspect of containment integrity, i.e. the ability to retain the radioactive substances, it has so far been applied less often. The physical phenomena and the course of events in the containment are subject to considerable uncertainties, which makes the analysis difficult. New approaches and methods are being applied to overcome these difficulties [6].

The advantage of PSA is that it integrates a broad spectrum of information from different fields such as plant design, operating experience, component reliability, human behaviour and accident phenomena. Further development of the methodology requires increased specialization. While there is as yet no generally accepted approach to the design and use of PSA, a certain degree of maturity has been reached. This is shown, for example, by the use of common data bases and standard fault tree code packages. The development of powerful modern computers has made it possible to run complete level 1 PSAs in a short time at practically no computing cost.

3.2.2 Application

PSA level 1 is used to an increasing extent for safety design assessment in order to identify significant risk contributors and provide a basis for safety improvement. For example, PSA results are successfully used for comparing various options and selecting the best solution for a particular safety-enhancing measure.

The end result of PSA level 1 is a measure of risk in terms of estimated core damage frequencies for nominal operating conditions. Most of the analyses consider only "internal" events, i.e. occurrences within the plant itself. The studies are extended to cover "external" events, such as earthquakes. Fires and flooding within the plant are usually also, somewhat inconsistently, regarded as external events.

The basic PSA studies are updated to take into account plant modifications and operating experience. Other operating regimes than full power are also being considered, such as refuelling and maintenance outage, shutdown and startup. Experience from incidents and PSA studies indicate that the risk contribution from such alternative operating modes is of the same order of magnitude as that from full power operation.

The scope of analysis is being extended to include PSA level 2. This reflects a trend of specifying probabilistic safety goals in terms of release frequencies of important radionuclides rather than in terms of core damage frequencies. PSA level 3 studies of health effects appear less urgent for the time being. Comparison of health risks from nuclear power with those from other man-made or natural activities, which was the original objective of the Rasmussen study, remains a controversial use of PSA results.

The regulatory authorities are using PSA as a tool for safety assessment and decision making. In Sweden, PSA forms an integral part of periodic reviews which are undertaken for each of the nuclear power plants every 8 - 10 years [7]. The first round of PSA level 1 studies has been completed. As a result, some safety-enhancing measures were implemented. The studies were subjected to a comprehensive review which suggested methodological improvements for future analyses.

In Finland, PSA level 1 studies have been performed and reviewed for all plants. A regulatory guide on the use of PSA in the design and operation of nuclear power plants was issued in 1987. A regulatory PSA code has been developed to support the requirements of the guide [8]. The code is shared by the nuclear utilities to promote the efficient use of PSA models and the associated plant-specific data base.

The PSA studies are mostly carried out by the nuclear utilities, who are directly responsible for plant safety. The utility application of PSA is being extended to include aspects of operational safety and plant maintenance. The term "living PSA" has been coined to designate a day-to-day safety management system, based on a plant-specific PSA and a supporting information system.

The various stages in the application of PSA are illustrated in Figure 4.

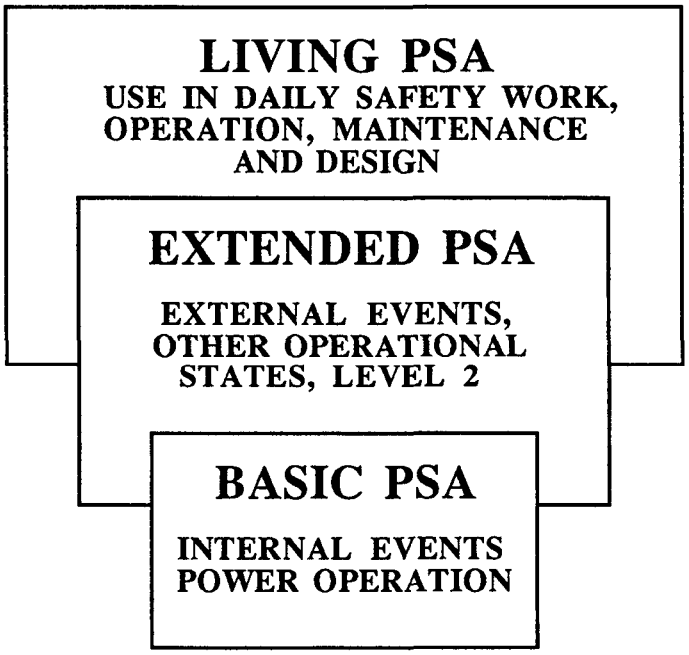


Figure 4 Different phases of PSA application

An example of the application of living PSA is the study of possible modifications of the technical specifications, carried out in the previous Nordic research programme on reactor safety [9]. It was shown that PSA can be used to compare optional schemes for plant operation during fault conditions and to identify the scheme with least probability that a safety function is unavailable when needed. It was also demonstrated that PSA can be used to justify changes in the rules for preventive maintenance in safety systems during plant operation, and to enhance the efficiency of surveillance tests on standby equipment and redundant subsystems.

A survey of the international development of living PSA and safety indicators, published in 1992 within the SIK-1 project [10] identified a growing interest in living PSA applications.

The most advanced living PSA application at present seems to be the Essential Systems Status Monitor (ESSM) at the Heysham 2 plant in the United Kingdom [11]. The ESSM is a computerized facility for monitoring the safety status of the plant and for planning risk-based maintenance.

Other living PSA application includes the Probabilistic Safety Information Management System (PRISIM) at the Arkansas Nuclear One-Unit 1 plant [12]. The system contains pre-processed information from baseline PSA results, which allows assessment of changes in plant safety caused by changes in plant conditions.

A methodology to monitor, on a monthly basis, the core damage frequency due to the operation of the River Bend Nuclear Station, USA, has been developed and implemented at the plant [13]. River Bend is a 934 MWel General Electric Mark III BWR which began commercial operation in 1986.

A Risk Monitor is being developed at the Gesellschaft für Reaktor-sicherheit (GRS) in Germany [14]. The aim is to support day to day decisions regarding system configuration and test and repair strategy by keeping decision makers informed of the actual increased risk level from random or planned component unavailabilities and providing advice on actions to restore the plant to nominal risk levels.

3.3 Objectives and structure

The results and recommendations of the joint Nordic research programmes on the optimization of technical specifications [9], and on PSA methods and uncertainties [15], carried out during 1985-1989, are the basis of the present SIK-1 project.

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 effective improvements in operational safety" [16].

A conceptual idea of using living PSA and safety indicators is illustrated in Figure 5. It is based on using plant-specific technical and operational information with living PSA and safety indicators for monitoring the safety status of the plant in support of safety-related decision-making.

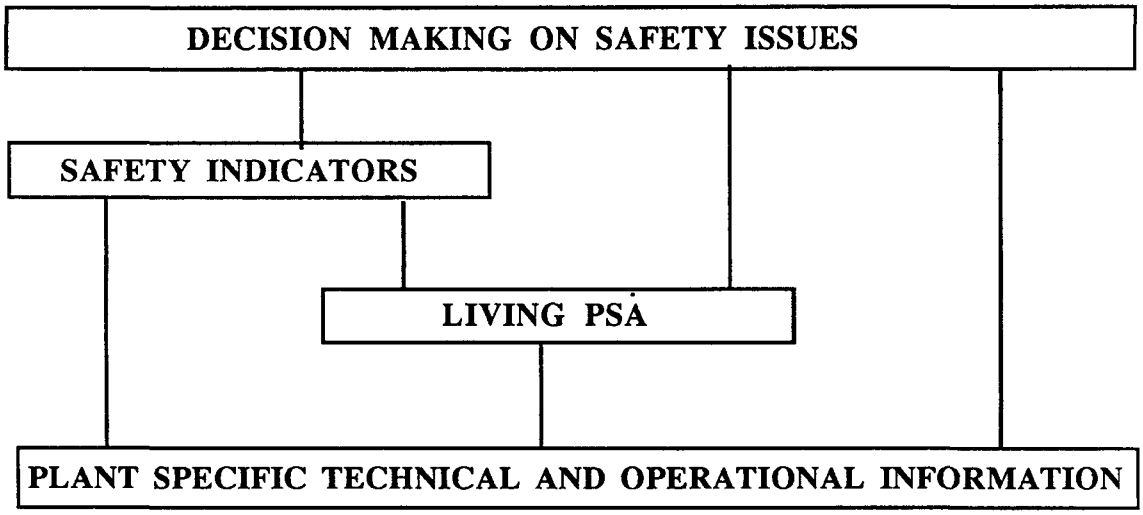


Figure 5 Conceptual idea of using living PSA and safety indicators

A survey of Nordic experiences and views on living PSAs and safety indicators was undertaken in 1990 [17]. Information was obtained from utilities, safety authorities, research institutes and consultants in the Nordic countries.

Based on the survey, a workplan for the project was drawn up for three main task areas, each containing a theoretical and conceptual part and practical application studies:

- Living PSA development and application
  - Definition of a living PSA concept
  - Case studies:
    Risk follow-up
    Risk monitoring

- Safety indicator development and use
  - Definition of an indicator system
  - Case studies:
    Pattern and trend analysis
    Unavailability and maintenance-related indicators

- Risk-based decision making
  - Uncertainty analysis in PSA
  - Pilot studies on exemption from technical specifications

3.4 Living PSA development and application

3.4.1 A living PSA concept

The living PSA concept developed in the SIK-1 project includes the outline of a system and the definition of application areas [18,19]. The system consists of a plant-specific PSA model and a plant status information system, integrated in a computerized user tool. The concept is illustrated in Figure 6.

Model development

Basic PSA uses average unavailabilities for safety-related components and systems to estimate a nominal risk. Living PSA attempts to use actually known or inferred information of component status and system configuration, which usually results in time-dependent unavailabilities and a variable instantaneous risk. This distinction is the fundamental difference between basic and living PSA.

In many cases, information of component status can be obtained by testing. For the time being, a parametric linear time-dependent model is suggested to represent the basic unavailability of standby components. If a failure is detected during testing or the component is in maintenance, the unavailability is set at 1.

Time-dependent unavailabilities and common cause failures (CCF) are not fully modelled in basic PSAs. A time-dependent CCF model analogous to the single failure time-dependent model has been studied in the SIK-1 project [20]. Further analysis is needed before the model can be adopted. It is desirable that the CCF model be based on observed CCF data rather than on a parametric representation.

Application areas

The LPSA applications can be divided in three areas:

- risk assessment
- risk monitoring
- risk follow-up

Risk assessment is the traditional purpose of basic PSA, i.e. estimation of the average risk of plant operation and identification of main risk contributors. The results are also used for *long term* planning of plant modifications to eliminate weaknesses in safety design, of testing arrangements, and of changes in the technical specifications. The basic Nordic PSA studies and their application are examples of risk assessment. Other application areas include the analysis of safety implications of system and component ageing, and the planning of accident management measures.

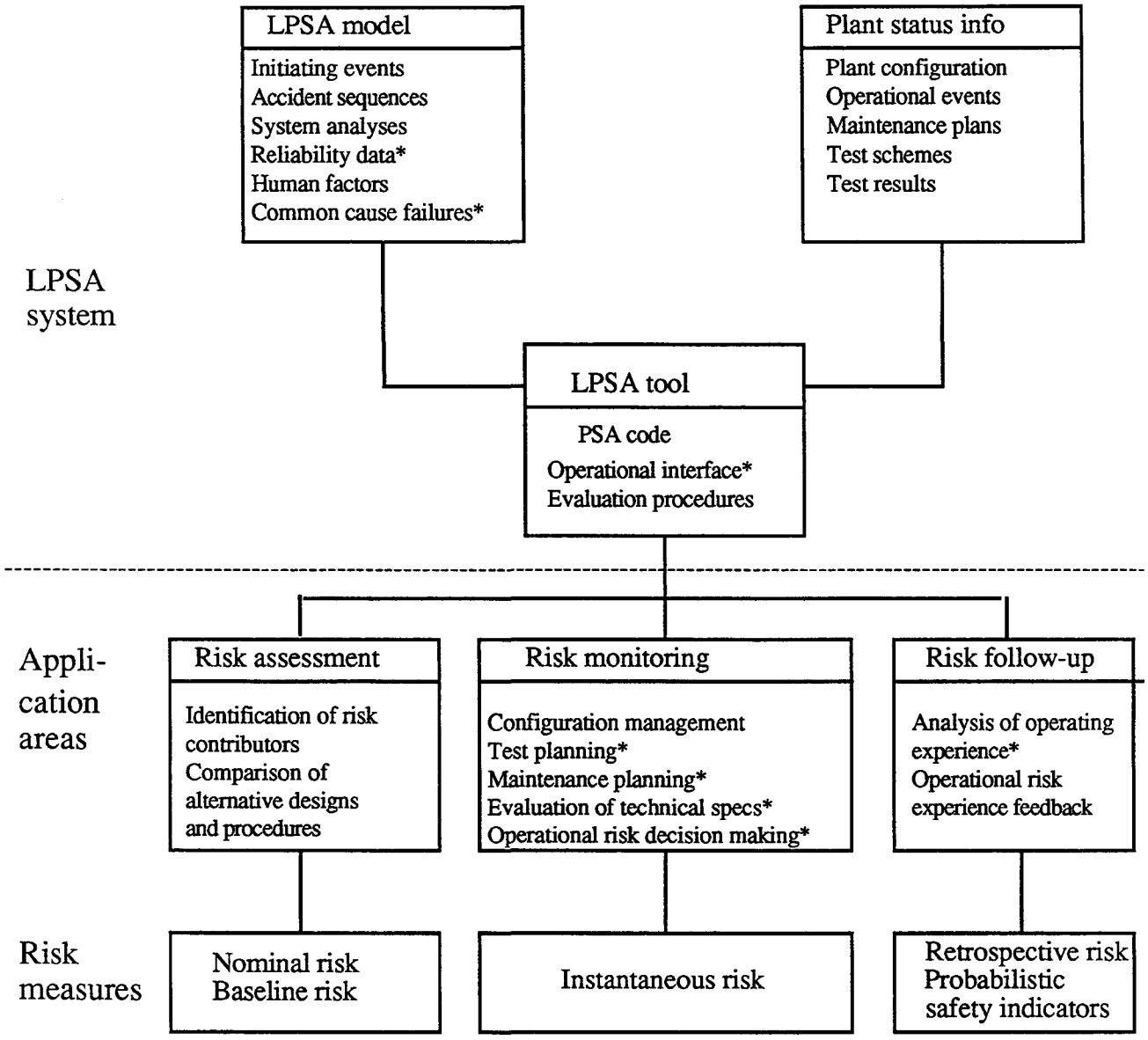


Figure 6 A living PSA concept
Activities in SIK-1 marked with asterisk

In contrast to risk assessment, where the average plant configuration is considered, risk monitoring applies to the actual configuration at the moment of operation or to a planned configuration. The resulting core damage frequency is a measure of the instantaneous risk. Risk monitoring can be performed on line or off line for *short term* operational support, such as for configuration management, planning of surveillance tests and preventive maintenance, optimization of technical specifications, and preventive accident management. So far there are only few examples of on line risk monitoring applications.

Risk follow-up is the term used for LPSA application to the analysis operational experience by estimating the *retrospective* risk, i.e. the risk experienced during the past operation of the plant. The results are used to evaluate the severity of occurred incidents and to provide feedback for safety improvement. Risk follow-up studies are also important for the verification of LPSA models and procedures. Risk follow-up has been the main application area in the SIK-1 project.

The classical approach to risk follow-up is the accident sequence precursor (ASP) studies carried out in USA and Germany [21, 22]. A precursor is an observed event which, if followed by one or several postulated events, may lead to core damage. The conditional probability of core damage, which is estimated by PSA, is a measure of the retrospective risk in the degraded state when the precursor has occurred.

Another approach is to predict the instantaneous core damage frequency (probability per time), using historic operational data and taking all potential core damage sequences into account. The instantaneous core damage frequency varies with the actual plant status, and is a measure of time-dependent risk. When used for risk follow-up it simulates on-line risk monitoring retrospectively.

Risk measures

The Rasmussen study defined risk as the product of the radionuclide release frequency in an accident and the associated consequences in terms of health effects. This has caused some confusion since "risk" is used in everyday speech to denote both a hazardous event and the likelihood of such an event. In this report, risk is used in the last sense, and the risk is expressed as the estimated frequency (probability per operating year) of core damage.

The basic risk measures for LPSA application are indicated in Figure 6. The *nominal risk* is the core damage frequency for an average plant configuration. It is obtained by using nominal failure probabilities for components and systems as well as for operator action, and by using nominal frequencies for initiating events. The nominal risk is used in risk assessment.

The *instantaneous risk* is obtained by modelling the basic events according to the actually known plant configuration. The instantaneous risk is used for risk monitoring and (retrospectively) for risk follow-up.

The *baseline risk* is obtained for a plant configuration, where no components are unavailable due to maintenance or repair and where all standby components have been recently tested without any failure indications. The baseline risk represents the lowest verifiable risk to be used as a reference level.

More application-oriented risk measures can be generated from the basic risk measures [23], e.g. risk importance measures which are used for identification of risk contributors. Probabilistic safety indicators, such as generic precursor frequency and risk dose, are derived from risk follow-up studies.

3.4.2 Risk follow-up studies

Pilot studies of risk follow-up were performed Forsmark 1, TVO I/II and Oskarshamn II. These are boiling water reactors of Asea-Atom's design, see Table 1.

In the Forsmark study [24], the retrospective risk during the 1989/90 operating period was estimated, using actual information of component unavailabilities due to maintenance or failures. The results are presented as a risk curve, Figure 7, showing the variation of the "risk increase factor" over the year. The risk increase factor is the ratio of the instantaneous to baseline risk. Most of the unavailablities resulted in only minor increases of the risk level. However, the unavailability of an auxiliary feedwater pump, because of failure to start, increased the risk level by a factor of eight during eight days.

The TVO risk follow-up study [25] showed the importance of preventive maintenance. The results led to changes of the maintenance strategy in the so-called diesel packages, so that important safety systems are not simultaneously unavailable. In the analysis of a pressure relief transient the time dependence of common cause failure was represented by a new model [20].

For Oskarshamn II, the year 1987 was selected for the analysis of retrospective risk [26]. The largest risk contribution during the year, or 65 % of the annual risk dose, was due to a feedwater transient, and the next largest contribution (18 %) was caused by the failure of a gas turbine. A lesson learned from the study is that a gas turbine should be tested directly after completed maintenance, and that the redundant turbine should be tested when a gas turbine has been found to have failed. If these rules had been followed, the risk increase would have been only 30 % of that which actually occurred.

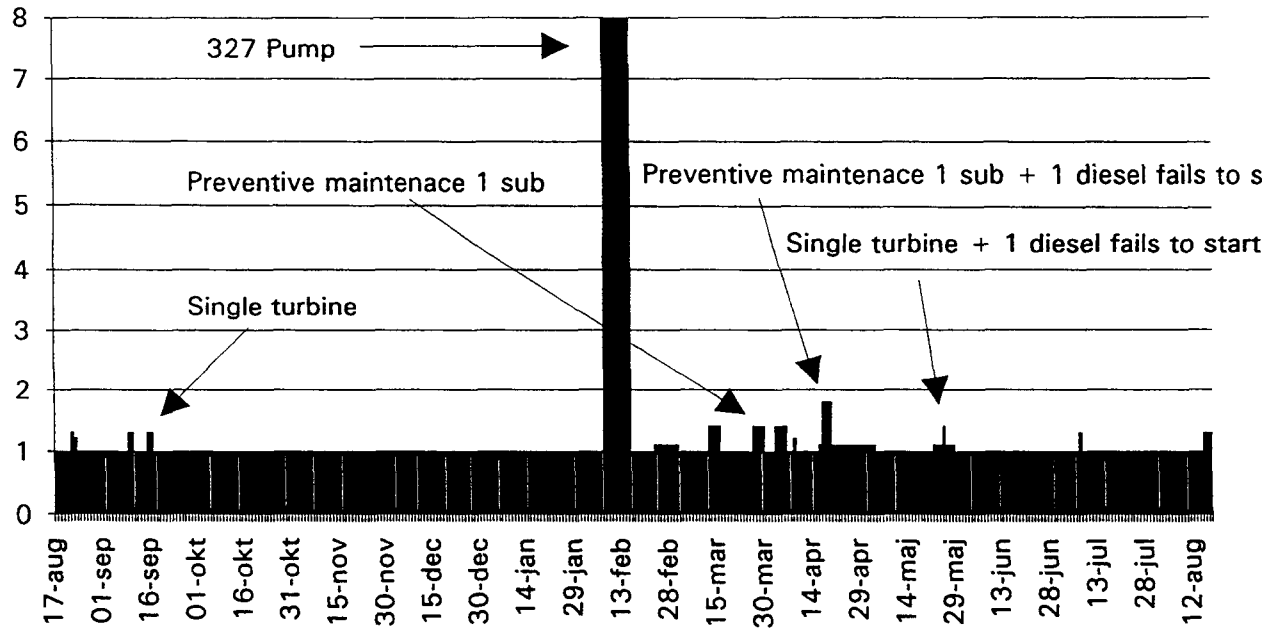


Figure 7 Retrospective risk increase factor for Forsmark 1 during 1989/90

The studies have successfully demonstrated that living PSA can be used to estimate retrospective risk levels and to evaluate the risk contribution of occurred events. The results have been used to improve maintenance and testing strategies for reducing risks. Further development is needed to increase the flexibility of the PSA models.

3.4.3 Risk monitoring studies

Whilst risk follow-up is used for retrospective analysis, risk monitoring applies to the actual plant status or to a planned configuration. Risk monitoring can be used off-line or on-line. Off-line applications have been demonstrated with the LPSA model for Oskarshamn II, for the evaluation of allowed outage times and test intervals [26].

The allowed outage time (AOT) is the time that a component is permitted to be out of service according to the technical specifications for plant operation. If the component is not restored during this time, the plant must be shut down. When a failure occurs, the component can be repaired while the plant is still in operation or after shutdown. For selecting the best strategy, the risk exposure of the two options should be compared.

The LPSA model for OII was used to predict the risk of continued operation and the risk of shutdown, in both cases with the component under consideration unavailable. In Table 8 the calculated AOT is compared to the AOT according the technical specifications for four different components. As can be seen, the AOTs in the present technical specifications are appreciably shorter than the calculated AOTs, except in the case of the gas turbine.

Table 8 Comparison of calculated and prescribed AOT for failed components in OII

Component	AOT (days) calculated with LPSA	AOT(days) prescribed in TS
Core cooling pump	6	2
Gas turbine	8,3	30
Diesel generator	4	2
Battery-backed busbar	14	1

The LPSA model for OII was also used evaluate the risk significance of test intervals. The purpose was to investigate the possibility of decreasing the number of tests prescribed in the technical specifications without affecting the average risk.

The predicted risk increase factor (RIF) during an operating year if tests and reconfigurations are performed according to the technical specifications is shown in Figure 9.

An alternative procedure was studied by which the test or reconfiguration providing the largest risk reduction is selected whenever the RIF reaches a predetermined value. It was found that the maximum RIF is reduced by more than 30 % for the same average RIF, see Figure 10. The total number of tests during the year is appreciably reduced as compared to the requirements of the technical specifications.

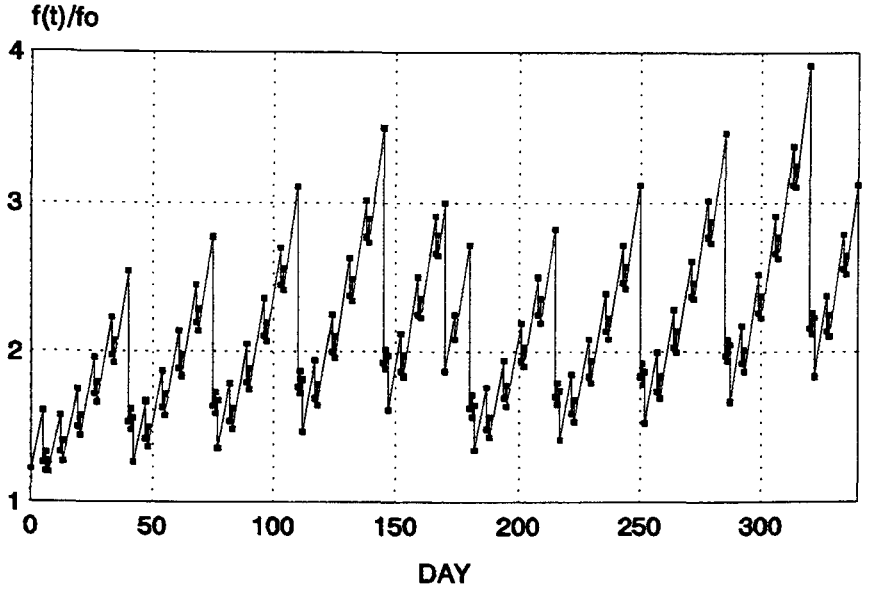


Figure 9 Variation of the risk increase factor over an operating year in Oskarshamn II, if tests and reconfigurations are performed according to the technical specifications.
f(t)/f(0) = risk increase factor

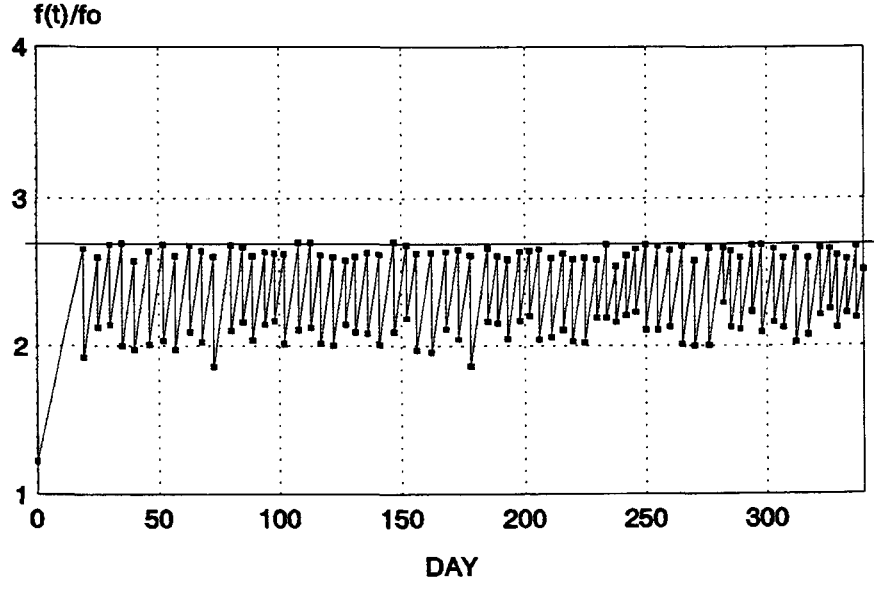


Figure 10 Variation of the risk increase factor when the procedure described in the text is used.
f(t)/f(0) = risk increase factor

3.5 Safety indicator development and use

Any observable safety-related condition, in qualitative or quantitative terms, may serve as a safety indicator. The term is used, however, for indicators that have a certain generality in their application and can be useful in several similar plants for extended periods of time.

Safety indicators can be direct or indirect. While the former focus on specific plant conditions, like component unavailabilities, the latter are based on observations with only indirect relation to safety, such as the number of licensee event reports per year.

3.5.1 Definition of safety indicators

The defence-in-depth strategy represents a suitable framework for the definition of safety indicators [27]. Accordingly, the indicators are designed to provide information of:

- the status of the *physical barriers* which prevent radioactive material from reaching the environment;
- the occurrence of *operational events* which threaten the integrity of the physical barriers;
- the availability of *safety systems* which prevent operational events to develop into accidents;
- the performance of *administrative programmes* and human behaviour for safe operation, maintenance and accident management.

The Swedish utility Vattenfall AB has suggested and tested a number of indicators along these lines [45]. The Vattenfall project was performed outside but in close contact with the SIK-1 project. The proposed set is shown in Table 11. Some of the indicators are identical to those adopted by the World Association of Nuclear Operators (WANO). Sample definitions of two indicators are given below.

Unplanned automatic scram: "The purpose of this indicator is to monitor performance in reducing the number of unplanned automatic reactor shutdowns. The indicator provides an indication of success in improving plant safety by reducing the number of undesired and unplanned thermo-hydraulic and reactivity transients requiring reactor scrams. It also provides an indication of how well a plant is operated an maintained.

The indicator is defined as the number of unplanned automatic scrams (reactor protection system logic actuations) that occur per 7000 hours of operation.

Transient index: The purpose of this indicator is to monitor performance in reducing the number of transient events that affect the lifetime of the reactor primary circuit pressure boundary, including the reactor vessel and connecting coolant lines. The number of transients is registered and compared with the design basis number of transients ("the transient budget"). The indicator also provides an indication of how well a plant is operated.

The indicator is tentatively defined as the number of transients per year exceeding 1 % of the transient budget for 40 years, expressed in percent of the total number of transients during the year. An alternative definition is also being tested: the number of transients during the past year, divided by the "remaining" annual mean number of transients. (The number of "remaining" transients is the difference of the transient budget and number of occurred transients).

An indicator system based on the principle of defence-in-depth has been proposed in a SIK-1 project [28]. A large number of unit-specific indicators are systematically defined. Application areas and user categories are identified. A selected number of indicators are recommended for use. Procedures are outlined for the validation of the indicators by computerized data collection and processing.

Table 11 Operational safety indicators suggested by Vattenfall AB.

Title	Definition	Type
PHYSICAL BARRIERS		
Fuel reliability	WANO	D
Chemistry index	WANO	I
Crack index	Vattenfall	D/I
Containment tightness	Vattenfall	D
OPERATIONAL EVENTS		
Unplanned automatic scram	WANO	D/I
Transient index	Vattenfall	I
SAFETY SYSTEMS		
Safety system performance	WANO	D
Valve failure index	Vattenfall	D
ADMINISTRATIVE PROGRAMMES		
Quality assurance index	Vattenfall	I
Regulatory exemptions index	Vattenfall	I
Licensee event report significance index	Vattenfall	D/I
Maintenance quality index	Vattenfall	I
Maintenance efficiency index	Vattenfall	I
Work order management index	Vattenfall	I
Unplanned capability loss factor	WANO	D/I

D = Direct indicator, I = Indirect indicator

3.5.2 Incident and trend analysis

Thousands of occurrences in nuclear power plants are reported each year, covering a broad spectrum of events. In the majority of cases, the events do not affect safety directly, and plant operation can continue without interruption. In some cases a safety function failed or a component on standby was unavailable when required.

Information of plant-specific significant events is collected, processed and stored in computerized data bases, operated by the utilities and the supervisory authorities. Information is exchanged on a worldwide basis. In Sweden, the ERF data base is operated by the Nuclear Training and Safety Center (KSU) for the utilities since the early 1980s [29]. The data base managed by SKI is known as STAGBAS. STAGBAS 2 presently contains about 6000 event descriptions since 1983. In Finland, the IVO utility has developed the LOTI information system for the Loviisa nuclear power plant.

For effective feedback of experience, it is necessary to screen the vast amount of data for significant information and to present the information in a condensed and usable form. Some of the indicators suggested in Table 11, such as "Unplanned automatic scram", "Transient index", "Safety system performance", and "Valve failure index", are easily obtained from the data bases.

In addition to providing direct indicators, the data bases can be used to generate indirect indicators. This is done by systematic analysis of "incidents" from the licensee event reports and reactor trip reports submitted to the safety authorities. *Incident catalogues* have been prepared for all Swedish nuclear power plants. The catalogues consist of statistical information of incident types, produced by computerized search patterns in STAGBAS 2 [30].

The incident catalogues are used to identify trends of improved performance or potential problems. Selected trends are further analyzed to identify causes. The extended analysis is documented in *trend catalogues* [31]. The results are displayed in diagrams, showing the annual variation of incidents related to a particular functional area or component group. An example is shown in Figure 12.

Trends are identified by inspection of the diagrams, or by computerized analysis. Models for quantitative trend analysis have been developed by Studsvik and VTT.

The identification of suitable search patterns is an important part of the analysis. A procedure for identifying search patterns by the statistical method of correspondence analysis has been tested [32].

A pilot study was made on the integrated use of operational safety indicators and living PSA by estimating the risk significance of candidate safety indicators [33].

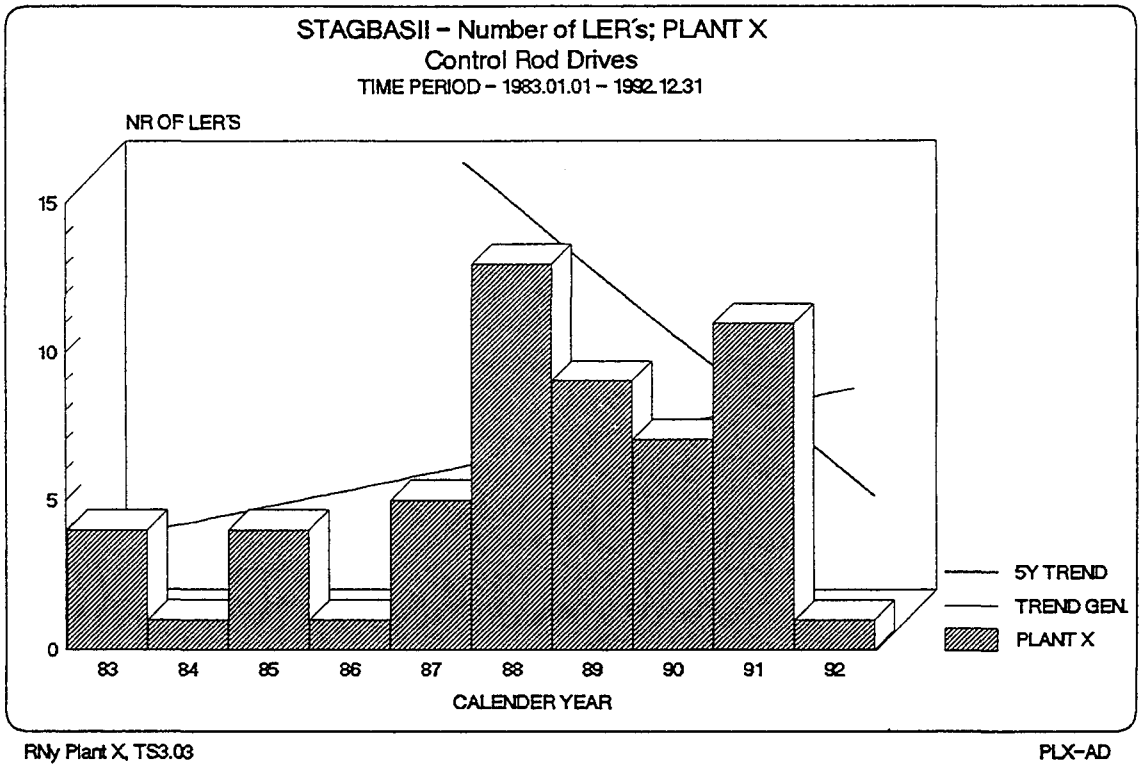


Figure 12 The annual number of safety-related occurrences due to faults in control rod drives in one unit.
LER = Licensee Event Report.

The studies have demonstrated that incident and trend analysis can be successfully used to generate indicators for both direct monitoring and predictive assessment of safety performance, and that living PSA can be used to identify the risk significance of the indicators.

3.5.3 Maintenance-related indicator studies

The data bases of operational experience can be used to generate maintenance-related indicators, such as "Safety system performance", "Maintenance quality index", and "Maintenance efficiency index in Table 12. Various approaches to the application of indicators for improving the maintenance of safety systems and components have been studied in three pilot projects. The basic objective is to answer the question of when and how often a component has to be maintained.

The unavailability and maintenance effectiveness of the emergency diesel generator system in Loviisa 2 was studied by VTT [34]. Use was made of the LOTI information system, developed by IVO, and the safety system unavailablity performance indicator, adopted by WANO.

In another pilot study, the combined use of component condition monitoring and failure report data for selected operating and standby systems in the Barsebäck nuclear power plant was investigated by the Risø National Laboratory in cooperation with the Sydkraft utility [35].

A third pilot study of reliability-centered maintenance and related indicators in the Forsmark 3 plant has been initiated [36]. The study includes failure data analysis and calculation of reliability and maintenance indicators.

The pilot studies have demonstrated the feasibility of using indicators for monitoring the performance of maintenance activities and identifying needs of improvements.

3.6 Risk-based decision making

The ultimate use of living PSA and operational safety indicator is to support decision-making on safety issues. Various approaches to decision-making were investigated in a pilot study of exemption from technical specifications.

3.6.1 Exemption from technical specifications

A pilot study was undertaken for a case related to an occurred event in the Oskarshamn III nuclear power plant. During periodic tests of isolation valves in the main feedwater system, one of the inner isolation valves, a check valve, did not indicate closure. According to the technical specifications, the check valve was declared inoperable, and reactor shutdown was required. The utility had, however, experiences of false indications in similar check valves. Moreover, only seven weeks remained before the planned shutdown for annual refuelling. In this situation, the utility and the safety authorities had to make rather quick decisions on the continued mode of operation. The safety authority agreed to an exemption from the technical specifications to the effect that continued operation until the scheduled outage was permitted.

The purpose of the pilot study was to simulate the decision situation and to analyze the various decision options. The study was performed in parallel by a Finnish and a Swedish team [37, 38]. The teams were allowed to choose the method of analysis freely.

The standard approach in decision analysis begins by specifying the decision alternatives and the objectives and criteria to be applied. In the actual case, when confronted with the indication of failed closure of the check valve, the decision-maker has three alternatives:

1) continue plant operation at full power,
2) isolate the affected feed water train and continue operation at reduced power (65 %),
3) shut down the reactor and inspect the check valve.

The hierarchy of objectives and criteria is illustrated in Figure 13.

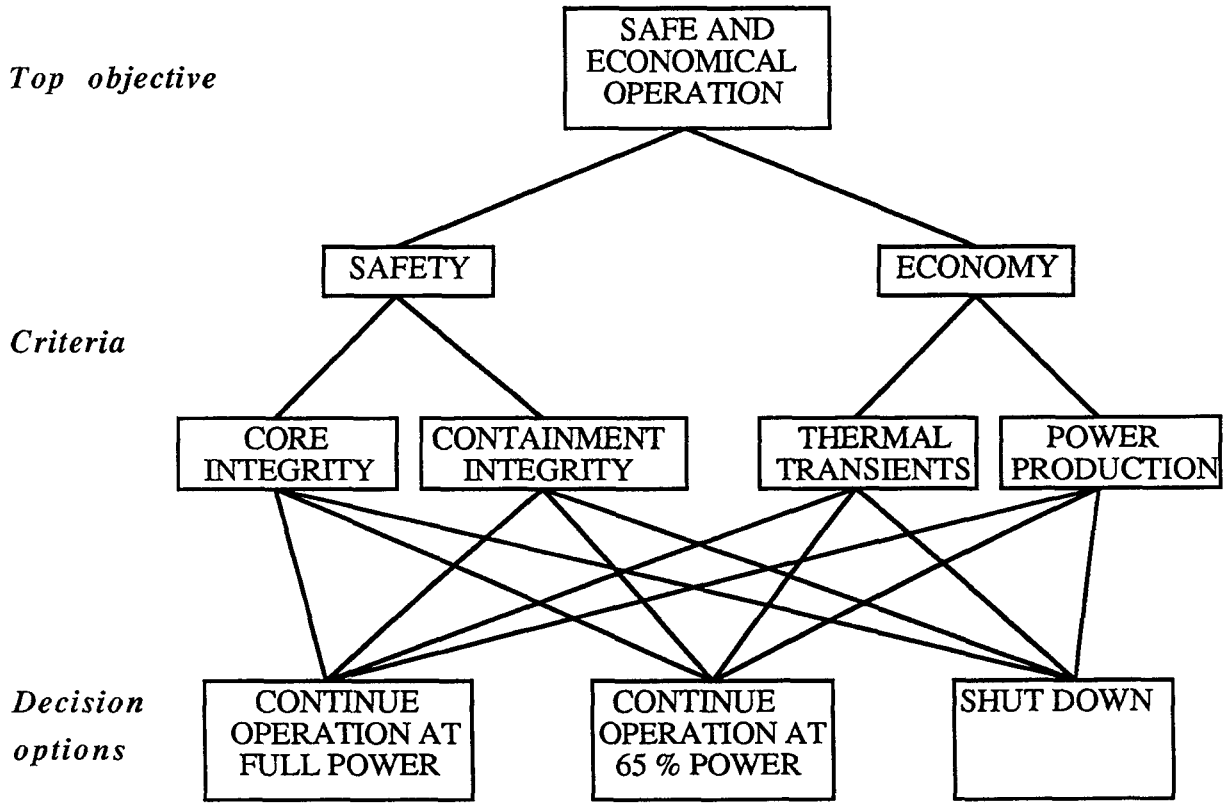


Figure 13 Decision alternatives, objectives and criteria.

After having established the decision alternatives, all events which may occur in each alternative are identified and the probability of each event is estimated. Next, the consequence of each combination of decision alternative and event is determined. The consequence can refer to safety, e.g. core damage, or economy, e.g. power production, depending on the perspective of the decision-maker.

The safety risk or economic value of each consequence is then defined and estimated. The assessment of a particular consequence in terms of risk or value depends on the selected decision criteria and evaluation models, which reflect the preferences of the decision-maker.

The total risk (value) of each decision alternative is obtained by summing the risks (values) of each consequence for the particular decision alternative. Obviously, the decision alternative with the least risk (highest value) is preferred. The "best" alternative can differ, subject to the criteria and models used.

In the Finnish study, several criteria and models were tested. In the simplest case, where the risk increase factor for core damage was used as the criterion, decision alternative 1 was found to be best. This was also the case when more advanced preference models were applied. Decision alternative 2 was ranked lowest.

In the Swedish study, account was taken of the uncertainty in the parameter values used for the analysis. Considering the risk of degraded check valve function as the basis for the decision analysis, it was found that decision alternative 2 was preferable, irrespective of whether the analysis was made with regard to safety or in economic terms.

The conflicting results of the Finnish and Swedish studies warrant further consideration of the criteria and development of the models used.

3.6.2 Uncertainty analysis in PSA

In the Swedish study, the parametric uncertainties were considered and treated in a manner described by Pörn and Shen [39]. Usually, the approach of error propagation is used to analyze parametric uncertainties in PSA. A new method, based on probability theory and called Integrated Uncertainty Analysis (IUA), is presented. Operational experience and state-of-knowledge dependence can be easily incorporated.

Application of IUA is demonstrated on a benchmark case of a core damage sequence from a previous study, where a conventional analysis by propagation was performed. The results are remarkably different. Although the mean values of the core damage frequency of the benchmark sequence are in close agreement, the probability distribution of the core damage frequency is much narrower in the IUA case.

Unlike the traditional view of uncertainty analysis as being a supplement to the main PSA study, the new approach is an integral part of the PSA. The method is simple and the results tractable. It is believed that IUA can be successfully used also in the context of living PSA.

3.7 Conclusions

Probabilistic safety analysis has been used for safety assessment of Nordic nuclear power plants since the mid-1970s. The methodology has been successively improved and extended to include external events and other operational states than full power, as well as containment and source term analysis. Traditional PSA usually focuses on identifying risk contributors in the safety design. New applications supporting plant operation and maintenance are rapidly growing.

The strength of the PSA approach is that a large amount of data and information can be handled in a systematic way and integrated into quantitative estimates of risk. The methodology has matured and modern computer technology has made it possible to run complete PSAs even on personal computers. The limitations of current PSA models should be borne in mind, however, such as incompleteness and oversimplification.

The SIK-1 project has seen the development of a living PSA concept, which integrates a plant-specific PSA model and information system, in a computerized user tool. Application areas and risk measures have been defined.

The use of living PSA has been successfully demonstrated in pilot studies for Nordic nuclear power plants. Risk follow-up studies have shown that LPSA can be effectively used for the feedback of operational experience by estimating the risk significance of occurred events and component failures. Off-line risk monitoring studies have demonstrated that LPSA can be used to evaluate and minimize the risk contribution of allowed outage times and test intervals for safety-related components.

Basic PSA models use average unavailabilities for components in standby, repair or maintenance to calculate a nominal risk. Living PSA attempts to take the real component status into account, which results in a time-dependent instantaneous risk. In the present studies, a linear time dependency of component unavailability was assumed. It is an open question, however, what failure probability should be assumed for a component in the time interval between tests. Further analysis is also needed for the modelling of time-dependent common cause failure, and for taking the effectiveness of testing into account.

The ultimate goal of LPSA is to provide a tool for daily safety management at the plant, including on-line risk monitoring. The present studies indicate that this is feasible, although basic PSA models must be further modified to allow sufficient flexibility. To give confidence in the results, the models should be as complete and realistic as possible. To gain wide acceptance, the tools must be easy to use and the results easy to interpret. Improving the models and streamlining the tools need further efforts.

The use of LPSA should be regarded as a complement to other means of safety assessment, such as safety indicators. Safety indicators attempt to express in a condensed way the safety status of the plant and to provide early warning of impending problems. A hierachical indicator system, based on the principle of defence-in-depth, has been proposed in the project, and a selected number of indicators has been recommended.

The feedback of experience from safety-related events during plant operation, testing and maintenance has been greatly facilitated by the introduction of computerized information systems for data collection and presentation. Statistical methods have been applied to computerized incident catalogues to identify trends of improved safety performance and potential problems. The analysis has demonstrated that suitable indicators can be generated for both direct monitoring and predictive assessment of safety characteristics. It has be shown that the risk significance of the indicators can be determined by LPSA.

Maintenance-related indicators have been investigated in two pilot studies for the Loviisa II and Barsebäck nuclear power plants. Several indicators were suggested and tested. The studies demonstrated the feasibility of using the indicators for monitoring the performance of maintenance activities and identifying the need of improvements. A third pilot study of reliability-centered maintenance and related indicators in Forsmark 3 has been initiated.

An important purpose of LPSA and operational safety indicators is to provide support for decision-making on safety issues by plant operators and safety authorities. The theory of decision analysis can give some guidance in this process. A pilot study was undertaken for a case related to an occurred event on the exemption from technical specifications for operation of the Oskarshamn III plant. Two independent approaches were used for simulating the decision situation and the various decision options. The studies led to conflicting results indicating that further consideration of the criteria and models is required.

Decision-making on safety issues often involves uncertainties. A new method for the treatment of uncertainties in PSA has been developed and applied in one of the pilot studies. The method is an integral part of the PSA and can be successfully used also in living PSA applications.

The overall conclusion of the SIK-1 project is that the objectives of developing a living PSA concept and operational safety indicators and demonstrating their applicability have been successfully met. The project has clearly improved the level of knowledge and stimulated activities in the area at the utilities and authorities in Finland and Sweden. An important remaining task is to achieve general user acceptance and establish routines and procedures for the application of living PSA at the nuclear power plants.

4 Severe accident research (SIK-2)

Two types of severe accidents may occur in nuclear reactors, broadly classified as core melt accidents (CMA) and core disruptive accidents (CDA). A CMA would result from inadequate core cooling leading to core heatup and meltdown in a time scale of hours. A CDA would be caused by uncontrolled reactivity increase leading to power runaway and fuel disintegration within seconds. The two types are illustrated by the Three Mile Island and Chernobyl accidents. A CDA is considered practically impossible in a light water reactor due to the inherent and engineered safety features provided. Therefore, severe accident research for light water reactors has been largely devoted to CMA phenomena.

4.1 Core melt accident progression and mitigation

Whilst SIK-1 dealt with the probabilistic analysis of potential accident sequences leading to core degradation, SIK-2 is concerned with the deterministic analysis of the behaviour of a molten core in the reactor vessel and containment. The analysis forms the basis for the design of equipment and procedures for preventing and mitigating the effects of severe accidents, which are now included in the licensing requirements for nuclear power plants in the Nordic countries.

4.1.1 In-vessel behaviour

If the water level in the reactor pressure vessel drops so that the core is uncovered, the fuel temperature will rapidly rise due to the decay heat of the radioactive fission products, even if the reactor is shut down and the nuclear chain reaction is stopped. When the cladding temperature reaches about 900 °C, chemical reaction between zirconium in the cladding and steam begins to produce hydrogen and generate heat. The heatup of fuel is accelerated and once the temperature exceeds about 1200 °C, the rate of chemical heat generation is greater than that of the decay heat.

In licensing calculations of design basis loss-of-coolant-accidents, 1200 °C is used as a bounding value for the maximum fuel cladding temperature. This temperature is also referred to as the "threshold for zirconium runaway oxidation", i.e. the temperature where the chemical reaction between zirconium and steam and the corresponding heat generation is beginning to accelerate rapidly.

If adequate core cooling is not restored, the temperature of the uncovered part of the core will rise at an increasing rate. Alloys can be formed between the fuel and cladding or control rod material. The alloys, like the control rod material itself, can melt at an appreciably lower temperature than the uranium dioxide fuel, which has a melting point of about 2800 °C. In the basic severe accident scenario for Nordic reactors, which is assumed to be caused by total loss of AC power

("station blackout"), control rod melting may start after about 20 minutes and fuel melting after about half an hour into the accident.

When control rods and fuel melt, drops of molten material will flow down the core and solidify in the lower cooler regions which have not yet been uncovered. This may cause blockage of the steam flow which reduces the rate of zirconium oxidation. A bowl-shaped crucible of solidified fuel may form which is supplied with molten fuel and fuel debris from above. The molten fuel will eventually collect in the bottom of the reactor vessel (lower plenum).The greater part of the core may have relocated to the lower plenum within half an hour after the onset of melting.

The way of melt relocation, whether it occurs gradually or suddenly, will have implications for the mode of reactor vessel failure. In the first case, if there is water left in the reactor vessel, a coolable bed of core debris may form in the lower plenum. When the remaining water has evaporated, the fragments will melt again and form a liquid mass, which may melt through the vessel wall. In the second case, a large amount of melt which suddenly falls into the lower plenum may cause melt-through of some of the many relatively thin-walled penetrations at the bottom of the vessel.

The scenario is typical of core meltdown at low pressure, such as during a large loss-of-coolant accident with failure of the emergency core cooling systems, or station blackout, i.e. complete loss of offsite and emergency electric power, with automatic depressurization in a boiling water reactor.

Core meltdown can also occur at high pressure in the reactor. A typical example is the case of station blackout in a pressurized water reactor. This will lead to core uncovery, heatup and meltdown within a few hours, if electric power cannot be restored. The melt will be rapidly ejected at high pressure through penetrations in the bottom of the reactor. High pressure melt ejection can damage the containment structure. Methods for intentional depressurization of the primary system are therefore installed in many PWRs.

The occurrence of a core melt accident can be prevented, or its progression interrupted, by intervention of the operating staff. This is known as preventive accident management. The basic objective is to recover core cooling as quickly as possible so as to avoid severe degradation of the core, thereby maintaining the integrity of the reactor pressure vessel. Cooling can often be restored by using existing plant systems in normal or unusual ways. Successful accident management requires adequate information of critical plant parameters. Guidelines for emergency operation are formulated and procedures are trained on full-scale plant simulators.

4.1.2 Ex-vessel behaviour

If accident management is unsuccessful in restoring core cooling, the reactor vessel could fail about an hour after the onset of core melting. Although this has so far never happened, large amounts of molten core material would then escape into the reactor containment. The melt will come into contact with the concrete floor under the reactor vessel. In PWRs, the region under the vessel is known as the reactor cavity. Any water in the cavity will boil off and contribute to the builup of pressure in the containment. If additional water is supplied, the melt may be quenched and form coolable debris under water in the bottom of the cavity. Otherwise the melt will interact with the concrete.

Early ABB Atom BWRs (except Oskarshamn I) have a drainage pipe and other penetrations in the floor of the region below the reactor vessel through which most of the melt will flow and fall into the condensation pool which occupies the entire bottom region of the containment. The molten fuel will then disintegrate and form fragments which are cooled by the pool water .

In later ABB Atom BWRs, the condensation pool forms an annular region close to the walls of the containment. In this case the core melt would fall onto the floor of the bottom part of the containment (lower drywell), melt through its steel liner and interact with the basemat concrete. In order to avoid severe core melt-concrete interaction and to protect penetrations, the lower drywell would be flooded with water from the condensation pool, if necessary.

When the hot core melt comes into contact with concrete, free and chemically bound water in the concrete will evaporate. The concrete itself will also disintegrate through chemical reactions. Non-condensible gases, particularly hydrogen, will then be formed. The steam and gases will contribute to the pressure buildup in the containment.

The melt will slowly erode the walls and base of the containment. The detailed processes during melt-concrete interaction are still not completely known. It cannot be predicted with certainty if and when the concrete basemat of the reactor building, which is several meters thick, will be melted through. The main question is whether the melt can be cooled by an overlying water pool, or if it remains molten at the melt-concrete interface.

The hydrogen formed during core melt-down, melt release from the reactor vessel, and melt-concrete interaction may form combustible mixtures with air and steam in the containment. Under certain conditions, combustion can take place extremely rapidly in a process known as detonation. A global explosion could seriously damage the containment. In order to avoid hydrogen detonation, the containment of ABB Atom BWRs is filled with nitrogen.

The purpose of mitigative accident management is to maintain the integrity of the reactor containment once core melt has occurred and the reactor vessel has been penetrated. This may involve flooding the containment to secure cooling of the debris and (in PWRs) avoiding critical gas mixtures by controlled hydrogen combustion.

4.1.3 Radionuclide release and transport

During core meltdown, gases and vapours are released and airborne particles (aerosols) are formed. The amount and composition depend on the inventory of materials in the reactor vessel and the physical and chemical properties of the individual substances. The vapours and aerosols are to a large extent retained in the primary reactor system by a variety of removal processes. Substances not retained could be transported into the reactor containment by gaseous flow.

To predict aerosol transport, all core constituents must be considered since the aerosol behaviour is determined by the total amount. Fission products represent only a fraction of the total amount of aerosols, and the radioactive fission products are only a small part of the total amount of fission products. In the German Reactor Safety Study, for example, the total mass of aerosols released to the containment in a typical severe accident was estimated at 3,5 tons, most of which are particles of control rod material, uranium dioxide and steel. Only about 260 kg are fission products, of which about 100 kg are radioactive [40]. The aerosol mass is substantially reduced in a matter of hours due to deposition on the floor and walls of the containment and washout by containment spraying.

The most important fission products from the radiological point of view are isotopes of noble gases, iodine and cesium. The noble gases are released to 100 %. They do not participate in any chemical reactions during their release from the fuel and transport in the reactor system and containment. Iodine was earlier assumed to occur mainly in gaseous molecular form and to a small extent as methyl iodine. It is now believed that most of the iodine is released in the form of alkaline iodides, especially cesium iodide, which is less volatile than elementary iodine and forms aerosol. Cesium mostly appears as cesium hydroxide aerosol.

The understanding of fission product release and transport has improved significantly since the accident at Three Mile Island, and so has the ability to predict the behaviour of radionuclides under severe accident conditions. It has been demonstrated that the retention of radionuclides in the reactor coolant system and containment significantly reduces the potential release of radioactive substances from a nuclear power plant during an accident.

The remaining uncertainty in the prediction of fission product release and transport in the reactor vessel and the containment is to a large extent due to the superficial treatment of fission product chemistry .

It should be noted that many of the phenomena which are neglected in current calculational models tend to increase the retention of radionuclides.

4.1.4 Mitigation strategy

The Nordic utilities have introduced measures for the mitigation of severe accidents, which can be considered as a fourth level in the defence-in-depth strategy (see Appendix 2). The measures include:

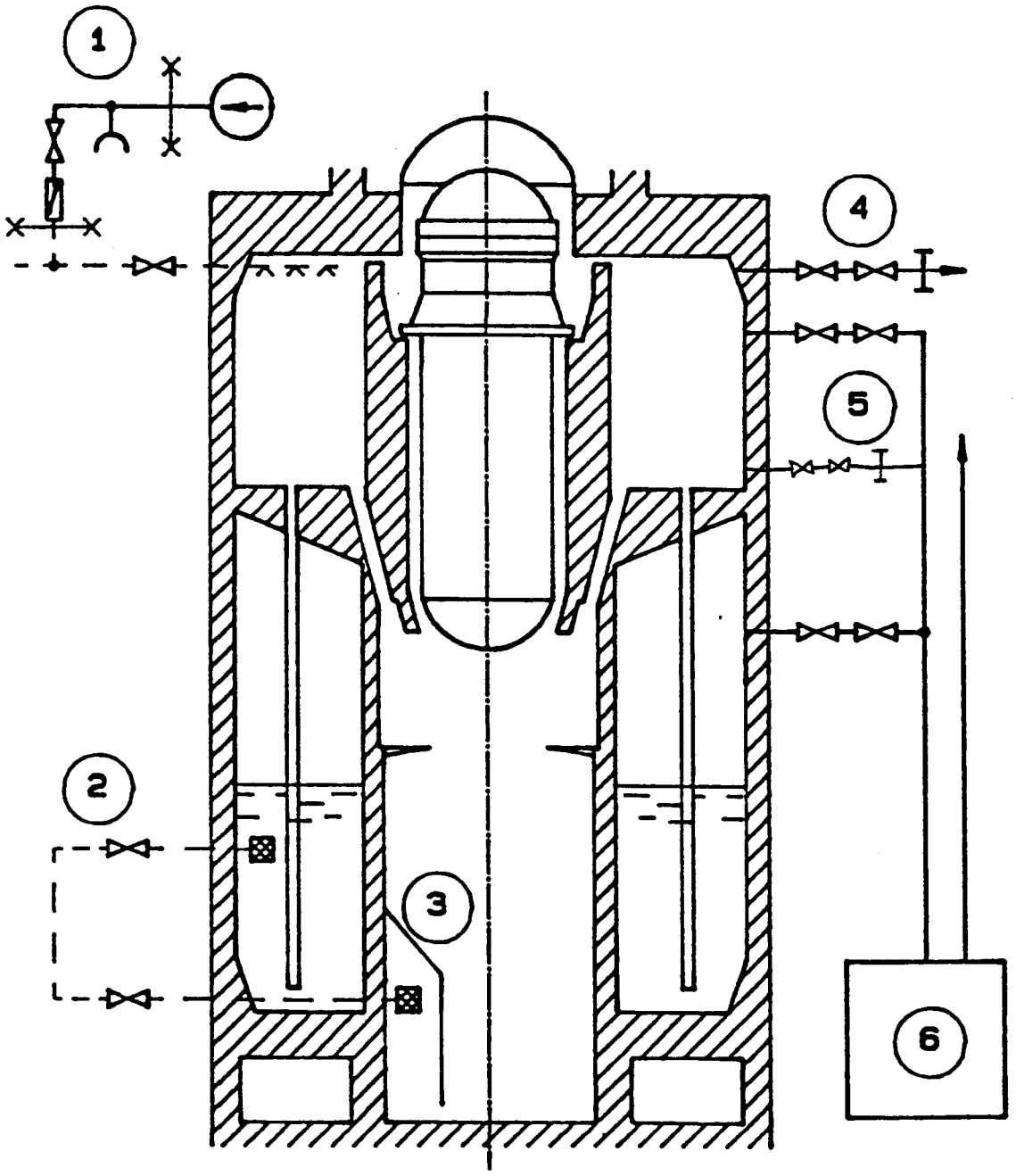
- modification of plant design to prevent core melt accidents
- installation of equipment for accident mitigation to reduce residual risks of environmental consequences
- procedures for preventive and mitigative accident management.

The mitigation systems are based on three considerations. First, the core melt shall always fall into a water pool. This does not require any special measures for first generation BWRs, as mentioned earlier. For modern BWRs, on the other hand, provisions have been made to flood the region below the reactor vessel when core melt is indicated. For some PWRs the reactor cavity will also be flooded with water.

Second, the capability of containment spray has been enhanced. This is achieved, in BWRs as well as in Swedish PWRs, by supplementing the existing spray system with an independent water supply, including diesel-driven pumps. The capacity is sufficient to flood the containment to the upper core level. The purpose of the spray systems is to cool the containment, thus delaying the pressure buildup, and to wash out aerosol particles, thus reducing the concentration of fission products in the containment atmosphere.

The third element of the mitigation strategy is filtered venting. For both BWRs and PWRs, filtered venting is used for reducing the containment pressure to ambient levels in sequences in which containment cooling is inadequate. For BWRs, in addition, the aim is to avoid early containment failure in large loss-of-coolant accidents combined with degraded pressure suppression function. The mitigation measures, as implemented in a BWR, are illustrated in Figure 14.

For the Finnish Loviisa reactors (PWRs), filtered venting was ruled out as the main measure because of the risk of creating subatmospheric pressure in the containment after venting. This could endanger the stability of the containment steel shell, which is designed for low internal overpressure and a very modest external pressure. Instead, containment overpressurization is prevented by means of an external spray system. The piping and spray nozzles are installed in the annular space between the inner steel shell and the outer conrete building. An interesting aspect of the Loviisa plant is the possibility of retaining the core melt in the reactor vessel by cooling the vessel from the outside via natural convection in the water-filled reactor cavity.



1	Water filling of the containment
2	Flooding of the lower drywell
3	Shielding of penetrations in the lower drywell
4	Containment overpressurization protection
5	Containment venting
6	Filter

Figure 14 Systems for severe accident mitigation in the TVO reactor containment

4.2 Research areas and Nordic efforts

4.2.1 Severe accident analysis

Deterministic analysis is used to assess the vulnerability of a plant to core melt accidents. The analysis can also be used to evaluate various design options and procedures for the prevention and mitigation of accidents. The calculations aim at best-estimate prediction of core melt behaviour and radionuclide release and transport in the reactor vessel and containment. The results are used in a variety of applications:

- design of safety systems for accident mitigation in existing plants
- evaluation of conditions for maintaining containment integrity
- prediction of source terms for radionuclide release
- development of improved accident management procedures
- training of plant personnel
- design of new plants with advanced safety features.

Severe accident research aims at supporting these applications by modelling basic phenomena and mechanisms in computer codes and verifying the models by comparison with experiments.

Code development

Accident progression is described in terms of the thermohydraulics of the processes involved. The in-vessel processes include core boiloff and heatup, meltdown, relocation, debris cooling, reflooding and recovery. If recovery is unsuccessful, vessel meltthrough and melt interaction with water and concrete in the containment will follow. The modelling of radionuclide release, transport and removal is based on an extensive experimental data base on release mechanisms, fission product chemistry and aerosol physics.

The models form part of computer codes for calculating the pressure, temperature, hydrogen generation, concrete attack, aerosol mass etc. as a function of time after the initiating event. The accident progression is largely determined by the initiating event, the design and performance of the reactor system and containment, and by any operator action undertaken. The codes must be adapted to the specific plant under consideration and be capable of describing the effects of accident management.

Two types of codes are being developed and used: integral codes (sometimes improperly referred to as "risk analysis codes") and mechanistic codes. The integral codes, which describe the entire progression of the accident from the initiating event to the possible

release of gases and radionuclides from the containment, use simplistic models to provide versatile codes for survey calculations. The mechanistic codes use sophisticated models for the study of separate effects. They tend to have long execution times and have so far been developed only for certain phases of a core melt accident.

Examples of integral codes are MARCH, MAAP and MELCOR, of which the last two are presently used in Nordic countries. SCDAP/RELAP5 is an example of a mechanistic code for detailed calculation of primary system phenomena, which is also available in Nordic countries.

The capabilities and accuracy of the codes can be assessed by comparative case studies, sensitivity studies, and comparison with experiments. The required accuracy depends on the type of application. A higher accuracy is generally needed in bounding analyses for safety system design than for comparisons of alternative designs and accident management strategies.

International cooperative programmes have been established for the exchange of information on the development, validation and use of severe accident codes. Some of them are listed in Table 15.

Table 15 International programmes for severe accident code development and use with participation from Nordic countries

Programme	Sponsor	Purpose
IDCOR[1)]	EPRI[2)]	MAAP
CSARP[3)]	U.S.NRC	MELCOR, SCDAP/RELAP, CONTAIN
CAMP[4)]	U.S.NRC	RELAP5
ISP[5)]	NEA/CSNI[6)]	Code validation

1) Industry Degraded Core Rulemaking Program
2) Electric Power Research Institute, USA
3) Cooperative Severe Accident Research Program
4) Code Application and Maintenance Program
5) International Standard Problems
6) OECD Nuclear Energy Agency Committee for the Safety of Nuclear Installations

In summary, several severe accident codes are available for various applications. While all codes have weaknesses and limitations, they can be considered adequate for the design of accident mitigation measures, if used with knowledge and judgement and if the results are carefully interpreted.

Experiments

Experiments are carried out to extend understanding and explore new issues. Two approaches are used: separate-effect tests and integral experiments. The former serve to validate the basic models and codes but are often subject to scaling difficulties. The integral experiments include system behaviour and interaction between basic phenomena but are generally difficult to interpret unambiguously.

Many severe accident experiments are carried out in international cooperation. Some large experimental programmes, in which organisations from Finland or Sweden participated, are listed in Table 16.

Table 16 Some international severe accident research programmes with Nordic participation

Programme	Purpose	Performed at	Participation
IN-VESSEL PHENOMENA			
SFD	Severe fuel damage	INEL[1], SNL[2]	Finland, Sweden
LOFT	Fuel damage and fission product release	INEL	Finland, Sweden
TMI	Melted core examination	INEL	Finland, Sweden
TMI-VIP	Vessel investigation project	INEL	Finland, Sweden
CORVIS	Pressure vessel melt-through	PSI[3]	Finland
MX-V-ATT	Aerosol transport	Marviken	Finland, Sweden
CONTAINMENT PHENOMENA			
LACE	Aerosol behaviour	HEDL[4]	Finland, Sweden
ACE	Filtered containment venting, Iodine behaviour, core concrete interaction	BPNL[5], ANL[6]	Finland, Sweden
MACE	Ex-vessel melt coolability	EPRI	Finland, Sweden
HDR	Hydrogen burning, aerosol behaviour	KfK[7]	Finland
FALCON	Aerosol transport	AEA[8]	Finland

1) Idaho National Engineering Laboratory, USA
2) Sandia National Laboratories, USA
3) Paul Scherrer Institute, Switzerland
4) Hanford Engineering Development Laboratory, USA
5) Battelle Pacific Northwest Laboratory, USA
6) Argonne National Laboratory, USA
7) Kernforschungszentrum Karlsruhe, Germany
8) Atomic Energy Authority Winfrith, UK

4.2.2 Nordic research programmes

A series of severe accident research projects were undertaken in the Nordic countries during the 1980s. The FILTRA and RAMA projects were conducted to meet the needs of information for the design and installation of mitigating systems in the Swedish nuclear power plants and for the development of accident management procedures. The Finnish VARA projects are carried out to acquire and maintain an understanding of important severe accident phenomena and to establish and use calculational tools for their analysis. The main purpose of the joint Nordic AKTI project was to follow and evaluate international research activities and to assess the methodology for severe accident analysis used in the Nordic countries.

FILTRA-RAMA

The idea of containment pressure relief as a safety measure was first pointed out in the Swedish Urban Siting Study 1974 [41]. A preliminary assessment of using a gravel bed filter for containment venting was made in the Swedish Reactor Safety Study 1979 [42]. The FILTRA project was inititiated in 1980 to explore filtered venting for the Barsebäck nuclear power plant. Several experiments gave new information on the condensation and filtering properties of gravel bed filters. FILTRA presented its final report in 1982 [43]. A filtered venting system was installed in Barsebäck and commissioned in 1985.

Following a government decision in 1981, also the other nuclear utilities were imposed to install mitigation systems before 1988. The mitigation strategy was slightly modified, and the gravel bed filter was substituted with diversified containment spray and the Multi Venturi Scrubber System (MVSS) for the remaining plants. The RAMA projects formed the basis for the design of the mitigation systems for these plants.

The main purpose of the RAMA I project was to establish a tool for accident analysis. Two areas were addressed: thermohydraulics and source terms. The project implemented and used the first version of the MAAP code and developed a Swedish version of the RETAIN aerosol code. It was concluded that MAAP had a number of shortcomings and that the outcome of an accident and its source terms are highly plant- and sequence-specific [44].

The RAMA II project was conducted to further evaluate the MAAP code and continue studies of, for example, revolatilization, and fission product chemistry [45]. The project benefitted from participation in a number of international research programmes, such as SFD, Marviken ATT, LACE, and LOFT. The schedule of RAMA II was tied to the final design of the mitigating systems for the Swedish plants.

Although the design of the mitigating systems had been completed, it was considered useful to continue the efforts to improve the knowledge of severe accident phenomena. The RAMA III project was launched in

1987 and particularly directed to code development and validation, participation in international experiments and their evaluation, and improvement of accident management strategies and procedures [46].

The general conclusions from eight years of severe accident research in the FILTRA-RAMA projects were that the proposed mitigation systems would provide the desired protection of the environment against severe accidents in Swedish reactors. The MAAP code was found to be a useful tool for the analysis of severe accidents, although careful interpretation of the results is necessary.

RAMA was succeeded by the HAFOS project during 1990-1991, which included participation in the international CSARP and ACE-MACE projects, and studies of the fragmentation and coolability of the core melt in the containment. These activities are continued in the ongoing APRI (Accident Phenomena of Risk Importance) project, which also includes studies of methodologies for severe accident phenomena in the containment, and verification of the MAAP 4.0 reflooding model.

VARA

The VARA project for the evaluation of severe accidents started in 1983 at the Technical Research Centre of Finland [47]. The work has focussed on acquiring and validating severe accident computer codes, mainly by participation in international research programmes. The results are used in support of PSA analyses and plant modification, and for the development of accident management procedures.

The first phase of the VARA project, included participation in the Marviken V-ATT and LACE projects and in the IDCOR programme. Code development and application was performed in cooperation with the Electric Power Research Institute, the Kernforschungszentrum Karlsruhe and the RAMA projects. Small-scale aerosol experiments were carried out at the University of Kuopio. Capabilities were established for the analysis of severe accidents in the Loviisa and TVO nuclear power plants, the main tool being the MAAP code.

At a later stage, various advanced USNRC codes have been implemented and applied in case studies. The project also participated in international experimental programmes, such as SFD and ACE in the USA and HDR Phase III in Germany. In 1992, the cooperation was extended to include participation in the FALCON aerosol transport experiments in the UK and the CORVIS pressure vessel melt-through programme in Switzerland.

The Finnish nuclear utilities joined the VARA project at an early stage in order to obtain computer codes and expertise for analyzing severe accidents. Because of the many unique features of the Loviisa nuclear power plants, independent efforts were needed to solve a number of safety issues. The TVO units at Olkiluoto have many features in common with their sister units in Sweden. Hence, TVO can benefit from cooperation with the Swedish utilities and the plant vendor.

NKA-AKTI

The joint Nordic AKTI programme, sponsored by NKA (the Nordic Liaison Committee for Atomic Energy), was carried out during 1985-1989. It consisted of three research projects dealing with selected severe accident issues: code comparison (AKTI-130), chemical phenomena (AKTI-150) and aerosol behaviour (AKTI-160). The programme was financed by the Nordic Council of Ministers and the participating organisations in Denmark, Finland, Norway and Sweden.

In AKTI-130 some benchmark calculations and sensitivity studies were performed to explore the capabilities of the MAAP 3.0 and MARCH3 codes and to provide comparison with similar studies performed in the RAMA III project. The studied sequences were used as enveloping cases for the design of mitigative measures for Forsmark-type BWRs. The studies demonstrated the feasibility of both codes to reasonably represent the course of the accidents but they also showed that considerable uncertainties remain [48].

The main reason for the AKTI-150 project was the rather simple modelling of chemical phenomena in the MAAP code. Accordingly, efforts were made to assess the significance of the simplifications in the code for prediction of the accident progression and source terms, particularly of cesium, iodine and boron. Relevant chemical data were compiled and sensitivity studies were performed using an extended chemistry model in the MAAP code [49].

The aerosol transport project AKTI-160 included code comparisons and studies of aerosol nucleation and hygroscopicity as well as of the effects of pool scrubbing. International research was reviewed and assessed. It was concluded that aerosol transport phenomena are rather well known and properly represented in a number of computer codes, but that the coupling between aerosol behaviour, thermohydraulics and chemistry is essential and less well modelled [50].

4.3 SIK-2 objectives and structure

A conclusion of the NKA-AKTI project was that uncertainties still existed in severe accident analysis, and that further code assessment, modelling and validation was needed. The SIK-2 project can be seen as a continuation of AKTI and was to a large extent laid out in response to the recommendations of this project and the RAMA project. The scope of activity was strongly influenced by ongoing and planned research in the participating countries such as in the VARA project.

The overall aim of SIK-2 has been to maintain and improve knowledge and expertise in the Nordic countries of severe accident phenomena, calculational tools, and accident management. The specific objectives of SIK-2 were set to include:

- review and assessment of computer codes for accident analysis
- case studies of unmitigated and mitigated in-vessel accident progression in selected sequences
- modelling of chemical phenomena and aerosol behaviour
- development of computerized systems for accident management.

The programme plan comprises seven subtasks:

SIK-2.1 Critical review of the MAAP 3.0B, MELCOR, SCDAP/RELAP5, and MAAP 4.0 computer codes with emphasis on in-vessel phenomena

SIK-2.2 Accident progression assuming no recovery actions

SIK-2.3 Accident progression assuming recovery actions, i.e. reflooding of a degraded core

SIK-2.4 Recriticality upon reflooding a degraded core

SIK-2.5 Chemical models for the MAAP code

SIK-2.6 Assessment of aerosol modelling in computer codes for in-vessel and ex-vessel severe accident analysis

SIK-2.7 Computerized accident management support system, CAMS

In addition, information on some severe accident research, conducted in the Nordic countries outside the SIK project, was made available to the project for review. This includes the behaviour of hydrogen in reactor containments, ex-vessel fragmentation and coolability of molten core material, and long-term accident progression and mitigation.

4.4 In-vessel core melt behaviour

The first four of the SIK-2 subtasks deal with the review and application of severe accident codes with particular emphasis on in-vessel phenomena. The area is still in development and new code versions appear from time to time. The following summary refers to the state of the art in the summer of 1993.

4.4.1 Code review

As indicated in section 4.2.1, a two-tier approach is generally used for severe accident analysis. Simplistic system codes are used for survey and design calculations, whilst detailed mechanistic codes are employed for studying separate effects. In the Nordic countries, MAAP is the workhorse for severe accident calculations. MELCOR and SCDAP/RELAP are used for independent verification. A review of the latest available versions of these codes was made in subtask SIK-2.1.

The approach has been to select key phenomena, based on expert judgments of their relevance for accident progression and plant safety. Next, the particular models in the codes are evaluated with reference to experiences gained in using the codes, especially of the observed deficiencies. Assumptions, important model parameters and options, uncertainities and missing models are identified. Focus has been on in-vessel degraded core behaviour. The results are presented in the form of detailed tabular comparisons of code characteristics in the SIK-2.1 final report [51]. In the following only some general features are summarized.

MAAP

MAAP is a relatively fast-running integral code with separate versions for BWR and PWR. The reviewed versions are MAAP 3.0B Revision 9 for BWR and Revision 19 for PWR, released in early 1993. Some features of the advanced version MAAP 4.0 are also mentioned.

MAAP models the complete in-vessel and ex-vessel progression of accident sequences, including operator intervention, and is executable on relatively powerful personal computers. The code has a modular architecture with type-specific reactor coolant system and containment modules and plant-specific modules for engineered safety features and remaining plant systems. The reactor core is represented by a number of regions, consisting of fuel, cladding and box material. Control rods are modelled as heat sinks associated with the corresponding core regions.

MAAP 3.0B does not describe in detail all the processes which can occur during a degraded core accident. The core melt progression, melt migration, and fuel-coolant interaction models are simplified. A simplified aerosol physics model is used, which is based on more detailed models and experimental results. Chemical processes and phenomena are based on pre-determined assumptions of the chemical species occurring in accident conditions. MAAP is considered to give a reasonable picture of accident progression, helpful for the design of mitigative measures. MAAP 4.0 will hopefully give better opportunities to study reflooding phenomena.

MELCOR

MELCOR is a second generation integral code which models accident progression from the initiating event through core uncovery, core degradation, fission product release and transport through the reactor coolant system and containment to the environment. The latest available version (April 1993) is MELCOR 1.8.2. Most of the SIK-2 calculations were made with earlier versions.

MELCOR is much larger and 10-20 times slower than MAAP 3.0B. It can be run on a powerful personal computer or a workstation. For an integral code, it contains many mechanistic or semi-mechanistic models with capabilities approaching those of the most detailed codes a few years ago. Plant nodalization and heat structure modelling are more flexible than with MAAP and aerosol and chemistry representation is more detailed. There are, however, still considerable simplifications and limitations in some of the models.

SCDAP/RELAP5

SCDAP/RELAP5 is a mechanistic best-estimate code which treats in-vessel core degradation up to and including vessel failure. The current version, SCDAP/RELAP5 Mod 3, has been available since mid-1992. It describes the coupled interactions between thermal-hydraulic and chemical phenomena occurring within the reactor coolant system during the accident. The user can freely describe different kinds of thermal-hydraulic structures, control systems and material properties. According to the peer review undertaken after the release of the code, improvements in some models is needed to achieve the high requirements on the code.

SCDAP/RELAP5 seems to be about 500 times slower than MAAP and requires an advanced workstation or a supercomputer for reasonable computing times. The code is intended to be used for benchmarking and can generally describe experimental facilities and test boundary conditions much better than the systems codes. For example, it has sufficient detail to allow simulation of the TMI-2 accident. SCDAP/RELAP5 is presently more suitable for PWRs than for BWRs.

4.4.2 Case studies

In subtask 2.2, MAAP 3.0B, MELCOR and SCDAP/RELAP5 have been used for two types of unmitigated core melt accidents in TVO I/II in Finland and Forsmark 3 in Sweden. The purpose has been to assess the modelling of important phenomena, to provide support for the implementation of MELCOR and SCDAP/RELAP5, and to compare the overall predictions. For a full account of the results, reference is made to the SIK-2.2 final report [52].

The studied sequences are station blackout and large steam line break (LOCA) with station blackout. They represent enveloping cases for the design of the mitigation systems. The automatic depressurization system is assumed to be activated in both sequences. Due to properly timed depressurization, the core will be completely uncovered before appreciable heating occurs. Accordingly, the core melt progression will be of the steam-starved, low oxidation type ("dry core meltdown").

Due to different values of corresponding or comparable model parameters, the study was more of a sensitivity test than a comparison of actual differences in modelling. With comparable modelling data, the predictions agree reasonably well with regard to vessel failure time

and in-vessel hydrogen generation. The range of uncertainty in the time to vessel failure is about 10 min to 1 hour, depending on the case studied.

It is recommended that MAAP reactor vessel geometry and initial water inventory be carefully checked and the code's predictions for the initial conditions be benchmarked against state-of-the-art thermo-hydraulic codes, such as RELAP5.

MAAP 3.0B predicts about 30 % less water inventory loss during depressurization than the other two codes. While MAAP predicts that the two-phase level will remain in the lower part of the core after depressurization in some of the sequences studied, the other codes predict complete core uncovery and a dry meltdown scenario.

In the previous cases, no safety systems were assumed available and no mitigative operator actions were supposed to be taken. In subtask 2.3, the effects of core cooling recovery by refilling the degraded core with water was investigated [53]. The studies were restricted to in-vessel phenomena in an overheated core, still geometrically intact at the start of reflooding. This restriction was imposed since the available computer codes do not yet have reliable models for treating situations where water is introduced in a partially molten core.

Reflooding was supposed to be achieved by the recovery of power and operation of the auxiliary feedwater system at a certain maximum core temperature reaches 1500 K. This temperature was chosen because the first eutectic reactions and melting of control blade material start at about 1500 K. The eutectic melting temperature of core material (fuel, cladding and box) is assumed to be 2500 K.

While there were appreciable differences in the maximum cladding temperature and the timing of events, all codes predicted an eventually decreasing temperature. The amount of hydrogen generated varied at most a factor of ten between MAAP and SCDAP/RELAP with MELCOR results intermediate. In all cases, a significant increase in hydrogen production occurred upon re-entry of water into the hot core.

4.4.3 Recriticality of a degraded core

The SIK-2.2 and 2.3 studies indicated that localized control rod melting may start prior to fuel melting in an overheated core. Thus, a time window may exist in which the control rods have relocated from regions of the core, where fuel rods still retain their original geometry. Water addition to the core during this time period opens the possibility of reactor recriticality and pressure buildup.

An analogous situation may occur upon reflooding of the core debris in the lower plenum. The core debris and reflood water might form a supercritical configuration, leading to a power excursion and steam formation as well as accelerated zirconium-water reaction and hydrogen generation.

Subtask SIK-2.4 was intended to investigate the likelihood and consequences of recriticality in the reflooding of a degraded core. It was planned to be initiated following the completion of subtask 2.3. Due to delays in concluding this project, subtask 2.4 had to be postponed.

The basic difference for recriticality in boiling and pressurized water reactors is that in PWRs, the primary and emergency core cooling water is always borated. Differences in core melt behaviour should also be kept in mind. In BWRs the reactor system is depressurized early in the accident and the core is rapidly uncovered. The recriticality issue applies therefore primarily to BWRs.

The possibility of recriticality in a rubble bed of core material is more difficult to analyze. The geometry, composition and porosity of the debris and the volume ratio of water to uranium are important parameters. Preliminary studies in the RAMA project indicate that the probability of critical configurations is low [45].

4.5 Chemistry and aerosol modelling

Integral codes, such as MAAP, use empirical correlations for aerosol and chemical phenomena. In mechanistic codes, the models are as far as possible based on first principles. In the early approaches, thermo-hydraulics, fission product chemistry and aerosol physics were treated separately, and the interaction between these phenomena was essentially neglected. In current system codes, the coupling between fission product decay heat and aerosol transport is taken into account, but chemical phenomena are only crudely represented.

4.5.1 Chemical models for the MAAP code

Efforts to develop improved chemistry models for MAAP began at the Chalmers University of Technology in 1985 as part of the NKA-AKTI programme. A first version of an extended MAAP code, was ready in 1989. It turned out that this version was not capable of handling all situations encountered during a typical severe accident. Further work was aimed at developing models and algorithms better suited to the conditions of severe accidents and to the structure of MAAP.

In subtask 2.5 of the SIK project, an improved code, called CHMAAP (CHemistry in MAAP), has been developed and tested [54]. CHMAAP is intended for sensitivity analysis of possible chemical effects and interactions between chemistry and transport phenomena, not normally modelled in the standard MAAP version, and to provide a chemical and thermodynamic data base. The general type of chemical modelling in CHMAAP allows inclusion of any chemical reaction and compunds, provided the necessary thermochemical data are available. Rate-limited chemical reactions can also be represented, if kinetic data are available.

In MAAP 3.0B, fission product and structural material releases from the core are treated in twelve substance groups. Empirical correlations are used to calculate the release rate of fission products. Removal of fission products, except noble gases, occurs by vapour condensation or aerosol deposition in the primary circuit and containment. The condensation and deposition processes are accounted for through correlations.

In CHMAAP, the chemical models introduced import data from MAAP on temperatures, flow rates, pressures and masses. The models are based on three steps which are applied to all subsystems in a region: (i) formation of a chemical system, which can be homogeneous, such as a mixture of gases, or heterogeneous, (ii) chemical change, e.g. gas reactions, heterogeneous reactions, or changes in aggregation state such as evaporation/condensation, (iii) effect on mass transport. Some processes, such as the generation and condensation of steam and the oxidation of zirconium, are considered adequately treated in the standard MAAP code.

Interactions of fission product vapours with surfaces can modify the magnitude and nature of the source term substantially. In order to demonstrate the importance of modelling the deposition velocity correctly, three test runs were performed with CHMAAP and one run with the standard MAAP 3.0B Rev6. The selected accident sequence was a total station blackout for the Oskarshamn I BWR plant. Only a few chemical species were included to simplify the comparison and minimize computation time. The conditions are shown in Table 17.

Table 17 Conditions for test runs

Case on	Code	Condensation/evaporation velocity	
		aerosol particles	walls
C I	CHMAAP	Intermediate	Intermediate
C II	CHMAAP	Intermediate	Rapid
C III	CHMAAP	Rapid	Intermediate
M	MAAP	Standard	Standard

"Rapid" condensation/evaporation velocity means that equilibrium is reached almost instantaneously if the process is isolated. Intermediate condensation/evaporation velocity results in equilibrium within 45 to 50 seconds in a closed system.

As an example of calculated results, the content of cesium in the reactor vessel and containment is shown in Figure 18. Detailed information on the deposition and distribution of CsI in various compartments in the reactor system and the corresponding temperatures is given in the project report. While the general trends are similar, there are significant quantitative differences depending on the assumptions. The only way to resolve the differences is to compare results of experiments with predictions from CHMAAP.

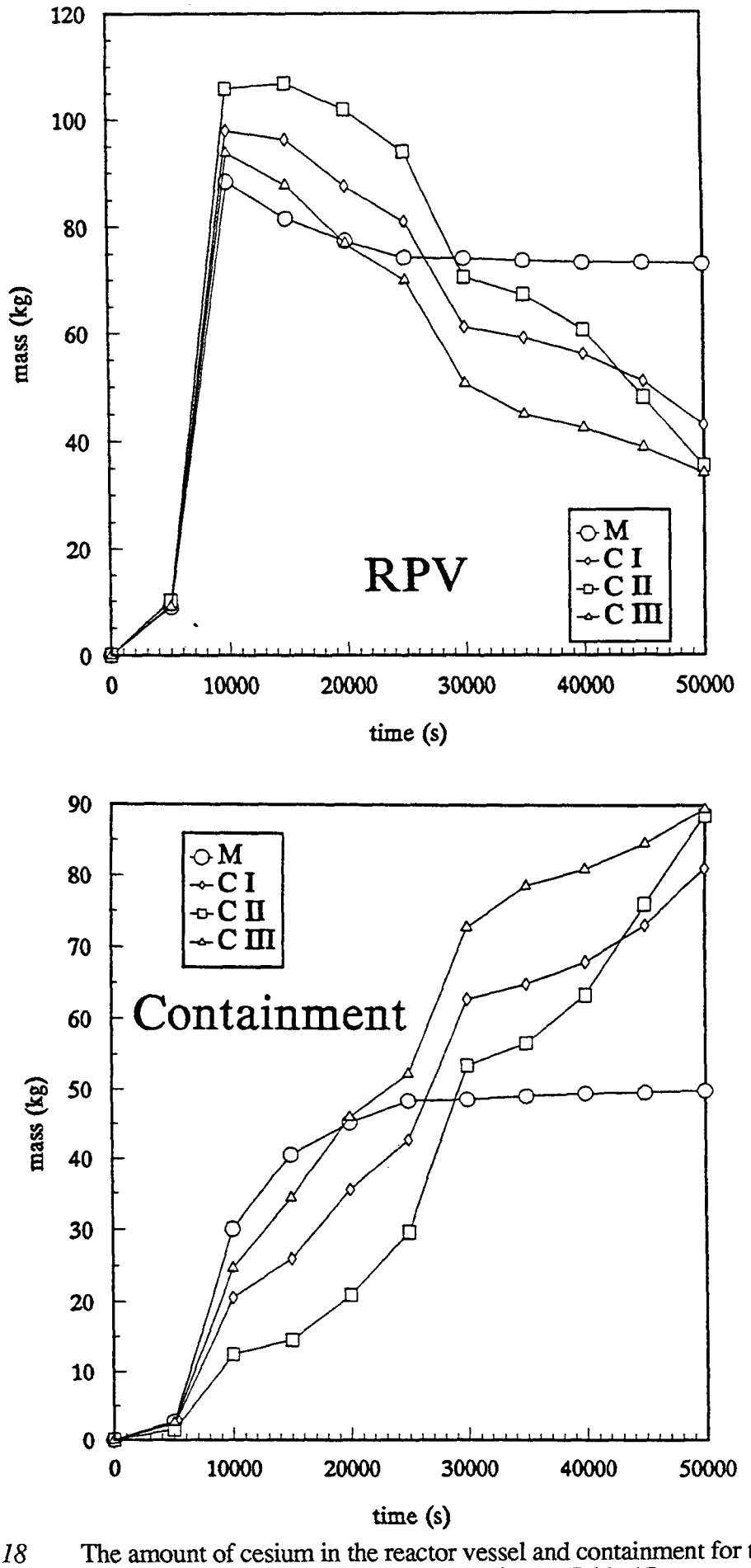


Figure 18 The amount of cesium in the reactor vessel and containment for test runs with CHMAAP and MAAP according to Table 17.

4.5.2 Assessment of aerosol models

The basic processes governing aerosol transport are generally well understood, although the application of the fundamental models to treatment of complex geometry and large-scale structures is less well developed. A large number of aerosol codes are available, based either on application of empirical models or a more mechanistic approach. The empirical models are used in integral codes, whilst the mechanistic codes are of the stand-alone type which have to be linked to thermal-hydraulic codes for obtaining boundary conditions.

In SIK- 2.6 a number of aerosol codes have been reviewed and assessed. Since the conditions in the reactor coolant system and the containment are quite different, it is convenient to use different codes for the two cases. Therefore, in a first project report, aerosol modelling in reactor coolant system codes is treated [55].

When fuel is damaged and melts, gaseous and volatile fission products are released. Due to the high temperature, the fission products and other core material are mostly released as vapours which are carried away into the upper plenum and further downstream in the reactor coolant system. The vapours may condense on cooler surfaces or form aerosols. The high temperature and the presence of hydrogen make many chemical reactions possible, some of which directly or indirectly involve fission products.

Aerosol particles are generated by condensation or nucleation of vapours. When the vapour pressure of a particular species reaches its saturation pressure, condensation will set in if sufficiently many particles are present. Otherwise, homogeneous nucleation will take place, if the supersaturation is high enough. The aerosol particles may grow or shrink due to further condensation or evaporation. In humid conditions, steam condenses on the particles.

Aerosol particles may grow by colliding and sticking together. This process, known as *agglomeration,* plays an important role for the particle size distribution, particularly at high number density. As a result a spectrum of particle sizes is obtained, where the particle diameter varies from less than 0,1 to about 10 microns (thousands of a millimeter) or more. The smallest particles can remain suspended for a very long time.

Aerosol particles are removed from the gaseous phase by various *deposition* mechanisms, such as gravity, diffusion, thermophoresis, turbulent flow deposition, and deposition in bends. In the reactor coolant system with large temperature gradients, aerosols are deposited by thermophoresis in cooler compartments. Particles not deposited are transported by convection to the reactor containment.

Under certain conditions, deposited particles are returned to the gaseous phase. *Revaporization* means that particles are released when deposited substances are heated by fission product decay heat. Mechanical resuspension may arise from strong gas streams or shocks and vibration in substrate structure, which dislodge and relevitate deposited particles.

In the first part of the SIK-2.6 project, aerosol modelling in the following codes was reviewed: TRAP-MELT3, SCDAP-RELAP5, MELCOR, VICTORIA and RAFT. For details, reference is made to the project report [82]. While each code makes different assumptions and approximations in modelling the phenomena, no code appears significantly better than the others in predicting deposition. No evidence that the current code versions have been checked against experiment has been reported. The importance of aerosol nucleation and resuspension phenomena should be evaluated.

4.6 Accident management support

4.6.1 Introduction

Modern nuclear power plants have engineered safety features to prevent severe accidents and limit the consequences if such an accident occurs. Emergency operating procedures have been established for the operating staff to maintain or restore critical safety functions during the course of accidents within the design basis. For potential accidents beyond the design, i.e. extreme events which the safety systems fail to control or which the safety systems are not designed to control, a strategy of accident management is applied.

Preventive accident management refers to actions by the operators during the evolution of an accident sequence after the conditions have come to exceed the design of the plant but before a core melt accident actually develops. Accident management also includes mitigative action by the operating staff to prevent further progress of a core melt accident, once it has occurred, and to limit any potential releases of radioactive material to the environment.

Timely and accurate plant status information must be available for plant personnel to successfully manage potential accidents. The information must be presented in a way which corresponds to the needs of the user to understand plant behaviour for a broad range of accident conditions. The different data bases in use at the plant must be mutually compatible and easily retrievable through a common data link system. The capability of instruments to function properly if an accident occurs should be clearly understood so that the availability of the instruments can be assessed.

The ability to benefit from accident management requires not only the provision of adequate information to the control room but also a capability for control of events from this location. Training of operator staff ensures familiarity with the symptoms of beyond-design accidents

and the procedures for accident management. Simulators are indispensible training tools in this respect. However, they must be able to represent correctly the way in which an accident would evolve. Advanced simulator and information systems might be used to provide on-line support for accident management action.

4.6.2 The CAMS project

Successful accident management includes several tasks, such as identification of the actual plant state, assessment of accident progression, and planning of mitigation strategies. The SIK-2.7 project was initiated at the OECD Halden Reactor Project to investigate the possibility of providing computerized support for these tasks [56].

The project, which is known by its acronym CAMS (Computerized Accident Management Support), is divided into a prototype phase and a product phase. The prototype does not attempt to cover the complete functionality of the ultimate product, but significant features and solutions are incorporated so that the system can be tested for some accident scenarios, with real operator interaction.

The Swedish Forsmark 1/2 BWR will be used as the test plant. It is assumed that the principles illustrated in the prototype can be adapted to other BWRs with a modest amount of modification and also to PWRs and even to other kinds of industrial plants, since many problems of accident simulation are similar, regardless of the type of plant:

- Is the available information correct?
- How can information be obtained of physical quantities not directly measurable?
- How far is the present state from relevant bounding conditions?
- Which subsystems are available and which are not?
- What will happen if nothing is done?
- What will happen if this particular plan is carried out?
- What is the best strategy in the present situation?

CAMS is presently (summer 1993) in the prototype phase. A program structure has been outlined, containing a data base, a tracking-mode simulator, an expert system for the generation of strategies, and man-machine interface. During development, the prototype is connected to a plant simulator, which has been installed at IFE Halden.

Although the CAMS project is as yet only in the prototype phase, it is believed that the approach is feasible. CAMS will permit structuring of verified and relevant information and adapting it to the needs of various groups engaged in accident management. In particular, the possibility of eliminating comprehensive but irrelevant and sometimes even erroneous information should be emphasized.

In the first stage, the prototype should concentrate on in-vessel accident progression and preventive accident management. Ex-vessel behaviour and mitigative accident management are more complex and difficult to simulate. Simple principles should be applied for the generation of strategies, and the information needed should be carefully selected and suitably displayed.

4.7 Conclusions

The Nordic approach to severe accident research is to follow and participate in, as appropriate, the comprehensive international research activities in progress, and to undertake independent research on selected topics of particular interest to Nordic reactors. The overall objective is to improve the understanding of severe accident phenomena and to acquire tools for the analysis of potential accidents as a basis for the design of safety-enhancing equipment and the specification of accident management procedures.

The SIK-2 project has included an in-depth review and intercomparison of computer codes for the analysis of severe accidents, case studies of selected accident sequences as well as some innovative modelling of chemical phenomena.

A two-stage approach to severe accident analysis has been pursued, implying that the MAAP code is used for survey calculations and detailed mechanistic codes for independent verification. The advanced MELCOR and SCDAP/RELAP5 codes have been successfully taken into active use. The long execution times indicate that these codes are unsuitable for routine calculations but should be used for validation of fast-running integral codes such as MAAP.

Comparisons between the advanced codes and the latest available MAAP version for design-basis severe accidents show qualitative agreement in the prediction of in-vessel accident progression but significant quantitative differences, such as in the amount of hydrogen generated and the time to reactor vessel failure. Some improvements of the codes are suggested as a result of the review. The current code versions are unable to treat reflooding of a degraded core correctly. It is expected that MAAP 4.0 will be able to simulate reflooding further into the accident.

It is concluded that the general understanding of severe accident phenomena has increased considerably during recent years, but that code predictions must still be treated with caution and interpreted with expertise, since the accuracy of the results is essentially unknown.

This is not surprising in view of the non-linear interactions, the chaotic behaviour and the intractable geometry involved. The area is still in development and new code versions appear continuously. Substantial improvements can only be achieved by comparison with well characterized experiments.

The question of recriticality upon reflooding was only reviewed qualitatively. Results from SIK-2.2 and 2.3 indicate that the time window for potential recriticality could be narrower than previously estimated.

It is important that the follow-up of international activities in severe accident code development and use continues, since the state-of-the-art cannot as yet be considered definite. Further studies of meltdown and reflood scenarios should be carried out. Planned case studies of possible recriticality in reflooded cores should be pursued.

Improved models of chemical phenomena have been incorporated in the CHMAAP code. Test results indicate the importance of chemical modelling and show considerable differences in the transport of radiologically important species, depending on the basic model assumptions. The ambiguities can only be resolved by comparison with experiments. More test calculations should be carried out.

The review carried out in the SIK-2.6 project indicates that basic aerosol phenomena are fairly well modelled in the mechanistic codes, but that weaknesses still exist in the treatment of aerosol behaviour in complex geometries. The interaction of chemical and aerosol phenomena seems to be less well represented. No numerical code intercomparisons were made, as originally planned. The comparisons should be completed, in particular to allow an assessment of the aerosol modelling in MAAP. If possible, the exercise should be extended to include comparison with experiments.

The CAMS project for the development of a computerized accident management support system has been initiated. A prototype concept has been defined, and some simulator software has been implemented. The project will not be completed within the time schedule of the SIK programme, but preliminary indications are that the approach is feasible.

The potential conflict between the existing emergency operating procedures and CAMS recommendations should be kept in mind. It is important to realize the limitations of a system like CAMS. All accident situations cannot be anticipated, and predictions must be treated with caution. In this case, the computer can support but never replace common sense and engineering judgement. It is possible that the best use of CAMS will be for training. The success of the project will depend on the continued support and participation of potential users.

5 Safety design of nuclear reactors in neighbouring countries (SIK-3)

5.1 Project outline

The Chernobyl accident in 1986 revealed a remarkable lack of information in the Nordic countries and elsewhere in the West on the safety design and performance of Russian reactors. Obviously, such information is needed for independent evaluation of accident progression and potential consequences, should a severe nuclear accident occur. It is also necessary to be able to inform the news media and the general public at short notice. Similar information is needed for Western reactors near to the borders of the Nordic countries.

The objective of the SIK-3 project was to collect information on each nuclear installation within about 500 km from the borders of the Nordic countries. Data should be compiled on a common format for easy reference, to be used primarily by the safety authorities in responding to general questions on a particular plant and in evaluating any safety-related occurrences in the plant and the potential consequences.

The plants of interest are located in Germany, Lithuania and Russia as shown in Figure 19. The corresponding reactor units are listed in Table 20.

The data were collected from the open literature and through plant visits. Detailed information is presented in seven plant reports [57 -63], and summarized in the final project report [3].

A technical report was also compiled on the Greifswald Nuclear Power Plant, located on the shore of the Baltic Sea about 20 km northeast of the town of Greifswald, Germany [64]. This plant had four VVER-440 of the old V-230 type in operation and four VVER-440/V-213 under construction, when a decision was taken, after the reunification of Germany, to abandon the plant.

Reviews of marine reactors were also undertaken and published in three reports on civilian nuclear ships [65], nuclear ship accidents [66], and nuclear-powered submarines [67]. The reason for including marine reactors is that nuclear-powered ships and submarines are known to operate in the seas near to the Nordic countries.

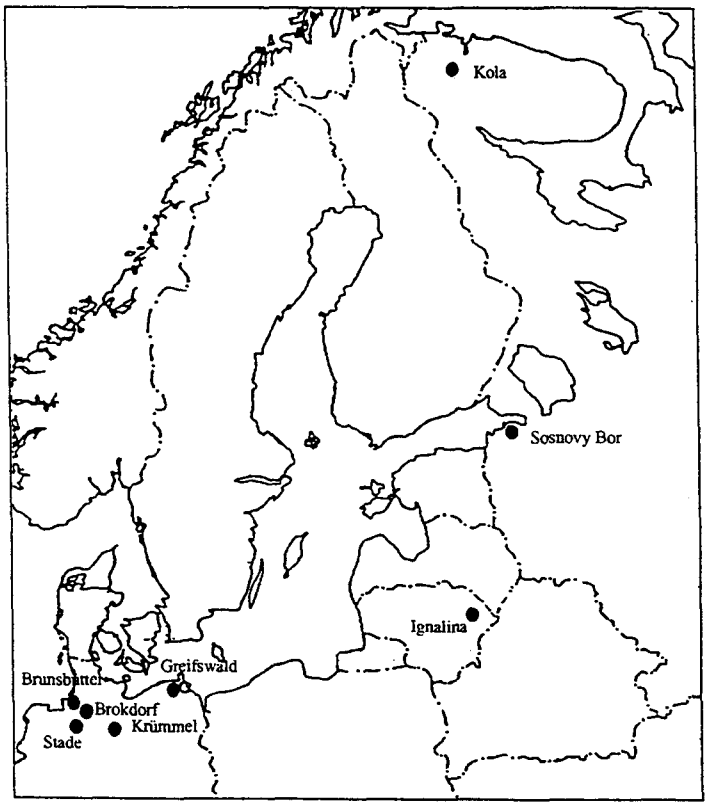


Figure 19 Location of nuclear power plants

Table 20 Nuclear power plants in neighbouring countries

Plant	Reactor type	Operator	NSSS supplier	Power MWel gross	Com-miss-ioned
Brunsbüttel	BWR	KKB	KWU	806	1976
Krümmel	BWR	KKK	KWU	1316	1983
Stade	PWR	KKS	KWU	672	1972
Brokdorf	PWR	KBR	KWU	1383	1986
Kola-1	VVER-440/230	Rosenergoatom		440	1973
Kola-2	VVER-440/230	"		440	1974
Kola-3	VVER-440/213	"		440	1981
Kola-4	VVER-440/213	"		440	1984
Leningrad-1	RBMK-1000	Leningrad NPP		1000	1973
Leningrad-2	RBMK-1000	"		1000	1975
Leningrad-3	RBMK-1000	"		1000	1979
Leningrad-4	RBMK-1000	"		1000	1981
Ignalina-1	RBMK-1500	Minatomenergoprom		1500	1983
Ignalina-2	RBMK-1500	"		1500	1987

5.2 German reactors

5.2.1 Safety regulation

The legal basis for nuclear licensing and inspection activities in Germany is the Atomic Energy Act of 1959. The responsibility for implementing the legislation lies with the individual States (Länder). The States have established their own safety authorities. Many authorities are therefore involved in the executive activities, in contrast to the situation in countries with a centralized structure, such as in Finland, Sweden and USA.

The federal Ministry of the Environment, Natural Protection and Reactor Safety (Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, BMU) is responsible for supervising the nuclear safety activities of the States. The Ministry is advised by the Commission for Reactor Safety (Reaktorsicherheitskommission, RSK) and the Commission for Radiological Protection (Strahlenschutzkommission, SSK). To a large extent, the State authorities use external organisations for safety analysis, site inspection, and expert opinion. In the majority of cases, the regional Technical Inspection Agencies (Technische Überwachungsvereine, TÜV) and the Society for Reactor Safety (Gesellschaft für Reaktorsicherheit, GRS) are entrusted with these tasks.

On the basis of the Atomic Energy Act, ordinances have been issued, e.g. on the licensing procedure. Licensing is a multi-step procedure, involving public display of the application documents to give all interested parties a possibility to intervene.

In order to implement the intentions of the Act and Ordinances, safety criteria and standards have been defined, including fundamental safety principles and safety analysis for plant design and operation. The criteria are based on the defence-in-depth principle. The safety approach gives priority to automatic measures for incident and accident prevention, complemented by actions for accident management.

The legal requirements are supplemented by regulatory guidelines issued by BMU and RSK, to be met in the design, construction and operation of nuclear power plants. Separate guidelines have been prepared for pressurized and boiling water reactors.

Standards are prepared by the Nuclear Safety Standards Commission (Kerntechnischer Ausschuss, KTA). When standards have been accepted, the corresponding guidelines become obsolete. The German Standards Institute (Deutsches Institut für Normung, DIN) also formulates standards with respect to nuclear safety. The work is coordinated with that of KTA, and the KTA standards are also DIN standards.

The hierarchy of regulations is illustrated in Figure 21.

Safety-related occurrences are reported to the supervisory authorities who pass them on to GRS for documentation and evaluation. Reporting criteria define the type of events to be reported and the time limits which must be adhered to. Once a year the BMU publishes a comprehensive description of the unusual events. On the basis of bilateral agreements, event reports from foreign NPPs are also documented and evaluated by GRS.

The Atomic Energy Act stipulates that persons responsible for the design, construction, operation and supervision of nuclear power plants must have the necessary qualifications. Special guidelines define the requirements of education, experience and knowledge to be placed on various personnel categories.

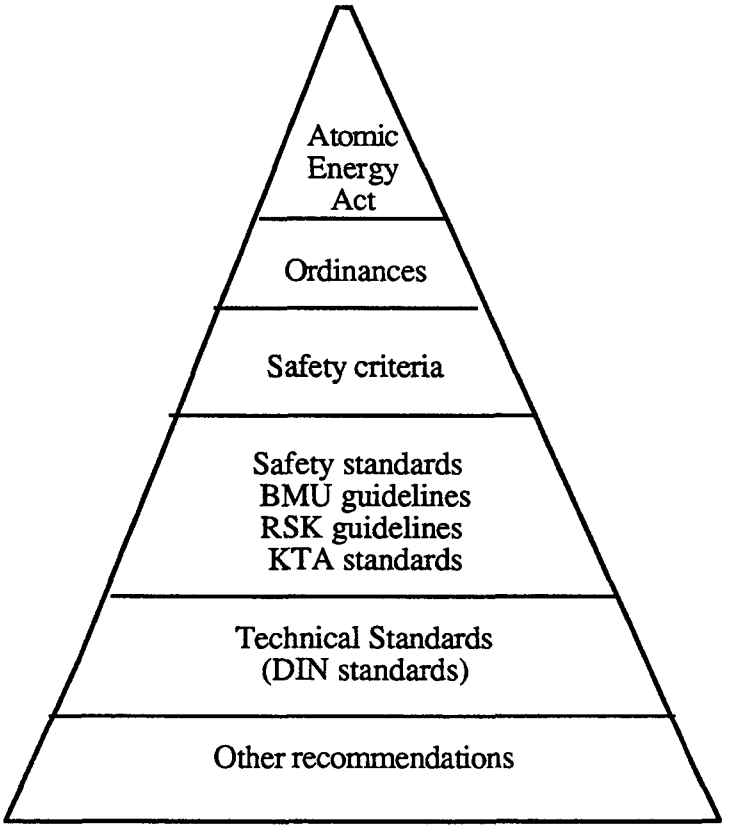


Figure 21 The structure of safety regulations in Germany

5.2.2 Boiling water reactors

Reactor development

The German BWR development started with the 17 MWe Kahl reactor, which operated from 1962 to 1985. The basic reactor concept was taken over from the General Electric Company in the USA, but the technical realization was carried out mainly by German companies. The next BWR plants were Gundremmingen A and Lingen. The Lingen reactor pioneered the use of fine-motion control rods with independent electromechanical and hydraulic drive mechanisms, designed by AEG-Telefunken (now KWU-Siemens). These reactors, which had external recirculation pumps and indirect steam cycle, have since been taken out of service.

In Germany, the direct steam cycle and the pressure suppression reactor containment was first introduced in the 670 MWe Würgassen plant, commissioned in 1975. The reactor has two external main recirculation pumps and 16 internal jet pumps, similar to General Electric BWRs.

The interaction between German vendors and the utilities soon led to deviations from the plant concepts originally adopted from General Electric on a license basis. The 806 MWe Brunsbüttel plant introduced a fully integrated primary coolant circuit with eight internal axial pumps. The plant was commissioned in 1977.

Brunsbüttel was the first plant in the 69-series ("Baulinie 69"), which also included two 900 MWe plants and the 1316 MWe Krümmel plant. Typical of the 69-series is the spherical steel containment building with an annular "hanging" condensation pool around the reactor pressure vessel.

The adoption of internal recirculation pumps led to a considerable improvement in safety. The maximum pipe break area is substantially reduced and the corresponding water discharge time is increased. Another consequence is that the design of the pressure suppression system is simplified. In Sweden, internal recirculation pumps were first introduced in the Forsmark series of reactors.

The engineered safety features in the 69-series of plants are similar to those of the ABB Atom BWR-75, as implemented in the TVO and Forsmark plants. The plants are automatically depressurized in case of a loss-of-coolant accident. Two kinds of auxiliary feed water systems are available to supply make-up water at all system pressures. One system has an electrically driven circulation pump and the other a steam-driven pump. At low pressure after depressurization, a core flooding system supplies water to the reactor vessel.

The spherical reactor containment has double steel walls. The annulus between the walls is maintained at subatmospheric pressure and enables monitoring of leaks from the inner shell. The containments were modified to include filtered venting in the late 1980s. Venting is done from the wetwell air space through a venturi scrubber and a filter unit.

The next development step was the 72-series ("Baulinie 72"), as realized in the 1310 MWe Gundremmingen B and C units. In these reactors the spherical steel containment is replaced by a cylindrical concrete containment with a steel liner and an annular wetwell surrounding the drywell, similar to BWR-75. The emergency core cooling and residual heat removal systems have three subsystems, each with 100 % cooling capacity, in contrast to the 4x50 % subdivision adopted for BWR-75.

The detailed design and performance of the Brunsbüttel and Krümmel nuclear power plants are described in the project reports [59, 60]. The operating experience is briefly summarized below.

Brunsbüttel

The Brunsbüttel NPP is located in the area of Dithmarschen in Schleswig-Holstein on the north side of the river Elbe, about 90 km from the city of Hamburg and 100 km from the Danish border. The plant is operated Kernkraftwerk Brunsbüttel GmbH and owned by Hamburgische Elektricitätswerke AG (2/3) and PreussenElektra AG (1/3). The plant has a net capacity of 771 MWe.

During the first cycle of operation in 1977, problems with the internal pumps caused an outage of five months. From mid-1978 through 1979 the plant was shut down for general repair and backfitting. Normal operation was not resumed until the end of 1980 due to difficulties in obtaining the necessary permits. From mid-1982 the plant was out of service for about a year for replacement of primary circuit piping, following a decision by the German authorities to change piping in all BWRs. During the major part of 1989 the plant was operated at reduced power due to problems with containment isolation valves.

The average load factor[1] for the plant from the start of commercial operation through 1991 was 55,8 %.

[1] The load factor is the net electrical energy produced during the reference period under consideration, divided by the net electrical energy which would have been produced at maximum net capacity under continuous operation during the whole of the reference period.

Krümmel

The Krümmel NPP is located in the state of Schleswig-Holstein by the northern side of Elbe, about 34 km upstreams of Hamburg. The plant is operated by Kernkraftwerk Krümmel GmbH, jointly owned by Hamburgische Elektricitätswerke AG (1/2) and PreussenElektra AG (1/2). The plant has a net capacity of 1260 MWe.

After commissioning in March 1983, numerous outages occurred throughout the rest of the year due to pump problems and tests of equipment. In early 1985 the unit was temporarily shut down following sabotage on a high voltage tower. In 1987 an IAEA operational safety review team visited the plant, giving a favourable overall report while recommending a number of improvements. The unit received its final operating license in April 1988, having operated on temporary permits since the start. In July the same year a court ruled against the last of some 400 intervenor cases challenging the unit's construction permit. The annual outage in 1989 was extended for nine weeks after a fuel assembly was dropped from the crane into the spent fuel pool during refuelling.

The average load factor from the start of commercial operation through 1991 was 81,3 %.

5.2.3 Pressurized water reactors

The design of the first German PWR for the 360 MWe Obrigheim plant, was initiated by Siemens AG in the early 1960s, based on licenses from the Westinghouse Corporation in the USA. Commercial operation began in 1969. The reactor is still in operation after 15 months of forced outage during 1990-1991 due to a series of contradictory court orders. Obrigheim was followed by the 672 MWe Stade NPP, commissioned in 1972.

The second generation of German PWRs is represented by the 1200 MWe Biblis A plant and three similar plants. This series of plants, which were designed in the early 1970s and placed into operation towards the end of the decade, is characterized by independent PWR technology, adapted to German conditions.

Further technology development and harmonization is incorporated in the next series of four PWRs, designed during the mid-1970s and commissioned in the first half of the 1980s.

The current generation of German PWRs is known as the Konvoi series. Three plants have so far been built and taken into operation in the late 1980s. The Konvoi plants have a high degree of standardization, allowing a simplified licensing procedure.

German PWRs have shown a very good availability. One of the third generation plants, the 1375 MWe Grohnde NPP, holds the world's record for annual power generation of 11,48 TWh in 1985.

Stade

The Stade NPP is located on the left side of the river Elbe, about 35 km downstreams of Hamburg. The plant is operated by Kernkraftwerk Stade GmbH, jointly owned by Nordwestdeutsche Kraftwerke AG and Hamburgische Elektricitätswerke AG. The plant has a net output of 640 MWe and is also for supplying heat to a nearby desalination plant.

The reactor has four main coolant loops, each containing a pump and a steam generator [57]. The emergency core cooling system has a high-pressure coolant injection system, an accumulator system, and a low-pressure injection system, as customary for PWRs. The pumps of the high-head injection system are identical to those of the three charging pumps of the chemical and volume control system, one of which is continuously in operation for coolant make-up. The low-head injection system is part of the residual heat removal system, normally used for decay heat cooling at shutdown. The use of common systems for both normal operation and emergency cooling is typical for PWRs and require operator action for realignment.

Like all German PWRs, Stade has a double reactor containment with an inner spherical steel shell and an outer hemispherical concrete structure. The space between the two shells is kept below atmospheric pressure by a ventilation system. Any minor leakage flow from the inner containment is filtered before reaching the environment.

The average load factor from the start of operations in 1972 through 1991 was 81,2 %.

Brokdorf

The Brokdorf NPP is located on the right side of Elbe about 70 km northwest of Hamburg. The plant is operated by Kernkraftwerk Brokdorf GmbH, jointly owned by PreussenElektra AG (80 %) and Hamburgische Elektricitätswerke AG (20 %). The plant has a net output of 1326 MWe.

Brokdorf was the fourth NPP to be built in the area. Plant construction was delayed by four years due to massive local resistance to nuclear power in the region.

Brokdorf is the last in the third generation of "harmonized" German PWRs to be taken into operation. The average availability from commissioning in 1986 through 1991 was 77,5 %. With an annual electricity generation of 11,33 TWh, Brokdorf produced more energy than any other nuclear reactor in the world during 1992.

Summary design data and technical description are presented in the project report [58].

5.3 Russian reactors

5.3.1 Safety standards

The Chernobyl accident revealed deficiencies in the design of RBMK reactors. The general safety standards of Russian reactors were put in question, e.g. regarding the quality and reliability of process equipment and control systems. In general, Russian reactors do not satisfy the safety requirements applied in the West, such as for physical separation, diagnostic and monitoring systems, and fire protection.

The Soviet safety philosophy seems to prefer designing for accident prevention over safety features for the mitigation of severe accidents. For example, the VVER reactors have better thermal margins than similar Western reactors, whilst proper reactor containment is lacking in the earlier versions.

Most of the nuclear power plants are state-owned by the Ministry of Atomic Energy (Minatom). An exception is the Leningrad NPP which is owned by an independent consortium. Safety regulations and guidelines for operation are issued by Minatom and the State Management for Supervision of Nuclear Power Plants (GPAN). Licensing and supervision are carried out by GPAN who have resident inspectors at the plants. Relevant operational events shall be reported within five hours to GPAN and Minatom. Regulations for testing the qualifications of plant personnel are issued by Minatom.

Countries like Lithuania and the Ukraine have earlier not had safety authorities of their own and still have no nuclear legislation. For the time being they retain the former Soviet regulatory system.

5.3.2 Pressurized water reactors (VVER)

Reactor development

The first VVER prototype was a 210 MWe reactor at Novo-Voronezh, commissioned in 1964 and shut down in 1988. The final version of the first generation, which is known as VVER-440 type 230, was built in 18 units during the 1970s. Ten of them are still in operation. This reactor has a nominal power of 440 MWe with two turbines. Typically, twin units are installed with a number of service buildings in common. The reactor has six main coolant loops with horizontal steam generators. The emergency core cooling systems are designed to cope only with small breaks and leakages in the main coolant system. The plant has no containment in the Western sense, but the main coolant system is enclosed in an airtight structure with safety valves which open to the atmosphere.

In comparison to present internationally accepted standards the early VVER has serious deficiences but is more "forgiving" to disturbances. The water inventory in the primary and secondary circuits is large compared to the core power. Thermal power transients are effectively

damped, and natural circulation is sufficient to remove decay heat at shutdown from full power. The flexibility designed into the power conversion system with six steam generators and two turbogenerator trains provide for stable operation over a wide range of conditions.

The second generation VVER-440 type 213 has been built in 16 units during the 1980s, all of which are in operation. The general characteristics are the same as those of the earlier type but the safety systems have been significantly upgraded. The emergency core cooling systems are designed for all sizes of pipe breaks, and the physical separation and redundancy of the safety systems are improved. A reactor containment with a condensing tower is provided.

Finland's Loviisa NPP consists of two VVER-440 type 213 units, adapted to Finnish conditions and safety requirements, which at the time of licensing were almost identical to the U.S. regulations. While the basic design features of VVER-440/213 are retained, many systems and components are improved, using up-to-date Western technology. A containment able to cope with the consequences of a large pipe break in the main coolant system was designed, utilizing the Westinghouse ice condenser concept. Many improvements have been implemented after the completion of the plant, which is reflected in the excellent operating history.

VVER-440s have a generic problem in that the reactor vessel is susceptible to radiation-induced embrittlement due to the comparatively narrow water gap between the active core and the vessel wall. Annealing of vessels in type 230 plants is one method which has been applied to regain steel strength. In the Loviisa reactors, the neutron exposure of the vessel wall has been reduced by replacing the outermost fuel assemblies with dummy elements made of stainless steel.

The third generation is represented by VVER-1000 type 320, of which 18 units are in operation and several under construction. The nominal power is 1000 MWe with one or two turbines. The main coolant system has four loops with horizontal steam generators. The emergency core cooling systems have threefold redundancy and are designed to cope with any break sizes. The reactor has a full-pressure containment of prestressed concrete.

Despite the fact that the basic physics and thermohydraulic principles of VVERs and Western PWRs are essentially identical, the design solutions differ considerably. This is the result of initial technical limitations, for example in vessel size, and the use of different structural materials and design priorities. Some basic features are summarized in Table 22.

Table 22 Comparison of VVER and PWR design features [68]

Item	VVER	PWR
Fuel pellet diameter, mm	9,1	9,5
Reactor lattice	triangular	square
Hole in pellet	yes	no
Fuel cladding material	Zr-Nb	Zircaloy
Reactor vessel diameter	less than PWR	larger than VVER
Inlet-outlet nozzles	two rows	one row
Steam generator	horizontal	vertical
Steam pressure, MPa	6	7
Net efficiency, %	32	34
Liquid waste, relative units	3-5	1
Occupational exposure, rel.units	1,5-3	1
Uranium consuption, rel. units	1,2-1,5	1
Concrete, rel.units	1,3-3	1
Metal, rel.units	2-3	1
Cable, rel.units	1,5-2	1
Staff, rel.units	2	1

Kola

The Kola NPP is situated on the southern shore of Lake Imandra on the Kola peninsula in Russia. The plant has four VVER-440 units, Kola-1 and 2 of type 230, and Kola-3 and 4 of type 213, and is operated by Rosenergoatom, the new Russian consortium for nuclear power plant operation. Kola-1 and 2 were commissioned in 1973 and 1974, and Kola-3 and 4 in 1981 and 1984, respectively. The net capacity of each unit is 411 MWe.

A detailed technical description of the Kola reactors is presented in the project report [61]. The information is to a large extent based on the material compiled during the IAEA mission to Kola in 1991-1992.

Following the basic safety design philosophy of early VVERs, more emphasis has been put on preventing accidents than on safety systems for accident mitigation. The operational records of the Kola NPP shows that the reactors are not very vulnerable to disturbances caused by operational transients. The average load factors through 1991 were: 78,7 % for Kola-1, 78,0 % for Kola-2, 82,9 % for Kola-3 and 83,8 % for Kola-4.

The design-basis accident for Kola-1 and 2 (model 230) is a 50-100 mm diameter pipe break in the primary system. An emergency core cooling system with a capacity of 30 l/s is available for high-pressure injection of borated water.

Kola-2 and 3 (model 213) have improved safety features. The design-basis accident is a guilliotine break of a 500 mm pipe, and emergency core cooling includes an accumulator system.

Both model 230 and 213 rely on Accident Localization Compartments (ALCs) for confining the effects of pipe breaks and uncontrolled steam releases. The ALCs are steel-lined concrete rooms surrounding the nuclear steam supply system. The rooms can be sealed off and hold steam/gas to an overpressure of 0,1-0,15 MPa. In model 230 the ALC volume is approximately 10 000 m^3, sufficient to prevent the steam release following a 32 mm diameter pipe break. Larger steam releases may have to be vented to the atmosphere.

The essential difference between the ALCs of model 230 and 213 is that the latter have a bubbler/condenser tower for steam condensation, supposed to be able to handle the consequences of even a large loss-of-coolant-accident. A schematic comparison of safety design features is shown in Figure 23.

The design service life of VVER-440s is 30-40 years, which means that Kola-1 and 2 should be kept in operation at least over the turn of the century, and Kola-3 and 4 still ten years longer. Being aware of the enhanced safety requirements currently placed on NPPs, the authorities have initiated a reconstruction programme at the Kola NPP. The programme focuses on the safety of model 230, and the technical content is defined in collaboration with WANO (World Association of Nuclear Operators).

Measures have already been implemented to improve the safety of Kola-1 and 2. The most important are pressure vessel annealing in 1989, installation of monitoring equipment in the primary circuit, and improvements in fire safety.

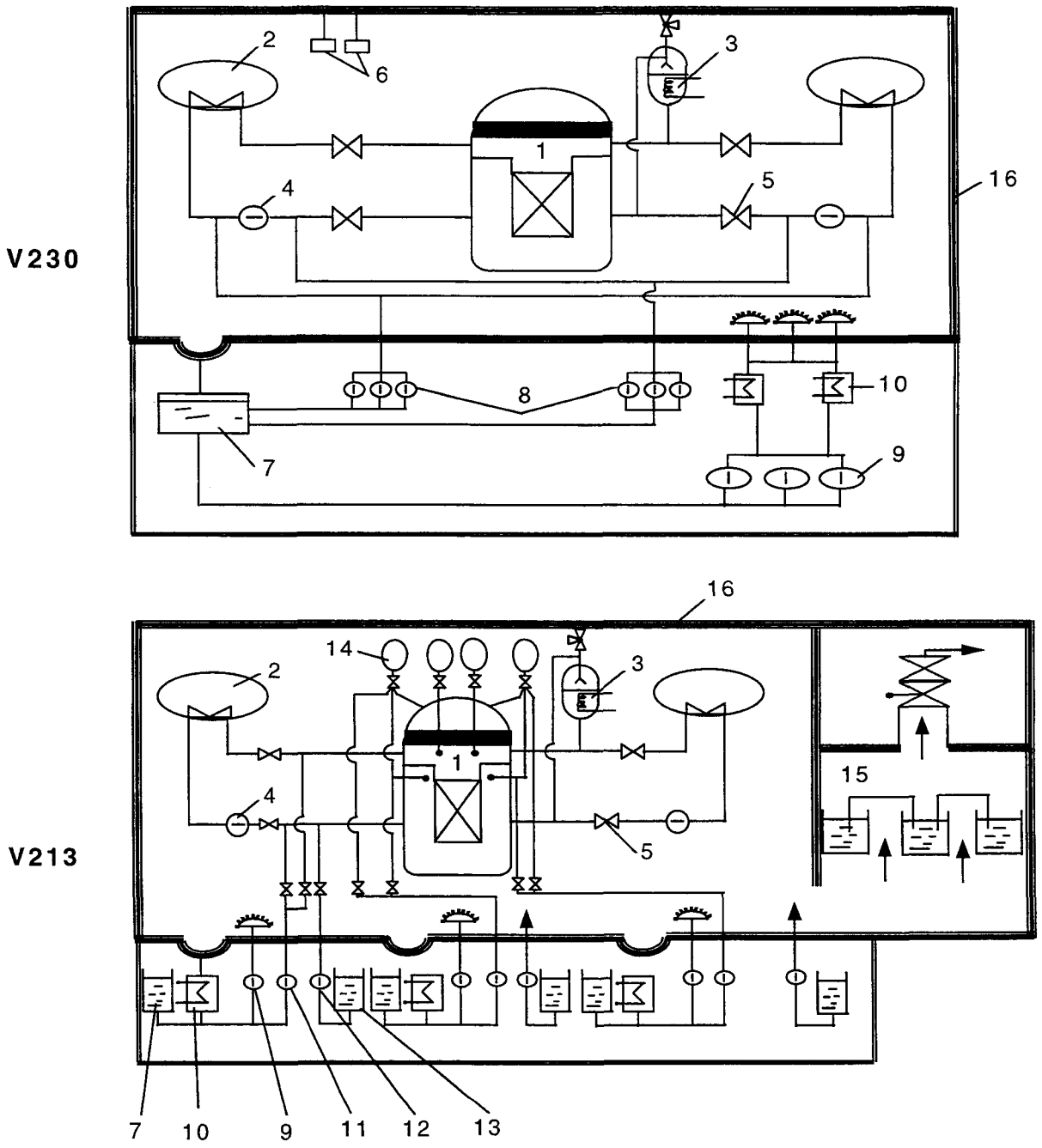


Figure 23 Design differences between VVER-440/230 and VVER-440/213.

1 Reactor
2 Steam generator
3 Pressurizer
4 Primary coolant pump
5 Shut-off valve
6 Pressure relief valve
7 Boric acid solution
8 High pressure pump
9 Sprinkler pump
10 Cooler
11 Low pressure pump
12 High pressure pump
13 Boric acid solution
14 Hydraulic accumulator
15 Condenser bubbler
16 Airtight compartment (ALC)

5.3.3 Boiling water graphite reactors (RBMK)

Reactor development

The RBMK is a graphite-moderated pressure tube reactor cooled by boiling water. The combination of a pressure-tube coolant circuit with a graphite moderator in a commercial nuclear power plant is unique to the ex-USSR. Its origin can be traced back to the early reactors built to produce military plutonium. In fact, the first experimental reactor in the world to produce a significant amount of electricity was the 5 MWe reactor at Obninsk, which was connected to the grid in June 1954.

Six graphite moderated, pressurized water cooled reactors for the dual purpose of plutonium and electricity production were taken into operation between 1958 and 1964 at Troitsk in the Krasnoyarsk area in Siberia. Each unit had a capacity of 600 MWe and a fuel loading of 200 tons of natural uranium metal. It is unknown if any of these reactors is still operating. Disregarding the value of plutonium, the fuel cost of dual-purpose reactors becomes very high due to the low burnup required to produce weapons-grade plutonium.

The Obninsk reactor was initially operated with pressurized water as coolant but later boiling conditions were introduced in some channels and then a superheating channel was added. The main initial problem was in developing the appropriate fuel element, which led to an inside cooled hollow cylinder of a slightly enriched uranium-molybdenum metallic alloy with inside and outside stainless steel cladding.

The next step towards commercial RBMK reactors was realized in the Ural NPP at Beloyarsk near Sverdlovsk where two graphite moderated, boiling water cooled reactors with superheating were installed and operated: the 108 MWe Beloyarsk-1 from 1956 to 1983 and the 160 MWe Beloyarsk-2 from 1962 to 1990. Both reactors used hollow, inside-cooled U-Mo fuel element for the boiling channels. Unit 1 used the same fuel also for the superheater channels, whilst unit 2 had stainless steel clad UO_2 fuel rods.

Superheating was subsequently abandoned, and the hollow inside-cooled metallic fuel elements were replaced by solid UO_2 rods. The main design features of current RBMK reactors are, see Figure 24:

- vertical pressure tubes, containing the fuel and coolant, enabling on-load refuelling

- fuel assemblies in the form of 18-rod clusters, each rod consisting of slightly enriched uranium fuel pellets with zirconium alloy cladding

- graphite moderator and reflector, enclosed in a leaktight calandria, filled with slowly circulating helium/nitrogen mixture

- boiling water coolant in forced circulation with external steam drum separators, supplying steam directly to the turbine.

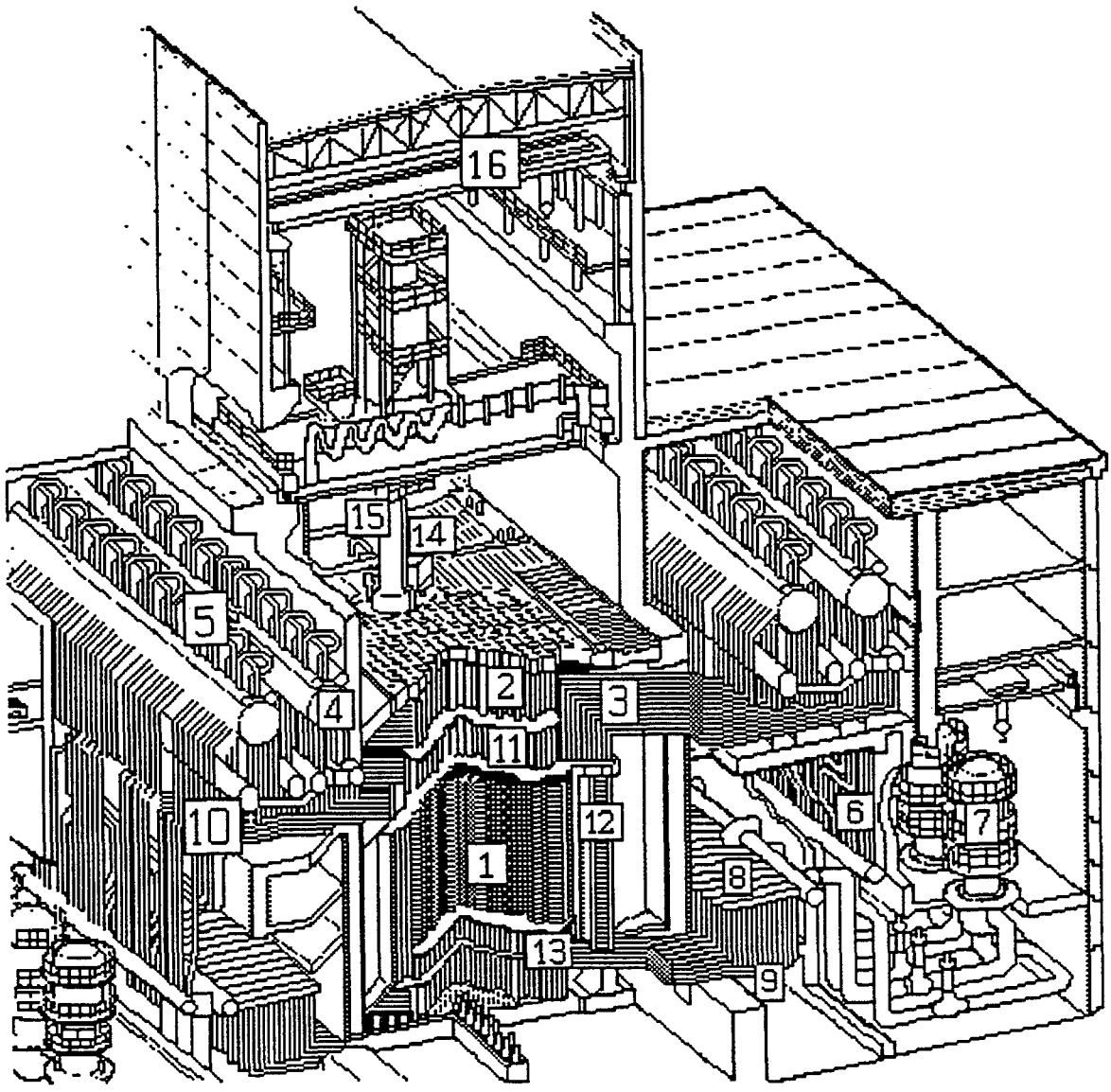


Figure 24 Cross-sectional view of an RBMK-1000.

1 Reactor
2 Fuel channel ducts
3 Steam/water riser pipes
4 Steam separators
5 Steam headers
6 Downcomers
7 Main circulation pumps
8 Distribution header
9 Reactor inlet water pipes
10 Fuel failure detection
11 Upper shield
12 Side shield
13 Lower shield
14 Irradiated fuel pond
15 Refuelling machine
16 Bridge crane

Four 12 MWe RBMKs were constructed during the 1970s at Bilibino in northeastern Siberia and are still in operation. The Russian government has approved plans for three additional units at this location for commissioning in the early 2000s.

Typical of RBMK is that the size of the core and the power output is not limited by the possibilities of fabricating and transporting large pressure vessels. The reactors can therefore be built in large unit sizes. Construction of 1000 MWe reactors started in 1970 with four units for the Leningrad NPP, commissioned between 1973 and 1981. They were followed by four similar units at Chernobyl in the Ukraine and Kursk in Russia, three units at Smolensk, Russia, and two 1500 MWe units at Ignalina, Lithuania. In all, 20 RBMK units are presently in operation with a total net capacity of 15 754 MWe.

Post-Chernobyl public opposition and tightening safety and siting criteria has stopped the further construction of large RBMK reactors, except for one almost finished unit at Kursk. Chernobyl-2 has been out of service since a turbine hall fire in 1991.

Safety considerations

The basic design of RBMK reactors has some shortcomings regarding safety, the most important being the unfavourable reactivity coefficients. The "optimized" RBMK has a positive void coefficient, a relatively small negative fuel temperature coefficient and a positive moderator temperature coefficient. The positive coefficients are inherently de-stabilizing. The large physical size of the core tends to cause instability not only of the power level but also of the power distribution over the core. The positive void coefficient contributed to the accident at Chernobyl as did the ineffectiveness of the control rods to rapidly shut down the reactor. After the accident, measures have been implemented in the other RBMKs to mitigate these deficiencies.

The safety design implies that at most 1 % of the fuel rods are allowed to leak during normal operation. Direct contact between water and fuel is allowed in at most 0,1 % of the fuel channels. The design-basis loss-of-coolant accident is initiated by a guilliotine break of a large diameter pipeline in the main cooling system. The criteria adopted for accident conditions are the same as those applied in the West for the maximum allowed fuel cladding temperature and oxidation.

To meet the safety requirements, the RBMK reactors are equipped with an automatic local power control system, including monitoring of the power distribution, an emergency protection system, an emergency core cooling system, systems for monitoring the coolant flow and fuel integrity in individual channels, a system for monitoring the temperature of the graphite and structures, a system for data sampling and signal validation, which calculates the parameters needed for operation of the plant, and an accident localization compartment (ALC) for condensation of steam in case of pipe breaks in the primary system, partly resembling the reactor containment in Western reactors.

The six units in the first generation of RBMKs (two units each at Leningrad, Chernobyl and Kursk) lack ALC systems, and their emergency core cooling systems have less capacity than that of second generation RBMKs.

The Leningrad NPP

The Leningrad NPP is located near the town of Sosnovy Bor on the coast of the Baltic Sea, about 70 km from St. Petersburg and 240 km from Helsinki. The plant, which has four RBMK-1000 units, was constructed in two stages. Units 1 and 2 were taken into commercial operation in 1973 and 1975, and units 3 and 4 in 1979 and 1981. The total net capacity of the station is 3700 MWe.

Each reactor has a thermal power of 3200 MW, and two main coolant loops, four steam separator drums, and two turbines. The equivalent core diameter is 11,8 m and the core height 7 m. The reactor contains 192 tons of uranium and 1700 tons of graphite. There are 1693 fuel channels in units 1 and 2 and 1661 channels in units 3 and 4. The pressure tubes have 88 mm outer diameter and are 4 mm thick. The maximum thermal power in a channel is 3000 kW, the pressure is 8,75 MPa at inlet and 7,5 MPa at outlet, and the temperature is 270 °C inlet and 284 °C outlet. The maximum graphite temperature is 750 °C.

The main differences in the two pairs of units are in the emergency core cooling system (the SAOR) and in the confinement system (the ALC). The design of the SAOR of units 1 and 2 is based on a break of a 300 mm diameter pipe, which corresponds to a break of a distribution header. To meet this event, the SAOR has two auxiliary feed water pumps, three emergency feed water pumps and two emergency water storages. The pumps are used to supply make-up water to the drum separators and also for emergency core cooling in case of a pipe break. The SAOR operates only in that half of the reactor which suffered the pipe break.

The design basis for units 3 and 4 is a break of a 900 mm pipe, which corresponds to the break of a pressure collector or at the inlet or outlet of a main circulation pump. The SAOR consists of pumps, pressurized water accumulators and water storage pools. The system is actuated by the opening of fast-acting gate valves. Power for the valves is supplied by batteries.

Only units 3 and 4 have an ALC system. The design philosophy is different from the western philosophy. The ALC is not a leaktight building around the reactor but a building where the discharged steam and gas mixture is condensed and purified. The design basis is a 300 mm break in the primary circuit.

A detailed technical description of the plant arrangement, buildings and structures, main process systems, safety systems and auxiliary systems as well as of the organization and plant performance is presented in the project report [62].

A comprehensive schedule of reconstruction is being implemented. For example, all of the some 1700 fuel channels of units 1 and 2 have been exchanged, and the same replacement will be carried out for units 3 and 4 in 1994-95 and 1996-97, respectively. Other main backfitting will include the construction of ALCs for units 1 and 2 in 1995.

Two major incidents have occurred. In 1975, a pressure tube in unit 1 ruptured when the operators increased the reactor power too fast after a scram, in violation of the technical specifications for reactor upstart. The pressure tube and ten fuel assemblies next to the damaged channel were replaced.

The other incident occurred in March 1992 at unit 3. The unit was operated at nominal power when the control valve of a pressure tube broke and the channel was blocked. Due to the flow blockage, the temperature of the fuel assembly rose to 1200 °C. The fuel assembly stretched and bent and eventually ruptured the pressure tube. The temperature rise in the gas circuit caused emergency shutdown, and the pressure rise caused the relief valves to open. The steam and gas mixture was discharged to the ALC. Unfortunately, one of the ALC valves was left open due to reconstruction and steam and gas were blown to the atmosphere. About an hour into the accident, the open valve was found and closed.

The average load factors from the start of operations to 1992 have been 56,4; 74,2; 82,4; and 84,2 % for units 1,2, 3 and 4, respectively.

Ignalina

The Ignalina NPP is located in Lithuania, close to the borders of Byelorussia and Latvia. The station is built on the shore of lake Drisvyaty. Nearest large cities are Vilnius at 130 km distance with over 600 000 inhabitants and Daugavpils in Latvia at 30 km with 150 000 inhabitants. At 8 km from the plant is the town of Visaginus with 32 000 inhabitants, residence of plant personnel. The first unit was commissioned in 1984 and the second unit in 1987. The plant was planned to accomodate four units. Construction of the third unit has been stopped at about 30 % completion.

The 1500 MWe Ignalina reactors have the same basic design data and layout as RBMK-1000 except that the thermal output has been raised by 50 % from 3200 to 4800 MW. This is obtained by allowing a 38 % higher maximum linear fuel heat rating and achieving a more even power distribution over the core. The coolant flow rate is roughly unchanged, whilst the steam flow rate is increased by about 50 %. A summary of design data is presented in the project report [63].

The design basis for the emergency core cooling system is the same as that of the Leningrad NPP units 3 and 4, i.e. a break of a 900 mm diameter pipe in the primary circuit. The short-term ECCS function is provided by an accumulator system, subdivided in two trains, each with 50 % capacity. Prolonged heat removal is achieved by three separate 50 % trains of emergency core cooling and auxiliary feedwater systems. Each of the six trains has two pumps.

The accident localization compartment (ALC) is designed on the basis of a 900 mm pipe break. It consists of leaktight compartments, surrounding most of the primary system pipes, except the steam drums, and two condensation towers for pressure suppression, Figure 25.

Unit 1 reached the rated capacity of 1500 MWe in May 1985. After the Chernobyl accident, the allowed output was decreased to 1050 MWe in June 1987. Following the completion of a package of safety-enhancing measures, the allowed capacity was raised to 1300 MWe.

Unit 2 was connected to the grid in August 1987 and reached 1400 MWe in January 1988. From August 1988, the unit is operated at a maximum allowed output of 1250 MWe.

Several operational disturbances have occurred due to turbogenerator problems, resulting in the shut down of one turbine, thus reducing the plant output by 50 %. The most serious event took place in September 1988 on Unit 2, when fire in a cable room under the main control room caused partial loss of the control room. The fire also resulted in the interruption of forced cooling in half the core. This part of the core remained cooled by natural circulation in accordance with the design intent.

The average load factor through 1992 has been 54,8 % for Unit 1 and 63,2 % for Unit 2.

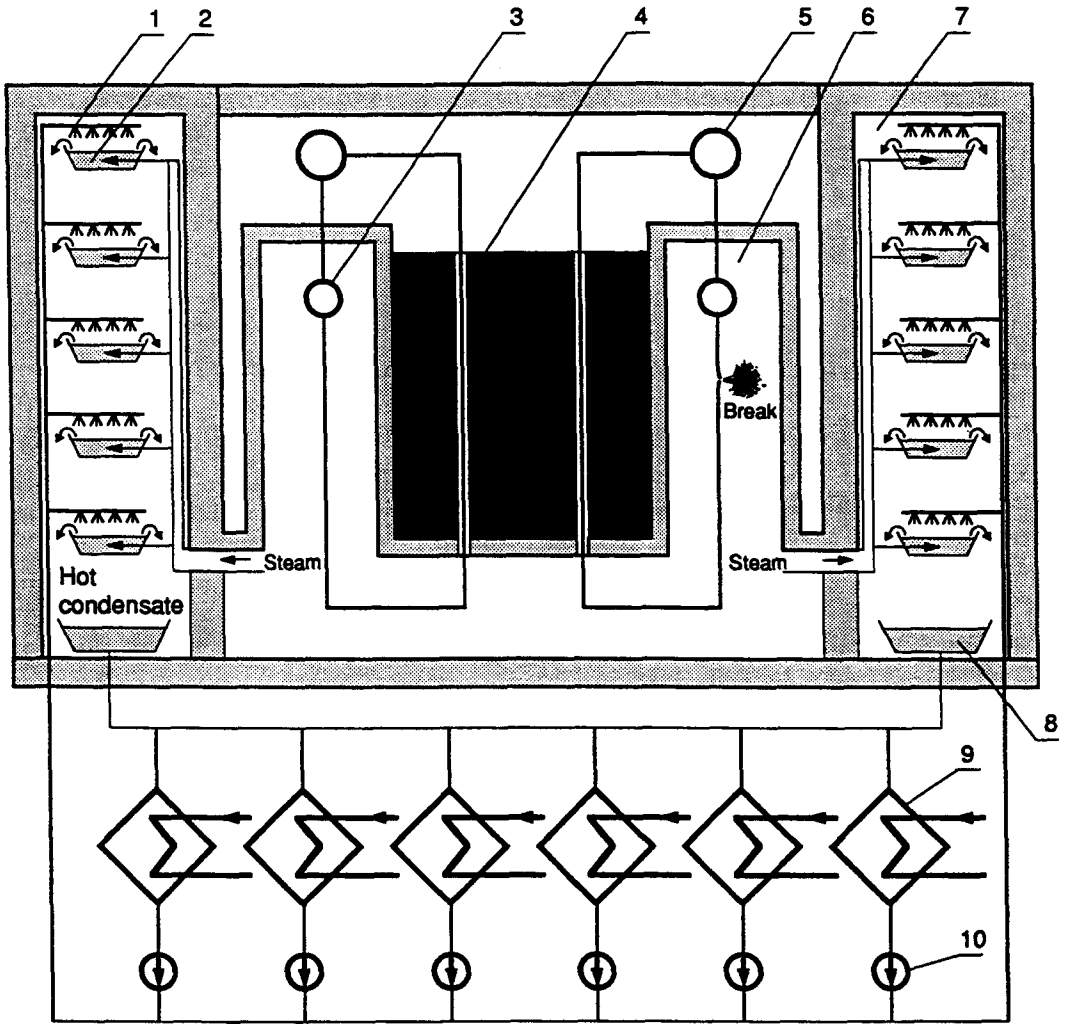


Figure 25 Accident localization system at Ignalina.

1 Spray system
2 Condensation pool
3 Main circulation pump
4 Reactor
5 Steam drum separator
6 Solid compact cubicles
7 Accident localization tower
8 Hot condensate tank
9 Heat exchanger
10 Cooling pump

5.4 Naval reactors

A large number of nuclear-powered naval vessels are operating in international waters, some of them near to the Nordic coasts. More than 400 of them are military submarines, about 80 of which are continuously present in the North Atlantic. Other military vessels include aircraft carriers and cruisers. In 1989, Russia had six nuclear-propellered icebreakers and one combined icebreaker-cargo ship in operation, see Table 26.

Table 26 Nuclear-powered naval vessels deployed or on order (in parenthesis) in 1989 [69].

Country	Sub-marines	Aircraft carriers	Cruisers	Ice-breakers	Cargo ships	Sum
France	12 (4)	1 (1)				13 (5)
Russia	214 (16)	(2)	2 (2)	6 (2)	1	224 (22)
UK	23 (3)					23 (3)
USA	157 (12)	5 (2)	9			171 (14)
Total	406 (35)	6 (5)	11 (2)	6 (2)	1	431 (44)

The safety authorities and the general public in the Nordic countries are becoming increasingly concerned about the potential risks involved, as evidenced by the three recent Russian submarine accidents in the Norwegian Sea. This is the reason for including a review of nuclear ships in the SIK-3 project.

5.4.1 Nuclear propulsion plant

A typical nuclear propulsion plant with a pressurized water reactor is shown in Figure 27. The nuclear steam supply system can be dispersed (loop design) as illustrated, or have the steam generators and the main coolant pumps integrated with the reactor pressure vessel (integral design). The plant has two turbines, one supplying power directly to the shaft via reduction gearing, and the other generating power for auxiliary equipment, such as the coolant pumps. The nuclear steam supply system is enclosed in a containment structure and has heavy shielding around all sides except the bottom.

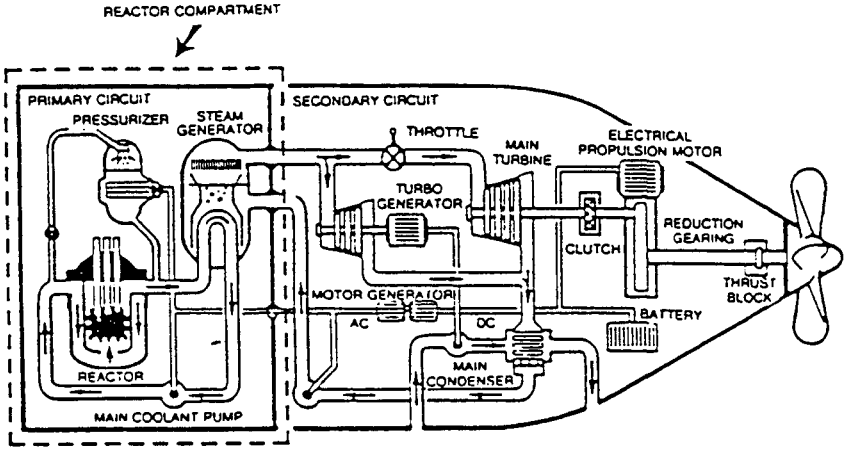


Figure 27 Layout of a nuclear propulsion plant

5.4.2 Merchant ships and icebreakers

Three nuclear ships have been built and operated by the United States, Germany and Japan: NS Savannah, NS Otto Hahn and NS Mutsu. All reactors were PWRs with slightly enriched UO_2 stainless steel clad fuel. Savannah and Mutsu were loop designs, whilst Otto Hahn had internal steam generators and integrated main coolant pumps. Although all of them are now out of service, it is of interest, for generic reasons, to compare the main data, Table 28.

The Russian icebreaker Lenin was the first civilian nuclear ship to be launched. Construction started in 1956 and operation in 1959. NS Lenin is provided with three stern screws. The hull is divided by 11 transverse waterproof bulkheads. It will not sink even if any two sections are flooded.

NS Lenin was originally provided with three 90 MWth pressurized water reactors, one of which was in reserve. During 1966-1970, a new reactor power plant was installed consisting of two 135 MWth reactors of a new design, known as KLT-40, which has since been used in all Russian icebreakers. Claims that NS Lenin suffered a serious reactor accident in 1966 have not been substantiated. The icebreaker was retired in 1989.

Table 28 Data for nuclear powered ships

	Savannah	Otto Hahn	Mutsu
Type of ship	Cargo and passenger	Ore carrier	Special cargo
Start of construction	1958	1963	1968
Initial criticality	1961	1968	1974
Full power	1962	1968	1990
Retired	1971	1979	1992
Length, m	182	172	130
Beam, m	23,8	23,4	19,0
Depth, m		14,5	13,2
Deadweight, ton		15 000	2430
Cargo, ton	9400	14 000	2400
Gross tonnage	15 600	16 900	8200
Shaft horsepower	22 000	10 000	10 000
Service speed, kn	20	16	16,5
Gross thermal power, MW	76	38	36
Pressure vessel diameter, m	3,3	2,9	
" height, m	8,2	9,8	
Core height, m	1,68	1,15	1,04
Number of fuel assemblies	32	12+4	32
Fuel enrichment, %	4,4	3,7	4,0
Core loading, kg U	7112	2622	2440
Fuel power density, kW/kg U	10,24	14,5	14,8
Core volumetric power, kW/l	23	33	33,5
Average burnup, MWd/t	7300	7260	5530
Number of coolant loops	2	3	2
Coolant velocity, m/s	2,7	1,7	1,1
Inlet temperature, °C	263	267	271
Outlet temperature, °C	272	278	285
Reactor pressure, MPa	12,3	6,35	11,0

Two second generation icebreakers were launched in 1975 and 1977. Three vessels of an improved design started operation in 1985, 1989 and 1992, and a fourth unit in this series is under construction. In order to extend the range of the nuclear icebreakers, a new type with lower draught has been developed. One ship of this type, which has only one KLT-40 reactor for propulsion, is in operation and another is under construction. The conventional parts are built at the Wärtsilä shipyard in Finland.

All Russian nuclear icebreakers are operated by the Murmansk Arctic Shipping Company. The KLT-40 plants have been in operation for more than 110 000 hours, corresponding to 125 operating years. The icebreakers have been able to operate continuously for 400 days in the Arctic. The availability has averaged 76-79 %, and the number of reactor scrams has averaged one per year.

The construction of an icebreaking transport/container ship, NS Sevmorput, started in 1984, and the ship was delivered to the customer in 1988. A substantial amount of information is available since the Russian safety report of the ship has been published in English. Data for the ship and the KLT-40 reactor are summarized in a SIK-3 project report [96].

KLT-40 is provided with emergency core cooling systems capable of supplying water to the primary system in case of a major leak. All the newer icebreakers have reactor containments of succesively improved design. NS Sevmorput has a high strength steel containment with a pressure suppression system, designed to cope with the consequences of a main coolant pipe break. Should the ship sink, a pressure equalizer system will flood the containment until the pressure is the same on both sides of the containment wall.

According to a published interview with a Russian nuclear safety official, a "near meltdown" event occurred in one of the reactors in the icebreaker NS Rossiya in November 1988. The ship was moored at the naval port of Murmansk while maintenance work was carried out on the reactors. Due to an erroneous command, a valve was opened which started to drain one of the two reactor vessels. Fuel damage was avoided because of actions by the crew and activation of an emergency system.

5.4.3 Submarines

The idea of using ordinary water as a moderator-coolant and enriched uranium as fuel in a pressurized water reactor originated in the US Navy during the second world war. In fact, the first power plant with a PWR started operation in 1953 as a prototype for the plant to be installed in the Nautilus submarine, first launched in 1955. It is hardly surprising that the first practical application of nuclear propulsion was in submarines, since the use of nuclear power permits the submarine to move submerged for almost any period of time.

The US Navy also introduced a liquid sodium-cooled propulsion plant in the early Sea Wolf class submarine. The advantage of liquid metal cooling is that a higher core power density can be achieved, thus saving weight or making a higher speed of the submerged submarine possible for a given weight, as compared to PWR powered plant. However, Sea Wolf was not a success and has since been replaced by PWR plant. No further attempts to install liquid metal-cooled propulsion plant in the US Navy have been reported.

Detailed information of military reactors is not available in the open literature. It is necessary to rely on generic information from land-based and civilian marine reactors. This might be adequate to a certain extent for safety assessment, although vital information on fuel design and performance is lacking. Some general design aspects on nuclear submarines are reviewed in a SIK-3 project report [67].

The hull is the ultimate barrier for the release of radioactive fission products from a nuclear submarine. Single hulls are most frequently used by Western fleets, whereas Russian designers seem to prefer double hulls. The Russians have introduced titanium in hulls and pipework. This material has higher strength and lighter weight than ordinary steel.

Most of the Russian submarines have double reactor systems, whilst the Western nations rely on a single reactor per submarine. Emergency core cooling systems are provided, as are reactor containment, at least in modern submarines. The containment can be flooded for pressure equalization, should the submarine sink. Special precautions are taken to increase the resistance against shocks caused by collisions, groundings and explosions.

Modern submarines probably use light-weight material like fibreglass and composites for various internal structures. Such materials may offer reduced resistance to fires. This could explain the rapid development of the fire in the Russian submarine of the Mike class which sank in the Norwegian Sea in April 1989.

5.4.4 Accidents involving nuclear submarines

A number of incidents and accidents with nuclear submarines are reviewed and commented in a SIK-3 project report [66]. Five events involve U.S. submarines. In four cases, leakage of sea water into the submarine occurred, and in two of these the submarines were lost. The fifth event is the only one that involved the nuclear plant; it was a small leakage in the primary system that could be repaired at sea without external assistance. Hence, it may be inferred that the early U.S. submarines had a weak design with respect to sea water leaks, but that the reactors seem to be very reliable. In 1989, the U.S. Navy pointed out that they had 3500 reactor operating years without nuclear accidents.

Of the reviewed incident/accidents, twenty involve Russian submarines. Seven were caused by fires/explosions, and in three cases the submarine was lost. In five events a leak developed in the reactor primary system. In an additional five cases, propulsion was lost, which may also have involved the reactor system. A tentative conclusion is that Russian submarines were not properly designed for fire prevention or that the crews were not sufficiently trained in this respect, and that the first generation of submarine reactors had a weak design for leaks in the primary system.

6 Conclusions and recommendations

The achievements of the SIK programme can be judged by the answers to the following questions:

- What are the main results of the SIK programme?
- Can risk-based techniques and safety indicators be used for supporting plant safety management?
- Is our understanding of severe accident phenomena adequate for current safety requirements?
- Do we have sufficient information about the design and safety features of reactors in neighbouring countries?

6.1 What are the main results of the SIK programme?

In the area of safety evaluation, the methodology of probabilistic safety assessment (PSA) has been extended to include operational safety. A concept of *living PSA* has been proposed and applied in case studies. A system of *safety indicators* for monitoring safety performance and maintenance activities has been proposed and tested. The work has indicated the feasibility of the proposed concept for supporting decision-making on safety issues.

In the area of *severe accident research*, the international state-of-the-art has been reviewed. Advanced computer codes have been taken into active use in Finland and Sweden. Models and predictions have been compared with those of the MAAP code, which is the commonly used tool for severe accident safety analysis in the Nordic countries. Improved models of chemical phenomena in core melt accidents have been developed. A concept for computerized support of accident management has been outlined and prototype development has started.

Information has been compiled of the *design and safety features of reactors near to the borders of the Nordic countries*. The safety of naval reactors in nuclear-powered ships and submarines has been reviewed The effort has resulted in a common data base to be used for evaluation and information by the safety authorities in case of accidents involving the release of radioactive material that may affect the Nordic countries.

The joint research programme has contributed to a *uniform view of nuclear safety issues in the Nordic countries*. The network of professional contacts has been reinforced. The sharing of research and information has encouraged efficient approaches to solve common problems.

6.2 Can risk-based techniques and safety indicators be used for supporting plant safety management?

PSA offers a methodology for risk evaluation of nuclear power plants. Since its introduction in the mid-1970's, PSA has been increasingly used for the assessment of engineered safety features and plant procedures as a complement to traditional deterministic analysis and engineering judgement. The methodology has been successively improved and extended.

Basic PSA provides a nominal value of the risk of core damage and release of radioactive materials, by using average data for component unavailability. In practice, a component may fail when needed or be unavailable due to maintenance. *Living PSA* attempts to take this variability into account by predicting an instantaneous, time-dependent risk. Living PSA can also be used to estimate the retrospective risk by feedback of operating history. Generally speaking, living PSA is referred to as the process of maintaining an updated plant-specific PSA model for use in the daily safety work at the plant and by the safety authorities.

Living PSA is already used for off-line assessment of safety design and procedures. In SIK-1, the living PSA concept has been extended to cover operational aspects. Application areas have been outlined and risk measures defined. The feasibility of the concept has been demonstrated in pilot studies of risk monitoring and risk follow-up. The risk monitoring studies indicate that living PSA can be used to improve the rules and procedures for reactor operation. The risk follow-up studies show that living PSA can provide an effective tool for the feedback of operating experience.

Basic PSA is well suited for comparing the risk significance of changes in the safety design and procedures of a specific plant. Risk values must, however, be treated with caution due to the intrinsic and practical limitations of the PSA methodology. The basic PSA models need to be modified to allow sufficient flexibility for living PSA application. The models should be as complete and realistic as reasonably achievable.

The ultimate goal for living PSA is to provide a tool for day-to-day safety management as a supplement to the technical specifications for plant operation and maintenance. The SIK-1 project has indicated that the proposed concept is feasible for this purpose. However, additional efforts are needed to improve certain basic models, to further demonstrate the applicability of the system, and to implement the tools at the individual plants.

The tool must be user-friendly and well-tested, yet flexible enough to allow modification and updating. The results should be easy to interpret also for the non-specialist. Confidence in the results can only be achieved by education and training of prospective users, bearing in mind the inevitable limitations and uncertainties of the PSA approach.

Living PSA is a complement to other methods of safety assessment such as operational safety indicators. Safety indicators are already used by some utilities. The indicators reflect the safety performance of the plant in a condensed way and are intended to provide early warning of potential problems but also to follow-up improvements in plant operation and maintenance.

In SIK-1, a coherent system of indicators has been proposed, based on the preservation of barriers to the release of radionuclides. The indicators use data collected in the information systems of plant operation and maintenance. They attempt to make the feedback of experience more systematic and effective. Methods for screening the data bases by computerized search patterns have been developed and tested. Advanced statistical methods have been used for trend analysis.

It is suggested that the selection and validation of suitable indicators continues and that the risk importance of the various indicators is evaluated by living PSA. An effective indicator system requires a well structured and motivated organization where all involved parties have access to the results and the data base. The administrative possibilities and problems with an extended use of safety indicators should be further investigated.

The project has demonstrated that risk-based techniques can be used to support decision-making on safety issues. Care must be taken to include the relevant criteria and decision options as well as the parametric uncertainties in the PSA approach.

The integrated use of living PSA and safety indicators can provide effective and improved means of safety management and help in maintaining a high level of safety. Additional efforts are required to implement the tools and systems for practical use at the nuclear power plants.

6.3 Is our understanding of severe accident phenomena adequate for current safety requirements?

Ever since the Three Mile Island accident in 1979, comprehensive international research programmes have been undertaken to improve the understanding of basic phenomena and mechanisms involved in severe accidents. Experiments have been carried out and models have been developed and incorporated in computer codes. The Nordic countries have participated in this work and also carried out independent research. Equipment for mitigating the effects of potential releases of radionuclides to the environment has been installed in all Nordic plants, and procedures for accident management have been established.

The state-of-the-art of severe accident code development was reviewed in the SIK-2 project. A two-stage approach is used in the Nordic countries. The integral MAAP code is used for survey and design

calculations, and more detailed codes are used for independent verification and benchmarking. The review and intercomparison indicated some areas for improvements.

The case studies showed qualitative agreement between the code predictions of the progression of accidents within the reactor vessel. However, some significant quantitative differences were observed, such as in the amount of hydrogen generated and in the time to reactor vessel failure. It should be recognized that this conclusion is tentative, since improved code versions appear from time to time.

The knowledge of severe accident phenomena has improved considerably during the last decade, and so have the models in the severe accident computer codes. The MAAP code has proved to be a versatile and well tested tool for survey calculations and remains the workhorse for severe accident analysis in the Nordic countries. An new version of MAAP will become available shortly, which will further extend the capability of the code.

An important independent development in the SIK programme is the CHMAAP code, which contains improved models of chemical behaviour during an accident. The studies demonstrate the importance of chemical phenomena. Validation of the models can, however, only be obtained by comparison with well characterized experiments, which are as yet lacking.

The studies show that the predictions of the severe accident codes must, in general, be treated with caution and carefully interpreted. This is due not so much to lack of knowledge of basic phenomena and mechanisms, as to the complex interactions and intractable geometries involved, and to the paucity of relevant experimental verification. This is true for the behaviour of the core melt in the reactor vessel and in the containment, as well as for the release and transport of radioactive materials. The problems can hardly be overcome by further improvement of the basic physical and chemical models or by code intercomparison. The uncertainties in the predictions are taken care of by providing for appropriate safety margins in the design of mitigative equipment and procedures.

The difficulties of predicting the progression of severe accidents will also affect the capabilities of systems for computerized accident management, such as CAMS, which was conceptualized and developed into a prototypical stage within the SIK programme. The preliminary indications are that the proposed approach is feasible. The system should be useful for operator training and support, provided the limitations of the system are recognized. It is suggested that the project be completed.

The Nordic countries have adopted a strategy of reinforcing the reactor containment function, so that large external radioactive releases are avoided for a wide range of accidents, regardless of the detailed course of the accident. In this way the dependence on the accuracy of the code

predictions is largely eliminated. This does not mean that further code development is unnecessary, however. Problem areas still exist which should be further explored. It is therefore suggested that severe accident research remains on the agenda for future Nordic research collaboration.

In general, the SIK-2 project has contributed to strengthening the common understanding in the Nordic countries of safety aspects with regard to the possibility of severe accidents and the measures taken to mitigate their consequences.

6.4 Do we have sufficient information about the design and safety features of reactors in neighbouring countries?

Information has been compiled about the safety design of Russian reactors, including four VVER units at Kola and four RBMK at Sosnovy Bor near St. Petersburg, two RBMK at Ignalina, Lithuania, and four German light water reactors. No attempt has been made to assess the safety of the plants, which was neither part of the objectives.

Special effort was devoted to the Russian-built reactors in view of the new openness which made it possible to visit the plants and get information which was previously very difficult, if not impossible, to obtain.

Both types of Russian reactors appear in different versions. The first generation of reactors, of which there are two VVERs at Kola and two RBMKs at Sosnovy Bor, have some clearly inferior safety features as compared to Western standards. The second generation VVER (two units at Kola) and the second generation RBMK (two each at Sosnovy Bor and Ignalina) have better safety features, in some respects comparable to those in the West. This does not mean, however, that weaknesses do not exist.

Safety-enhancing measures have been and are being introduced; for the RBMKs partly with Nordic assistance. It is likely that the old VVERs will be shut down as soon as conditions allow. Four old VVERs at the Greifswald Nuclear Power Plant in former DDR have already been closed. For the old RBMKs the situation is unclear.

The German reactors included in the study are located in the lower region of the river Elbe. Two units are boiling water reactors and two are pressurized water reactors, manufactured by KWU/Siemens. The safety design corresponds to the best of Western standards, and all units except one have excellent operating records.

It is concluded that the collected data are sufficient as a source of general information for the time being. Regular updating is suggested for taking into account any modifications and changes that may occur.

References

1 K Laakso (Ed.); *NKS/SIK-1. Safety evaluation by use of living PSA and safety indicators,* Final Report, to be published.

2 W Frid (Ed.); *NKS/SIK-2. Severe accidents in LWR. Studies of computer codes, selected aspects of phenomenology and accident management,* Final Report, to be published.

3 E Nonbøl (Ed.) *NKS/SIK-3, Design and safety features of nuclear power plants in neighbouring countries,* Final Report, to be published.

4 G Bengtsson (Ed.), *Risk analysis and safety rationale*, Final report of a joint Nordic research programme in nuclear safety, NKA, Nordic liaison committee for atomic energy, December 1989.

5 *Reliability data of components in Nordic nuclear power plants* (T-boken) 3rd ed. Prepared by ATV Office and Studsvik AB. Vattenfall AB 1992

6 H James, M J Harris, S F Hall; *Comparison of methods for containment analysis in probabilistic safety assessment*, PSA'91, Proc. of an International Symposium, Vienna, 3-7 June 1991, International Atomic Energy Agency, Vienna 1992.

7 L Carlsson. L Hammar; *Probabilistic safety analysis as a component of periodic safety reassessment of Swedish NPPs - Experience from the eighties and prospects for the nineties*, PSA'91, Proc. of an International Symposium, Vienna 3-7 June 1991, International Atomic Energy Agency, Vienna, 1992.

8 R K Virolainen; *Regulatory review of PSA studies made for operating Finnish nuclear power plants and its implications for regualtory decision making and living PSA*, PSA'91, Proc. of an International Symposium, Vienna 3-7 June 1991, International Atomic Energy Agency, Vienna, 1992.

9 K Laakso, M Knochenhauer, T Mankamo, K Pörn; *Optimization of technical specifications by use of probabilistic methods - A Nordic perspective,* NKA/RAS 470 Final Report, NKA, Nordic Liaison Committee for Atomic Energy, 1990.

10 J Holmberg, K Laakso, E Lehtinen, G Johansson, S Björe; *International survey of living PSA and safety indicators,* VTT Research Notes 1326, VTT Technical Research Centre of Finland, Espoo 1992.

11 B Horne, *The use of probabilistic safety analysis methods for planning the maintenance and testing unavailabilities of essential plant at Heysham 2 AGR power station,* Report IAEA-TECDOC-599 of a Technical Committee Meeting, Vienna 18-22 June 1990, International Atomic Energy Agency, Vienna 1991.

12 J W Kirkman, J B Fussel, D J Campbell; *PRISIM at Arkansas Nuclear One-Unit 1: Daily in-plant use of PSA information,* Reliability and Engineering System Safety 22(1988)441.

13 RF Christie, W D Salyer, J S Miller, J L Burton, O A Holbert; *River Bend Nuclear Station time dependent core damage frequency,* 3rd TÜV-Workshop on Living PSA Application, Hamburg 11-12 May 1992, Technischer Überwachungs-Verein Norddeutschland e.V. 1992.

14 H Adrian, P Kafka, J Prock; *Modeling uncertainties in computer-based operator support systems (OSS),* ESRC '92, Proc. of the European Safety and Reliability Conference '92, Copenhagen, Denmark 10-12 June 1992, ESRA Conference Series, Elsevier 1992.

15 S Hirschberg (Ed.); *Dependences, human interactions and uncertainties in probabilistic safety assessment,* NKA/RAS-450 Final Report, NKA, Nordic Liaison Committee for Atomic Energy, 1990.

16 K Laakso, G Johansson, S Björe, R Virolainen, L Gunsell; *Safety evaluation by use of living PSA and safety indicators. Work plan 1990-1993*, NKS/SIK-1(90) August 1990.

17 J Holmberg, K Laakso, E Lehtinen, G Johansson, S Björe; *Preproject report: Nordic survey on safety evaluation by use of living PSA and safety indicators*; SKI Technical Report 91:3, Swedish Nuclear Power Inspectorate, Stockholm 1991.

18 G Johansson, J Holmberg; *The use of living PSA. A procedure developed in the Nordic project "Safety Evaluation, NKS/SIK-1",* PSA'93, Proc. of the International Topical Meeting on Probabilistic Safety Assessment, Clearwater Beach, Florida, January 26-29, 1993, American Nuclear Society 1993.

19 J Holmberg, G Johansson; *Definition of a concept for safety evaluation by use of living PSA: the Nordic project "Safety Evaluation NKS/SIK-1",* ESRC '92, Proc. of the European Safety and Reliability Conference '92, Copenhagen, Denmark 10-12 June 1992, ESRA Conference Series, Elsevier 1992.

20 T Mankamo; *A time dependent model of dependent failures - application to a pairwise symmetric structure of four components,* NKS/SIK-1(92)13, Draft, Avaplan Oy 1992.

21 J W Minarick; *The US NRC accident sequence precursor program: Present methods and findings,* Reliability and Engineering and System Safety 27(1990)1.

22 G Skoff, H P Berg; *Approach to systematic precursor evaluation,* 3rd TÜV-Workshop on Living PSA Application, Hamburg 11-12 May 1992, Technischer Überwachungs-Verein Norddeutschland e.V. 1992.

23 J Holmberg, G Johansson, I Niemelä; *Risk measures in living PSA assessment,* VTT Publications 146, Technical Research Centre of Finland, Espoo 1993.

24 U-K Erhardsson, Y Flodin; *Momentan risknivå* (Instantaneous risk level), NKS/SIK-1(91)30, Vattenfall Report PK-79/91, Vattenfall AB, 1991. In Swedish with English summary.

25 J Holmberg, U Pulkkinen, K Laakso, T Mankamo; *The risk follow-up by PSA - report of the Finnish pilot study,* NKS/SIK-1(91)27, VTT Report VTT/SÄH 14/91, Technical Research Centre of Finland, 1992.

26 J Sandstedt; *Demonstration case studies on living PSA,* NKS/SIK-1(92)27, SKI Technical Report 93:33, Swedish Nuclear Power Inspectorate August 1993.

27 K Laakso, E Lehtinen, H Eriksson, C Rollenhagen, R Nyman, A Angner; *Development of operational safety indicators for use in experience feedback - A part of the Nordic SIK-1 project,* NKS/SIK-1(92)6, ESRC '92, Proc. of the European Safety and Reliability Conference '92, Copenhagen, Denmark 10-12 June 1992, ESRA Conference Series, Elsevier 1992.

28 E Lehtinen; *Condensed description of an indicator system,* NKS/SIK-1(93)2, VTT Technical Research Centre of Finland, Espoo 1993 (Draft).

29 P G Sjölin; *ERF - the KSU event data base - now and in the future,* Presentation at the WANO-PC/ENEL Workshop on Event Data Bases, Rome, 1-2 December 1992.

30 R Nyman, A Angner; *The STAGBAS 2 data base and the production of the incident catalogue and trend catalogue,* ESREL '93, Munich, 10-12 May 1993.

31 R Nyman, A Angner; *BWR generation 2, Barsebäck 1, Barsebäck 2, Oskarshamn 2,* SKI Technical Report 93:01, Swedish Nuclear Power Inspectorate, 1993.

32 K Simola; *Trial application of multiple correspondence analysis to nuclear power plant incident data,* NKS/SKI-1(92)32, RISKI(92)11, VTT Technical Research Centre of Finland, 1992

33 J Sandstedt; *Betydelseanalys och känslighetsanalys O2 indikatorer* (Importance analysis and sensitivity analysis of Oskarshamn II NPP operational safety indicators(, NKS/SIK-1(92)49, RELCON Report 13/92, RELCON Teknik AB, 1992. In Swedish.

34 E Lehtinen, P Saarelainen; *Monitoring of a safety system's unavailability and maintenance performance using LOTI information system and operational safety indicators,* ESRC'92, Proc. of the European Safety and Reliability Conference '92, Copenhagen, Denmark 10-12 June 1992, ESRA Conference Series, Elsevier 1992

35 J L Paulsen, M Clementz; *Pilot study on maintenance indicators,* NKS/SIK-1(92)18, Risø National Laboratory, 1992.

36 K Laakso; *Experience-based RCM and maintenance indicators applied to a safety system of a modern Swedish BWR,* Draft project proposal, December 1992

37 J Holmberg, U Pulkkinen; *Decision analysis on an exemption from the technical specifications,* NKS/SIK-1(92)8, VTT/SÄH 4/92, Technical Research Centre of Finland, Espoo, 1992.

38 K Pörn, K Shen; *Decision making under uncertainty - A pilot study on exemption from technical specifications,* NKS/SIK-1(91)29, STUDSVIK/NS-91/90, Studsvik AB, 1992.

39 K Pörn, K Shen; *On the integrated uncertainty analysis in probabilistic safety assessment,* ESRC '92, Proc. of the European Safety and Reliability Conference '92, Copenhagen, Denmark 10-12 June 1992, ESRA Conference Series, Elsevier 1992.

40 J P Hosemann; *Wechselwirkungen mit der Containmentstruktur und Spaltproduktfreisetzung beim Kernschmelzunfall,* Atomwirtschaft Vol 27, No 10, 1982.

41 *Urban siting of nuclear power plants,* Report by the Urban Siting Commission, State Public Investigation SOU 1974:56 (In Swedish)

42 *Safe nuclear power?* Report by the Reactor Safety Committee, State Public Investigation SOU 1979:86 (In Swedish with English summary)

43 K Johansson (Ed.); *Filtered atmospheric venting of light water reactor containments (FILTRA),* Final report, Studsvik AB, 1982

44 K Johansson (Ed.); *RAMA I Final Report,* Studsvik AB, 1985

45 E Söderman (Ed.); *RAMA II Final Report,* Studsvik AB, 1987

46 E Söderman (Ed.); *RAMA III Final Report,* Studsvik AB, 1989

47 L Mattila, T Vanttola (Eds.); *YKÄ Research programme on nuclear power plant system behaviour and operational aspects of safety,* Ministry of Trade and Industry Reviews B:119, Helsinki 1992

48 I Aro, R Blomquist, P Fynbo, E Pekkarinen, B Schougard; *Study of risk analysis codes for severe accident analysis,* Final report of the NKA Project AKTI-130, April 1989

49 R Alenljung, L G Johansson, O Lindqvist, L Hammar, A Hautojärvi, J Jokiniemi, J O Liljenzin, J P Omtvedt, T Raunemaa, K Koistinen, P Pasanen, U Steiner; *The influence of chemistry on core melt accidents,* Final report of the NKA Project AKTI-150, September1990

50 P Fynbo, H Häggblom, J Jokiniemi; *Aerosol transport in severe reactor accidents,* Final report of the NKA Project AKTI-160, March 1990

51 Y Waaranperä; *SIK-2 - Critical review of MAAP 3.0B, MELCOR, SCDAP/RELAP5 and MAAP 4.0 with emphasis on in-vessel phenomena,* ABB Atom report RP 92-30, February 1933

52 Y Waaranperä, G Jung, I Lindholm, L Nilsson, E Pekkarinen, H Sjövall; *Analysis of unmitigated core melt progression in Forsmark 3 and TVO I/II BWRs: A comparison of MAAP 3.0B, MELCOR and SCDAP/RELAP5,* ABB Report RP 93-29, May 1933

53 I Lindholm, E Pekkarinen, H Sjövall; *Application of codes MAAP, MELCOR and SCDAP/R5 for TVO NPP in case of 10 % main steam line break with reflooding of overheated reactor,* VTT Technical Report VARA-3/93, May 1933

54 J O Liljenzin, R Alenljung, H Dubik, O Lindqvist; *Development, implementation and use of CHMAAP,* Chalmers University of Technology, 1993

55 P Fynbo; *Aerosol modelling in severe accident codes, 1. Reactor system coolant codes,* Draft Report Risø-I-671, January 1993

56 Ø Berg, T Endestad, O Scot Jørgensen, M Sirola, A Sørensen, J G Waalman, F Øwre, K A Ådlandsvik; *CAMS: Computerized accident management support,* Proc of the Specialist Meeting on Operator Aids for Severe Accident Management and Training, Halden, Norway 8-10 June 1993, NEA/CSNI/R(93)9, Halden Reactor Project, 1993

57 A Siljeström; *Stade. General plant description,* SIK-3.9, 1993

58 A Siljeström; *Brokdorf. General plant description,* SIK-3.10, 1993

59 B G Olofsson; *Brunsbüttel nuclear power plant,* SIK-3.6, 1992

60 B G Olofsson; *Krümmel nuclear power plant,* SIK-3.7, 1992

61 E Stokke; *Description of Kola nuclear power plant,* SIK-3.8, 1993

62 T Eurasto, J Sandberg, J Marttila; *The Leningrad nuclear power plant. A general description,* STUK-YTO-TR 44, SIK-3.2, 1993

63 J-P Bento; *Ignalina 1-2. General plant description,* KSU UK331, SIK-3.3, 1993

64 E Nonbøl, P L Ølgaard; *Description of Greifswald nuclear power plant I-VIII,* SIK-3(91)01, 1991

65 P L Ølgaard; *Civilian nuclear ships,* Dep of Electrophysics Report NT-1(Rev), SIK-3.4.2, The Technical University of Denmark, 1993

66 P L Ølgaard; *Nuclear ship accidents. Description and analysis,* Dep of Electrophysics Report NT-4, SIK-3.4.3, The Technical University of Denmark, 1993

67 P I Wethe; *Nuclear powered vessels - Marine reactors,* SIK-3.4.1, Institutt for energiteknikk, 1992

68 A Yu Gagarinski, V V Ignatiev, V M Novikov, S A Subbotin; *Advanced LWRs: analysis of new approaches and ideas,* Nuclear Society International, Moscow, 1992

69 V O Eriksen; *Sunken nuclear submarines,* Norwegian University Press, 1990

APPENDIX 1

PROJECT ORGANISATION

The Nordic nuclear safety research programme ("the NKS programme") is governed by an agreement of cooperation between a group of Nordic government agencies ("the consortium group"), see Figure A1. The programme is directed by an *executive committee,* the members of which are appointed by the contracting parties. The executive committee has a *project secretariat*, located at Risø, Denmark.

The executive committee agrees each year on the scope of activities and funding. The committee appoints the *programme coordinators*, who also manage the meeting activities in each programme area, and the *project managers*, who report to the committee. Each area also has a *reference group* for advice and review of plans and results. Members of the executive committee serve as chairmen of the reference group.

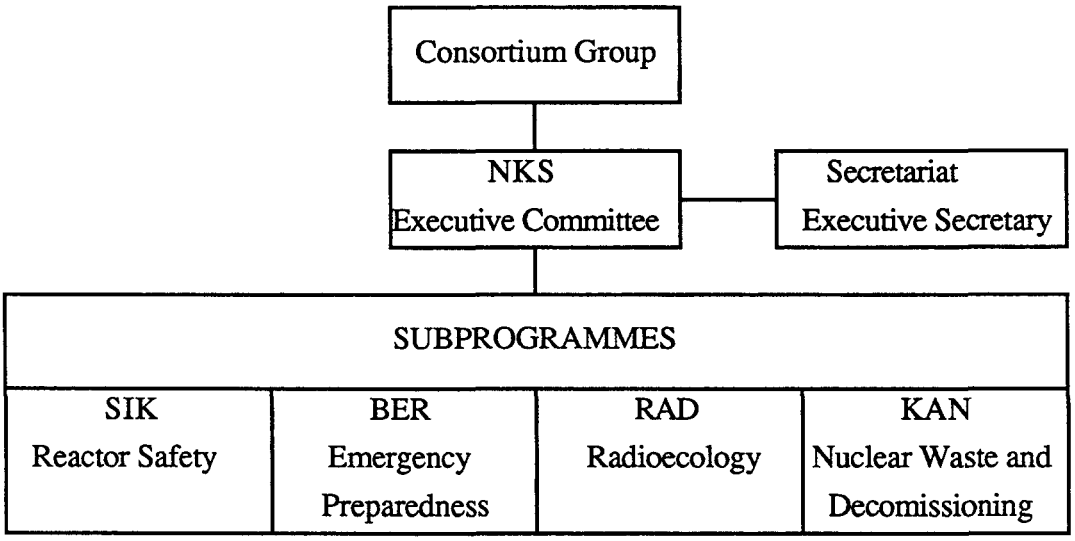


Figure A1 Nordic Nuclear Safety Research Programme 1990 -1993 (NKS)

The SIK programme has three subprogrammes as shown in Table A2.

The contracting parties have agreed to contribute to a basic fund, which covers up to 50 % of the project cost. In addition, various interested parties in the Nordic countries, such as the nuclear utilities, also contribute to the basic fund. The balance is mainly covered by national in kind contributions from the participating organisations.

The volume of efforts is shown in Table A3 and the total costs in Table A4.

Table A2 Nordic Nuclear Safety (NKS) Reactor Safety Programme (SIK)

SIK-1 Safety Evaluation by Use of Living PSA and Safety Indicators
Project Manager Kari Laakso, VTT, Finland

SIK-2 Severe Accident Phenomena
Project Manager Wiktor Frid, SKI, Sweden

SIK-3 Design and Safety Features of Nuclear Installations in Neighbouring Countries
Project Manager Erik Nonbøl, Risø, Denmark

Programme Coordinator Risto Sairanen, VTT

Reference Group
Lennart Hammar, SKI, *Chairman*
Ralf Espefält, Vattenfall AB
Markku Friberg, TVO
Magnus Kjellander/Anders Siljeström/P G Sjölin, KSU
Jukka Laaksonen/Lasse Reiman, STUK
Franz Marcus, NKS
Helge Smidt Olsen, IFE
Erik Söderman, ES-konsult
Björn Thorlaksen, TNA
Harri Tuomisto, IVO

Corresponding Members
Emil Bachofner, OKG AB
Carl-Gunnar Holm, Sydkraft AB

Table A3 SIK programme volume of efforts

	Person months			
	1990	1991	1992	1993
SIK-1	23	60	60	57
SIK-2	23	49	34	37
SIK-3	9	10	10	8
Total	55	119	104	102

Table A4 SIK programme funding levels

	Total costs in thousand DKK			
	1990	1991	1992	1993
SIK-1	1380	4220	4700	4450
SIK-2	1340	2870	2950	2700
SIK-3	370	450	440	390
Sum	3090	7540	8090	7540

APPENDIX 2

The approach to reactor safety
Some fundamental principles and events

Defence-in-depth

The health hazard from nuclear power plants stems from the radioactive substances (radionuclides) produced during reactor operation. Most of the radionuclides are contained in the reactor fuel where they are formed. The fundamental objective of reactor safety is to prevent the radionuclides from being released and reaching the environment. Large releases can only occur if the fuel is overheated and melts or disintegrates. The strategy of reactor safety is to preserve fuel integrity by avoiding fuel overheating or disruption.

The technical means of achieving reactor safety is to confine the radionuclides by physical barriers, which can be natural or engineered. The first barrier is the ceramic matrix of the uranium oxide fuel itself, which tends to retain the radionuclides where they are born. The second barrier is represented by the sealed cans that enclose the fuel. In light water reactors, the third barrier is provided by the reactor pressure vessel, which houses the reactor core with the fuel, and the connecting pressure-bearing pipelines and process systems. A fourth barrier is the pressure- and leaktight reactor containment building which surrounds the whole nuclear steam supply system.

The integrity of the physical barriers is maintained by the consistent application of a safety strategy known as defence-in-depth during all stages of reactor design, construction and operation. This strategy provides guidance for the safety design and safe operation on three overlapping levels, Table A5.

The first level implies that the reactor is designed and operated for maximum safety during normal operation. Releases of radionuclides are kept as low as reasonably achievable. Safety efforts focus on the *prevention* of accidents. Disturbances of normal operation shall be tolerated without exceeding the prescribed release limits. No single mechanical or human failure shall lead to excessive releases.

The second level presupposes that incidents will occur in spite of the preventive measures. Systems and measures of *protection* are therefore provided to counteract and prevent incidents from developing into accidents.

The third level is based on the fact that accidents can occur in spite of the preventive and protective measures. Systems and measures for accident *mitigation* are therefore provided to limit and reduce the consequences of radioactive releases to the environment.

Table A 5 The defence-in-depth strategy

Level	Measures	Examples
I	Preventive	Reliable systems for safe operation and control Inherently stable design features Adequate safety margins Quality assurance Rules for safe operation Operator training
II	Protective	Engineered safety systems which are redundant, diversified and physically segregated. Rules for emergency operation
III	Mitigative	Reactor containment Activity removal systems Containment venting Accident management Emergency preparedness

Safety design

Reactors in the Nordic countries are designed and operated on the basis of the defence-in-depth principle. This means that proven engineering practices are used, and that a high level of quality assurance is applied in all activities of design, construction, operation and maintenance.

The design of the safety systems is based on the analysis of certain postulated events, called *design basis accidents*, which the plant must be able to manage without excessive release of radionuclides to the environment. The design basis accident for the emergency core cooling system and the reactor containment is the loss-of-coolant accident (LOCA), following a large pipe break in the reactor primary coolant system.

Much of the reactor safety research during the 1970s was devoted to LOCA studies. Sophisticated calculational models and computer codes were developed and validated in full-scale thermo-hydraulic experiments. The results were used to verify that the emergency core cooling criteria, as specified by the licensing authorities, are met.

The use of design-basis-accidents represents a deterministic approach to safety design and licensing, which was introduced in the USA at the end of the 1960s. In the beginning it was tacitly assumed that if a plant fulfilled the safety criteria for the design basis accidents, safety would also be ensured for other, seemingly less severe events. This assumption would prove to be incorrect, however, by more detailed studies of potential accident sequences in the years to come.

Probabilistic safety assessment

A major step forward was taken in 1975, when probabilistic safety assessment (PSA) was used to study the safety of two nuclear plants in the USA. This pioneering effort, known as the Rasmussen study, showed, for example, that a small LOCA could result in greater risk for the environment than the design basis large LOCA. PSA has since then been extensively used for safety assessment as a complement to deterministic analysis.

PSA is used to identify sequences of events that can lead to core melting, and to estimate the reliability of safety systems and mitigative measures. The results are expressed as frequencies (probabilities per reactor operating year) of core damage (PSA level 1) and of reactor containment failure and radionuclide release (PSA level 2). The consequences of an accident are usually estimated in a separate calculation. Risk is defined in terms of the frequency of occurrence of an accident and its consequences. Risk analysis is referred to as PSA level 3.

Plant-specific PSA studies have been carried out for each of the Nordic reactors. PSA level 1 has come to be regarded as a natural part in the continuing efforts of plant operators and safety authorities to improve safety and maintain a high safety level. The collected and evaluated information in a PSA makes it a useful tool for decisions on safety issues.

An international group of experts, set up by the International Atomic Energy Agency, has agreed on a target for the frequency of severe core damage that is below one such events per ten thousand reactor operating year in existing plants and below one in a hundred thousand reactor years in future plants. Accident management and mitigative measures should further reduce the probability of large off-site releases in case of core damage by at least a factor of ten.

Nearly 5000 reactor operating years have now been accumulated with commercial light water reactors. One large accident has taken place, leading to severe core damage in such a reactor; this was the accident at Three Mile Island. Statistically, the record of one severe accident in about 5000 reactor years is not inconsistent with the target for existing plants.

The significance of the long-term target can be illustrated as follows. In a world of 1000 reactors, which is more than twice the present number, the time between accidents of the Three Mile Island type with insignificant radioactive releases would be a hundred years on the average. Correspondingly, if the target is met, the mean time between severe accidents with large releases, like the one at Chernobyl, would statistically be a thousand years.

PSA studies indicate that the safety-enhancing measures implemented in the Nordic reactors have led to a safety level near to the above long-term target level, except for the Loviisa reactors, for which the core damage frequency is estimated at about one per ten thousand reactor years.

The Three Mile Island accident

The accident at Unit 2 of the Three Mile Island nuclear power plant at Harrisburg, USA in March 1979 demonstrated what the probabilistic analyses had indicated, that other events than the design basis accidents contribute significantly to the risk of power reactor operation. The accident also confirmed the reality of core melting and the wisdom of having a tight containment around the reactor. While large amounts of radionuclides were freed from the destroyed core, thus penetrating the first three protective barriers, the release from the containment building to the surroundings was insignificant in terms of health effects.

The accident at Three Mile Island demonstrated the importance of a number of safety aspects, such as operator training, man-machine interaction, analysis and feedback of operating experience, and the need of taking severe accidents into account in the design and operation of nuclear power plants. A broad spectrum of requirements and measures were introduced for plants already in operation as well as for new plants, Comprehensive research programmes were initiated, for example in the area of severe accident progression and mitigation.

During the 1980's, mitigative measures were introduced in Nordic reactors, underpinned by calculations and research on the behaviour of a melted core in the reactor containment and the release of radio-nuclides to the containment atmosphere. Rough estimates were also made of the releases to the environment, which is the source term for consequence calculations in case of containment failure.

In 1986, guidelines were issued in Sweden to the effect that the source terms of cesium and other nuclides of relevance to land contamination from a reactor of Barsebäck's size (1800 MWth) shall not exceed 0,1 % of the amount present in the reactor. If this criterion is fulfilled, it is expected that no early fatalities and no intolerable land contamination will occur. Similar guidelines, now mandatory requirements, were issued in Finland in 1986.

The guidelines imply that severe accidents must be included in the design basis for the reactor containment. The residual risk from events beyond the design basis, having a very small likelihood of occurrence but with potentially large source terms, is deemed negligibly small. These beyond-design events include events with very low initial frequency, such as rupture of the reactor pressure vessel and certain external events, e.g. airplane crash or large earthquake.

Human factors

The Three Mile Island accident showed that the human element had not been adequately included in previous safety considerations. This observation prompted numerous improvements in design and operational practices at nuclear plants. The accident stimulated the development of advanced instrumentation and control systems. Great innovation and progress has been achieved in computer-aided information systems for supervision and control of the plant during both normal operation and accident events.

Attention to human factors at the design stage should ensure that plants are tolerant of human error. This is achieved by the use of automatic control and protection systems. A basic safety rule implies that operator intervention in off-normal situations should only be resorted to in cases where there is sufficient time for diagnosis and corrective action. In future reactors, increased emphasis is put on inherent safety features and passive safety systems, which do not require human action or external energy supply.

Even with a high degree of automation, the operator staff plays an important role for the safe operation of the plant, particularly when the operating conditions are changed, for example during startup and at shutdown, and in off-normal situations. Technical specifications for safe reactor operation help to protect against violations of the safety provisions. Improved aids for plant operation, maintenance and inspection are developed. Staff training and retraining are receiving strong emphasis.

The approach to reactor safety has been extended to include also behavioural aspects. The Three Mile Island accident clearly illustrated how the interaction between human, technical and organizational factors contributed to the progression of events. Research and analysis in this area is receiving increased attention by the nuclear utilities and safety authorities as a complement to other methods of system analysis for improving the reliability and safety of nuclear plant.

Accident management

Experience has shown that humans can cause an accident but also intervene to prevent and mitigate the effects of an accident. Accident management includes action to be taken by the operator staff during the evolution of a beyond-design accident, in order to preserve the basic safety functions of controlling the reactor power, keeping the fuel cooled, and confining the radioactive materials.

Preventive accident management is directed to maintaining the integrity of the reactor pressure vessel and main coolant circuit so that further progression of the accident is obviated. Preventive accident management aims at restoring core cooling in incipient beyond-design events, thereby reducing the probability of core damage.

Mitigative accident management is directed to maintaining the integrity of the reactor containment once core melting has occurred so that the environmental effects are alleviated. As a result, the likelihood of a severe accident with large off-site consequences will be further reduced.

Accident management is achieved by *emergency operating procedures* using existing plant systems in normal or unusual ways or special plant features provided for the purpose. The procedures are symptom-oriented, which means that critical safety parameters are monitored, and that action is directed to preventing the parameters from reaching limiting values. Benefitting from accident management requires training of operator staff and the provision of adequate information in the control room.

The Nordic nuclear utilities have put great efforts into the development of emergency operating procedures, staff organization for accident management, and training to interpret control room information, including the choice of relevant corrective action and the understanding of system response in severe accident situations. Most of the efforts are directed to preventive accident management.

As a first priority, the emergency operating procedures aim at interrupting the nuclear chain reaction and securing core cooling. Secondly, and as soon as possible after the start of an accident, water is supplied to the containment for condensation of steam to avoid rapid pressure buildup. In boiling water reactors, due to their relatively small containment volume, pressure relief will sooner or later be necessary. All Nordic BWRs are therefore equipped with filtered containment venting systems. Also Nordic PWRs have similar or other systems for avoiding overpressure in the containment.

The impact of Chernobyl

The accident at Unit 4 of the Chernobyl nuclear power station in the Ukraine in April 1986 is the largest accident to have occurred in a nuclear reactor. The reactor core and parts of the reactor and turbine buildings were destroyed. Large amounts of radioactive materials were released to the atmosphere. Evacuation of the surrounding area was required, and fallout from the radioactive cloud affected wide areas also in countries outside the USSR.

The accident was triggered by an almost instantaneous increase of the nuclear chain reaction rate, causing a rapid power runaway, severe fuel destruction, and violent fuel-coolant interaction. It was mainly due to fundamental design deficiencies accompanied by erroneous operator action under off-normal operating conditions. No unknown phenomena or mechanisms were revealed, although there are still difficulties in determining the exact course of the accident.

While the Chernobyl reactor was of a different type than the light water reactors in the Nordic countries and elsewhere, the accident highlighted some important aspects of reactor design, operation and safety analysis. The most important lesson was perhaps the truly international implications of a severe nuclear accident with large radionuclide releases.

One of the issues raised was if a similar accident could occur in a light water reactor. Reactivity-induced accidents should be prevented by design and inherent safety features in light water reactors. They are included in the design basis for the reactor protection system and are evaluated in the safety analysis report submitted for licensing. Re-analysis of these and other design-basis accidents confirmed the earlier conclusions that the design criteria are not exceeded.

Safety culture and "eastern" reactors

In the wake of Chernobyl the concept of "safety culture" was coined to characterize the dedication and attitude of individuals and organisations involved in safety activities. Key elements of safety culture are: knowledge and competence, motivation and commitment, supervision practices and management responsibilities. Obviously, very high standards are required for personnel directly engaged in plant operation.

The Chernobyl accident drew attention to the generic safety deficiencies of the RBMK reactor type. Some improvements have been introduced after the accident. Serious deficiencies also exist in earlier versions of Russian pressurized water reactors. For example, the first generation of this reactor (VVER 440 Type V-230) lacks reactor containment. Ten such units are still in operation, four of which in Russia, four in Bulgaria, and two in Slovakia.

The demise of communism has opened up Central and Eastern Europe and the former Soviet Union and made possible bilateral and multilateral agreements of assistance for improving the safety of Russian-built reactors. The Nordic countries are supporting activities at the RBMK plants at Sosnovy Bor, Russia, and Ignalina, Lithuania, and at the VVER 440 Type V-230 at Kola, Russia.

APPENDIX 3

TERMS AND ABBREVIATIONS

accident occurrence involving substantial deviations from normal operation that may lead to release of significant quantities of radioactive materials if appropriate *engineered safety features* or administrative controls were not provided

accident management planning and execution of activities to prevent the progression or mitigate the consequences of an *accident*

accident mitigation *engineered safety features* and procedures to preserve the integrity of the *reactor containment* and to minimize the offsite releases of radioactive materials when an *accident* has occurred

accident sequence chain of events in an *accident*

ACE Advanced Containment Experiments

aerosol suspension of solid or liquid particles in gas, usually air

AKTI joint Nordic research project on activity releases in nuclear accidents and their dispersion and impact in the environment, carried out 1985-1989

AOT Allowed Outage Time, the time that a component is allowed to be out of service according to the *technical specifications* for safe plant operation

APRI Swedish severe accident research programme, initiated in 1992

ASAR As-built Safety Analysis Report, recurrent safety review of Swedish nuclear power plants

ATT Aerosol Transport Tests

barrier *inherent* or *engineered safety feature* which delays or prevents the dispersion of radioactive materials

baseline risk reference level of *risk*, obtained for a plant configuration where no components are unavailable due to maintenance or repair, and where all standby components have been recently tested without indication of failure

basic PSA *probabilistic safety assessment* assuming average values for the unavailablity of safety-related components and systems

blackout see *station blackout*

BWR boiling water reactor

CAMS Computerized Accident Management Support, a joint Nordic research project in the SIK programme

CCF see *common cause failure*

CHMAAP CHemistry in MAAP, a computer code for calculating chemical effects and interactions between chemistry and transport phenomena in *MAAP*

cladding tight enclosure for nuclear fuel, usually a long cylindrical tube, to prevent chemical reactions between fuel and coolant, to confine radioactive substances formed in the fuel during operation, and to provide mechanical support the fuel

common cause failure multiple failures attributable to a common cause, such as an *external event*, a manufacturing defect, or a manoeuvring error

containment see *reactor containment*

core part of a reactor where the nuclear chain reaction takes place.

core damage degradation of the core due to loss of cooling or power control

core damage frequency estimated risk of *core damage*, expressed as the probability of core damage per operating year

core melt core damage in which the whole *core* or parts of it has melted

criticality state where a reactor is able to maintain a self-sustaining chain reaction

decay heat heat generation caused by remaining radioactivity

defence-in-depth safety principle for the design and operation of nuclear reactors providing guidelines for safety measures on three levels: the preventive, protective, and mitigative levels

design basis accident postulated *accident* which is prescribed to serve as basis for the design of *engineered safety features* and procedures

deterministic safety analysis the study of plant behaviour after an assumed initial event with calculational models describing the physical and chemical processes in the main plant systems

diversification design principle for increasing the reliability of a safety function by providing at least two systems with different ways of action for performing the safety function

drywell compartment in the *reactor containment* where steam is allowed to expand when it escapes from the *primary coolant circuit* in a *loss-of-coolant-accident*

emergency core cooling cooling of the reactor core when primary coolant has been lost

emergency operating procedures guidelines for preventing unexpected events from developing into *accidents*

engineered safety feature component or system designed to maintain safety in off-normal events

EPRI Electric Power Research Institute, USA

external event *initiating event* caused by natural phenomenon or human activity outside the plant

filtered venting method of preventing overpressurization of the reactor containment and limiting the offsite releases of radioactive materials

FILTRA Swedish severe accident research programme, carried out 1980-1982

fission partition of a heavy atomic nucleus in two or more nuclei

fission product atomic nucleus formed in *fission*

HAFOS Swedish severe accident research programme, carried out 1990-1992

IAEA International Atomic Energy Agency

IFE Institutt for Energiteknikk

inherent safety intrinsic property of the reactor system which eliminates the risk of a harmful event

initiating event first event in a sequence of events which may lead to *core damage*

instantaneous risk estimate of *core damage frequency* using actual time-dependent values of component and system unavailabilities

internal event *initiating event* caused by component failure or system malfunction

LACE LWR Aerosol Containment Experiment

living PSA *probabilistic safety assessment* of the actual configuration of an operating plant

LOCA see *loss-of-coolant-accident*

LOFT Loss Of Fluid Test

loss-of-coolant-accident core damage due to loss of coolant, for example due to a pipe break in the *primary coolant circuit*

lower drywell part of the *drywell* located below the reactor vessel in a boiling water reactor

lower plenum part of the reactor vessel located below the *core*

LPSA Living Probabilistic Safety Assessment

MAAP computer code for predicting the progression of *severe accidents*

mitigation see *accident mitigation*

mitigative accident management activities to minimize the offsite releases of radioactive materials when a severe accident has occurred

nominal risk estimated reference level of the core damage frequency using average values for component and system unavailbilities

NPP Nuclear Power Plant

NRC U.S. Nuclear Regulatory Commission

NSSS Nuclear Steam Supply System, the reactor with the primary and secondary process systems needed for its operation

operating rules requirements, guidelines and procedures for safe operation

outage period of reactor shutdown

passive safety system *safety system* which does not require external energy or action for operation

pressure suppression system system for reducing the pressure in the *reactor containment* for events which lead to pressure increase in the containment

preventive accident management activities to restore core cooling and preserve the integrity of the *primary coolant circuit* when core cooling has deteriorated

primary coolant circuit coolant system by which heat is transferred and transported from the reactor core

probabilistic safety analysis see *probabilistic safety assessement*

probabilistic safety assessment method for the analysis of plant safety, based on mapping potential accident sequences and estimating the reliability of safety functions

PSA see *probabilistic safety assessment*

PWR Pressurized Water Reactor

RAMA Swedish severe accident research programmes, carried out 1983-1989

RBMK boiling-water-cooled graphite-moderated reactor

radionuclide a radioactive species of atom

reactivity measure of the deviation from *criticality* in a nuclear reactor

reactivity-induced accident core damage caused by uncontrolled *reactivity* increase

reactor cavity part of the *reactor containment* located below the reactor vessel in a pressurized water reactor

reactor containment pressure-tight building surrounding the *nuclear steam supply system*, mainly for retaining radioactive substances during normal and off-normal operating conditions

recriticality state where a degraded core or core debris becomes *critical* upon *reflooding*

redundancy design principle for increasing the reliability of a safety function by providing two or more identical components or systems to perform the safety function

reflooding *emergency core cooling* by refilling the reactor vessel with water after core uncovery and degradation

release frequency estimated risk of *severe release* , expressed as the probability of release per operating year

retrospective risk estimate of *core damage frequency* using historic operational data

risk probabilistic measure of safety, e.g. *core damage frequency* or *release frequency*

risk follow-up application area for living PSA in which the *retrospective risk* is estimated

risk increase factor ratio of *instantaneous risk* and a reference risk level, usually the *nominal risk*

risk monitoring application area for living PSA in which the *instantaneous risk* is estimated

RPV Reactor Pressure Vessel

safety system system for maintaining plant safety in off-normal events

scram automatic or manual shutdown of the reactor by insertion of control rods in the *core* which stops the chain reaction

severe accident *accident* involving *core melt* and potential offsite release of radioactive materials

severe release the offsite release of radioactive materials in an *accident* involving *core melt* and *containment* failure

SKI Swedish Nuclear Power Inspectorate

source term release of radioactive materials from the *primary coolant circuit* to the *reactor containment* or from the containment to the environment

station blackout complete loss of electric power for the operation of plant systems

STUK Finnish Centre for Radiation and Nuclear Safety

technical specifications for safe operation see *operating rules*

TS *Technical Specifications for safe operation*

VARA Finnish severe accident research programme, initiated in 1983

void coefficient the incremental change of *reactivity* per incremental change of void volume in the coolant by the formation of steam in boiling

VTT Technical Research Centre of Finland

VVER pressurized water reactor of Russian type

wetwell compartment in the *reactor containment* of a boiling water reactor containing a water pool for condensation of steam

Nordic Studies in Reactor Safety

There are 16 nuclear power reactors in the Nordic countries, and additional ones in the surrounding regions. It is joint of Nordic interest to understand the safety features of these reactors and to contribute to their improvement. Through the Nordic project work described in this report, the practical use of methods for safety evaluation is enhanced. Improved methods to predict abnormal sequences and their possible effects are developed, in order that corrective action can be taken in time. More complete information about reactors in neighbouring countries is also available.

The Nordic Committee for Nuclear Safety Research - NKS
organizes pluriannual joint research programmes. The aim is to achieve a better understanding in the Nordic countries of the factors influencing the safety of nuclear installations. The programme also permits involvement in new developments in nuclear safety, radiation protection, and emergency provisions. The three first programmes, from 1977 to 1989, were partly financed by the Nordic Council of Ministers.

The 1990 - 93 Programme
Comprises four areas:

* Emergency preparedness (The BER-Programme)
* Waste and decommissioning (The KAN-Programme)
* Radioecology (The RAD-Programme)
* Reactor safety (The SIK-Programme)

The programme is managed - and financed - by a consortium comprising the Danish Emergency Management Agency, the Finnish Ministry of Trade and Industry, Icelands's National Institute of Radiation Protection, the Norwegian Radiation Protection Authority, and the Swedish Nuclear Power Inspectorate. Additional financing is offered by the IVO and TVO power companies, Finland, as well as by the following Swedish organizations: KSU, OKG, SKN, SRV, Vattenfall, Sydkraft, SKB.

ADDITIONAL INFORMATION is available from
the NKS secretary general, POB 49, DK-4000 Roskilde, fax (+45) 46322206

The Nordic Council of Ministers

ISBN 92 9120 461 1
ISSN 0908-6692