IAEA-TECDOC-737

Advances in reliability analysis and probabilistic safety assessment for nuclear power reactors

Report of a Technical Committee meeting held in Budapest, 7–11 September 1992

INTERNATIONAL ATOMIC ENERGY AGENCY

The IAEA does not normally maintain stocks of reports in this series. However, microfiche copies of these reports can be obtained from

INIS Clearinghouse
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

Orders should be accompanied by prepayment of Austrian Schillings 100,— in the form of a cheque or in the form of IAEA microfiche service coupons which may be ordered separately from the INIS Clearinghouse.

The originating Section of this document in the IAEA was:

Nuclear Safety Section
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

ADVANCES IN RELIABILITY ANALYSIS AND PROBABILISTIC SAFETY ASSESSMENT
FOR NUCLEAR POWER REACTORS
IAEA, VIENNA, 1994
IAEA-TECDOC-737
ISSN 1011–4289

Printed by the IAEA in Austria
March 1994

FOREWORD

Over the last ten years, there has been considerable growth in the use of probabilistic safety assessment (PSA) for assessing the safety of nuclear power plants. PSAs are increasingly being performed, to complement deterministic analyses, both in the industrial and the regulatory environment, to address almost every aspect of the nuclear power plant life cycle.

The benefits of PSA have been recognized in many countries that are not well advanced in using PSA techniques. Recently, efforts have been made to apply PSA techniques in central and eastern European countries and in the newly independent states of the former USSR. The results of PSAs for some specific reactor types (such as WWERs) are now becoming available.

Although most plant specific PSAs have been performed to assess overall plant safety (or risk) and to identify specific weaknesses in design and operation, the comprehensive logical modelling in a PSA make it desirable for use in optimizing various operational tasks.

Recently, attention has been paid to other kinds of PSA applications, including risk based regulation and inspection, plant configuration control and operator training. Many such applications have the potential for providing guidance on the optimal use of resources and reduction of the burden on the operating organization. These different PSA applications set new requirements on the scope of PSAs, the necessary level of detail, quality and coverage of data, and the capabilities of computer tools used to run the models.

In order to promote the use of risk and reliability techniques in this important and fast developing area, the IAEA convened a Technical Committee Meeting (TCM) on Advances in Reliability Analysis and Probabilistic Safety Assessment in Budapest from 7 to 11 September 1992. The meeting was organized with the co-operation of the Hungarian Institute for Electrical Power Research (VEIKI). The TCM was attended by 79 participants from 23 countries. The 41 papers presented at the meeting address recent developments in the area of PSA applications as well as advanced techniques/methods for various applications. In addition, comprehensive information was presented concerning PSA programmes in central and eastern European countries (CEEC) and the newly independent states (NIS) of the former USSR.

This TECDOC, which was prepared by the participants in the TCM, summarizes insights from the papers presented at the meeting and from the plenary discussions. The most important topics related to PSA methods and to various applications of PSA technique that were discussed during the working group sessions are also presented.

EDITORIAL NOTE

In preparing this document for press, staff of the IAEA have made up the pages from the original manuscripts as submitted by the authors. The views expressed do not necessarily reflect those of the governments of the nominating Member States or of the nominating organizations.

Throughout the text names of Member States are retained as they were when the text was compiled.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

The authors are responsible for having obtained the necessary permission for the IAEA to reproduce, translate or use material from sources already protected by copyrights.

CONTENTS

APPENDIX: PAPERS PRESENTED AT THE TECHNICAL COMMITTEE MEETING

1. INTRODUCTION

The purpose of the Technical Committee Meeting (TCM) on Advances in Reliability Analysis and Probabilistic Safety Assessment held in Budapest from 7 to 11 September 1992 was to exchange experience in the area of PSA and in particular of PSA applications, and to promote international co-operation in this area. Plant specific PSAs as well as experience and trends in applying insights from PSA to optimize plant tasks were discussed at the meeting.

This TECDOC is a documentation of the meeting. The document reviews the present status and the aims of PSA efforts in different countries and related international activities; it includes an overview of the presentations and insights from the working group discussions on selected topics related to both methods and applications and papers presented at the meeting. The main text is divided into several sections, each devoted to a separate subject. This structure reflects the division of the meeting into working sessions.

The status of PSA in the former USSR and eastern European countries is presented in Section 2. It includes an overview of presentations as well as the results of the working group discussions. Brief information on PSA programmes is provided and PSA methods used in each country or organization are described. Open issues that require further consideration and/or external assistance are also discussed.

Section 3 is devoted to advances in the area of PSA methods and new applications. Two topics covered by the presentations are highlighted. 'Living PSA' and Risk Monitor is addressed as one of the subjects that has recently attracted significant interest, in the context of both methods and practical applications. The second topic covered in Section 3 is related to PSA oriented plant response analysis.

Section 4 is devoted to risk based regulation. In addition to an overview of the presentations, some insights from the working group discussions are given. Selected issues are addressed to present a regulatory perspective on PSA applications.

Section 5 provides brief information on selected PSA applications. A variety of practical applications in the area of plant operation are discussed. Risk based Technical Specifications are specifically addressed as one of the most important and promising areas of application.

The appendix reproduces a selection of papers presented at the meeting. A list of participants is included.

2. SELECTED PSA PROGRAMMES

2.1. INTRODUCTION

Over the last few years extensive training for and transfer of technology on PSA and related topics have been provided to eastern European and CIS countries, mainly for WWER type reactors (e.g. within the framework of the IAEA Regional Programme RER/9/005, PSA for WWER Type Reactors). As a result, all WWER users now have sizable PSA programmes aimed at developing a PSA for each operating reactor in the region. The first PSA activities in this region focused primarily on identification of possible design weaknesses, but other potential applications are being considered or are already being implemented.

A separate technical session of the TCM was devoted to PSA programmes in countries of the Commonwealth of Independent States and eastern European countries. In addition to this general session, a closed session was organized especially to address IAEA TC Project RER/9/005.

An overview of the presentations related to PSA activities in Bulgaria, the former CSFR, Hungary, the Russian Federation and Lithuania is given in Section 2.2.

More detailed information concerning the status of PSA in CIS and eastern European countries is provided in Section 2.3. The material prepared by the working group addresses both PSA related activities and the status of PSA methods. Some open issues that need further consideration or that require the transfer of expertise or assistance are also discussed. Information is also given on future activities and related IAEA assistance.

2.2. OVERVIEW OF THE PRESENTATIONS

There were ten presentations devoted to PSA programmes (one in written form only). Four reviewed PSA activities in Hungary, the Russian Federation, Bulgaria and the CSFR; the fifth paper expanded on information presented in the CSFR overview. All these contributions served as a basic material for the preparation of working material from this session (working group) and gave a good picture of PSA activities in the four countries.

The Hungarian presentation was oriented mainly to the AGNES project/Level 1 PSA which accounts for the main activities. The main aims, targets and tasks of the project scheduled for 1993 and 1994 were presented. The preliminary list of 65 initiating events for the PSA of Paks NPP Unit 3 and a detailed plan of tasks with a time schedule are included.

In the Russian paper, several items were pointed out:

- PSA studies are included in SARs for all new NPPs;

- PSA studies for the NPPs in operation are obligatory for further operation of these NPPs (by decision of the regulatory body);

- Methods and software have been adopted for Level 1 PSA;

- Several preliminary studies have been performed for the WWER-1000 reactor (related results and comments are presented):

  (a) standardized V-320 (Rostov plus Unit 4 Balakovo);
  (b) backfitting design V-320 (Unit 5, 6 Balakovo);
  (c) V-392 (Loviisa);
  (d) new design V-392 (NPP-92 project).

A list of initiators was presented (eight groups of initiators). Analyses were performed for full power operation. A generic database was used. Common cause failures (CCFs), human errors (HEs) and accident management measures were taken into account.

The goals of these PSA analyses include:

- contribution of studied IE groups to core damage frequency (CMF);
- dominant contributors to CDF identification;
- development of measures for improving safety;
- evaluation and verification of new designs.

The conclusions of this paper address several problems that have to be solved in order to perform full scale PSAs.

The Bulgarian contribution gave a project background of the PSA study for Units 5 and 6 of the Kozloduy NPP. This study will provide input for FSAR upgrading (Level 1). Accident sequences from internal events, including fires, and accident sequences from earthquakes are in the project scope. It is intended to use the computer code PSAPACK (version 4.2) for the analysis. The overall period of this study is 26 months from 1 June 1992. The project organization and quality assurance were also presented.

The background to the preparation of the Dukovany NPP probabilistic safety assessment study, its goals and its programme are mentioned in the CSFR contribution. This study was done in co-operation with almost all Czechoslovak institutions working in the field of PSA. Fourteen initiating events were chosen and analysed for the preliminary PSA study and reviewed by the Czechoslovak PSA team and by the Dukovany NPP staff in early 1992. The Risk Spectrum FT PLUS code was used for analyses of 21 front line and support system fault trees. The course of the project, assumptions, methods used, database, common cause failures and human factor analyses are briefly described. Some experiences in the preparation of this study and comments on its results are also presented. The expected course of additional analyses for the final version of the PSA study and PSA activities for 1992 and the near future in Czechoslovakia are added in conclusion. References in reliability analysis and PSA analysis in Czechoslovakia are included. The fifth contribution extended information given in the CSFR 'overview paper'; further information concerning a reliability analysis with Tree Master code for Bohunice NPP which has a V-230 reactor was provided.

The next three contributions comprise information on a co-operation between western and eastern specialists devoted to NPPs in eastern European countries. In addition, this contribution provided information on the status and the scope of the PSA activities in eastern Europe.

The first of these contributions is devoted to the UK-Russian collaboration on PSA for RBMK reactors. It presented urgent steps which were taken after the Chernobyl accident to prevent any recurrence of such an accident on the RBMK reactors and subsequent improvements in the longer term which have further reduced the probabilities of severe accident. As the older reactors are reconstructed, major improvements in safety systems are made possible. Preliminary results of safety assessments suggest that RBMK safety may become comparable with that of many older western plants, which have also been subject to requirements to improve safety.

The next contribution, from RELCON, Sweden concerned the Barselina project, which was initiated in mid-1991. The project is a multinational co-operation between Lithuania, Russia and Sweden, with the long range objective of establishing common perspectives and unified bases for the assessment of severe accident risks and needs for remedial measures for the RBMK reactors. The Swedish BWR Barsebäck is used as reference plant and the Lithuanian RBMK Ignalina as application plant. The Barselina project cannot be looked upon as a traditional PSA; the scope and objectives of the PSA activities were modified according to the general objective. PSA is in this context used as a tool to achieve this common understanding between the project parties. This report constituted a status report for Phase 2 of the project prepared in August 1992. The project will last until October 1993; the qualitative part of the initiating event analysis and the qualitative part of the accident sequence analysis have already been performed.

The last contribution in this group concerns the participation of Westinghouse in the WANO Six Month Programme for Kozloduy. The project is in four parts:

Part 1: To assess the applicability of the Greifswald PSA to the Kozloduy plant (to identify initiating events that could lead to pressurized thermal shock to the reactor vessel).

Part 2: Reliability analysis of the safety injection system, the confinement system and the emergency feedwater system (fault tree, generic data, recommendations for improvements).

Part 3: Probabilistic pressurized thermal shock evaluation.

Part 4: Preparation of the Kozloduy specific MAAP input parameter file (for large steamline break and station blackout analyses).

The last contribution of this session was prepared by the utility operating Temelin NPP in the CSFR. Construction of Temelin NPP was started in 1986 and four units of the Soviet WWER type 1000 were planned originally. In 1989 the construction of Units 3 and 4 was canceled and Units 1 and 2 became the subject of several reviews and many important design changes. The goal of this process is the so-called 'westernization' of the plant (i.e. the NPP should be able to meet licensing requirements assumed to apply in western countries in the mid-1990s). A formal tendering process to perform a PSA study was started in February 1992. The general purpose of this task is to provide systematic examination of Temelin NPP Unit 1 for severe accident vulnerability resulting from a Level 2 PSA. The scope includes both internal and external hazards.

2.3. STATUS OF PSA IN CIS AND EASTERN EUROPE: SUMMARY OF WORKING GROUP ACTIVITIES

2.3.1. PSA activities

The status of PSA related activities that are carried out in eastern Europe and in the CIS countries is presented on the basis of information made available during the TCM, either in the papers presented or in the course of working group discussions. Since not all countries in the region that operate NPPs were represented at the meeting, the information is not complete. All available information concerning PSA related activities is presented in the form of project information sheets and summary tables. Project information sheets give the operating country, the plant name and type, project schedule, sponsors and organizations in charge, and the project objectives and the scope. Further comments are included.

A summary of information is provided in tabular form. Table I includes brief information on NPPs operated in the region. Tables II–VI present basic information on PSA projects carried out (or performed recently) in the region. Various types of NPPs are addressed. Information included is limited to plant name, PSA scope and the project objectives. Reference to specific presentations is also made where applicable.

*Text cont. on p.*17.

TABLE I. NPPs OPERATED IN CIS AND EASTERN EUROPEAN COUNTRIES

COUNTRY	PLANT	REACTOR TYPE
CZECHOSLOVAKIA	V1 - BOHUNICE	WWER - V230 × 2
	V2 - BOHUNICE	WWER - V213 × 2
	DUKOVANY	
	MOCHOVCE	WWER - V213 × 4
	TEMELIN	WWER - V213 × 4
		WWER - V320 × 2
ROMANIA	CERNAVODA	CANDU 600
LITHUANIA	IGNALINA	RBMK - 1500 × 2
HUNGARY	PAKS	WWER - V213 × 4
SLOVENIA	KRSKO	PWR W
POLAND	ZARNOWIEC	WWER - V213 × 2
FINLAND	LOVIISA	WWER - V230 × 2
BULGARIA	KOZLODUY	WWER - V230 × 4
UKRAINE	ROVENSKAYA	WWER - V213 × 2
		WWER - V320 × 2
	CHERNOBYL	RBMK 1000 × 2
RUSSIA	ZAPOROZHSKAYA	WWER - V320 × 5
	KOLA	WWER - V213 × 2
		WWER - V230 × 2
	NOVO-VORONEZH	WWER - V230 × 2
	BALAKOSKAYA	WWER - V320 × 4
	KALININSKAYA	WWER - V320 × 1
	VORONEZH	NDHP AST-500 × 2
	NIZHNY NOVGOROD	NDHP AST-500 × 2
	LENINGRAD	RBMK × 1000 × 4
	SMOLENSK	RBMK × 1000 × 3
	KURSK	RBMK × 1000 × 4
	BELOYRSKAYA [DESIGN]	BN 600 BREEDER 600 MWe

TABLE II. PSA PROJECTS CARRIED OUT FOR RBMK NPPs

PLANT	No.	PSA SCOPE	OBJECTIVES	COMMENTS
IGNALINA 1&2 (LITHUANIA)	2	LEVEL 1. NO. EEs, LIMITED TREATMENT OF THE HUMAN FACTOR	ASSESSMENT OF THE RISK OF THE RBMK	RBMK 1500 REF: PAPER OF Mr. D. WILSON
CHERNOBYL 1&3 (UKRAINE)	2			
LENINGRAD 1-4 (RUSSIA)	4	PRELIMINARY Level1 MADE FOR UNIT 1 WILL SOON BE COMPLETED	ASSESS THE EFFICIENCY OF THE CHERNOBYL IMPROVEMENTS	PAPER OF MR. HOLLOWAY
SMOLENSK 1-2-3 (RUSSIA)	3			
KURSK 1, 2, 3, 4 (RUSSIA)	4			
TOTAL	15 (in operation)			

TABLE III. PSA PROJECTS CARRIED OUT FOR WWER-320 NPPs

PLANT	No. OF UNITS	PSA SCOPE	OBJECTIVES	COMMENTS
TEMELIN 1.2 (CZECH)	2*	LEVEL 2 - + EEs PARTIAL SHUTDOWN LIVING PSA	1. FULFILL IAEA RECOMMENDATIONS 2. ASSESS AND UNDERSTAND PLANT RESPONSE 3. TRANSPORT PSA TO EVERYDAY USE	PAPER OF MR. FERJENCIK
KOZLODUY 5.6 (BULGARIA)	2	LEVEL 1 + FIRE + SEISMIC		MAY BE BROADENED TO INCLUDE ALL CCI AND EE. REF: PAPER OF MR. KOLEV
ZAPOROZHKAYA (UKRAINE 1 TO 5)	5	FULL SCALE LEVEL 2 + ESTIMATED DOSES AT DIFFERENT DISTANCE OF NPP. IEs AND EEs.		INCLUDED COLD SHUTDOWN AND FUEL OPERATION
ROVENSKAYA 3 (UKRAINE)	1	FULL SCALE LEVEL 2 + ESTIMATED DOSES AT DIFFERENT DISTANCE OF NPP. IEs and EEs.		INCLUDED COLD SHUTDOWN AND FUEL OPERATION
BALAKOSKAYA (RUSSIA)	4	PRELIMINARY MADE FOR UNIT 4 MODIFICATION OF THE STANDARDIZED DESIGN, SOME IEs FULL POWER OPERATION ONLY	EVALUATE THE CONTRIBUTION OF IEs. IDENTIFY MAIN CONTRIBUTIONS. EVALUATE MAIN MODIFICATION SEVERE ACCIDENT MANAGEMENT	---------
KALINISKAYA	1*			
TOTAL				

* In construction.

For the Russian reactors, see reference paper of Mr. Shvyrayev.

TABLE IV. PSA PROJECTS CARRIED OUT FOR WWER 213 NPPs

PLANT	No. OF UNITS	PSA's SCOPE	OBJECTIVES	COMMENTS
BOHUNICE 3&4 (CZECH)	2	LEVEL 1 SEISMIC	RE-EVALUATION OF FSAR	FOLLOWS DUKOVANY PSA
DUKOVANY 1-2-3-4 (CZECH)	4	LEVEL 1 + FIRE	SAFETY ANALYSES MODIFICATION SAFETY ASSESSMENT	
MOCHOVCE 1-2-3-4 (CZECH)	4*	LEVEL 1		INTENTION AT THE PRESENT TIME
PAKS 1-2-3-4 (HUNGARY)	4	LEVEL 1 + IEs	QUANTIFICATION OF CDF	REF: PAPER OF MR. HOLLO
KOLA 3&4 (RUSSIA)	2	NOT FORESEEN AT THE PRESENT TIME		
ROVENSKAYA 1&2 (UKRAINE)	2	FULL SCALE LEVEL 2 IEs AND EEs SHUTDOWN CONDITIONS AND FUEL TRANSPORT OPERATION		
ZARNOWIEC 1&2 (POLAND)	2**	LEVEL 1. LIMITED NUMBER OF IEs (6). LIMITED TREATMENT OF HEs	IDENTIFICATION OF WEAKNESS SUPPORT OF INSPECTIONS AND HQ PROCESS	
TOTAL	20 (+2)	14 IN OPERATION 4 UNDER CONSTRUCTION 2 CANCELLED	+ 2 LOVIISA 213 MODIFIED LEVEL 1 COMPLETED + IE DEVELOPMENT: LEVEL 2 LIVING PSA	

* Under construction.

** Cancelled.

TABLE V. PSA PROJECTS CARRIED OUT FOR WWER 230 NPPs

PLANT	No. OF UNITS	PSA SCOPE	OBJECTIVES	COMMENTS
BOHUNICE 1&2 (CZECH)	2	LEVEL 1 + IEs (FIRE AND FLOOD)	SAFETY EVALUATION OF THE MODIFICATION	MADE BY ELECTRO-WATT
KOZLODUY 1-4 (BULGARIA)	4	(1) TOP LEVEL RISK STUDY (2) 6-MONTH WANO PROGRAMME	SAFETY ASSESSMENT OF THE MODIFICATION EVALUATE BY PSA TECHNIQUES THE MOST PRESSING ISSUES DETECTED DURING WANO MISSIONS	
KOLA 1&2 (RUSSIA)	2			
NOVO-VORONEZH 3&4 (RUSSIA)	2			
TOTAL	10 (in operation) 4 units (Greifswald) 2 units (Armenia, out of service)			

TABLE VI. PSA PROJECTS CARRIED OUT FOR OTHER TYPES OF NPPs

PLANT	No. OF UNITS	PSA's SCOPE	OBJECTIVES	COMMENTS
CERNAVODA (ROMANIA)	1	FULL SCOPE LEVEL 1 - 1994 + LEVEL 2,3 + LIVING PSA	- FOR LICENSING PURPOSE - DESIGN EVALUATION	CANDU
KRSKO (SLOVENIA)	1			PWR W
VORONEZH	2	LEVEL 1 (92-93) LEVEL 2 PRELIMINARY (93-94)	QUANTIFICATION OF CDF	NDHP AST-500
NIZHNY NOVGOROD	2	LEVEL 1 - IEs		
BELOYRSKAYA	1	LEVEL 1	QUANTIFICATION OF CDF	BREEDER
[DESIGN]	X	LEVEL 1 - SOME TASKS OF LEVEL 2 (92- 94)	QUANTIFICATION OF CDF	600 MWe ENHANCED SAFETY PLANT

Based on the information provided during the TCM, some general observations can be made concerning PSA activities carried out in the region.

It may be concluded that PSA work on relatively new designs/plants (WWER-1000/V320, WWER-440/V213) is relatively well advanced. With very few exceptions these plants are the subject of PSA analysis (5 out of 6 listed NPPs of the V320-type and 6 out of 7 listed NPPs of the V213-type were addressed).

However, the scope of PSA projects (completed or under way) is limited. All these projects cover Level 1 analyses. Shutdown risk and detailed external event analyses have not been performed. Some methodological shortcomings are also observed (see Sections 2.3.2 and 2.3.3).

Older designs/plants are not well covered by current PSA activities. For WWER-440/V230 NPPs only a few projects were reported:

- A full scope (internal events) PSA study for Bohunice 1 and 2 (Level 1) has just been started (performed by EWI, United Kingdom, financed by PHARE). It is expected to be ready within 14 months.

- The Kola PSA is not complete; it was done by a relatively inexperienced team without any PSA background (to be reviewed by the IAEA soon).

- The Greifswald PSA is not complete; no cut-sets were generated and the results are not useful for any other plant.

- A full scope PSA study for Kozloduy 1–4 has not been started yet (a six months WANO programme which was started after the change of TS is not leading to a PSA study).

- No project for PSA for Novovoronezh 3–4 is reported to be carried out or planned.

- There are only very limited activities concerning PSA for RBMK NPPs.

- A Level 1 PSA (for internal events only and with limited treatment of HEs) is carried out within the framework of the Ignalina project and a preliminary Level 1 study will be completed soon for Leningrad (Unit 1).

2.3.2. PSA methodology

Detailed information concerning the status of PSA methodology gathered from countries participating in the TCM was arranged in the form of information sheets. The most important elements of PSA modelling were addressed, including:

- accident sequence modelling;
- system analysis;
- data assessment;
- treatment of dependencies;
- treatment of human errors;
- accident sequence quantification;
- external events modelling;
- living PSA.

The following general observations were made concerning the PSA methodological approach as implemented in eastern Europe and CIS countries:

- Methodological framework for Level 1 PSA is adopted, practically in all countries of the region. It includes procedural/methodological aspects and computer software as well as some practical experience in performing Level 1 PSA;

- Not all capabilities and expertise has been implemented in plant specific PSA, completed so far. However, PSA practitioners are aware of existing limitations. Appropriate improvements are under way;

- Certain PSA areas need more consideration. Some assistance in providing the out-of-region expertise will be needed for completion of the current PSA projects and their extension to satisfy the world's standard, and to establish the basis for use of PSA results in safety related decision making. More detailed information concerning open issues in PSA methodology is provided in Section 2.3.3.

2.3.3. Open issues

Based on the information provided during the meeting on PSA methodological status and the status of PSA projects carried out in various countries a number of issues was identified, that require some more attention in the future. These issues are related to both methodological aspects of existing PSAs and to the status of PSA activities in the countries. The following general issues have been identified:

Data assessment

Credibility of existing and future PSAs should be increased by improving the data assessment process. Existing PSAs are based mainly on generic sources. WWER specific data for IEs do not exist either.

There are no systematic component reliability data collection systems in NPPs, so that the feasibility of plant specific data is generally limited. The exchange of available reliability data is almost inevitable. This data exchange is supposed to be done in the framework of RER/9/005.

Plant specific data gathering systems established in some plants are not always appropriate for PSA use. The problem is even more severe in case of future applications (e.g. optimization of operational strategies) where more advanced data analysis techniques should be implemented.

Plant response evidence

Available plant response evidence has been found to be insufficient to support PSA models in most of the existing PSAs. This shortcoming is related to both IE grouping and to ET logic. For some types of plants the situation is very unsatisfactory (e.g. RBMK, WWER/V230).

Analyses are being done for major accidents under the six month WANO programme for Kozloduy but PSA related scenarios are not covered.

Additional analyses has been made for Bohunice 1 and 2 (VUJE, Trnava) but may not be sufficient for realistic ET modelling (additional clarification is necessary).

More effort should be made to clarify LOCA categorization and to define best estimate success criteria. In some cases a more precise modelling of core behaviour is also required, e.g. calculation of core asymmetry in order to determine possible local criticality or even core damage.

2.3.4. Future activities

The future activities in the region should be directed to the following major areas:

- Improvement in quality of PSA;
- Broadening range of PSA applications;
- Increasing practical implementation to address every operating plant in the region.

Improvement in quality of PSA should concentrate on specific topics discussed in Section 2.3.3, i.e. data assessment, initiating events, plant response thermal hydraulic analysis, human reliability and incorporation of external hazards analysis.

The scope of PSA should be extended to consider shutdown risk. Extension of PSA from Level 1 to Level 2 is also very advisable, since it establishes the basis for accident management measures and development of emergency procedures.

In order to establish risk oriented safety management, the PSA extension directed to optimization of operational tasks, risk based regulation, and assessment of operational experience is of particular interest.

Majority of topics mentioned above are covered by the Regional Programme RER/9/005 "PSA for WWER type Reactors" that is extended for the years 1993-1994.

The work plan for this project for 1993 was discussed during the special session of the TCM.

2.3.5. Summary tables on PSA projects

Country	:	Bulgaria.
Plant(s)	:	Kozloduy 1 and 2 (Units 1-4).
Type	:	WWER/440-230.
Schedule	:	November 1991 - March 1992.
Sponsor(s)	:	Bulgarian Government.
Organization(s) in charge	:	EQE International.
Objective(s)	:	Logical approach to identify the modification significantly increasing the plant safety by assessment of qualitative risks.
Scope	:	Adopted western type fault schedule. ET model based on plant response knowledge. Quantification based on engineering judgement and data from the available analyses. Simplified risk model and comparative analyses of existing and modified configuration including associated costs.
Comment(s)	:	Top level risk study (not a PSA).

Country : Bulgaria.

Plant(s) : Kozloduy 1 & 2 (units 1-4).

Type : WWER/440-230.

Schedule : June-November 1992.

Sponsor(s) : PHARE PR-ME of CEC.

Organization(s) in charge : West ESI, Belgium Branch.

Objective(s) : Evaluate by PSA techniques the most pressing issues identified during WANO and IAEA missions to Kozloduy.

Scope : Review of Greifswald PSA and its applicabilities to Kozloduy.

SRA for three safety systems.

To identify IEs and sequences leading to excessive cooldown (PTS) of RPV.

Preparation of MAAP parameter file and test runs.

Comment(s) : WANO six month programme for Kozloduy (item 4 PSA); it may be continued to a Level 1 PSA.

Country	:	Bulgaria.
Plant(s)	:	Kozloduy 3 (Units 5 and 6).
Type	:	WWER-1000.
Schedule	:	June 1992–September 1994.
Sponsor(s)	:	Utility.
Organization(s) in charge	:	Risk Engineering Ltd.
Objective(s)	:	Provide support for upgrading FSAR.
		Provide assess of plant safety.
		Provide base for the use of PSA for plant operational issues.
Scope	:	Through analysis, grouping of IEs and corresponding frequency.
		Accident sequence and for all internal independent initiators.
		Analysis of fire risk as dominating CCI.
		Seismic risk and dominating external initiators.
Comment(s)	:	Kozloduy 3 PSA project; it may be broadened to include all CCI and external events.

Country : Hungary.

Plant(s) : Paks NPP.

Type : V213 × 4.

Schedule : 1991-1993.

Sponsor(s) : Hungarian Atomic Energy Commission — Level 1 PSA.
Paks Utility — PSA application.

Organization(s) in charge : VEIKI — co-ordination.
EROTERV Design Company.
Budapest Technical University.
KFKI AEKI.

Objective(s) : Quantification of core damage frequency by analysis of event sequences.

Scope : Level 1 PSA for internal IEs.

Comment(s) : The Level 1 PSA of Paks NPP is part of the AGNES project. The primary objective of AGNES is to assess the safety level of PAKS NPP by the use of up-to-date techniques (see also paper by E. Hollo, Hungary). All PSA activities in AGNES are co-ordinated by VEIKI but other national and foreign institutions are involved in the analyses too. The future goal is to extend the PSA to external events and shutdown risk. These activities are planned for the second half of 1993.

Not all the necessary thermal hydraulic calculations have been performed so far to support event developments and accident sequence modelling.

Country	:	Czechoslovakia.
Plant(s)	:	Temelin.
Type	:	WWER-V320 × 2 under construction + core design replacement.
Schedule	:	Level 1 is to start in the first half of 1993.
Sponsor(s)	:	CEZ a.s. (Czech Electricity Board).
Organization(s) in charge	:	Is being selected.
Objective(s)	:	To fulfill IAEA recommendations.
		To assess and understand plant response.
		To transfer PSA to everyday use.
Scope	:	Levels 1 and 2 + external events.
		Partial shutdown.
		Living PSA model.
Comment(s)	:	
Reference(s)	:	Paper by Mr. Ferjencik.

Country	:	Czechoslovakia.
Plant(s)	:	Mochovce.
Type	:	WWER-V213 × 4 under construction.
Schedule	:	Start in 1994.
Sponsor(s)	:	
Organization(s) in charge	:	
Objective(s)	:	
Scope	:	Level 1.
Comment(s)	:	Is intended.

Country	:	Czechoslovakia.
Plant(s)	:	Dukovany.
Type	:	WWER-V213 × 4.
Schedule	:	Preliminary, 1989–1991. Provisional, 1992–06.1993. Final, 06.1993–12.1993. Living PSA model, 1992–1994.
Sponsor(s)	:	CSAEC (CSKAE) - Czechoslovak Regulatory Body.
Organization(s) in charge	:	NRI (UJV) Řež.
Objective(s)	:	Tool to safety analyses to assess safety problems in NPP operation to determine usefulness of possible modifications.
Living PSA	:	Risk based technical specifications assessment. Results of the above mentioned Dukovany Unit 1 PSA will be involved.
Scope	:	Level 1 + internal fires.
Comment(s)	:	Reference study for next specific studies for V-213. Basis for living PSA.
Reference(s)	:	Papers by Mr. Dusek, Ms. Novakova, Mr. Stanicek, Mr. Hojny and Mr. Čillík.

Country	Czechoslovakia.
Plant(s)	V2-Bohunice.
Type	WWER-V213 2 × 2 under construction.
Schedule	Start in 1993. Duration: 18 months.
Sponsor(s)	Slovak Government.
Organization(s) in charge	NPPRI (VUJE) Trnava.
Objective(s)	Re-evaluation of FSAR.
Scope	Level 1 + external events (seismic).
Comment(s)	In frame of after years period re-evaluation of FSAR. Results of PSA for Dukovany will be extensively used.
Reference(s)	Paper by Mr. Čillík.

Country	Czechoslovakia.
Plant(s)	V1-Bohunice.
Type	WWER-V230 × 2.
Schedule	Start August 1992. Duration: 16 months.
Sponsor(s)	PHARE (CEC).
Organization(s) in charge	Electrowatt with assistance from VUPEX and VUJE.
Objective(s)	Level 1 PSA of plant (as of July 1991) and evaluation of proposed modifications of safety systems.
Scope	Level 1 + internal events (includes fires and floods).
Comment(s)	This analysis is in the initial phase with the main activities being those of documentation collection and plant familiarization.

Country	:	Finland (more details from Reino Virolainen (STUK), Jussi Vaurio (IVO).
Plant(s)	:	Loviisa 1/11.
Type	:	WWER-440.
Schedule	:	Level 1, completed 1991 — (internal events) including human reliability.
Sponsor(s)	:	Imatran Voima Oy (IVO).
Organization(s) in charge	:	Imatran Voima Oy (IVO).
Objective(s)	:	Assess the safety of the plant and detect the weak points. Improve plant operation training.
Scope	:	Level 1 - internal events.
Comments(s)	:	Fire analysis completed recently. Refuelling analysis in planning. Level 2 analysis in planning. Living PSA development started.

Country	:	Lithuania.
Plant(s)	:	Ignalina.
Type	:	RBMK-1500 MW.
Schedule	:	Phase 1 (mini-PSA), October 1991 - April 1992. Phase 2 (limited Level 1), April 1992 - December 1992. Phase 3 (extension Level 1), December 1992 - October 1993.
Sponsor(s)	:	Multilateral co-operation between Lithuania, Russia and Sweden.
Organization(s) in charge	:	*Sweden* — ES-Konsult AB, IPS AB, RELCON AB, Sydkraft Konsult AB, ABB Atom AB, Studsvik AB. *Russia* — Research and Development Institute of Power Engineering, RDIPE, Kurchatov Institute, Russian Federation Regulatory Body. *Lithuania* — Ignalina NPP, Lithuanian Energy Institute of Kaunas.
Objective(s)	:	*General*: Establish common perspectives and unified bases for assessment of severe accident risks and needs for remedial measures for the RBMK reactors.
Scope	:	**Phase 2**: Limited Level 1 PSA excluding external events and limited treatment of human factors. **Phase 3**: Extension of the Level 1 PSA in areas selected in Phase 2.
Comment(s)	:	The project includes the training of the Russian and Lithuanian PSA teams in Sweden and at the Ignalina NPP.

Country : Poland.

Plant(s) : Zarnowiec.

Type : WWER-440/V213.

Schedule : 1988/1991.

Sponsor(s) : Regulatory Authorities.

Organization(s) in charge : Institute of Atomic Energy, Swierk and Central Lab. for Radiological Protection.

Objective(s) : Understanding of safety implication of plant design details, identification of weak points, supporting inspections and quality assurance process.

Scope : Level 1, limited number of IEs (6), limited treatment of HEs.

Comment(s) : The PSA was terminated due to cancellation of NPP project in 1991. Some activities are continued as an exercise in creating and perfecting methodological framework and in preserving existing expertise. PSA work is also continued with relation to off-site emergency preparedness, geared to an accident in foreign installation.

Country	:	Romania.
Plant(s)	:	Cernavoda. Under construction. Planned operation 1994 (first unit).
Type	:	CANDU-600.
Schedule	:	CPSE (Cernavoda Probabilistic Safety Evaluation). Limited scope CPSE Level 1, 1991. Full scope CPSE Level 1, 1994. Data collection system, 1994. Living CPSE, 1995. Levels 2 & 3 CPSE, 1994.
Sponsor(s)	:	Romanian Power Utility (RENEL). Technical Assistance: IAEA.
Organization(s) in charge	:	Institute for Power Studies and Design, Nuclear Department. Institute for Nuclear Research. Cernavoda Nuclear Safety Group.
Objective(s)	:	Develop the probabilistic model of Cernavoda plant and applications in order to be used for providing the PSA study required for licensing (as support documentation); early design evaluation; nuclear safety evaluations during plant operation.
Scope	:	Full scope Level 1 PSA. Levels 2 and 3.
Comment(s)	:	Limited scope CPSE Level 1 (about 50% of full scope CPSE) was completed in 1991. An IAEA IPERS mission reviewed the study at the end of 1990.

Country	:	Russia.
Plant(s)	:	Zapozozhskaya.
Type	:	WWER-320 × 5.
Schedule	:	1992–1994.
Sponsor(s)	:	Zapozozhskaya NPP.
Organization(s) in charge	:	Atomenergoprojekt, OCB Hydropress, Kurchatov Institute.
Objective(s)	:	Full scale Level 2 PSA with estimated population dose commitments at different distances from NPP. Internal and external IEs (involved seismic, air crash, internal fire and flooding). Operational mode: - power operation, - cold shutdown (refuelling), - fuel transport operation into containment. Radioactive sources: - core, - spent fuel pool. Specific database on IE and component reliability.

Country : Russia.

Plant(s) : Beloyzskaya NPP (Unit 3) Ekaterinburg.

Type : Fast reactor (breeder) 5H-600.

Schedule : 1992–1994.

Sponsor(s) : Beloyzskaya NPP.

Organization(s) in charge : OKB Mechanical Engineering Physical Power Institute (Obninsk).
Beloyzskaya NPP.

Objective(s) : Quantification of core damage frequency by analysis of event trees sequences (internal events).

Scope : Level 1 PSA.

Comments :

Country : Russia.

Plant(s) : Nuclear District Heating Plant (NDHP), Voronezh.

Type : AST-500 (reactor with enhanced safety).

Schedule : 1992–1994 (Level 1).
1993–1994 (Level 2 preliminary).

Sponsor(s) : Voronezh NDHP.

Organization(s) in charge : OKB Mechanical Engineering N. Novgozod Atomenergoprojekt.

Objective(s) : Quantification of core damage frequency by analysis of event trees sequences (internal, some external events).

Scope : Level 1 PSA.

Level 2 PSA (preliminary).

Comment(s) : Operational mode:
- power operation,
- fuel transport operation.

PSA is used in confirmation of the achieved enhanced safety level.

Country	:	Russia.
Plant(s)	:	Nuclear District Heating Plant (NDHP), Nizhuy Novgorod .
Type	:	AST-500 2 × 500 (enhanced safety reactor).
Schedule	:	1992.
Sponsor(s)	:	Government.
Organization(s) in charge	:	OKB Mechanical Engineering (N. Novgozod).
Objective(s)	:	Quantification of core damage frequency by analysis of event trees sequences (internal events).
Scope	:	Level 1 PSA for internal events.
Comment(s)	:	Operational mode: - power operation, - fuel transport operation. PSA is used in confirmation of the achieved enhanced safety level.

Country	:	Russia.
Plant(s)	:	(Design).
Type	:	Water enhanced safety power reactor, 600 MWe [WPBER-600], (new generation reactor with enhanced safety).
Schedule	:	1992–1994.
Sponsor(s)	:	Government.
Organization(s) in charge	:	OKB Mechanical Engineering, N. Novgozod Atomenergoprojekt.
Objective(s)	:	Quantification of core damage frequency by analysis of event trees sequences (internal and external events).
Scope	:	Level 1 PSA . Some tasks of Level 2 PSA.
Comment(s)	:	PSA is used for engineering decisions choice (at early stages) and in conformation of the achieved safety level.

Country	:	Ukraine.
Plant(s)	:	Rovenskaya NPP.
Type	:	WWER-1000/320, WWER-440/213.
Schedule	:	1992–1993 (for V-213 Units 1, 2). 1994–1996 (for V-320 Unit 3).
Sponsor(s)	:	Ukrainian Government.
Organization(s) in charge	:	General designer of the NPP: Kiev Institute, "Energoprojekt"; designer of the reactor units: Hydropress; scientific consultant: Kurchatov Institute.
Objective(s)	:	Full scale Level 2. Internal and external IE. Operational mode: – power operation, – cold shutdown, – fuel transport operation.

2.3.6. Summary tables on PSA methodology

STATUS OF PSA METHODOLOGY IN BULGARIA

Accident sequence modelling

- due to lack of T/H analyses, ETs often based on engineering judgement;

- for Kozloduy-3 PSS, extensive T/H analyses would be done for ET modelling and plant success criteria (MAAP code is planned to be used);

- core damage states' definitions depend on Level 2 methodology and are not sufficiently clear.

System reliability analysis

- number of systems for Kozloduy 1 and 2 analysed;

- problems exist with some aspects of modelling, when there are complex functional dependencies between components and/or subsystems, especially in C&I circuitry.

Data

- generic data used up to now;

- operational data not sufficient for plant specific database. Additional guidance necessary on the use of Bayesian analysis for combining generic data with plant evidence;

- component unavailability processed using PSAPACK options; they are not flexible enough.

Dependent events

- MGL and B-factor methods used with generic data;
- CCF explicitly modelled on FT level.

Human factors

- Swain-Guttmann methodology used with different level of complexity;
- use of full scope S-G Handbook impossible because of lack of data.

Quantification

- PSAPACK version 4.2 (problems exist in both user interface and inter-module interfaces. The results often cannot be documented in a convenient way).

Living PSA and risk monitoring

- no base-risk study is ready yet;

- methodologically, risk monitoring tools have to be prepared in advance.

External events

- Internal CCI: fire hazard methodology available, but not computer codes.
- EQs: seismic risk integration methods necessary.

Accident sequence modelling

Over 60 event trees have been developed for Paks PSA until now. These event trees are based on currently available thermohydraulic analysis results (limited scope) and simulator experience. The upgrading of event trees is planned for 1993. Presently it is an open issue whether all the necessary plant response calculations can be carried out to verify existing accident sequences within this timeframe.

System analysis

PSA related system analyses have been carried out in close co-operation with four national institutions including the utility itself. The only open issue related to this topic is the level of detail to which C & I subsystems should be modelled. It should be noted that this problem is strongly linked with the issue of available failure data (see below).

Data assessment

A combined plant specific and generic database is going to be used for component as well as for initiating event data. The PSA oriented data collection system has been in use at Paks NPP since 1989. The analysis of collected plant specific data is currently going on. The compilation and feasibility of generic database (in the sense of WWER type specific data) is of real concern. WWER type specific data are planned to be gathered by the help of the IAEA and GRS, Germany.

Treatment of dependencies

The analysis of dependencies is going in parallel with fault tree and event tree modelling. The main deficiency here is the input data again for common cause failures. This problem arises whatever model is used for quantification of CCFs because currently available type specific data doesn't support CCF analysis. At this stage it seems to be more beneficial to get some qualitative insights concerning the impact of CCFs in overall risk of the plant.

Treatment of human errors

Human errors are broken down to three categories in the Paks PSA as follows:

- human errors as initiators;
- pre-accident human errors;
- post-accident human errors.

The human errors as initiators are taken into account in the frequency of initiating events by analysis of available data. Pre-accident human errors are analyzed according to the ASEP HRA Procedure Guide (plant specific data are also processed to quantify HE probabilities). For the modelling of post-accident human errors and analysis of user performance during accident conditions a sequence of operator reliability experiments will be carried out using the full scope simulator at Paks NPP.

Accident sequence quantification

According to the time schedule of Paks PSA, this task is planned for 1993. RISK SPECTRUM PSA code is to be used for quantification.

STATUS OF PSA METHODOLOGY IN HUNGARY (cont.)

External events and shutdown risk

Concerning the PSA in the AGNES project the continuation of current activity will be the extension of Level 1 PSA to the analysis of external events and plant shutdown conditions. These activities are planned to be performed from the second half of 1993. No prioritization has been set up for these analyses (i.e. shutdown risk versus external events). No practical experience exists in treatment of external events nor shutdown risk.

PSA applications

PSA results will be used depending on the needs of the utility. This statement applies to living PSA, Technical Specification evaluation, AOT and STI optimization as well. Some experience exists in the area of technical specification evaluation.

STATUS OF PSA METHODOLOGY IN CZECHOSLOVAKIA

Accident sequence modelling

State of the art:

- the conventional event tree method was used for 14 initiating events (PSA NPP Dukovany) — RISK SPECTRUM PSA code;
- conservative approach — interval 24 hours was accepted as a maximum time interval for development of accident sequences; no recovery action was considered (NPP Dukovany);
- some events were analysed by two independent groups of analysts (PSA Dukovany);
- analysis was reviewed during the spring 1992 by all members of the PSA Dukovany team.

Problems:

- best estimate assessment criteria;
- ET modelling versus lack of thermohydraulic analyses.

System analysis

State of the art:

- 21 safety significant systems were analysed by the fault tree method — RISK SPECTRUM PSA code (NPP Dukovany PSA study).

Problems:

- boundary of systems, modularization;
- transfer of FT from other ET;
- level of detail of FT analysis is unbalanced in some ET models.

STATUS OF PSA METHODOLOGY IN CZECHOSLOVAKIA (cont.)

Data assessment (including initiators)

State of the art: - data for preliminary PSA study (draft) of NPP Dukovany was prepared step-by-step from generic to specific data; three versions of database were developed gradually. NPP Dukovany staff will prepare and verify database for final version of PSA study.

Problems:
- collection and verification of data in NPPs for PSA user;
- expression of real duration of maintenance and repair;
- boundary of components;
- a lack of data for initiators;
- completeness of initiators.

Treatment of dependencies

State of the art:
- CCF methodology was compiled from different approach;
- B-factor was used for quantification (generic B-factor or based on engineering judgement);
- structural dependencies = priority events;
- a refinement of CCF consideration.

Problems:
- common cause initiators;
- B-factor for more than two redundant components.
- HRA modelling according to its importance and frequency of operational actions.

Treatment of human error

State of the art:
- ASEP-HRA methodology (Swain, A.D., NUREG/CR-4772) partially modified by some procedures from the THERP methodology (Swain, A.D., Guttmann, H.E., NUREG/CR-1278), expert recommendations provided within the framework of IAEA Regional Project RER/9/005 (J.K. Vaurio);
- human errors related to normal operational conditions before an accident and human errors made after event (only prescribed activities) were taken into account.

Problems:
- human error quantification;
- conservatism of recovery actions.

Accident sequence quantification

State of the art: - RISK SPECTRUM PSA code is used.

Living PSA

State of the art: - no experience exists.

Problems: - choice of software, transfer of ‘know-how’.

External events

State of the art: - fire (internal) initiating events were analyzed in preliminary NPP Dukovany PSA study.

Accident sequence modelling

Small ET/large FT approach adopted.

Previous PSA was not well supported by thermal hydraulic analyses particularly in the area of transients. Existing capabilities for PSA oriented response analyses are sufficient for PSA Level 1 models. Level 2 methodology and computer codes should be improved.

Systems analysis

Fault tree method adopted and used in all PSA work.

Level of detail in system modelling was limited.

Modularization process was used to much extent.

Data Assessment

Existing PSA analyses based on generic data. Bayesian approach adopted for combining generic data with operational plant specific data. No operational experience available in Poland for NPPs.

Treatment of dependencies

Simplified treatment of dependencies in previous PSA based on B-factor CCF model and generic data. No WWER operational experience available in this area.

Treatment of human errors

The scope of HE analysis in previous PSAs was limited to simplified assignment of screening probabilities. No systematic HE analysis based on plant specific information. Limited use of ASEP-HRA.

Accident sequence quantification

PC based FT analysis codes — FTAP, SETS (within the PSAPACK), TREE MASTER and SETS in mainframe version — were used in previous PSA work. Capabilities of these codes have been found sufficient. No experience in performing uncertainty analysis.

Living PSA

Some research work under way in several organizations on risk monitoring software. No applications in the area of NPPs.

External events

None.

STATUS OF PSA METHODOLOGY — OKB MECHANICAL ENGINEERING, NIZHY NOVGOROD, RUSSIA

Accident sequence modelling

- event tree approach;
- thermohydraulic support analysis;
- accident management measures included;
- unfavourable states criteria used in modelling.

System analysis

- component's independent failures, common cause failures of the same type of equipment and personnel errors taken into account;
- MCS method;
- normally monitored and non-monitored components taken into account.
- system's serviceability success criteria condition are presented as sequential-parallel diagram (or fault tree);
- using of high effectiveness MCS generation (modularization FT, convolution of cut-sets, etc.);
- reliability calculations with the account of CCF (BFR model, B-factor model).

Data assessment

- statistical data based on the analogs operational experience from NPP's with WWER reactors and nuclear ice-breakers are used;
- IAEA data bank;
- specific data for every NPP.

Treatment of dependencies

- Different types of dependencies are analysed:
  (1) dependence upon initial event;
  (2) structural-functional dependencies due to common structural elements or auxiliary systems;
  (3) dependencies due to equipment design similarity and personnel errors.
- Two first types of dependencies were taken into account in accident sequence model.
  BFR model is used for dependencies due to equipment design similarity and personnel errors.

Treatment of human errors

- Following personnel errors types were taken into account:
  (a) personnel errors made before accident initiation;
  (b) personnel errors, initiating the accident situation;
  (c) personnel errors related to emergency control of the plant.
- errors of the first group were analysed in the course of safety systems reliability assessment;
- errors of the second group were taken into account in the assessment of initiating event occurrence rate;
- errors of the third group were taken into account at event trees level;
- human reliability analysis is based on THERP method (personnel error probability depending on available time margin);
- multiparameter dependence model ('time-personnel reliability') is developed taking into account the following factors: relationship between available and necessary time for action performance, personnel qualification, stress level, available means for process and system state control; type of the problem under consideration;

- operator actions were analyzed using operator actions trees and various home and foreign data banks for quantification of errors probability (both foreign and country developed).

Accident sequence quantification

- computer code TREES developed in OKBM was used;
- TREES consists of two independent programmes, one applied for safety systems reliability analysis, the other one - for event tree development and analysis;
- TREES code is suitable for large fault tree analysis (safety systems combinations) and forming emergency sequences in the event tree;
- event tree is constructed based on:
  - matrix of dependencies between safety systems;
  - matrix of consequences for accident sequences.
- TREES code capabilities include importance, sensitivity and uncertainty analysis;
- Monte-Carlo method is used in uncertainty analysis.

Accident sequence modelling

Functional-systemic event tree analysis (ETA).

Thermohydraulic supporting analysis.

System analysis

FMEA and fault tree analysis (FTA). Detailed component failure mode classification. All important system's (frontline, supporting, control and instrumentation systems) are involved. Detailed MCS classification. Quantification of MCS using time dependent unavailability function.

Data assessment

Generic database on IEs, component reliability and CCFs. Simulator, specific and generic database for HE.

Treatment of dependencies

Three level of dependency analysis:

- functional dependencies (ETA);
- system interaction dependencies (ETA, FTA);
- component dependencies (FMEA, FTA).

Three classes of CCFs:

- common design and construction;
- common environmental conditions;
- same maintenance and/or inspection procedures.

An implicit method of introducing CCFs into logical model using analysis of reference MCS resulted from independent failure analysis.

Detailed assessment of protection measures against CCFs.

A quantitative assessment of CCFs with the use of parametric models (MBP, MGL, BM).

Treatment of human factors

Three groups of human error (HE):

- maintenance and operation errors leading to accident IE;
- maintenance errors leading to safety system unavailability;
- control and management errors leading to severe accidents.

Human error trees (HET) for human reliability analysis.

Detailed algorithm and supporting thermohydraulic analysis for HET development.

Accident sequence quantification

Detailed (large) FT for each accident sequence (AS) developed. Separate quantification assessment of independent failures (IF), CCFs, HEs, accident management measures and test/maintenance strategies, involving allowed outage time.

Importance, sensitivity and uncertainty analysis.

Atomenergoprojekt PSA software package for AS quantification involves the following codes:

- APRA and VNF codes for evaluation of AS conditional probabilities with account of IFs, CCFs, HEs and maintenance/test strategies;
- ANTES code for HE probability evaluation;
- UNAS code for uncertainty evaluation.

External events

ETA, FTA and probabilistic fracture mechanics strength modelling for external events (seismic, air crash , internal fire and flooding).

STATUS OF PSA METHODOLOGY IN THE SCIENTIFIC AND TECHNICAL CENTRE ON NUCLEAR AND RADIATION SAFETY OF UKRAINE

Accident sequence modelling

Systemic event tree analysis. Thermohydraulic supporting analysis.

System analysis

FMEA and fault trees. Detailed component failure mode classification. All systems are considered.

Data assessment

Specific data based on IEs component reliability and CCFs.

Treatment of dependencies

Three level of dependencies analysis:

- functional dependencies;
- system interaction dependencies;
- component dependencies.

Three classes of CCF:

- common design and construction;
- common environmental conditions;
- some maintenance and/or inspection procedures.

A quantitative assessment of CCFs using parametric models (MGL).

Treatment of human errors

Three groups of human errors:

- maintenance errors leading to IE;
- maintenance errors leading to safety system unavailability;
- control and management leading to severe accidents.

Accident sequence quantification

Detailed FT for each accident sequence, taking into account common failures and human errors. Atomenergoprojekt (Moscow) PSA software package for quantification of AS: VNF for evaluation of AS conditional probabilities with account of IF, CFFs, HEs.

External events

Deterministic techniques of safety assessment for IEs:

- external flooding;
- fires;
- aircrash;
- seismic.

Accident sequence modelling

Identification of the safety function (SF).

Relationship between SF and systems:

- front line systems,
- support systems.

Definition of 4 core damage categories.

System analysis

Performed by using fault tree technique.

Project report written to specify the procedures and requirement.

Data (initiating events frequency and component reliability)

Plant specific or RBMK type specific data are not available yet. If not available when needed, Swedish data will be used.

Treatment of dependencies

Analysis in progress to identify functional, physical and human interaction dependencies. This work is made in close co-operation with plant personnel.

Treatment of human errors

Task limited to screening analysis to identify dominant contributors. Five categories of human interaction will be modelled.

Accident sequence quantification

Use of RISK SPECTRUM code.

Living PSA

Not included.

External events

None. (Internal events: only fire.)

3. ADVANCED TECHNIQUES/METHODS

3.1. INTRODUCTION

A separate session (Session 2) was devoted to THE latest advancements in PSA methodology. The topics covered by the presentations focus on ongoing investigations related to methodology improvements concerning both the existing methodological framework and those associated with new applications. A more detailed overview of the presentations is provided in Section 3.2.

Working group activities concentrated on the survey of the methodology and activities carried out in the field, identification of open issues and future activities, as well as information on some suggestions for international co-operation. More detailed information on working group conclusions is given in Section 3.3.

3.2. OVERVIEW OF THE PRESENTATIONS

The papers presented in Session 2 focus on current, ongoing investigations in the field and reference relevant supporting material.

The papers can be grouped under three topics:

(1) Computerized models/programmes for living PSA application, risk monitoring and data handling;
(2) Plant response calculations and tools;
(3) Special issues in PSA including interface Level 1–Level 2 PSA, relationship between safety culture–PSA.

Observations and insights from the material presented and the discussions are summarized below:

Topic 1

There is increasing interest in the use of a PSA model not only for design improvements and balancing but also for operational support concerning risk configuration management and maintenance, test and repair strategies in the plants, etc. Trending of safety/risk indicators versus plant lifetime is also of great interest.

A distinction between Living PSA and Risk Monitor is pointed out. Living PSA is an update (trending) versus longer time periods; a monitor is an approach to provide quick response supporting actual operational decisions related to plant safety. To solve the latter problem an intelligent computerization of the PSA model is needed, capable of handling the large number of data and information contained in a PSA. Computerized systems/models are also needed to store raw data and to aggregate it to statistically meaningful reliability characteristics for PSA applications. The main ideas for living PSA and a risk monitor shown by the various authors are similar; tricky details applied in a specific project may have some spin-off for other projects in the future.

Topic 2

Ongoing code developments on MAAP4 and initial tests on WWERs show the capability to use MAAP4 for severe accident modelling. There is a trend to simulate for an initiator the various accident sequences differing with the containment response, the operator response and safety system functions within one PC session. System response calculations for LOCAs and transients on WWER-440 plants are more and more refined with respect to the various initiator categories and the success criteria for the various system functions. Relatively large matrices of calculated cases agreed by experts in different countries operating WWERs are available. There is a tendency to cover the various plant response possibilities using relatively small event trees.

Topic 3

Concerning the extension of Level 1 PSA to Level 2, respective containment response investigations are shown based on the event tree approach. In this context the various accident sequences from Level 1 are linked with the relevant event trees describing the various possibilities of containment response. No other modelling techniques, e.g. Markov models, are considered by the author for comparisons.

Safety culture and managerial aspects become one of the most interesting issues which should be considered and treated within the process of a PSA. The human role appears to be dominant in the loop representing plant operation and management activities. It is shown through historical evidence as well as the dominant contributions identified in precursor and PSA studies. An integrated risk management (IRM) is strongly recommended to account for organizational factors. If incorporated, it provides a well established knowledge and instruments to understand and to analyse key issues. Interdisciplinary initiatives are needed to bridge the practice of PSA and the IRM technology.

3.3. INSIGHTS FROM WORKING GROUP DISCUSSIONS

3.3.1. Living PSA/risk monitor

Related definitions

Living PSA and risk monitoring are to be differentiated from the point of view of the objectives.

Living PSA
- investigation of safety status for a given plant after a given time interval, based on an updated plant specific PSA;
- is to be used for periodic safety evaluation by the utility (as it is required in Germany, the United Kingdom, etc.).

Risk monitor
- investigation of safety impact of specific parameters for a given plant at a given time, based on real time re-calculation of specific values using a plant specific PSA;
- is to be used for both short term and long term safety decisions by the utility as well as PSA analysts.

Risk monitoring and living PSA can be helpful for defining measures to re-assess abnormal events and to define additional safety measures (off-line diagnostic tool).

Risk monitors and living PSA as defined here are not intended to assist in real time accident management. A specific development for these needs should be investigated on the basis of PSA technology.

Recent activities

In general, the same thinking on living PSA and risk monitor methodology and ways of application were found to be pursued in all countries that are developing and/or applying PSA.

Living PSA and risk monitors are based on an integrated software package that combines data processing, fault trees, event trees calculations and importance calculations.

For risk monitors an expert system shell software is useful.

Examples of risk monitor systems are:

RISK MONITOR (Germany, under development);

ESSM (United Kingdom, under operation);
LIPSAS (Japan, under development);
PRISIM (USA, under operation);
PEPSI (Rep. of Korea, under development).

Examples of living PSA tools are:

SAIS (Germany, under development);
LESSEPS/FIGARO (France, under operation);
IRRAS (USA, under development);
RISK SPECTRUM (Sweden, under development).

Methodological issues

Risk monitor calculates risk changes (measured as frequencies on different levels — component, system function, sequence, core damage level) caused by changes of input parameters (e.g. change components, parameters of components, etc.).

To cope with the operational requirements of NPP risk monitor calculations should be performed in a short time scale (a couple of minutes).

For risk monitor and living PSA calculations full PSA (Level 1, 1+) must be available. PSA input should be user friendly to assure fast response.

To assure correct evaluation of plant risk all plant states have to be taken into account (e.g. hot and cold shutdown states are recommended to be included).

Risk monitor and living PSA calculations have to be based on the current plant status and data. For risk monitoring an updating of plant models and data is recommended in the period of every six months.

Open issues and future activities

The following issues were found important for further development:

Development of software for automatic fault tree calculations to minimize the routine work is considered to be useful (long term issue).

Risk monitoring and living PSA require a specific data collection and treatment that is to be implemented in the NPP. Data update should not be automatic.

Time dependent effects associated with component and system functions should be taken into account (e.g. ageing of components).

There is a need for providing guidance on the use of risk monitor and living PSA tools in the decision making process (experience for the operators).

Risk monitoring and living PSA are based on Levels 1, 1+. They calculate valuable results that can be used for operational safety decisions. However, for the future a step-by-step extension of the PSA based on Levels 2 and 3 is recommended.

There is a need to define clearly which information and in what form the results of risk monitoring and living PSA should be displayed.

WARNING: Information supplied from risk monitors must not contradict other information such as technical specifications or licensing requirements available to the operator (this may indicate a need to re-assess deterministic technical specifications).

There is a need to define very clearly the role of risk monitoring with respect to the technical specifications.

The use of risk monitors and living PSA for operational decisions has to be licensed by the regulatory body.

Desired assistance

The following activities of the IAEA would be valuable to promote the progress in the field:

- To prepare guidelines on the utilization of living PSA and risk monitors.

- To prepare functional requirements for risk monitors and living PSA systems.

- To organize a meeting on the use of risk monitors and living PSA to support the use by the utilities (operators and systems analysts). The meeting should be intended to give a special support to eastern utilities. In organization of such a meeting the French experience should be taken into account.

3.3.2. NPP response analysis

Methodology issues

Large and small event trees — the specific approach depends on available code capability. In principle, both strategies can be used in the PSA process. In practice, a small event tree/large fault tree approach seems to be preferred.

Macro-components in fault tree — they are possible to be used provided that there are no dependencies among them. Their use also depends on availability of data.

It is necessary to use the best estimate procedures and data in a PSA Level 1 to be realistic. Design basis parameter values such as the maximum clad temperature are usually conservative. Either revised values or new parameters should be applied. Best estimate cases must include realistic operator actions. Time delays and improper actions should also be considered.

In sequence calculations the effect of assuming minimum success versus full success of the system function should be clarified.

Computer codes

The use of any code for plant response calculations in Level 1 analyses encounters a common list of requirements and issues:

- Accuracy. Has the code been validated? Is it being used properly by a trained user? RELAP, TRAC, CATHARE, etc. are widely regarded as adequate for transient analyses. MAAP models are less sophisticated for transients thermal hydraulics, but they can be used for the majority of transients (as shown by the US experience).

- Sensitivity. Even sophisticated codes have model uncertainty. It should be possible to investigate code sensitivity to model assumptions. For example, the void fraction describing the amount of liquid carried over during feed and bleed cooling is important but potentially an uncertain parameter.

TABLE VII. EXAMPLES OF CODES USED IN PSAs FOR THE SYSTEMS RESPONSE AND SUCCESS CRITERIA

COUNTRY	RELIABILITY CODES	THERMOHYDRAULIC CODES
GERMANY	RISK SPECTRUM, RALLY	ATHLET, RELAP, CATHARE, MELCOR
CSFR	RISK SPECTRUM	LOCA, RELAP5, Transients - D4, Reactivity initial accidents, REPA1D - CSFR codes
ROMANIA (CANDU reactor)	PSA B (Romanian code) PSAPACK THPSA FRANTIC	Canadian codes: FIREBIRD (for LOCA) FORSIM (dynamic problems) HYDNA (for fuel channel)
UNITED KINGDOM	RISK SPECTRUM	MAAP, RELAP5, MELCOR
KOREA, REP. OF	KIRAP	MAAP, SCDAP/RELAP, CONTAIN
MEXICO	PSAPACK, SETS, FTRAP, TEMAC	STCP, TRAC, RELAP5
HUNGARY	FRANTIC, RISK SPECTRUM	RELAP5, STCP (WWER mode), MELCOR, ATHLET
UNITED STATES OF AMERICA		MAAP3, RELAP, RETRAN, MELCOR
CANADA	SETS, CAFTA, TREEMASTER	FIREBIRD III, SOPHT, CATHENA, TUF

Open issues/future activities

Verification is required for western codes before their use in WWER analyses. RELAP5 and STCP have been adopted already.

Feed and bleed mode of the WWER-440 core cooling has not been sufficiently analysed. For future needs some computations are planned to be performed. It should be clarified whether the feed and bleed cooling is associated with WWER design limitations (e.g. set points) or represents only modelling problems related to the code.

Required assistance

Computer codes

3-D code for hexagonal core physics computation is needed for certain type of transients.

Shutdown risk

The following issues were discussed and found to require further investigation:

- boron dilution in the start-up phase of PWR (limited analyses have been performed by EGP Prague for the reconnection of an isolated steam generator loop at 80% power level);
- LOCA frequencies — different frequencies of pipe break for different reactor states.

External events

Few full scope seismic PSAs exist. Scoping seismic analyses of varying degrees of detail have been performed on many western reactors. Seismic experience of WWER plants is limited. It is recommended that earthquake analyses should be considered in consistent way within PSA analysis. The guidelines for systematic analysis taking into account the site relevant external events should be provided.

Fire and flood analyses

Fire and flood analyses should be included within PSA Level 1. Specific recommendations are expected as a result of the Fire Risk Analysis Workshop in VUPEX, Bratislava, 21-25 September 1992.

4. RISK BASED REGULATIONS

4.1. INTRODUCTION

A separate session (Session 3) was devoted to the use of PSA in regulatory activities. The topics covered by the presentations are related mostly to specific examples of regulatory oriented applications but some more general concepts of risk based regulations were also discussed. Detailed overview of the presentations is given in Section 4.2.

The working group discussions concentrated on selected topics related to risk based regulation. They address the regulatory point of view in using PSA both for design and operation, use of best estimate approach in the PSA, probabilistic safety criteria (PSC) and others. Detailed information on working group conclusions is provided in Section 4.3.

4.2. OVERVIEW OF THE PRESENTATIONS

Six papers were presented in Session 3. The concept of risk based regulation (RBR) was discussed in the first paper. It was considered that RBR could make plants safer and more economic, and thus satisfy both the regulator and the utility.

It was noted that the uncertainty of the PSA results, usually about 1/2–1 order of magnitude, could be small compared to the changes due to actual plant operation where the core melt frequency (CMF) may have orders of magnitude greater in certain plant configurations.

The number of components which had a significant effect on CMF was thought to be of the order of 100, less than 1% of the components on a plant. Currently the technical specifications do not require different levels of surveillance according to the component importance. It was thought that more attention could be paid to some components and less to others.

It was recognized that RBR would need to be phased in (if it were adopted) over a period of time.

The role of PSA in the licensing of Angra 1 NPP was discussed in the second paper. Angra 1 is a two loop Westinghouse designed PWR. A PSA was requested by the regulator, Comissão Nacional de Energia Nuclear (CNEN) in the early 1980s. This was performed with generic data. The PSA identified the need for further analysis of the anticipated transient without scram (ATWS) condition. Subsequently, a further PSA has been requested which will more correctly model the plant (in particular model design changes more fully). This more up-to-date PSA will be used by CNEN to identify if any 'backfits' are required or technical specification procedures need to be changed.

The utility will also use the results of the PSA to help it further develop the emergency operating procedures.

A Survey of German PSA investigations for nuclear power plants was provided in the next paper. A number of projects are under way in Germany related to the subject of PSA. These cover the following areas:

PSA comparisons: The comparison of PSAs from many countries was being performed to provide a guideline to be used for reviewers of PSAs.

Special projects under way:
- Fire analysis;
- External events;
- Precursor reports proposal;
- PSA for low power and shutdown states.

Development of methods:	- Common cause failure; - human reliability analysis; - time dependence effects in PSA; - Data collection.
PSA guideline used to:	- Evaluate plant modifications; - Optimize backfits; - Optimize technical specifications; - Evaluate actual operating experience.

It was noted that PSA was a powerful tool and was used in Germany although risk based regulation was not being promoted.

Use of PSA in a regulatory framework in Nuclear Electric, UK, was the subject of the next paper. It was noted that PSA had been used in the licensing of the Sizewell 'B' PWR from the very early stages. A preliminary PSA had been performed to support the application to begin construction of Sizewell 'B'. That PSA had been subject to review by the regulatory authorities.

At that time the utility agreed to expand the scope of the PSA in an attempt to be 'complete' and to justify the assumptions behind the PSA. This led to a significant increase in the amount of analysis and the complexity of the PSA. In order to reduce the amount of work required many pessimistic and boarding assumptions had been made. This in turn led to some very pessimistic results which had themselves been reviewed to identify the 'real lessons' from the PSA.

Although the work was extensive and highly complex many significant lessons had been learned — principally that the use of conservative assumptions could be very misleading and that quantification was not really possible for all contributors to risk. The work had, however, left Nuclear Electric with a much greater undertaking of the plant and the systems interactions.

The status and future prospects of regulatory issues in the Ukraine were presented in the next paper. PSAs have been performed for the various WWER units currently operating in the Ukraine. Although such PSAs have been performed the use of generic data is thought to limit their usefulness. However, some minor design changes have been proposed to improve the safety of the plants. Also the PSA has been used to provide a case for relaxation of certain insignificant operating restrictions.

The role of PSA in licensing, regulation and design as applied in the Netherlands was the subject of the next presentation. Before the Chernobyl accident the regulatory authorities had proposed some PSA based criteria for new reactors. The proposal was that the individual risk of early death would be unacceptable more frequently than 10^{-8}/year. Between these values some consideration of design improvements would be needed.

Since the Chernobyl accident no nuclear plants are to be built and so attention has turned to the two existing BWRs in the Netherlands. Level 1+ PSAs have been performed with an assessment of the containment loadings and responses.

These PSAs have been used to identify: the dominant accident sequences and components; weak points in the designs; dependencies in the designs (spatial, functional and human). The intention is to develop these PSAs into living PSAs and to use these as operational tools to evaluate future modifications to the plant and procedures.

4.3. INSIGHTS FROM WORKING GROUP DISCUSSIONS

4.3.1. Regulatory position on PSA application

Some opinions have been expressed by the working group concerning acceptability of risk based regulations. It was stated that PSA is a useful tool and is one element in the decision making process.

Design by a good engineering/deterministic practice preceded PSA development and use. Decisions based on determinism (single failure, diversity, separatism, etc.) can be more onerous than those required to meet risk criteria. PSA is therefore regarded as necessary in the decision making process, but it is not sufficient in itself.

The use of a risk monitor tool at a NPP can assist in reducing plant risk levels in planning/scheduling for maintenance and outage activities.

Development of a risk monitor is still in its infancy and therefore there are many dangers in placing too much reliance upon the risk monitor tool. In particular the dangers perceived are:

- the status of the monitor may not coincide with the status of the plant (due to human error). This is particularly true during the busy outage periods;

- the monitor could be applied to a configuration of the plant for which the monitor was not designed.

Nevertheless, the development of risk monitors is to be supported but it is judged too early to place regulatory controls or criteria upon the utility in a formal sense.

4.3.2. Best estimate approach to PSA

It is accepted that PSA generally involves a degree of conservatism in some aspects of its application. It is judged, however, that PSA is most useful when applied in a best estimate mode consistently throughout all aspects of the PSA. 'Best estimate' includes not only numerical data but also best estimate calculation for determination of the success criteria and best estimate radiological analyses for consequence calculation. It is recognized that cost or technical difficulties may result in the use of a bounding or conservative approach and this can, under certain circumstances, be acceptable.

The use of bounding PSA, while acceptable for comparison with a prescribed risk target, places a burden upon utility and regulator alike should subsequent plant modifications be proposed. This burden arises because the existing PSA may neither clearly identify the true risk dominator, and because the true benefits proposed by the utility may be disguised by the conservatism in the analysis. Best estimate PSA should be supplemented by some measure of uncertainty or sensitivity analyses as this allows a judgement to be formed on the acceptability of the analyses.

4.3.3. Probabilistic safety criteria

PSA is a useful tool for both the regulatory bodies and the utilities. However, both must realize the limitations of their analyses when used in an absolute sense. Incompleteness, which is sometimes subjective in nature, especially in those areas depending on expert judgement, lack of standardization of approach, make that comparison with probabilistic safety criteria (PSC) or the outcomes/results of another PSA cannot be made in an absolute sense. The final PSA outcomes are no more than an indicator and need to be considered along with the underlying assumptions.

In the case of comparison with PSC, one should keep in mind that the PSC are only meaningful if there is a consistency between the PSC and the scope, definitions, assumptions being made and the boundary conditions of the PSC.

It has been recognized that the role of PSAs in relation to PSC does not only have its value for operational plants but also for new and/or conceptual designs. Even a generic PSA of a conceptual design can, in principle, be used to help to demonstrate the acceptability of that design, provided all the limitations of doing so are recognized.

Absolute quantitative safety goals and/or criteria (PSC) are useful as a yardstick in assessing the risk of a nuclear power plant (NPP). It has been recognized that PSC are increasingly used in different countries. However, some countries, especially those which are depending on NPPs of an 'older' design for their electricity generation, are not yet in a position to adopt PSC. Therefore, the use of PSC should be promoted; in addition, some external guidance to those countries which still have difficulties in adopting those should be provided.

4.3.4. Old plant versus new plant

The issue is whether there should be differing probabilistic requirements to address new and old plants.

Old plant needs to be assessed against current criteria using state of the art techniques and exceptions need to be addressed in some way. The use of PSA should identify dominant contributors and acceptable solutions found where there is a need for risk reduction. Such measures may include backfit, accident management actions, further probabilistic analyses, deterministic argument, etc.

All plants need to be assessed on an individual basis.

4.3.5. Recognized needs for further development

Several topics related to risk based regulation have been pointed out as requiring further development and possible assistance from the IAEA. They include:

- Development of PSC and associated methods with appropriate databases for research reactors, fuel cycle facilities and decommissioning facilities;
- Development/promotion of risk monitor tools.

5. PSA APPLICATIONS

5.1. INTRODUCTION

A separate session (Session 4) was devoted to various PSA applications. The majority of papers addressed topics related to evaluation of operational activities. However, other topics were also covered, such as simplified PSA for research reactors, the way of better communication of PSA results, etc. Detailed overview of the presentations is given in Section 5.2.

The working group has reviewed the following technical topics:

- Application of PSA techniques to technical specification (TS) optimization, particularly to optimize AOTs and STIs;

- Application of PSA techniques to maintenance planning;

- Review of IAEA draft report on TS optimization.

The working group discussed the general issues of the use of PSA techniques to TS optimization and how TS are defined and used in different countries, especially in France, Germany, Hungary, the Czech Republic, the Slovak Republic, the Nordic Countries and the USA. From this discussion emerged a number of technical and regulatory issues and recommendations associated with this PSA application. In addition, a limited review was made at the IAEA report on this topic. The results of these activities are summarized below (Section 5.3).

5.2. OVERVIEW OF THE PRESENTATIONS

Session 4 covered the following topics:

- use of PSA to optimize AOTs and STIs with full power PSA considerations;
- TS optimization with considerations of alternate modes and shutdown events PSA;
- diverse PSA applications;
- simplified PSA of research and non-power reactors;
- better communication of PSA results.

In general, the papers demonstrated strong interest in a very large number of PSA applications. In addition, the papers on technical specification optimization indicated a relatively mature state of the art for this particular application.

PSA application to technical specifications

The papers on TS optimization highlighted both common points and different approaches to the same issue in different countries such as France, Sweden, Finland, Bulgaria, Spain, Mexico, Germany, the Czech Republic, the Slovak Republic and the USA. Some of the highlights of the technical aspects and issues are itemized below.

Different countries are using or proposing three or perhaps four different types of risk acceptance criteria that are used to decide the acceptability of TS changes. These include:

(a) percentage of annual average CM frequency with plant specific baseline (USA);
(b) absolute risk level for each separate maintenance event (France);
(c) instantaneous risk level during maintenance event;
(d) annual unavailability budget (hours/year of downtime).

AOTs and STIs can be specified at different levels including component, system, subsystem or train level.

PSA models employ various parameters to model AOT and STI changes. These include: standby and shock failure rates, frequencies of preventative and corrective maintenance, mean repair times, maintenance out of service times and common cause parameters.

Papers on alternate modes/shutdown models, especially the contribution from EDF, stressed the importance of considering whether in fact a plant shutdown at the end of an AOT usually results in a higher margin of safety as assumed in traditional technical specifications.

Different approaches are being used to establish the baseline risk profile against which either time dependent risk or risk changes are compared. One is to equate the baseline with a nominal plant alignment with no test and maintenance in progress and another incorporates contributors from all alignments with average probability weights.

Additional PSA applications

The papers in Session 4 included a number of examples of PSA applications other than technical specifications such as:

- use of simplified PSAs for non power reactors;
- diverse applications in design, regulation, accident management, emergency planning and communicating PSA results to non-PSA practitioners.

5.3. INSIGHTS FROM WORKING GROUP DISCUSSIONS

A variety of methods for applying PSA models for TS optimization have been proposed and employed in actual proposals that have been submitted and reviewed by various regulatory bodies. The working group supports this application of PSA techniques and offers the following comments and recommendations.

5.3.1. Decision criteria for TS optimization

The success of TS optimization via PSA methods hinges on the use of appropriate decision criteria to decide the acceptability of changes to AOTs and STIs. While the actual decision criteria must be resolved for each country separately, the working group identified several qualities of the decision criteria that should be considered.

Risk importance

AOTs and STIs should be established related to the risk importance level.

Absolute versus relative risk level

Each of these approaches has advantages and disadvantages that need to be appreciated. Absolute levels are based on a numerical value of risk in absolute terms while the relative approach refers to some variable baseline risk profile for each plant.

Cumulative versus discrete criteria

Current deterministic AOT criteria and the French PSA criteria are expressed separately for each maintenance event. Cumulative criteria such as the Nordic approach for preventive maintenance and the US approach based on annual average CM frequency account for cumulative unavailability of multiple maintenance events.

Shutdown risk

A complete treatment of the risk aspect of maintenance requires consideration of shutdown risk; sometimes, plant shutdown at the end of an AOT period creates increased risk state.

Practicality of utility personnel

Revised technical specifications based on PSA must be uncomplicated and easy to use by the utility personnel. For different plants AOTs and STIs may be fixed at the system, subsystem or train levels. Unique AOTs for each component may not be practical nor advisable due to their transient nature.

5.3.2. PSA methods for TS optimization

The working group made the following comments on the use of PSA methods for TS optimization:

- Ideally, the evaluation should include alternative operating modes/shutdown PSA;

- PSA models must have explicit dependence on AOTs and STIs, i.e. need to model maintenance unavailability separate from failures;

- STIs must consider shock failures as well as standby failures. Better databases and analyses are needed to address this issue;

- Maintenance frequencies must not be confused with failure rates;

- AOTs must not be confused with actual maintenance durations; actual maintenance durations are not the same as repair times;

- PSA model simplifications should be reviewed for application to TS;

- PSA models must be extended to Level 2 to address certain TS issues;

- Time dependent models used for AOT and STI evaluations do not adequately treat special testing and maintenance considerations for common cause failures;

- Some questions regarding the validity of STI dependent models should be answered.

5.3.3. PSA databases

All countries have varying degrees of problems with inadequate PSA databases, such as:

- incomplete generic database;
- inapplicability of generic data;
- little or no plant specific data;
- shock versus standby failures;
- common cause failures;
- maintenance data not distinguished from failure data.

The above mentioned problems should be solved to provide appropriate input for TS optimization.

LIST OF ABBREVIATIONS

AOT	Allowable outage time
AS	Accident sequence
BWR	Boiling water reactor
CCI	Common cause initiator
CCF	Common cause failure
CDF	Core damage frequency
CMF	Core melt frequency
ET	Event tree
FMEA	Failure mode and effect analysis
FSAR	Failure safety analysis report
FTA	Fault tree analysis
HE	Human error
HRA	Human reliability analysis
IE	Initiating event
IPERS	International Peer Review Service
LOCA	Loss of coolant accident
NPP	Nuclear power plant
PSC	Probabilistic safety criteria
PWR	Pressurized water reactor
PRA	Probabilistic risk assessment
PSA	Probabilistic safety assessment
RBR	Risk based regulation
RBMK	Soviet designed graphite moderated, water cooled reactor
RPV	Reactor pressure vessel
SAR	Safety analysis report
STI	Surveillance test interval
TS	Technical specifications
WWER	Soviet designed PWR (water moderated, water cooled reactor)

Appendix

PAPERS PRESENTED AT THE TECHNICAL COMMITTEE MEETING

EXPERIENCE FROM THE PRELIMINARY NUCLEAR POWER PLANT DUKOVANY PSA STUDY

J. DUŠEK
Nuclear Research Institute,
Řež, Czechoslovakia

Abstract

A background of the Nuclear Power Plant Dukovany Probabilistic Safety Assessment Study preparation and its goals and its programme are mentioned This study has been being done in cooperation with almost all Czechoslovak institutions working in the field of PSA

Fourteen initiating events were chosen and analyzed for the preliminary PSA Study and reviewed by the Czechoslovak PSA team and by the NPP Dukovany staff during the spring of 1992. The Risk Spectrum FT PLUS code was used for analyses of 21 front-line and support systems fault trees.

The course of the project, assumptions, used methods, database, common cause failures and human factor analyses are briefly described Some experience with a preparation of this Study and comments to its results are also presented.

In conclusion an expected course of additional analyses for final version of the PSA Study and PSA activities for 1992 and next future in Czechoslovakia are added. The list of references to reliability and PSA analysis in Czechoslovakia is attached.

1. INTRODUCTION

In eighties the reliability and PSA analyses (e.g. [7] - [19]) were carried out in several Czechoslovak organizations under a number of sponsors and, therefore, also in an uncoordinated manner.

Outcomes of this research can be observed in:

- good acquaintance with the systems,
- possibility to compare the results and the procedures of particular analyses,
- recognizing and developing methods and computation programs ([1] - [6]) for these analyses,
- marking some important problems to be solved in the domain of thermal hydraulic analyses,
- establishing weak points of the design
- setting proposals of technical and organization measures for an increase of reliability of the systems.

Many of these proposals were in the Czechoslovak nuclear power plants accepted and realized

International activities in the domain of PSA for power reactors and research reactor have been mainly developed in cooperation with the IAEA ([20] - [26]).

Our first IAEA Contract was started in 1985 in the framework of a coordinated research programme "Development of Risk Criteria for the Whole Nuclear Fuel Cycle". The cooperation with IAEA in this domain has continued in the research programmes "Probabilistic Modeling of a Small LOCA" and in the IAEA Regional Programme RER/9/005 "PSA for VVER-Type Reactors".

Apart from studies for Czechoslovak nuclear power plants, also PSA analyses for research reactor LVR-15 have been carried out in the framework of an IAEA coordinated research programme "PSA for Research Reactors" and later this cooperation has continued in the IAEA research programme "Data Acquisition for Research Reactor PSA Studies" .

The year 1989 is possible to understand as a milestone for PSA analyses in Czechoslovakia. Since this year a full-scope probabilistic safety assessment of the nuclear power plant (NPP) Dukovany with VVER-440 type 213 reactors is being done in Czechoslovakia with the Nuclear Research Institute (NRI) in Řež being a coordinator of it.

This contribution is based on [56] and extended, the comprehensive list of references to reliability and PSA analysis in Czechoslovakia is attached. More next information is included in [60] - [65].

2. NPP DUKOVANY PSA STUDY

2.1. Background

The PSA analyses of the NPP Dukovany were started with the aim to complete a full-scope PSA level-1 safety study for this plant to the end of 1993. The PSA is being done in cooperation with almost all Czechoslovak institutions working in the field of probabilistic safety analyses and the NRI Řež coordinates research carried out in other five Czechoslovak organizations:

VÚJE Trnava (Nuclear Power Plant Research Institute),
VUPEX Bratislava
EGP Prague (Energoprojekt)
EGÚ Prague (Power Institute in Běchovice)
Škoda Works, Plzeň.

2.2. Goals

The main goal of this study is to create a tool to safety analyses. This tool make it possible to assess safety problems in

NPP's operation and to determine usefulness of possible modification. There were several next reasons and advantages of this study. It means for example

- design weaknesses
- operating technical specifications and operating procedures
- scheduled tests and in-service maintenance
- identifying areas of next research
- reference study for next specific NPP PSA Studies in ČSFR
- forming of one PSA team in ČSFR (with one "reliability and PSA language")
- tools for preparing of "living PSA" (for the NPP and the Czechoslovak Regulatory Body uses)

2.3. The Study programme

The planned work on the NPP Dukovany PSA Study has taken place between 1989 and 1993 in three main phases:

Preliminary phase (1989 to 1991)
It consists of initial analysis of the system and accident sequences. Purpose of this phase was to determine the scope of the additional studies required. The Preliminary PSA Study was prepared and used as a working material for the PSA team [27] - [48]).

Provisional phase (1992 to June 1993)
It includs a full in-depth review of the preliminary study by experts from other organizations of the PSA team and by the staff of the NPP Dukovany. This part a provisional phase was finished in June of this year.
During this period a preparation of a final version of database and performing of additional thermal hydraulic analyses will be expected.
A final product of this period should consider all technical improvements and take into account changes which are deadlined by the end of March 1993. Main efforts will also be concentrated to a criticism of conservative approach used in the preliminary study. Some parts of this study will be subjected to an review by an external specialists (e.g. IAEA Mission "Fire Risk Analysis Seminar", Bratislava, September 21-25, 1992).

Final phase (July 1993 to December 1993)
During this phase the final quantification will be established, and the final documents will be drafted. During second and third phases a preparation of a "living PSA" model is also expected for the NPP Dukovany staff and the Regulatory Body needs and uses.

2.4. Performing of the PSA analyses

2.4.1. Initiating events

Several documents were used to prepare a list of initiating events for the preliminary NPP Dukovany PSA Study [49].

- a list of IEs which are analyzed in the Czechoslovak Safety Analyses Reports (Preliminary and Pre-operational SARs)
- a list of IEs recommended for SARs by the USNRC (Regulatory Guide 1.70)
- a list of IEs presented in the PRA Procedures Guide (NUREG, CR-2300)

Eight groups of initiators has been chosen in the beginning. Seven of them were events of internal origin and last one contained internal fires and floods events which are often classified as events of external origin.

A. Reactivity initiated accidents

A number of events were taken into account, for example:

a) Uncontrolled withdrawal of a group of control assemblies
b) Fast withdrawal of a control assembly
c) Inlet of cold water into the core
d) Uncontrolled reducing of a boron acid concentration
e) Spurious boron sediments releasing from a core construction
f) Holding of a working group of control assemblies in an upper or a lower position
g) Holding of the most effective control assembly in an upper position during scram

Only first two events were included to the NPP Dukovany IEs list. All other events were excluded because of their existence was connected with a sabotage (c) or their course was similar as in case a) (d) and b) (e) or a positive reactivity was not inserted in the active core (f,g).

B. Loss of coolant accident

These accident were chosen on the base of thermal hydraulic analyses in accordance with success criteria of safety systems. Original six events were reduced during a preliminary phase of the PSA Study to four according additional analyses.

The workshop on Plant Response for VVER-440 NPPs was held in Trnava, ČSFR (4-6 May 1992) in frame of the IAEA TC Project RER/9/005 - PSA for VVER-440 Type Reactors. Existing differences in LOCA accident sequence modeling were discussed there and clarified basing on currently available thermal hydraulic analyses.The proposed System Success Criteria for LOCAs are summarized in the TAB.1. It is expected to accept six LOCA categories in the final NPP Dukovany PSA Study after confirming of this recommendation by next analyses.

The initiating event "Rupture of one steam generator tube" is not very meaningful for VVER reactors (main valve in primary circuit) and it was not included to the preliminary IEs list. But this one will be added to the list of IEs for the final PSA Study [53].

TAB.1. System Success Criteria for LOCAs accepted at the Workshop held in Trnava, ČSFR, 4-6 May 1992
IAEA TC Project RER/9/005 - PSA for VVER-440 Type Reactors

LOCA	Break size range	System success criteria						
categ.	mm	HPI	HPR	LPI	LPR	CFS	EFS	SCS
L1	10<D<20	1			1		1	PM
		1	1					PM
				1	1	0-4*	1	HR
L2	20<D<(50-70)	1	1					
		1			1			
				1	1	0-4*	1	HR
L3	(50-70)<D<(120-150)	1	1					
		1			1			
L4	(120-150)<D<200	1	1					
		1			1			
				1	1	1+1		
L5	200<D<300	1			1			
				1	1	1+1		
L6	300<D<500			1	1	1+1		

HPI - High Pressure Injection System
HPR - High Pressure Recirculation System
LPI - Low Pressure Injection System
LPR - Low Pressure Recirculation System
HPR - High Pressure Recirculation System
EFS - Emergency/Auxiliary Feedwater System
CFS - Core Flooding System (Hydroaccumulators)
SCS - Secondary Pressure Control System
PM - Pressure maintenance mode
HR - Heat removal mode (30K/h)
*)Availability of CFS affects timing requirements for secondary cooling initiation and related probability of the operator error

C. Great loss of steam from secondary circuit

For this group was take into account next events:

a) Spurious opening of steam dump system to the condenser (blocking)
b) Spurious opening of steam dump system to the atmosphere (blocking)
c) Break of the line between header of steam generator and fast quick-acting valve
d) Break of the line between fast quick-acting valve and steam generator
e) Opening of steam generator safety valve (blocking)
f) Break of the main steam header

On the base of analyses of parameters and a response of systems was decided to take into account two groups. The first one involved a), b), c) and f) events, as a representative of this group an event f) was chosen. The second one consisted of two d) and e) events and an event e) was chosen.

D. Great loss of feedwater from secondary circuit

Three events were considered:

a) Break of the main feeding header
b) Break of water feeding piping between main feeding header and check valve
c) Break of water feeding piping between steam generator and check valve

Events a) and b) were grouped to one event a).

E. Loss of service water system

This event conditions a function of safety systems and its importance was assessed.

F. Failure of both turbogenerators, the causes of failure are considered

The reason for choice of this event was its very high frequency (experience from the NPP).

G. Collapse of the grid with both turbogenerators out of control for power plant internal load

During this event all circulating pumps and most of systems of a nominal operation are lost and cooling of the active core is going down. This event also covers all loss of flow combinations.

H. Fires and floods in the NPP

It was not supposed to consider internal and external hazards in the beginning but fires was incorporated to the IEs list for its importance.

During a preliminary phase the original IEs list of 18 initiating events was reduced to current 14 which are analyzed in detail in the Preliminary PSA Study (TAB.2.).

2.4.2. Accident sequences

The accident sequences were determine using the conventional event tree method. Analysis of the sequences has been conducted either to the point of core meltdown or to state in which risk can be considered to be negligible. The interval of twenty four hours was accepted as a maximum time interval for development of accident sequences. All considerations were based on a conservative approach (e.g. no recovery action).

TAB.2. List of initiating events selected for the Preliminary NPP Dukovany PSA Study

1. Uncontrolled withdrawal of a group of control assemblies
2. Fast withdrawal of a control assembly
3. Coolant leakage through the rupture of an equivalent diameter up to 20 mm - small LOCA
4. Same for the range 20-200 mm - medium LOCA
5. Same for the range 200-300 mm - large LOCA
6. Same for the range for the diameter greater than 300 mm (max. 2x500 mm) - large LOCA
7. Break of the line between header of steam generator and fast quick-acting valve
8. Break of the main steam header
9. Break of water feeding piping between steam generator and check valve
10. Break of the main feeding header
11. Loss of service water system
12. Failure of both turbogenerators, the causes of failure are considered
13. Collapse of the grid with both turbogenerators out of control for power plant internal load
14. Fires in nuclear power plant

Each initiating event was analyzed separately, some of events were analyzed by two independent groups of analysts (large and medium LOCA, [29] - [32]).

2.4.3. Systems analysis

System analysis was carried out using a fault tree model. Familiarization with systems was based on the design and corrected and reviewed by the NPP staff. Several fault trees were prepared independently for different initiating events.

For this purpose RISK SPECTRUM FT Plus code has been purchased and it has been used for the evaluation of all trees in this PSA study. The list of main fault trees for safety significant systems (they were prepared in English version), which were necessary for the analysis of the initiating events set, is in the TAB.3.

From the beginning of 1992 the new version RISK SPECTRUM PSA is used for description and quantification of fault trees and event trees.

2.4.4. Reliability data

A collection of data for the preliminary NPP Dukovany PSA Study has been going step by step from generic to specific data. Three version of database were prepared gradually and permanently commented, checked and developed by members of the PSA team and also by the NPP Dukovany personnel. The third version of this database set was used for Preliminary Study. The gradual system specific NPP Dukovany data, specific NPP Bohunice data, generic VVER data, generic data and engineering judgment was preferred.

TAB.3. Safety significant systems of NPP Dukovany

1. Reactor building pressure suppression system
2. Core flooding system
3. Low-pressure injection and recirculation system (LPIS)
4. High-pressure injection and recirculation system (HPIS)
5. Spray system
6. Intermediate component cooling system
7. Technological compartment cooling system
8. Uninterruptible power system (1st category)
9. Essential power system (2nd category)
10. Service water system
11. Unit protection system
12. Gradual start-up automatics
13. Emergency feedwater system (steam generators)
14. Auxiliary feedwater system (steam generators)
15. Steam dump station (blow-off into atmosphere of technological condensor)

The preparation of a database for a final version of PSA study is going now in cooperation with the NPP Dukovany staff. The NPP Dukovany will be responsible for verification of this set.

2.4.5. Common cause failures

The methodology of the CCF was compiled from different approach used abroad which were adapted to contemporary Czechoslovak conditions. The beta-factor was used for the quantification of the CCF.

In this methodology structural dependencies were taken into account on principle as usual primary events. For specific CCF (i.e. common cause failures of a statistical nature which affect components which are not identical) quantification with the help of a beta-factor method using a base beta factor value and engineering judgment was used.

CCF's of redundant components were considered for all principal components of front-line and support systems (on the component level, quantification with the help of a beta-factor method using generic values - TAB.4.). An refinement of CCF consideration after the PSA quantification was also considered.

TAB.4. Generic beta factor values

Component Type	Beta Factor
Pump	
Safety Injection System	0.17
Residual Heat Removal System	0.11
Containment Spray System	0.05
Auxiliary Feedwater System	0.03
Service Water System	0.03
Motor-Operated Valve	0.08
Check Valve	0.06
Safety/Relief Valve	0.07
Diesel Generator	0.05
Fan	0.13
Chiller	0.11
Reactor Trip Breaker	0.19
Base Value (average component)	0.10

2.4.6. Human factor

The methodology of human factor for the preliminary NPP Dukovany PSA Study was based on the ASEP-HRA methodology (Swain A.D., NUREG/CR-4772) and it was partly modified by some procedures from the THERP methodology (Swain A.D., Guttmann H.E., NUREG/CR-1278) and Mr. J.K.Vaurio recommendations (IAEA Regional Project RER/9/005).

Human errors during a nominal operation before an accident and human errors after accident (only prescribed activity) were taken into account.

2.5. Some experience with the PSA Study

The project PSA Study has started as "research project" and it has been financed by a central budget. In the beginning it was concentrated on the methodology and familiarization with the PSA techniques and nuclear power plant systems. There were several people in several Czechoslovak organizations who were interested in reliability analysis and had started with the PSA methods. In this first period the VVER-440 reactor type 213 was chosen as a representative for a reference study.

Some "old analyses" were also finished during this period in all engaged institutes (e.g. reliability analyses for NPP V1 Jaslovské Bohunice). One team was being formed during first year with one goal. Later the NPP Dukovany was elected for a specific PSA Study.In this time the NPP Dukovany staff was not engaged very much in this project.

Second year of the project is possible to characterize as "one team - one methodology - one language" year. The task of one language was solved by a purchase of the RISK SPECTRUM code.

The third year is possible to designate as a "preliminary PSA Study" year. This decision was accepted additionally during a preparation of the Study and helped very much because of founding of many lacks in time before the end of this Study. During this period a cooperation with the NPP Dukovany staff has become much more better and it is a necessary condition for a successful finishing of this study.

The results of the preliminary Study showed very conservative presumptions, a lack of reliable data (mainly for initiating events), a lack of thermal hydraulic analyses and faults in the project (e.g. some descriptions of systems, in some considerations). This is also a main reason not publishing and not releasing of this study and accepting of it as a "working version". During this period was appeared a necessity to have a very compact team for such purposes and meetings of this team with very low frequency has helped to overcome a little bit this problem.

3. PSA ACTIVITIES FOR 1992 AND NEXT FUTURE IN ČSFR

The work on the Final NPP Dukovany PSA Study will continue during 1992 on the base of the Preliminary report. The Risk Spectrum PSA version will be used for evaluation. Some activities for a preparation of a "living PSA model" for the NPP Dukovany has been started.

In September 1992 is expected to start with PSA Study - first level for the NPP Jaslovské Bohunice (first two units with VVER-440 type 230 reactors). These activities will be supervised by foreign experts in frame of the CEC PHARE Programme. The competition was finished the Electrowatt company from England was pointed as a leader of this project. The final version of this Study has been planned to release very soon, the middle of 1993 has been expected (but beginning of a start was postponed roughly 6 months)

The tender for PSA Study of our NPP Temelín with VVER-1000 reactors was prepared several weeks ago (more information see in [66]). Six foreign organizations have taken part in this competition and decision about the start of it and the scope of it (probably the second level will be asked) will be clear during this year.

REFERENCES

[1] Briš R., Ferjenčík M., Hojný V., Cyrániová J., Dušek J.: Comparison of codes which are used in NRI Řež for NPP safety system reliability analyses, Report ÚJV 7411 A, Řež, June 1985 (in Czech), 60 p.

[2] Holý J.: SIGASEN - the Code for Sensitivity Analysis, Report ÚJV 8839 A, Řež, January 1987 (in Czech),

[3] Patrík M.: FRANTIC-Code modified according to the NRI needs. Report ÚJV 8500 A, Řež, May 1988 (in Czech), 43 p.

[4] Hojný V.: CRAFT - user's guide. Report ÚJV 8938 A, Řež, October 1989 (in Czech), 75 p.

[5] Holý J.: Program COSMOS (analysis of fault tree uncertainty propagation), Report ÚJV 8839 A, Řež, June 1989 (in Czech),

[6] Patrík M.: Verification of function and modification of the integrated PC package for PSA - PSAPACK. Report ÚJV 8951 A, Řež, October 1989 (in Czech), 38 p.

[7] Krett V., Dach K., Dušek J.: Application of fault tree analysis to bubbling depressurization system of the nuclear power plant with the WWER-440 reactor. In: Proceedings of the International Workshop on Technological Risk in Modern Society, Laxenburg (Austria), March 1987, 26 p.

[8] Dach K., Dušek J., Hojný V.: Investigation of independent and dependent human error to reactor WWER-440 safety related systems reliability. In: Proceedings of the Second International Workshop on Advances in RA and PSA, Seregélyes (Hungary), September 1987, 25 p.

[9] Holý J.: Input Data Uncertainties in Reliability Analysis of the Low Pressure ECCS System of the WWER-440 Reactor in NPP Dukovany and NPP Mochovce, Report ÚJV 8505 T, Řež, May 1988, (in Czech)

[10] Dušek J.: Reliability analysis of the WWER-440 type 213 safety systems, In: Proceedings of the Czechoslovak - British Seminar on Nuclear Power, Brno (Czechoslovakia), Nov. 8 - 9, 1988, pp. 193-214

[11] Najih A.M. Al-Kaisi, Dušek J., HPIS-ECCS PSA of Paks - Hungary NPP, Rep. NRI, Řež, Nov.1989, 48 p.

[12] Kašpar J.: Probabilistic Safety Analysis of the NPP WWER-440 and the LVR-15 Research Reactor with Modelling of Accident Sequences. Ph.D. Thesis, Moscow 1991 (in Russian)

[13] Dušek J., Dach K.: Application of reliability analyses of WWER NPP safety systems to PSA. In: Proceedings of the PSA'87 - International Topical Conference on Probabilistic Safety Assessment and Risk Management, Zurich (Switzerland), Aug.30 - Sept.4, 1987, pp. 395-399

[14] Dach K., Dušek J., Investigation of human action influence on Czechoslovak WWER-440 NPP with LPIS-ECCS reliability for PSA study, In: Proceedings of the PSA 89 - International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh (USA), April 1989, 8p.

[15] Dušek J., Use of PSA and its development and trends in Czechoslovakia, In: Proceedings of the PSA 91 - International Symposium on the Use of PSA for Operational Safety, IAEA-SM-321/67P, Vienna (Austria), June 1991

[16] Holý J.: Uncertainty analysis in the process of reliability estimation. In: Proceedings of the IAEA Technical Committee Meeting on the Use of Probabilistic Safety Analysis to Evaluate Nuclear Power Plants' Technical Specifications, Vienna (Austria), June 18 - 22, 1990

[17] Dušek J., Probabilistic safety assessment in Czechoslovakia, American Nuclear Society - Czech and Slovak Nuclear Society Seminar on PWR Safety, Prague, April 1991, 25 p.

[18] Holý J.: Numerical Evaluation of Uncertainty Propagation through Fault Tree, NRI Řež - NUS Corporation Seminar on PSA and its Application, Řež (Rep. NRI 9417 T), May 1991

[19] Dušek J., Probabilistic safety assessment study of NPP Dukovany, NRI Řež - NUS Corporation Seminar on PSA and its Application, Řež, May 1991, 7 p.

[20] Dach K., Dušek J., Hojný V., Holý J., Patrík M., Vitázková J., Babič P., Final report of the IAEA research contract no. 4032/RB Importance of Independent and Dependent Human Error to System Reliability and Plant Safety (a part of the IAEA coordinated programme on development of risk criteria for the whole nuclear fuel cycle), Time Period: Dec.1984 to Dec. 1987, 72. p

[21] Hron M., Dušek J., Kašpar J., Macek J., Holý J., Malačka M. Horyna J., Listík E., Pittermann P.: Final report of the IAEA research contract no. 4355/RB - Probabilistic Safety Assessment for Research Reactor LVR-15 (a part of the IAEA coordinated programme on PSA for research reactors), Time period: March 1986 to March 1989, 147 p.

[22] Kašpar J., Hojný V., Najih Al-Kaisi, Šamal V., Patrík M., Dušek J., Aldorf R., Husťák S.: Progress reports of the IAEA research contract no.5045/RB Modelling of a Small LOCA Accident (a part of the IAEA coordinated programme on reference studies on probabilistic modelling of accident sequences) - summary report, Time period: July 1988 to March 1991 , 182 p.

[23] Kašpar J.: Experience from International Participation in IAEA CRP "Reference Studies on Probabilistic Modelling of Accident Sequences" for WWER-440 Reactor and its using in Application of PSA in Czechoslovakia, ref. na Technical Committee Meeting on PSA Requirements for Use in Safety Management, 16-20 September 1991, Stockholm

[24] Dach K., Hojný V., Patrík M., Šamal V., Hájek R., Aldorf R., Antes M.: Final report. IAEA Regional Programme RER/9/005 "PSA for VVER-Type Reactor", March 1990, 148 p.

[25] Hojný V., Patrík M., Aldorf R., Husťák S.: PSA of the NPP Dukovany - Large Break LOCA Initiating Event, Summary report prepared for the purpose of the peer review carried out on April 15-19, 1991. IAEA Regional Programme RER/9/005, NRI Řež, January 1991, 42 p.

[26] Dušek J., Štěpánek V., Kašpar J., Holý J., Ryšavý J.: Progress report of the IAEA research contract no. 5686/RB Data Acquisition for the LVR-15 Research Reactor (a part of the IAEA coordinated programme on data acquisition for research reactor PSA study), Time period: June 1990 to July 1991, 55 p.

[27] Hojný V.: Human error in fault tree methodics, NRI Řež, August 1991, 8 p. (In Czech)

[28] Staníček J., Tinka I.: Preliminary NPP Dukovany PSA Study - Appendix C - Reactivity initiating events, Report EGP Prague No.221-6-910958, November 1991, 25 p. (In Czech)

[29] Kovács Z. et al.: Project EDU for first unit NPP Dukovany PSA Study purposes, VUPEK Report No.823-001-003-4/1, Bratislava, Dec.1991, 17 p. + 400 p.(suppl.), (In Slovak)

[30] Kovács. Z. et al.: Preliminary first unit NPP Dukovany PSA Study - Appendix D - LOCA, part 1, System description, VUPEK Report, Bratislava, March 1992, 223 p. (In Slovak)

[31] Hojný V., Patrík M., Husťák S., Aldorf R.: Preliminary NPP Dukovany PSA Study - Appendix E - LOCA with the rupture of an equivalent diameter greater than 300 mm, NRI Report No.9630 T, Řež, February 1992, 147 p. (+ supplement No.1, July 1992, 39 p.)

[32] Babič P., Adamec P.: Preliminary analysis of first unit NPP Dukovany response to medium LOCA accident - Appendix F, Supplement No.1 to the EGÚ Prague Report No.21511230, Běchovice, December 1991, 285 p. (two volume), (In Czech)

[33] Staníček J., Borský M., Kreim R.,: Preliminary NPP Dukovany PSA Study - Appendix G - Leakage from secondary circuit accident, Report EGP Prague No.221-6-911000, December 1991, 72 p. (In Czech)

[34] Pospíšil B., Halada P.: Event trees development for the Preliminary NPP Dukovany PSA Study, VÚJE Report No.224/91, Trnava, December 1991, 81 p., (In Slovak)

[35] Markech B. et al.: Assessment of initiating events "Collapse of the grid with both TG out of control for the NPP internal load" and "Loss of service water system", VÚJE Report No.248/91, Trnava, December 1991, 114 p. + 126 p. (two volumes), (In Slovak)

[36] Borský M., Dolejší J., Kreim R., Staníček J.: Preliminary NPP Dukovany PSA Study - Appendix I - Failure of both turbogenerators, the causes of failure are considered, Report EGP Prague No.221-6-911001, Dec.1991, 41 p. (In Czech)

[37] Kandráč J. et al.: Fire as an initiating event of first unit NPP Dukovany accidents (second part), report VUPEK 823-001-003-4/2, Bratislava, November 1991, 36 p. (In Slovak)

[38] Kandráč J. et al.: Preliminary first unit NPP Dukovany PSA Study - Appendix K - Fire as an initiating event of first unit NPP Dukovany accidents, report VUPEK 823-001-003-4/3, Bratislava, March 1992, 52 p. (In Slovak)

[39] Baszó Z., Mišák J., Václav E.: Small and medium LOCA analyses of WWER 440/213 with HPIS failure - app.L1, VÚJE Report No.283/90, Trnava, December 1990, 102 p. (In Slovak)

[40] Dienstbier J., Hojný V.: Influence of pressure suppresion system failures on LOCA mitigation in a NPP woth the VVER-440 type reactor - App.L2, NRI Report No.9307-T, Řež, December 1990

[41] Kovács Z., Sopira V., Charvát L.: Internal floods as initiating events of accidents - App.L3, VÚPEK Report, Bratislava, December 1989, 8 p. (In Slovak)

[42] Petrlík J, Staníček J., Nágl J.: Preliminary NPP Dukovany PSA Study - Appendix L4 - Leakage from secondary circuit accident, failure of both turbogenerators. Thermal hydraulic analyses, Report EGP Prague No.221-6-911002, December 1991, 85 p. (In Czech)

[43] Patrík M.: Reliability of the Electric Power Supply System using GSA and DG starts during an Accident in Comparison with Reliability of the Electric Power Supply System using Safety Pump starts by UPS and Offsite Power Supplying - App.M1, Report ÚJV 9344 T, Řež, April 1991, (in Czech)

[44] Husťák S.: The Analysis of Performed Modifications in the Signal Paths for Formation HO-1 and HO-3 Signals Following Turbine Quick-acting Valves Closing and in the Signal Paths of HO-1 Signal to Turbine Quick-acting Valves Closing - App.M2, Report ÚJV 9476 P, Řež, July 1991 (in Czech), 76 p.

[45] Aldorf R., Hájek R.: Reliability Analysis of DG in NPPs with VVER Reactors - App.M3, Report ÚJV 9478 P, Řež, July 1991 (in Czech), 36 p.

[46] Husťák S.: Reliability Analysis of the Level Regulation System in the Heat Exchanger - App.M4, Report ÚJV 9477 T, Řež, August 1991 (in Czech), 83 p.

[47] Hep J., Smutný V., Valenta V.: IDE computations for surrounding of the NPP Dukovany during fast withdrawal of a control assembly accident, Škoda Report No.Ae 7555/Dok., Plzeň, August 1991, 77 p. (In Czech)

[48] Valenta V., Hep J.: NPP Dukovany PSA Study - Appendix N - Possibilities of third level PSA analyses in Czechoslovakia, Škoda Report, Plzeň, November 1991, 97 p. (In Czech)

[49] Staníček J.: Personal communication

[50] Babič P.: Engineering safety features taking place after long time from an accident initiation and possibilities of decreasing of conservatism of the model, Report EGÚ Prague No.21511230, December 1991, 29 p.(In Czech)

[51] Holý J.: New suggestion for uncertainty analysis methodics, NRI Report No.9264 T, Řež, January 1992, 131 p. (In Czech)

[52] Babič P.: LOCA computations for NPP Dukovany with specific data, Supplement No.2 to the EGÚ Prague Report No.21511230, Běchovice, April 1992, 45 p. (In Czech)

[53] Borský M., Kreim R., Petrlík J, Staníček J.: Rupture of one steam generator tube, EGP Prague Report No.40-0832-71-004, June 1992, 63 p. (In Czech)

[54] Husťák S.: Internal floods as initiating events of accidents, NRI Report No.9706 T, Řež, July 1992, 12 p. (In Czech)

[55] Holý L.: Some Interesting Problems Connected with Uncertainty Analysis Performance as a Part of PSA, Multilateral Symposium on Safety Research for VVER, 7.-9.7.1992, Cologne, Germany

[56] Dušek J.: Acquired Experience during the NPP Dukovany PSA Study Preparation, Multilateral Symposium on Safety Research for VVER, 7.-9.7.1992, Cologne, Germany

[57] Hojný V.: Large Break LOCA Initiating Event in the NPP Dukovany PSA Study, Multilateral Symposium on Safety Research for VVER, 7.-9.7.1992, Cologne, Germany

[58] Patrík M.: Prospect for PSA Application in the NRI Řež, Multilateral Symposium on Safety Research for VVER, 7.-9.7.1992, Cologne, Germany

[59] Aldorf R.: DG Start-up Reliability Analysis for the NPP Dukovany, Multilateral Symposium on Safety Research for VVER, 7.-9.7.1992, Cologne, Germany

[60] Nováková H.: PSA programme in VUPEX Bratislava (this meeting)

[61] Čillík I.: Basckward influence of PSA Methodology on specific data collection on NPP (this meeting)

[62] Staníček J.: Analysis of transients for PSA of Dukovany NPP (this meeting)

[63] Hojný V.: Presentation and basic application of PSA results (this meeting)

[64] Valenta V.: Probabilistic and safety assessment in SKODA (this meeting)

[65] Sedlák J.: Probabilistic reliability and safety assessment in SKODA (this meeting)

[66] Ferjenčík M.: PSA activity of the NPP Temelín (this meeting)

THE PSA PROGRAMME IN VUPEX BRATISLAVA

H. NOVÁKOVÁ
VUPEX, J.S. Co.,
Bratislava, Czechoslovakia

Abstract

The areas in which VUPEX is active reflect problemś arising in the nuclear power plant operation. Main fields of activities are systems analyses which include reliability analyses of safety systems, probabilistic safety assessment and fire protection for VVER 440s.

The system reliability analyses are concentrated on the front-line and support systems of V213 and V230 type reactors. Examples are the high pressure safety system and reactor building spray system of V230 type reactors and numerous single system studies sponsored by utility for design, review and reconstruction purposes. The fault tree method by TREE MASTER code has been used for analyses.

VUPEX performs research into Probabilistic Safety Assessment within the Level I PSA study of the unit 1 of Dukovany Nuclear Power Plant. The work was started in 1989 and the Level 1 study will be finished in 1993. The systems analysed in VUPEX are those V213 type front-line systems identified in event trees. Also analysed are the support systems whose action is required by the front-line systems during the course of an accident. The RISK SPECTRUM-PSA code is used for analyses.

Introduction

Two nuclear power plants, located in Jaslovské Bohunice and Dukovany, are in operation in our country. Both are equiped with WWER 440 reactors. The Jaslovské Bohunice plant consists of two V 230 type units and two V 213 type units. Dukovany plant has four identical V 213 type reactors.

The first generation WWER 440s, designated as model V 230, have few features to mitigate the effects of a severe accident. Safety related additions to the basic design were incorporated into the second generation, designated as model V 213. These additions include an emergency core cooling system with high pressure and low pressure pumps, core flooding system, cladding on the interior of the reactor vessel, reactor building pressure suppression system to reduce compartment pressures in the event of a loss of coolant accident, etc.

The areas in which VUPEX Bratislava is active reflect problems arising in the operation of these nuclear power plants. Main fields of activities are system analyses which include reliability analysis of safety systems, probabilistic safety assessment and fire protection.

System Reliability Analyses

The system reliability analyses are concentrated on the front-line and support systems of V 213 and V 230 type reactors. Examples are the emergency core cooling system, reactor building spray system, load sequencing system, emergency power supply system, serwice water system, auxiliary feed water system, reactor protection system of V 230 type reactors, technical specification evaluation for reactor protection system of V 213 type reactors and numerous single system studies sponsored by utility for design, review and reconstruction purposes. The fault tree method has been used for analyses. At the present time the TREE MASTER code (version TM2) is used for it. This is a commercial code for personal computers developed by Mr. Antonin Wild from Canada.

Probabilistic Safety Assessment

VUPEX performs research into Probabilistic Safety Assessment within the level 1 PSA study of the unit 1 of Dukovany Nuclear Power Station. The work was started in 1989 and the level 1 study will be finished in the end 1993. It is coordinated by Mr. Dušek, ÚJV ŘEŽ.

In VUPEX the following works are being performed:

- fault tree construction and reliability analyses for front-line and support systems,
- functional and systemic event tree construction for loss of coolant accidents using results of thermal-hydraulic analyses from VÚJE Trnava (Nuclear Power Plant Station Research Institute),
- event tree accident sequence quantification for LOCAs and transients.

The system analyzed in VUPEX are those V213 type front-line systems identified in event trees These include the high pressure system, low pressure system and reactor building spray system in injection and recirculation mode, the reactor protection system, core flooding system, emergency feedwater system, auxilliary emergency feedwater system and the secondary side heat removal system

Also the support systems are analyzed whose action is required by the front-line systems during the course of an accident Those support systems are load sequencing system, engineered safeguards actuation system, uninterruptible and essential emergency power supply system, serwice water system, intermediate component cooling system, technological compartment cooling system and demineralized water system.

Common cause contributors and human errors associated with the testing, maintenance or operation are included in the system models. Component data used in the analyses are generic WWER 440 data and plant specific data.

The RISK SPECTRUM - PSA code is used for these analyses

The success criteria of the front-line systems were obtained from thermal-hydraulic analyses performed in VÚJE Trnava.

Fire and Flood Safety Analyses

The VUPEX fire analyses consist of:

- fire hazard analyses with identification of critical plant location and evaluation of fire occurence,
- fire propagation analyses in critical areas with use of mathematical simulation, the computer code COMPBRN III is used for modelling of compartment fire behaviour

All this works was based on the plant system analyses, where cable routes for safety important systems were analyzed for V 213 and V 230 units

The flood analyses for Dukovany are at an early stage, but the important flood sources have been identified

THE STATE AND PROBLEMS OF PSA FOR WWER PLANTS

Y V SHVIRAYEV, V B MOROZOV, A F BARSUKOV,
G V TOKMACHEV, A A DEREVYANKIN
Atomenergoprojekt,
Moscow, Russian Federation

Abstract

In compliance with the current regulatory documents issued by the State Supervisory Authority of the Russian Federation PSAs shall be incorporated in the NPP design process. PSA results shall demonstrate that the estimated values of core damage frequencies and excessive releases do not exceed the set target values of 1.0E-5 and 1.0E-7 per reactor/year, respectively. An excessive release is a release that may require population evacuation from the areas located at certain distances from the site set in the NPP Siting Rules.

Thus NPP design shall incorporate level 2 PSA (with some elements of the third level) that shall define a complete variety of possible NPP radiation incidents (when the set excessive release values are exceeded) and evaluate their frequencies of occurrence, amounts and consequences (dose commitments). Consequently, a PSA is an integral part of a NPP design required for licensing. Moreover, presently PSAs along with deterministic analyses have become the main tool for decision-making in the field of safety improvement of the NPPs operating and being designed.

The report tackles the following issues:

1. The status of methodology (procedures and codes) for PSAs.

2. PSA results for the WWER plants and their application for optimizing the design solutions and developing safety measures for the operating WWER-1000 plants located in the CIS countries.

3. Major problems of further PSA development and application for the WWER plants in the Russian Federation.

1. PSA Status

In compliance with the major Russian regulatory document on NPP safety "General Safety Provisions for NPP Design, Construction and Operation" (ОПБ-88) /1/ the estimated values of core damage frequencies and excessive releases incorporated in the plant design basis should not exceed the ОПБ -88 values of 1.0E-5 and 1.0E-7 per reactor/year, respectively. An excessive release is a release that may require population evacuation from the areas located at certain distances from the site specified in the NPP Siting Rules. In practice, these distances correspond to NPP distances from major populated areas with the population of several tens of thousands people.

Similar target values for core damage frequencies are specified in the IAEA recommendations /2/ - 1.0E-4 and 1.0E-5 per reactor/year for operating plants and plants being designed, respectively. According to /2/ the frequencies of severe accidents requiring immediate off-site countermeasures shall be at least 10 times less core damage frequencies due to the use of accident management measures.

The ОПБ-88 requirements mean that NPP design shall incorporate level 2 PSAs with estimated population dose committments at different distances from the NPP. As a result of PSA core damage and excessive release frequences, total for all accident sequences (AS), shall be estimated, and these frequences shall be proved to be lower than ОПБ-88 targets. PSAs are incorporated in NPP designs because they are essential for licensing

It should be noted that PSA performance entails certain difficulties related to the application of targets listed in /1/ and /2/. They stem from the fact that neither /1/, nor /2/ describe the procedures used for correlating the obtained project-specific PSA results with targets In particular, it is not clear whether targets have the meanings of median, average values or of the values obtained for certain probabilistic confidence levels Neither is it clear whether PSA shall account for internal initiating events (IEs) only, or for external IEs as well We think that "Gosatomenergonadzor" of the Russian Federation and IAEA should make apropriate additions, comments or explanations in order to avoid these major uncertainties.

2. The state of PSA technology

Atomenergoproekt has developed a PSA-1 technology consisting of a package of procedures and computer codes for IBM PC AT. Based on this technology a Guide has been prepared the scope of which includes:

2.1. Probabilisitic modelling aimed at defining core damage states. Functional event trees (FET) used as models are built similarly to the Western ones.

2.2. Systems reliability analysis

The reliability analysis technique based on fault trees (FT) accounts for almost all reliability-important features of the systems, such as: structure, operation modes, status monitoring, maintenance and repair strategy. A reliability analysis consists of two stages: 1) failure mode and effect analysis (FMEA) is performed with a detailed failure mode classification depending on the above-mentioned features of system components, and a system fault tree is built; 2) a set of minimal cut secs (MCS) is defined on the basis of the fault tree and their quantitative assessment is made based on time-dependent unavailability functions for each MCS with a subsequent averaging for the studied time periods. This technique allows for a detailed assessment of different factors affecting system reliability

2.3. CCF modelling

Characteristic of the methodology is an implicit reflection of common-cause failures (CCFs) in a logical model and detailed qualitative and quantitative modelling of different characteristics of individual events.

An implicit method of introducing CCFs into the logical model implies an analysis of reference MCS made up of independent failures only. If such a MCS contains failures of at least two components susceptible to a CCF, additional MCS are generated containing CCFs instead of independent failures of the respective components. Also the so called "enveloping" MCS are generated that contain the following event: a CCF of the reference MCS components along with other components included in the CCF group. The procedure of generating additional MCS with CCFs envisages their check for uniqueness and screening.

Detailed modelling of CCFs is accomplished by:

1) defining probabilities or occurrence rates of CCFs through separate modelling of the events with sources of different origines. A quantitative assessment of these characteristics is made by means of reference parameter models: binominal, greek letter, -factor or -factor models. All groups of components susceptible to CCFs are divided into three classes. The criteria for placing the groups of elements into this or that class are as follows:

class 1 - common design
class 2 - common environmental conditions
class 3 - same maintenance and/or inspection procedures;

2) identifying the mode and monitoring frequency of CCFs with consideration for the monitoring type, frquency and strategy of individual component failures,

3) calculating a mean time period of CCF removal with regard of the strategy and average time of recovery for individual failed components, their effect on the system operation, specified limitations

The detailed modelling allows to make a quantitative prediction of the failure impact on probabilistic safety parameters with as low uncertainty as possible, as well as to use various design solutions aimed at improving protection of the safety system equipment.

2.4. Personnel reliability modelling

Personnel reliability analysis is based on human error trees (HET). The following three groups of human errors are considered.

- maintenance errors leading to accident initiating events (IE);
- maintenance errors leading to safety system unavailability;
- system control errors during accidents leading to accident sequences with core damage.

HET are based on the detailed algorythms of personnel actions developed on the basis of design and operation documents and accident analysis results.

In the course of HET quantification the human error probabilities are determined with consideration for the time on decision-making and action-taking, for stress levels, etc. Later on they are used for evaluating conditional probabilities of AS occurrences or probabilities of loss of safety functions as a result of human errors.

2.5. Quantitative assessment of accident sequences (AS)

AS quantification is based on the development of detailed (large) fault trees (FTs) for each AS or of functional event trees with subsequent modelling and quantifying independent failures, CCFs, and human errors. The modelling and quantification results serve as a basis for determining conditional probabilities of AS occurrences

2.6. Assessment of PSA results

The assessment of PSA results consists in:

- defining core damage frequencies (total for all AS and their correlation with the target values;

- identifying dominant contributors to core damage frequencies and "weak points" of the project;

- analysing significance and sensitivity;

- analysing uncertainties;

- evaluating the project and giving recommendations with respect to safety improvement.

Software package for PSA

PSA software package comprises: 1) computation modules for calculating AS probabilities by means of MCS; 2) graphics editors (used to generate the required initial data on fault trees and event trees), and 3) a component reliability database. The software package permits to calculate AS probabilities not only for component independent failures but for CCF and human errors as well.

The software package incorporates the following computer codes run on PC AT:

- APRA, intended to estimate AS probabilities with consideration for data onindependent failures, CCFs and human errors;

- VNF, intended for verification of AS probabilities with account of the maintenance strategy features;

- ANTES, intended for human reliability calculations;

- UNAS, intended to analyse the uncertainties of PSA-1 results as a function of component reliability uncertainties.

3. PSA results for WWER-type NPPs

3.1. Preliminary PSAs have been performed for the following designs of nuclear power plants with WWER-1000 reactors:

1. Standardized B-320 NPP design used for the Rostovskaya NPP, Unit No 4 of the Balakovskava NPP (Russia), the "Temelin" NPP, (Chechoslovakia). This design is implemented in the operating units of the Balakovskaya NPP (Units 1-3), Zaporozhye, Khmelnitskaya, Rovno NPPs and "Kozloduy" NPP, Bulgaria. It is based on the application of three-train active safety systems performing core heat removal functions during accidents with/without primary coolant losses, and of a full-pressure reinforced concrete containment.

2. A backfitted design of B-320 NPP used for Units 5 and 6 of the Balakovskaya NPP, which besides the active safety systems similar to those of the standardized design, incorporates a passive system of heat removal through the secondary circuit (PHRS) and an emergency boron injection system. Also hydrogen discharge system and a filtered containment vent system are provided.

3. B-392 NPP design for the Loviiza NPP, Finland. It is based on the use of four-train active safety systems and a full-pressure double containment with a filtered atmospheric exhaust system.

4. A new design of the B-392 NPP of improved safety (NPP 92 Project). Mutually redundant multy-train active and passive safety systems are provided to fulfil major safety functions in this project.

The function of making and maintaining the reactor subcritical is accomplished by one of the following mutually independent systems:

- mechanical reactor protection system with 121 control rods;
- fluid emergency boron injection system.

The function of long-term core heat removal during accidents without primary coolant losses can be performed by one the following mutually independent systems:

- passive system of heat removal from SGs;
- four-train active system of heat removal in the secondary circuit, 4 x 100%.

Each of the these systems is capable of SG heat removal during an unlimited time period. Therefore, they are completely mutually redundant as regards the long-term heat removal function.

The function of maintaining the core coolant inventory during LOCAs can be accomplished by the following mutually independent systems:

- passive ECCS with level-1 and 2 storage tanks that can perform its prescribed functions during 24 hours following the accident initiation;
- four-train active ECCS, 4 x 100%, that can perform its prescribed functions during the whole period of time required to make the unit safe.

The use of a passive ECCS must ensure enhanced reliability of long-term core coolant maintenance due to the margin of 24 hours for implementing accident management activities (for example, for restoring functionability of the active ECCS in case of its total failure).

The use of diverse mutually redundant passive and active safety systems is a better protection against CCFs because such systems either do not have components similar or identical in design or their number is minimal. As a result, the impact of CCFs is greatly reduced and the reliability of major safety functions is drastically improved.

The use of passive systems and an active heat removal system of the secondary circuit (CAP) capable of long-term functioning after the accident initiation practically eliminates the need for the personnel to operate safety systems during accidents.

To increase the active safety system availability their trains can be used for normal operation with the reactor operating on power. The majority of components of these trains (pumps, valves, heat exchangers, etc.) are in the state similar to that during the accident. This allows to avoid complete latent failures and reduce the effect of CCFs. It also leads to a substantial reduction of the equipment and components used in safety systems and normal operation systems and, hence, to increased technical and economic parameters.

The containment system is a full-pressure reinforced concrete containment equipped with a hydrogen discharge system, melted core trap and containment atmospheric dump system for beyond the design basis accidents. The safety concept imbedded in the NPP-92 project is based on the evolutionary principles which imply the use of well-proven, verified and supported by a long-term operational experience decisions and new decisions based on obvious and well-studied physical and technological processes. This concept may serve as a basis for nuclear power development for the nearest 15-20 years.

3.2 PSAs for the projects listed above were performed for a limited number of major groups of internal IEs including

- NPP de-energization, i.e. loss of on-site normal power and off-site A.C. power during various periods of time (LOOP):
    - less than an hour;
    - within 10 hours;
    - within 24 hours;
    - within 72 hours;
    - within 720 hours;

- long-term normal heat removal failures in the secondary circuit requiring cold shut-down of the Unit without loss of power and secondary piping ruptures (LONHRS on ss);

- main steam header rupture (MSHR);

- ruptures of SG steamlines and feedwater lines in the non-isolated parts (SGTR);

- small-break LOCAs (SBLOCA) in the primary circuit;

- medium-break LOCAs (MBLOCA) in the primary circuit;

- large-break LOCAs (LBLOCA) in the primary circuit;

- leak from the primary into the secondary circuit (SGHR).

3.3. PSAs were performed only for one operating mode, namely for the full power operation of NPP.

3.4. Mainly a general database on component reliability /3/, as well as data from /4/, personnel reliability data available at "Atomenergoproekt", and CCF model parameters from /5/ were used for PSA. Finnish data were used for a number of components (diesel-generators, fast-acting atmospheric exhaust system) in the course of PSA for the "Loviiza" NPP.

3.5. Core damage frequencies for each AS were estimated separately for indeoendent failures (IE), IE+CCF, and IE+CCF+HE (human errors).

3.6. Accident-management measures for beyond DBAs were taken into consideration in PSAs for the "Loviiza" NPP, Unit 4 of the Balakovskaya NPP and NPP-92 Project.

3.7. PSAs were performed to reach the following main purposes:

- to evaluate the contribution of the studied groups of IEs into core damage frequencies;
- to identify dominant contributors to core damage frequencies (IE, functions, ssystems and components, CCF, HE);

- to develop safety improving measures, including accident management measures, optimization of design solutions on structure, mechanical systems and maintenance;
- to evaluate and verify major design solutions on NPPs with improved safety.

3.9. Table 3.1. contains PSA results for the standardized B-320 NPP exemplified by Unit 4 of the Balakovskaya NPP. The values of core damage frequencies, total for all AS, for the reviewed list of major internal IEs are 1.9E-5 and 4.2E-4 per reactor/year with and without accident management activities, respectively. On the basis of PSA results a variant incorporating the recommended beyond DBA management measures was selected as a basic design. Such measures include:

1. The use of feed and bleed mode.

2. Water supply from the emergency service water system into water inventory tanks of the SG emergency feedwater system, so that the latter is able to operate over 10 hours

TABLE 3 1 CONTRIBUTION TO CD FREQUENCY FOR WWER 320 NPP

IF	IE frequency 1/year	CD frequency, 1/year			
		Without AM		With AM	
		1/year	%	1/year	%
1 SBLOCA	3.2E-3	3.3E-6	0.8	9.4E-7	~5
2 MBLOCA	1.0E-3	1.8E-7	<1	1.8E-7	~1
3 LBLOCA	3.0E-4	1.3E-6	<1	1.3E-6	~6,8
4. SGHR	1.0E-3	1.1E-6	<1	1.1E-6	~6
5. LOOP 5.1.LOOP in 72 h	7.0E-3	9.8E-5	23	1.3E-5	~68
5.2.LOOP in 720 h	1.0E-4	2,2E-6	<1	7.8E-7	~4
6. LONHR on SS 6.1.With loss of TC	3.0E-2	2.9E-4	69	7.3E-7	~4
6.2.Without loss of TC	7.0E-2	4.5E-6	1	1.7E-7	~4
7. SGTR	1.0E-4	4.0E-7	<1	4.0E-7	~2
8 MSHR	1.0E-3	1.4E-5	3	4.6E-7	~2
All IF		4.2E-4		1.9E-5	

The introduction of these accident management measures permits to reduce core damage frequency more than 20 times.

In the basic design the largest contribution to the core damage frequency (68%) is made by IEs with long-term loss of power, followed by failures of all three diesel-generators

It was also found that CCFs are the main contributor to the core damage frequency.

3.10 Table 3.2. gives PSA results for the "Loviiza" NPP (NPP-91) and NPP-92 designs. Core damage frequencies are estimated only for the 24-hour operation of safety systems following the accident initiation, while for NPP-92 they are estimated both for 24 and 720 hours. For NPP-91 core damage frequencies were estimated with and without the allowance for accident management measures. Table 3.2. gives the results for NPP-91 with allowance made for such measures, including the use of feed and bleed mode and of auxiliary feed pumps connected to additional diesel-generators in the secondary circuit. The above measures are performed by the personnel in both this and B-320 NPP designs. The introduction of accident management measures into the NPP-91 design allows to reduce core damage frequencies more than 15 times. While evaluating core damage frequencies in the NPP-91 PSA it was assumed sufficient to buy equipment items similar in working principle and design (diesel-generators, pumps) from different manufactures in order to avoid CCFs.

For NPP-91 the main contribution to the core damage frequencies is made by IEs with normal heat removal failures on the secondary side (66%) and de-energization (15%) resulting from CCFs in emergency heat removal systems of the secondary circuit and human errors during accident management activities, and by IEs with large leaks due to CCFs in ECCS (15%). Human errors contribute appr. 66%, while CCFs - 28% into core damage frequencies.

The use of mutually redundant and diverse active and passive safety systems in the NPP-92 project allows to reduce core damage frequencies by more that two orders of magnitude for 24 hours following the accident initiation as compared to the NPP-91 project based on the use of active systems.

TABLE 3 2 CONTRIBUTION TO CORE DAMAGE FREQUENCY

IF	IF frequency, 1/year	NPP	Dominant Safety function	CD frequency , 1/year			
				IF	IF+CCF	IF+CCF+P	%
1	2	3	4	5	6	7	8
1 SBLOCA	3.2E-3	AC-91	EHR on SS	9.9E-11	6.7E-9	8.8E-9	<1
		AC-92	EHR on SS	1 8E-13	8 8E-11	8.8E-11	2.7
			ECC	2.4E-8	1.4E-7	1.4E-7*)	52
2 MBLOCA	1.0E-3	AC 91	ECC	2.6E-10	2.7E-8	2.7E-8	1.3
		AC-92	ECC	5.4E-17	5.4E-12	5.3E-12	<1
			ECC	7.5E-9	4.2E-8	4.2E 8*)	15 0
3 LBLOCA	1.0E-3	AC 91	ECC	9.3E-8	3.2E-7	3.2E-7	15
		AC-92	ECC	1.7E-17	1.7E-12	1.7E-12	<1
			ECC	2.5E-9	1.4E-8	1.4E 8*)	5 2
4 SGTR	1 0E-3	AC 91	EHR on SS	4.8E-9	3.0E-8	4.7E-8	2
		AC-92	EHR on SS	1.3E-10	7.9E-10	7.9E-10	25
			EHR on SS	1.3E-10	7.9E-10	7.9E-10*)	<1
5 LOOP	4 4E 2	AC 91	EHR on SS	3.3E-9	4.3E-8	3.2E-7	15
	4.4E 2	AC-92	EHR on SS	1.8E-10	2.3E-9	2.3E-9	72
	7 0E 3		EHR on SS	1.0E-8	7.0E-8	7.0E-8*)	26
6 LOHR on SS	1 0E 1 (24 h)	AC 91	EHR on SS	3.0E-9	1.6E-7	1.3E-6	66
	1.0E-1 (24 h)	AC-92	EHR on SS	1.2E-15	4.5E-13	1.4E-11	<1
	3 0E 2 (720 h)		EHR on SS	7.6E-15	2.14E-12	6.2E-12*)	<1
All IF		AC 91	24 h	1 1E-7	5 9E-7	2.1E-6	100
		AC 92		3.0E-10	3.2E-9	3.2E-9	100
		AC 91	720 h	-	-	-	-
		AC-92		4.4E-8	2.7E-7	2.7E-7	100

*) For mission time 720 h

As is shown in Table 3.2. core damage frequencies for the NPP-92 project do not depend on human errors during accident management activities because of the use of active and passive systems that do not require personnel actions. Table 3.2. also shows that core damage frequencies for the NPP-92 project increase almost by two orders of magnitude with the increase of operation time following the accident from 24 to 720 hours. This is explained by the fact that during this period of time core collant inventory is maintained by active systems in case of primary circuit leaks.

In conclusion it should be noted that preliminary PSA-1 for WWER -1000 NPPs that have been performed by now show the contributions of major IEs to the cumulative core damage frequency for all Power units. Full-scale PSAs are required to evaluate the actual values of these parameters.

4. PSA Problems

The following problems have to be solved in order to perform full-scale PSAs:

4.1. Reactor-specific databases on component reliability, CCF model parameters and personnel reliability shall be developed on the basis of collected and processed data from the operating NPPs.

4.2. Complete lists of internal and external IEs for the standardized nuclear power units under operation and design shall be prepared.

4.3. Russian advanced technologies shall be developed or Western ones shall be acquired and mastered, including:

4.3.1. PSA procedure for external IEs (seismic effects, aircrash, etc.);

4.3.2. Procedure for modelling civil structure and containment reliability for various conditions, including severe accidents.

4.3.3 Combined PSA-2 and 3 procedures.

4.3.4. PSA procedures for on-site fires and floodings

4.3.5. Procedure for the reliability analysis of passive components (pipelines, vessels, heat exchangers).

4.3.6 Digital process control system reliability analysis, including software reliability analysis and CCF analysis.

The majority of the above problems are beginning to be solved and further progress in these spheres requires help and support from the World Community. We think that certain support can be supplied by IAEA in the form of materials on the above topics that are available or being prepared now, and wide involvement of Russian organizations in IAEA PSA programs.

REFERENCES

1. Общие положения обеспечения безопасности атомных станций при проектировании, сооружении и эксплуатации (ОПБ-88) ПН АЭГ-1-011-89. Энергоатомиздат.

2. Основные принципы безопасности атомных электростанций. Отчет международной консультативной группы по ядерной безопасности. Серия безопасности N 75 INSAG-3. МАГАТЭ, Вена, февраль 1988 года.

3. IEAE-TEC DOC-508.Survey of ranges of component reliability date for use in probabilistic safety assessment. 1989.

4. A.D.Swain and H.E.Guttemann. Handbook of Human Reliability Analisis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278, US. Nuclear Regulator Commission, 1983.

5. J.k.Vaurio. A procedure for parametric common cause failure assessment proposed for IAEA project RER/9/005. IAEA, Vienna, 1990.

THE BARSELINA PROJECT, A MULTILATERAL COOPERATION BETWEEN LITHUANIA, RUSSIA AND SWEDEN

Status report phase 2

E SÖDERMAN
ES-Konsult AB,
Stockholm, Sweden

G. JOHANSON
IPS AB,
Stockholm, Sweden

E. SHIVERSKIY
RDIPE,
Moscow, Russian Federation

D. WILSON, A. ENERHOLM, P. HELLSTRÖM
RELCON AB,
Solna, Sweden

Abstract

The Barselina Project was initiated in the summer 1991 The project is a multilateral cooperation between Lithuania, Russia and Sweden with the long range objective to establish common perspectives and unified bases for assessment of severe accident risks and needs for remedial measures for the RBMK reactors. The Swedish BWR Barseback is used as reference plant and the Lithuanian RBMK Ignalina as application plant The Barselina project cannot be looked upon as a traditional PSA, scope and objectives of the PSA activities are modified according to the general objectives PSA is in this context used as a tool to achieve this common understanding between the project parties. This report constitute a status report for phase 2 of the Project prepared in August, 1992, to be presented at the IAEA Technical Committee Meeting in Budapest September 7-11, 1992

PROJECT OBJECTIVES AND GENERAL DESCRIPTION

<u>General project objectives</u>

The long range objective is

- to establish common perspectives and unified bases for assessment of severe accident risks and needs for remedial measures

Immediate task Objectives are

- to carry out a pilot study providing preliminary, scoping assessments of risk and a proposal for additional stages in achieving above long range objective

- to evaluate currently employed general approaches, methodology and available data bases, related to the reliability of RBMK components and systems, in regard of weaknesses as well as of usefulness for the purpose of RBMK safety analysis

Specific Russian and Lithuanian objectives

The primary objective with conducting PSA, the Ignalina 2 PSA, is to assess the level of plant safety and to identify the most effective areas for safety improvement In more specific terms this objective include the following activities

I Identification of dominant accident sequences
II Identification of systems, components, human interaction important to safety
III Assessment of important dependencies
IV Identification and evaluation of (new and old) safety issues
V Decision support on backfitting of generic and plant specific items

Specific Swedish objectives

On the Swedish side additional objectives can be formulated as follows

- to enhance the knowledge and understanding of RBMK features so as to allow own independent evaluations of safety issues and operational events of RBMK reactors

- to enhance the knowledge and understanding of RBMK features so as to contribute to the international project "Safety of Design Solutions and Operation of NPPs with RBMK Reactors"

- to develop Swedish PSA analysis competence and to document principles of quality assurance for PSA implementation

Project Plan

The project plan is generated based on the IAEA Guidelines for conducting PSA

The parties participating in the project are

- From Sweden ES KONSULT AB, IPS AB, RELCON AB, Sydkraft Konsult AB, ABB Atom AB and Studsvik AB

- From Russia The Research and Development Institute of Power Engineering RDIPE The Kurchatov Institute and the Russian Federation Regulatory Body

- From Lithuania The Ignalina Nuclear Power Plant and The Lithuanian Energy Institute of Kaunas (former Institute for Physical and Engineering Problems of Energy Research, IPEPER)

In general the methodology of the I2/PSA follow the format of a Swedish PSA This approach is based on small event tree and large fault trees

Definition of Scope

In brief terms the scope can be defined as

The source of radioactivity
- The reactor core

Final consequence of accident
- Core damage (local or global)

Operational states included
- Full power

Initiating events included
- Internal initiating events (transients and LOCA)
- Internal hazards (fire)

Special issues
- The human interaction modelling will be performed in detail and the main categories of human interaction will be include in the plant models However the quantification will be limited to conservative screening and the use of best estimates will be limited to a few important actions

- The dependency analysis will include a rigor analysis of all types of dependencies

- Uncertainty and sensitivity analysis will be performed in both a qualitative and quantitative manner The use of conservatism will be evaluated and controlled through the sensitivity analysis

- The time duration of the analysis following the initiating event will initially be one (1) day This limitation will be evaluated and removed if shown necessary

The project will run for a period of two years and be split into three phases

Phase 1 Familiarization and Mini-PSA

This phase will include the familiarization and structuring of a limited number of safety systems and one single initiating event October 1991 to end march 1992, closing with Working Group Meeting in Ignalina March 31 to april 4th 1992

Phase 2 Limited level 1 PSA

This phase will include principal System Analysis for all important safety systems and extension to several initiating events but excluding external events and limited treatment of human factors April to december 1992 closing with a seminar in Stockholm scheduled to early december

Phase 3 PSA Level 1 extended in selected areas

This phase will extend the Level 1 PSA in areas selected during phase 2 Even for this phase the aim is not to perform a full scope PSA analysis December 1992 - october 1993, closing with a joint seminar place and date to be decided

PSA Team Training

Training of the Russian and Lithuanian PSA teams will be performed at the Ignalina plant in the project PSA course, in Sweden by Russian and Lithuanian engineers participating in the Swedish working groups for periods of two to six weeks The training consist of work with the Ignalina plant modelling, the Risk Spectrum Code and the TSEBA code for parameter estimation under supervision of senior staff

PLANT MODEL GENERATION

Initiating Event Selection

The definition and categorization of initiating events includes three major tasks The work preformed up till this point deal with the first two of these tasks

- to review the plant design to determine what failure and transient events that can occur that could possibly lead to severe core damage

  to determine plant specific conditions created by the failure or transient event

The initiating transient event screening analysis has been presented The listing comprises events covered in EPRI s list of both BWR and PWR transients and also contains the events listed by Polyakov and Shiversky as RBMK type reactor initiating events

The initiating event screening cover the following main areas

LOCA event screening
Primary circuit event screening
Power conversion system event screening
Protection and reactivity control event screening
Electric power event screening
External and support system event screening

The end product of this task is a list of initiating events (IEs) that is as complete as possible

Grouping of Initiating Events

When the plant system requirements has been assessed the Initiating Events can be grouped in such way that all events in the group impose essentially the same success criteria on the systems as well as the same special conditions (operator challenge, automatic plant response e t c) and thus can be modelled using the same event/fault tree analysis

A set of initiating events are suggested for event tree analysis The initiating event list below define 6 transient events 3 blockage events and 15 LOCA events (if S3 are excluded or collapsed with S2) At this point are the CCI events not included

Transients

TM	Manual Shutdown with all main functions available
TS_{AZ}	Normal Scram with all Main Functions available
TS_{FAS}	Fast acting Scram with all Main Functions available
TT_{AZ}	Normal Scram with Turbine trip and by pass failure or steam dump to condesers
TF_{AZ}	Normal Scram with Loss of feed Water
TE_{AZ}	Normal Scram with Loss off-Site Power

Circulation blockage

PCB_1	Primary circuit blockage One to three pressure tube riser
PCB_2	Primary circuit blockage Four or more pressure tubes
PCB_3	Primary circuit blockage Blockage of GDH upstream ECCS mixer i e blockage by pass is possible

Loss of Coolant Accidents

The categorization of LOCA events reflect guillotine ruptures characterized by four different sizes The size categories are then represented by 5 different zones that characterize the LOCA event by the location of the rupture

A Large LOCA (d>300mm)

A 1	Zone 1	Inside the primary circuit confinement before (upstream of) the Group Distribution Header check valve
A 2	Zone 2	Inside the primary circuit confinement after (downstream of) the GDH check valve
A 3	Zone 3	Inside the reactor cavity
A 4	Zone 4	Outside the primary circuit confinement on the primary circuit side of isolation check valves

A.5 Zone 5: Outside the primary circuit confinement, on the secondary side or interfacing system side of isolation check valves.

S1: Medium LOCA (100<d<300mm)
S1.1, S1.2, S1.3, S1.4 and S1.5 defined with the same zones as above.

S2: Small LOCA (50<d<100mm)
S2.1, S2.2, S2.3, S2.4 and S2.5 defined with the same zones as above.

S3: Very small LOCA (d<50mm)
S3.1, S3.2, S3.3, S3.4 and S3.5 defined with the same zones as above.

Common cause initiators:

Common cause initiators are not included at this stage, a CCI screening analysis will be performed when a plant model exists.

Accident Sequence Modelling

As first step is it necessary to identify all safety functions needed for preventing core damage. The safety functions of the Ignalina NPP has been identified. Normally, in swedish PSAs, the plant model is concentrated on the main functions, i e front line systems functions and include these as main headings in the event trees. All support functions, including alarm signal generation and power supply are normally modeled with fault trees which are transferred to from the front line system (the safety systems) fault trees. Presented in Table 1 are the proposal for safety functions and system relationship to be used for the Ignalina NPP PSA model. The relationship applies between the main safety functions identified above and the systems available for performing these functions:

The required safety function has been illustrated by functional block diagrams for successful accident protection. For each IE the safety functions that need to be performed in order to prevent core damage are identified. A preliminary set of plant function block diagrams for successful event response has been generated in the first phase. This work will be an object for plant operator review of the plant behaviour as modelled.

Qualitative accident sequence analysis, event trees, has been performed. This work presents event descriptions for the functional events contained in the accident sequence analysis and their success criteria.

A Level 1 PSA usually implies the assessment of plant failures leading to severe core damage and of corresponding frequencies. Additional events, however, that may be appropriately included in a Level 1 PSA are those that involve partial core damage or potential, conservatively assumed, core damage. There are several possible "degrees" of core damage. It should be emphasized that the final result greatly depends on the definition of what constitutes a core damage.

Table 1

Safety function	Front line system
Reactivity control	1) Reactor Control and Protection System 2) Control Rods
Confinement and core cavity integrity	1) Pressure Suppression System 2) Core Cavity Pressure Relief System
Primary circuit pressure control	1) Condenser and the BRU-K Valves (turbine bypass) 2) BRU-B valves (condensation pool relief valves) 3) Main Steam Relief Valves
Core cooling - core injection, drum separator makeup and heat removal	1) Pressurized Tanks (ECCS) 2) ECCS Pumps 3) Auxiliary Feedwater System 4) Main Feedwater System
Residual Heat Removal	1) Blowdown and Cooling System

The following definitions of hazards states are proposed for this phase. The analysis carried out at this point include detailed investigations, including severe accident process analyses, of define the RBMK core hazard states to use in the analysis. Four core damage categories has been defined with their corresponding probabilistic safety indices (PSIs):

1) Safe heat removal conditions (category S) when the safe operating levels are not violated.

2) Violation of the reactor heat removal conditions (category V). The conditions mean an achievement of such a temperature of fuel elements and their cladding (of one Technical Channel or equivalent number in the core) at which the cladding failure and fission product release into the coolant are possible. One pressure tube rupture or blockage is also included into this category. At the same time there is no transition to catastrophic accidental processes, the geometry of the reactor components and the core is preserved. This category can be treated as a "mild consequence".

3) Reactor core damage (category D, or "medium" consequence) These conditions are characterized by the severe accidental processes caused by their significant deviation from the design scenario The final reactor states can lead to partial fuel melting, fuel/cladding damage in 1 2 GDH technological channels, several pressure tube rupture at low pressure

4) Reactor core severe accident (category A) accompanied by multiple pressure tube rupture (MPTR) at high pressure or core fuel melting This category is characterized by multiple PT rupture leading to raising of reactor upper plate at high pressure or melting of a part or all the core (the most heavy consequence)

For the hazard states of type V and D radiation consequences must be estimated with account of accident localization system (ALS) operation For the category A ALS will turn out be ineffective

Correspondence between RBMK core hazard categories and International Nuclear Event Scale (INES) Levels can be presented approximately as follows category V can be referred to Levels 3-4, category D corresponds to Levels 5-6 and category A - to Levels 6 7

The core hazard states due to the development of accident event sequences resulting in conditions of V, D and A type, were determined by process analysis (within the framework of design safety analysis and special PSA 1 RBMK investigations) including the extrapolation of obtained relationships as well as by expert estimation method with a required margin

Proposed criteria to assign consequence hazard categories on the base of process analysis results are presented in Table 2

Table 2 *Criterias to assign core hazard states*

Channel Power MWt	First criteria t(PTwall) > 600°C		Second criteria t(cladding)		
	Low Pr	High Pr	<1200°C	>1200°C	>1500°C
29 20	S	V	S	V	D
<20	V	A	S	D	A

Notes

1 S safe state
V core cooling violation
D core damage
A severe accident
t temperature
Pr pressure

2. When two criteria are applicable, the more severe must be assigned

3 Channel power range shows a number of technological channels that are undergoing identical conditions

Systems Modelling

System analysis will be performed using fault tree technique A project report specify the specific procedures and requirement to fulfil this task A demonstration of the system analysis for the Auxiliary Feedwater System, Emergency Core Cooling System, Main Relief Valve System and Emergency Power Supply System has been carried out in the first phase This work will be a major task to continue in the second phase Currently a number of system analyzes are in progress and there are still more systems to initiate

Human Performance Analysis

This task will be limited to screening analysis The PSA model will concentrate on identifying the critical element of humnn interaction Five categories/types of Human Interaction will be addressed and modelled separately in the plant models The complexity and difficulties of addressing the Tvpe 4 ictions may lead to that these will not be addressed properlv

Type 1	Operator inadvertently disable equipment maintenance, testing or calibration errors
Type 2	By committing error plant personnel initiate an accident
Type 3	Operator fails to terminate the accident by following procedures and operating stand by equipment
Type 4	Operator aggravates the situation by making errors when attempting to following procedures and operating stand-by equipment
Type 5	Plant personnel fails to improvise or restore and operate initially unavailable equipment to terminate the accident

In the quantitative screening evaluation will conservative values (0,1 0,01) be assigned For dominating human interactions identified in the screening, can additional analysis be performed in a third phase to create a balance in the accident sequence results

Qualitative Dependence Analysis

The qualitative dependence analysis shall identify dependencies for the main types of dependencies Functional Physical and Hum in interaction dependencies

1 Functional dependencies due to shared equipment or process couplings.

2 Physical dependencies.
a) Caused by the initiating event, CCI.
b) Caused by environmental stresses.

3 Human Interaction dependencies.
a) Cognitive behavioral induced.
b) Procedural behavioral induced, multiple maintenance errors.

Preparation for plant visit done, qualitative dependency forms have been filled out, additional questions necessary.

Initiating Events Frequency Assessment and Component Reliability Assessment

The IE frequency assessment will follow that of the Swedish I-book, including a plausible learning model. Available data sources are currently reviewed. If plant specific component reliability data, or RBMK specific, can be obtained the data assessment will be based on this data. The assessment procedure will follow that of the Swedish T-book.

SUMMARY

A number of systems are by today modeled but still remain several central systems to model. A larger portion of the system analysis task than initially planned has been performed in Moscow and Ignalina/Kaunas. The qualitative part of the initiating event analysis and the qualitative part of the accident sequence analysis has been performed and are presented in draft project reports. This work will be an object for plant operator review and is a central part of the August project meeting agenda.

Even if no quantitative results exist a this point the work is proceeding as planned. The possibilities seems good that during this year or early next year the objective to make initial plant applications using a basic PSA model will be fulfilled.

SAIS APPLICATION TO WWER REACTORS

J. RUMPF
TÜV Norddeutschland e.V.,
Hamburg, Germany

Abstract

The paper presents recent developments in the area of computer information system SAIS to be used in preparing PSA as well as to provide aid in safety related operational decision making. The basic aims, methodology and applications of the system are briefly described. Specific practical applications to WWER reactors including Greifswald , Kola, Stendal and Zaporozje NPPs are mentioned. Capabilities of the SAIS to be available by the end of 1993, at its final state, are also described.

1. Introduction

The Safety Analysis and Information System - SAIS - has been developed since 1989. The following overall objectives of SAIS were defined:

- to provide an adequate tool that can be used to prepare PSA, ecspecially "living PSA"
- to aid operators with safety information that can be used to make their operational decision more reliable.

Based on these objectives several reference applications of SAIS are under work. The aimes of these analyses are:

- to develop SAIS methodology as well as to demonstrate its applicability to different types of NPP
- to prepare safety information needed for PSA
- to give insights in the safety status of NPPs.

Special VVER applications were started to Greifswald (VVER-440/V213), Kola (VVER-440/V213), Stendal (VVER-1000) and Saporoshje NPP (VVER-1000).

This paper presents

- shortly the main features of SAIS and
- a description of the subjects of SAIS application to VVER reactors.

As general results of applying SAIS to VVER-440/V213 reactors it was found that

- SAIS methodology is able to map VVER structure and safety information very well and

- because of its special features SAIS is able to provide aid not only on what information is needed to perform PSA but also on what information is necessary to operate the plant and how this information can be appropriately structured and displayed.

2. SAIS methodology

SAIS, applied to a NPP, comprises

- a data base that combines all features of a NPP that are important to safety as well as
- a plant-specific probabilistic safety assessment based on the current plant status (living PSA).

The data base includes

- a definition of safety important features,
- the possibility to appropriately select safety relevant information,
- a computer-aided structuring, processing and displaying of this information.

The living PSA tool allows the user to conveniently perform periodic safety evaluation as it is required for every German NPP about every ten years.

In addition processing of information within SAIS makes the PSA and its results more transparent compared to known PSA documentation.

SAIS is based on a data form approach. It is structured in five information levels:

- event tree data level,
- event tree functions data level,
- system data level,
- component data level,
- event data/probabilistic data level.

(As an example three typical data forms are attached to this paper.)
For a more detailed description of SAIS methodology see e.g. /1/.

3. VVER application

SAIS VVER application started in 1991.
A first analysis of Greifswald unit 5 NPP (Germany VVER-440/V213, shut down state) demonstrated the applicability of SAIS to VVER reactors.

Other applications were started for Stendal NPP (Germany, VVER-1000, taken out of construction) and Saporoshje NPP (Russia, VVER-1000, in operation).

As a main part of the project SAIS is being applied to Kola NPP (Russia, VVER-440/V213, in operation).
A working group of specialists from Kola NPP and TÜV Norddeutschland was founded to perform the analysis. It was agreed upon that the main part of the analysis has to be done by the plant personel.

The following objectives were defined for SAIS VVER application:

- development and testing of SAIS with respect to specific VVER features
- utilization of SAIS to improve the operational procedures and safety documentation of VVER reactors
- trainig of the operators to improve their comprehension on what is important to safety, to enable them to select the appropriate safety information and to adequately use SAIS soft- and hardware
- preparation of generic information that can be used by other VVER plant personel.

The SAIS VVER project is based on experiences gained from VVER construction and operation in both Russia and Germany. The following institutions take part in SAIS cooperation:

international: Kola NPP (Russia)
OKB Hydropress, Podolsk (Russia)
Scientific nad Engineering Centre of the regulatory body, Moscow (Russia)

national: TÜV Norddeutschland, Hamburg
Gesellschaft für Anlagen- und Reaktorsicherheit (GRS), Berlin/Cologne/Munich
Ingenieurgesellschaft für technische Sicherheit (IGTS), Berlin
RISA GmbH, Berlin.

The subjects covered by the Kola project can be seen from the table.

As a first reference example a SBLOCA was chosen.
In addition the following initiating events are being analysed for Kola NPP:

- steam generator tube rupture (more than one tube) or
- steam generator collector break
- loss of off-site power

- leakage of connection lines to the primary circuit from outside the confinment.

SAIS will be applied at a full-scope level for these initiating events (PSA level 1) includung all information levels of the system

Table: SAIS Kola project

Application of SAIS to Kola NPP (VVER-440/V213)	Genric results applicable to other VVER NPP	Compariosn of safety documentation
Reference: SBLOCA	establishment of a general data base	exchange of safety documentation of Kola and Brokdorf NPP
other initiating events	reference list of initiating events	comparison of scope, contents and depth of both safety documentations
data base of plant-specific data	generally applicable results	safety documentation requirements from SAIS
software and hardware training of Russian specialists		
establishment of necessary hardware conditions in Kola NPP		

A generic reliability data base for VVER-440/V213 is planned to be established based on the following data sources:

- plant-specific data of Kola NPP
- data of Greifswald NPP
- other sources, e.g.
  other Russian NPP and
  international VVER data bases.

In additon to these analyses a comparison of operational procedures and safety documentation of Kola and Brokdorf NPP is being performed. The concept for this task is given by SAIS methodology.

4. Final remarks

The SAIS VVER project will be finished by the end of 1993. At the final state SAIS application to VVER reactors will provide

- a computer tool that is able to perform PSA level 1 for VVER reactors based on an updated plant status as well as to aid operators in their operational decisions
- information on the safety status of Kola and Saporoshje NPP
- information on operational procedures and safety documentation of Kola NPP with respect to safety
- generic safety information on VVER reactors that can be used by other utilities (e.g. probabilistic data, reference list of initiating events, success criteria of safety systems).

REFERENCE

/1/ Experiences from the Development and Application of the Computer Code System "Safety Analysis and Information System" (SAIS)
Balfanz, H.-P. and Musekamp, W. ; 3rd TÜV-Workshop on Living PSA Application, Hamburg 11-12 May 1992

SAIS	System Specification	SS
	System code: System name:	

	E.T. heading	related min.red.	AOT	referen-ces
01 High pressure injection				
02 High pressure inj. switch off				
03 Accumulator injection				
04 Accumulator switch off				
05 Low pressure injection				
06 Low pressure recirculation				
07 Pressure decrease, spray system				
08 Pressure decrease, condenser				
09 Pressure barrier against p. c.				
10 Confinement				

Important system parameters	normal	min	max		Refe-rences
		level			
HP-tank				mm	
Accumulator				mm	
LP-tank				mm	
		flow rates			
HP-pump				m³/h	
LP-pump				m³/h	
Spray pump				m³/h	

System interfaces	System functions

TÜV-N. worked out: verified:
Revision: modified: verified:

SAIS	Component Specification		Valves, general		KS SA

Name:
Group code: Fault tree name:

System code:YC System functions	ope-ning A1	keep open A9	clo-sing A2	keep closd A0	cage inte-grity M3	con-trol A3
01 HP-injection						
02 Switch off HP-injection						
03 Accumulator injection						
04 Accumulator switch off						
05 LP-injection						
06 LP-recirculation						
07 Pressure decrease, spray system						
08 Pressure decrease, condenser						
09 Pressure barrier against p.c.						
10 Confinement isolation						

System related design data and features	AS : Pressure /bar/: Nom.diam. : Temperature /°C/: Accident proved: Valve housing protection: _ yes _ no Valve locking: Position: Room :	
Component related design data and features	Valve type: ND: Name: Manufacturer: Material: Pressure/bar: Temp./°C/:	
	Actuator type: Name: Manufacturer: Travel time /s/: Control mode / torque/Nm/ Open: _torque _limit switch Closed: _torque _limit switch	
Operational mode	Basic position: Operating cycles:	

TÜV-N. worked out: verified:
revision: modified: verified:

SAIS	FMEA Description				KM 1/2

Name: FT denotation:
Component group code:

System function code	Failure code	Failure effect	Description of the failure effect with respect to the system function

TÜV-N. made by: verified by:
Revision: modified by: verified by:

WESTINGHOUSE PSA ACTIVITIES FOR KOZLODUY (UNITS 1-4)

F.P. WOLVAARDT
Westinghouse Electric Nuclear Energy Systems,
Brussels, Belgium

Abstract

Brief overview of current PSA activities carried out by Westinghouse for Kozloduy (units 1-4) within the framework of "WANO Six-Month Programme for Kozloduy". The main project tasks are described and the methodology followed in the study is presented. The project covers several areas. It includes review of the Greifswald PSA with respect to applicability of the models and the results of this study to Kozloduy NPP. Some work is also discussed concerning reliability analysis for some safety systems that may contribute to overall plant safety. Another important task addresses probabilistic evaluation of pressurized thermal shock. Recent developments on WWER-related model for the MAAP code severe accident analysis programme are also mentioned.

1. Introduction

Westinghouse PSA activities for Kozloduy are performed as part of the first WANO Six Months Programme for Kozloduy. As the work is still in progress, the purpose of this paper is to give an overview of the activities and the methodology followed, without any presentation of results. Westinghouse is acting as overall project leader, while use is made of Eastern European subcontractors. The project consists of four main parts :

- review of the Greifswald PSA,
- reliability study of critical safety systems for Kozloduy,
- initial steps toward a probabilistic Pressurized Thermal Shock evaluation, and
- the preparation of an input parameter file representing Kozloduy for MAAP severe accident analysis program.

Each of these items are discussed in more detail below.

2 Review of Greifswald PSA

The Level 1 PSA for Greifswald was initiated in 1989 and finished at the end of 1990 This study was done in response to a request by the former State Board of Nuclear Safety and Radiation Protection The goals were to establish the then current status of the plant in order to identify weaknesses in the plant design and operation, developing a decision aid for the ranking of backfit proposals, and to illustrate the improvement in safety as a result of the backfit measures The study was performed by the Berlin branch of Energiewerke Nord AG

The first objective of the review of the study is to provide an overview covering the methodology and scope used, the fault tree analysis code developed for the project, the initiating events, the accident sequence analysis, the system reliability analysis, the database, and finally, the results and conclusions

The second objective is to identify the main design differences between the Kozloduy plant and the Greifswald Unit 1 The Kozloduy Units 1 and 2 are VVER 230 reactors (like Greifswald Unit 1), while the units 3 and 4 contain design features found in the VVER 213 plants The main differences for Kozloduy Units 1 and 2 lie in the main steam isolation system and the service water system For Units 3 and 4 the differences in addition to those for Units 1 and 2 include a low head safety injection systems Based on the identified design differences, an assessment will be made as to the applicability of the initiating events, the event trees, the system reliability analysis, the data base, and the results and conclusions to the Kozloduy plant The general insight gained during this study is expected to be useful for identifying possible backfit measures for the Kozloduy units

The third objective of this review is to identify all the accident sequences in the Greifswald PSA that could lead to pressurized thermal shock

3 Reliability Analysis for Critical Safety Systems

The reliability of three safety systems (the high pressure safety injection, confinement spray, and emergency feedwater systems) will be determined in the unmodified configuration The objective of the analyses is to determine the dominant causes for system failure, and thereby any weaknesses in these systems Standard fault tree modelling techniques will be used The dependent failure analysis will include the dependence of front line systems on support systems The support systems will be introduced explicitely into the fault trees

Generic data will be used for the quantification of human error, while the generic IAEA VVER database will be used to quantify the fault trees As far as possible, available Kozloduy data will be included

This work is performed in Bulgaria by a subcontractor, allowing the transfer of technology to the subcontractor The insights gained from the Reliability studies of the Greifswald PSA will be fed into this study

It is expected that this work would give valuable insights into the reliability of these systems for VVER 230 reactors in general

4 Probabilistic Pressurized Thermal Shock Evaluation

A probabilistic thermal shock (PTS) evaluation consists of two main parts a broad scope and a narrow scope evaluation The objective of the broad scope evaluation is to identify the dominating initiating events and accident sequences using event tree analysis and probabilistic fracture mechanics The narrow scope analysis consists of a detailed investigation of the dominating sequences using thermal hydraulic and deterministic fracture mechanics methods This approach is necessary as the systematic event tree analysis can literally identify thousands of accident sequences and it is not practical to do a detailed investigation of each

The first step in the broad scope analysis is to identify the initiating event vector A plant event tree and a mitigation event tree is then constructed for the particular nuclear power station The plant event tree models the events occurring after an initiating event that may aggravate the PTS concern of the initiating event Four types of sequences are identified by the plant event tree

- non-PTS initiator remains non-PTS initiator,
- non PTS initiator becomes PTS sequences as a result of subsequent plant failures such as the failure to reseat of a steam dump valve,
- a PTS initiator remains as is, or
- a-PTS initiator is transformed into more severe PTS transient because of system failures

The PTS accident sequences are grouped together in cooldown states. This represents the first "pinch point" in the analysis.

The next step in the broad scope analysis is to construct the mitigation event tree for the plant. The mitigation event tree represents those operator actions and automatic plant responses that can mitigate the consequences of the cooldown sequences identified in the plant event tree (this could be for example the isolation of a steam generator experiencing blowdown). The sequences resulting from the mitigation event tree are grouped together in end states.

The overall process is illustrated in figure 1. The event tree approach is the only systematic approach for identifying all the possible cooldown transients.

The next step in the broadscope analysis is to determine the frequency of each end state, and to characterize each end state using a characteristic final temperature, final pressure, and cooldown rate. Probabilistic fracture mechanics is used to determine the conditional probability for vessel failure given each end state. This allows the identification of the dominating end states for the narrow scope analysis.

The project for Kozloduy involves determining the initiating event vector and and construction of the plant and mitigation event trees in unquantified form. The accident sequences and end states will be identified by qualifying the plant/mitigation event trees for each initiating event.

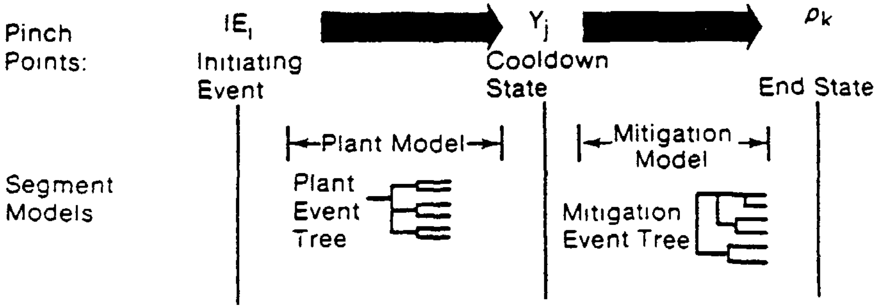


FIGURE 1. : OVERVIEW OF THE ASSEMBLY PROCESS

As no quantification is done, the qualitative results will be valid for VVER 230 reactors in general.

5. MAAP Parameter File Preparation

Westinghouse has developed a model of VVER type reactors for the MAAP severe accident analysis program. The objective of this task is to develop a Kozloduy specific input parameter file. Two test runs (such as a cooldown transient, or a station blackout accident) will be modeled for Kozloduy. A more detailed description of this task can be found in reference [1], a paper presented in the second technical session of this conference.

Reference

Plys, M. G., "VVER Severe Accident Modeling with MAAP 4", IAEA Technical Committe Meeting on Advances in Reliability Analysis and Probabilistic Safety Assessment, Budapest, 1992.

OVERVIEW OF THE PROGRAMME PLAN FOR KOZLODUY-3 NPP PROBABILISTIC SAFETY STUDY

I G KOLEV
Risk Engineering Limited,
Sofia, Bulgaria

Abstract

This paper describes the background, objectives and scope, organisation and time-table of the Kozloduy-3 NPP Probabilistic Safety Study, financed by the Kozloduy NPP Branch of the Bulgarian National Electric Company, and being currently performed by Risk Engineering Ltd

The study is essentially a level-1 PSA with fire hazard and seismic hazard analyses included, as well as extensive thermal hydraulic analysis of plant behaviour under accident conditions for determination of realistic success criteria The organisational scheme includes a site team for gathering of the necessary information in a PSA format and investigation of plant experience and operational practices

A brief outlines of the proposed methodological basis as well as quality assurance aspects are also included The paper ends with the current status of the study

1. Project Background

1.1. Kozloduy-3 NPP

Kozloduy-3 NPP is the newest double-unit plant (units 5 and 6) with VVER-1000 reactors at Kozloduy site, that also accommodates four other units (units 1-4) of older VVER-440 type (see Fig 1) There are no major differences between the two units of Kozloduy-3, accept on component level (some of the equipment is from different suppliers, but of the same design) Unlike the older part of the plant, Kozloduy-3 units are practically stand-alone units with only chemical and some other services being common to both units However, all units at the site share common switchyard attached to three different grids (400, 220 and 110 kV) and common heat sink in the form of inlet and outlet water channels from/to Danube river This do not apply to Kozloduy-3 Essential Service Water Systems, that are provided with spray pools

The plant has been supplied by Russian ATOMENERGOEXPORT and built in 1981-1990 by several Bulgarian organisations under the supervision of ATOMENERGOINVEST - branch of the National Electric Company of Bulgaria (NEC) The plant is operated by EP-2 Directorate of the Kozloduy NPP Branch of NEC Unit 5 is officially in operation since the spring of 1989 (with the average annual load factor of about 0 35) and unit 6 is undergoing the final tests before full-power operation (unit 6 is actually in operation on 50, than 75% power levels since 1990) The total number of reactor-years of power operation is 5, including initial lower level operation

Kozloduy 3 units' main features include

- VVER 1000 reactors, designed by Russian OKB "GIDROPRESS" in early 70-s (reactor pressure vessels produced by SKODA plants in Chehoslovakia) without burnable poisons in the core,
- standardised plant layout, common for most VVER-1000 plants, designed by Russian ATOMENERGOPROEKT,
- four reactor cooling loops (without isolation valves) with horizontal SGs,
- one TG of 1000 MWe,
- 3 independent trains of all active safety feature systems (HPIS and LPIS trains does not have 100% capacity for all LOCA sizes), hydroaccumulators available for core flooding in case of LOCA,
- large dry containment made of pre-stressed concrete with internal steel layer,
- design-basis accidents cover all LOCA sizes and a limited spectrum of transients but feed-and bleed procedures are not explicitly included for accidents with loss of secondary side cooling, no means are explicitly provided for management of severe accidents, FSAR is far from being full and complete according to Western standards,
- nuclear island structures and systems are seismically designed, not all of the balance of the plant is seismically qualified

The operational experience of unit 5 shows quite unreliable operation with low annual load factors and a big number of small incidents Most of the latter may be associated with the initial period of operation but may also be treated as pointers to design deficiencies

The operational documentation management is somewhat better than on older units and some assessment of operational experience is possible for updating of generic data However, the plant design documentation is in formats that require substantial efforts for compilation of the information necessary for PSA system notebooks

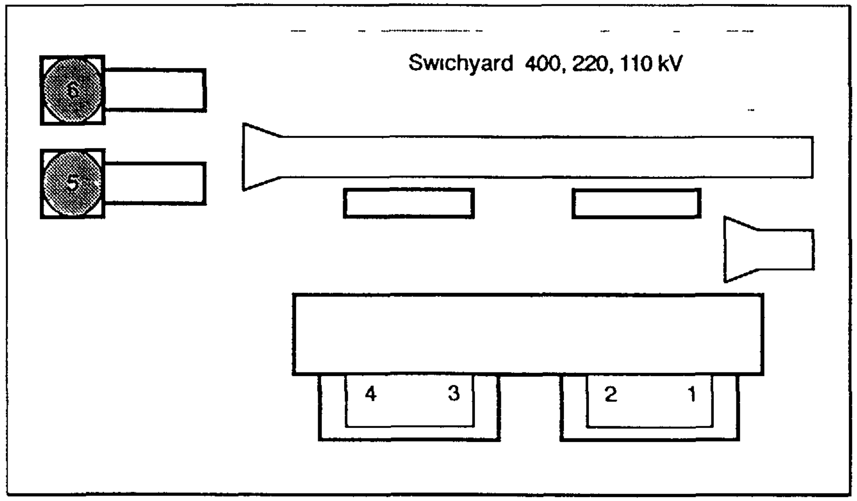


Fig. 1 Layout of the Kozloduy site.

1.2. Project Initialisation

Most of the PSA activities in Bulgaria in past years has been devoted to older units for understandable reasons Recently, the PSA activities for older units are on-going under WANO Six-Months Programme for Kozloduy, sponsored by PHARE Programme of the CEC At the same time, the unreliable operation of unit 5, as well as obvious deficiencies of Kozloduy-3 FSAR leaded to regulatory requirements for upgrading of the existing FSAR, including probabilistic analyses

An important argument for the initialisation of a full-scope level 1 study for Kozloduy-3 has been the fact, that similar plant, that was built in Belene, was cancelled due to public criticism and after an extensive evaluation of the project, done by Bulgarian Academy of Sciences Naturally, the concerns about Belene project were transferred to Kozloduy-3 units There was an obvious necessity for evaluation of plant safety

1.3. Project Financing

Kozloduy-3 PSA has been ordered by the utility, namely the Kozloduy NPP Branch of the National Electric Company of Bulgaria The general specifications and scope, as well as the general time-frame of the study has been initially cleared with the regulatory body - the Committee for Use of Atomic Energy for Peaceful Purposes, as well as with NEC top management

Bids for the study were presented by ENERGOPROECT State-Owned Company, a consortium of Russian organizations, and the newly established private Bulgarian company RISK ENGINEERING LTD (REL) Bids were discussed in detail by a the Technical and Economic Expert Council of the Utility, and the contract was placed with REL for professional rather than financial reasons The contract placement procedure has been thoroughly checked by a special commission from NEC headquarters

The contract provides for a level-1 PSA as described below, and a special annex is devoted to eventual continuation of the study to cover other important issues, as well as to extend it to level-2 and level-3 PSA

2. Objectives and Scope of the Study

2.1. Objectives

General objectives of the Kozloduy-3 Probabilistic Safety Study reflect the reasons for study initialisation as described earlier, and may be formulated in the following way

- the study have to provide input for the upgrading of plant FSAR, according to regulatory requirements,
- a safety assessment of the plant, that is to be used for evaluation of risks and decision making for the operation of this plant and eventually for continuation of Belene project, public concerns have to be answered with an acceptable assessment of the risk,
- the complete study is to serve as a basis for evaluation of different operational issues
- the study is to be used as a base for system reliability improvement as well as for reduction of initiators frequencies,

- the study has to identify any serious plant deficiencies that would eventually require modernizations during next years
- the study has to provide an assessment of the available operational data regarding system and component operation as well as data on incidents

The study objectives have to be achieved in a situation when little is known about the plant behaviour under accident conditions and in multiple failures situations There is no thermohydraulic evidence for realistic accident sequence modelling, nor exact emergency procedures In this situation, most of the necessary thermohydraulic analyses will have to be done within the study, and expert panels are to assess the operator behaviour for realistic results

The study objectives, as defined, cover a broad area, that includes both exact technical analyses and top-level assessments to be communicated to the public, the analyses are to be conservative enough to be acceptable for the no-nuclear-option organizations, and in the same time to provide realistic assessment of system reliability and plant safety, that is later to be used for evaluations of eventual plant modifications

2.2. Scope

The initial scope of Kozloduy-3 PSA has been determined by the regulatory requirements for the upgrading ot plant FSAR In addition, specific PSA issues has been included, as well as the requirements of the Utility The present scope includes the level-1 PSA tasks, as follows

- analysis, categorization, grouping and quantification of initiating events,
- analysis of accident sequences from internal initiators,
- fire hazard analysis and modelling of fire-induced sequences,
- seismic hazard analysis and modelling of seismic-induced sequences,
- thermohydraulic analysis to support accident sequence modelling,
- processing of the available operational experience data,
- quantification of CDF and corresponding fractions associated with IEs, systems etc ,
- evaluation of eventual changes in the technical specifications made during the study period

This scope of the study may be extended during the Study period, depending on additional regulatory requirements and agreements with the utility, as described in Section 2 4

2.3. Limitations

The limitations of Kozloduy-3 PSA correspond to the study objectives, to the international practices in performing of level 1 NPP PSA, as well as to the limited time available to perform the study, limited resources, provided by the utility and the limited man-power available in Bulgaria in the PSA field

General limitations are as follows

- the only source of radioactivity considered as potential danger is the reactor core, consecutively, only core damage frequencies (CDFs) will be evaluated as measure of risk,
- only the normal power level operation considered for initiators application (this includes a spectrum of power levels with normal-operation configuration of plant systems)

- thermohydraulic analyses are to be performed with relatively simple process analysis codes or with simple models to allow for broader coverage of different accident sequences, including those with multiple failures or with different operator action options following the initiator
- a stand alone unit is to be considered (unit 5 chosen as reference), a simplified screening analysis of interdependencies between the two units is to be made and only those dependencies found to be important, are to be included explicitly in the models,
- generally, the possible interdependencies with other plants at the site are not to be considered unless sufficient evidence provided for their importance,
- only fires are to be considered as internal common-cause initiators (CCIs) this do not apply to CCIs in connection with malfunctions of power supply systems,
- only earthquakes are to be considered as external events

Some of the limitations listed will be eventually re-considered during the sudy period as mentioned below

2.4. Project Perspectives

During the study period, especially after the completion of task 1, devoted to preliminary analyses, some modificatons are possible in the study Programme-Plan to broaden the spectrum of investigations done within the study They will depend on the posision of the regulatory body, which is to review the task reports, as well as on the position of international institutions that will be eventually controlling the quality of analyses The modifications may also depend on the resources available to the utility As mentioned in previous sections, such modifications may include

- coverage of all relevant internal CCIs, such as internal floods, missiles etc,
- full analysis of all applicable external hazards, imposed by the near-by industrial activity, severe weather conditions, loss of the ultimate heat sink etc (a non-probabilistic investigation of such hazards has been done last year)

In addition to this modifications, a continuation of the study is possible, according to a special annex to the contract, that describes the tasks for a full-scope PSA (up to level 3) and tasks for a full utilization of PSA results In addition to the tasks, that are part of the present study, the following tasks are also included in that annex

- level-2 accident progression analysis,
- level-3 analysis of societal risks (depending on the availability of PSA studies for older units, this may be done for the site, rather then for Kozloduy-3 plant),
- development of risk-monitoring systems for utility and for the regulatory body,
- compilation of plant-specific data base and re-quantification of the models

According to the recent international interest to the issues of PSA analysis for cold-shutdown and transition power level situations, this issues will be proposed to the utility for inclusion in the present level-1 study

3. Methodology Overview

3.1. General Outlines

The Kozloduy-3 PSA is to be the first VVER 1000 PSA study that intends to follow the existing Western-type PSA methodology The general methodological framework of the study will follow as much as possible the recommendations of the well known NRC publications

"Interim Reliability Evaluation Program Procedures Guide", NUREG/CR 2728, 1983

"Probabilistic Risk Assessment (PRA) Reference Document", NUREG 1050, 1984

"PRA Procedures Guide", NUREG/CR 2300, 1983

with the special attention payd to the more recent

"Severe Accident Risks An Assessment for Five U S Nuclear Power Plants", NUREG-1150, 1990,

and to the recommendations of IAEA in

"Procedures for conducting of Probabilistic Safety Assessments of Nuclear Power Plants", IAEA Safety Practice Series

Compliance with the general recommendations for conducting a level-1 PSA contained in the above documents has been requested by both utility and the regulator in connection with this study

The actual methodological basis for each task is to be developed as part of the study, in accordance with the state-of-the-art in PSA and with study resource and time-frame limitations However, the methodological basis considered initially for different aspects of the study, is briefly described in the following section

3.2. Specific Topics

3.2.1. Analysis of Initiating Events

The IEs analysis started with compilation of generic list of initiators, which has been screened as to their applicability to Kozloduy-3, as well as updated to include specific initiators, found to be important or on request from the regulator The updated list is to be quantified with generic data, and then updated according to the experience in Kozloduy and in other similar plants in Russia and Ukraine

The LOCA initiators have to be initially divided into categories depending on the success criteria and specific VVER 1000 features, including operating instructions and practices The categorisation of LOCAs has also to reflect the possibilities for quantification of the defined categories

The final list of transients after quantification has to underpass a logical procedure for grouping of IEs into categories for further modelling The logical procedure has to reflect the plant success criteria and the safety functions challenged by the IE

3.2.2. Analysis of Accident Sequences

The Accident Sequence Analysis has to be performed by the Event Tree (ET) - Fault Tree (FT) methodology with time-independent yearly-averaged quantification, using small ET - big FT approach whenever possible The ETs are not to be too conservative by inclusion of realistic assumptions based on expert panel judgements, about operator behaviour The operator interactions including recovery actions, will be included in the ETs headings and modelled, depending on their definitions independently, or in combination with the associated hardware faults

The ET headings have to reflect the actual safety functions and system success criteria, rather then generalised system functions This generally leads to several FTs for different functions of the same hardware, and require combining and Boolean reduction of accident sequences to be performed prior to their quantification

The general approach to hardware FTs will be to start with the functional output of the system and move in the direction contrary to the fluid flow for fluid systems or in the direction of power source for electrical chains, and systematically investigating the possible sources of failures in the corresponding system segments

The safety function unavailability models are to include a full-scope investigation of all support systems, including automatics logic and control and instrumentation circuits The FT models will explicitly include different component unavailability contributors as basic events, including those caused by pre-accident human errors or failures to buck-up the automatics signals

The described extensive modelling approach require the corresponding level of detail in the information on systems and their operation and maintenance A PSA-oriented format for system notebooks has been developed and has to be filled with information that is normally located in different departments of Kozloduy-3 plant

The quantification of basic events has to be done with generic data, because of small operating experience in Kozloduy-3, and unavailability of any firm data from similar plants in Russia and Ukraine However, all available data will be used for Bayesian adaptation of generic data, whenever possible

3.2.3. Analysis of CCFs

The analysis of Common Cause Failures (CCFs) will be performed for all similar components located in one or in different trains The CCF are to be quantified with generic data, and the data availability will be the factor to choose between a beta-factor or MGL methods However, the same approach will be used throughout the study The investigation of available documentation on CCF modelling will be done to provide the methodological basis

3.2.4 Human Reliability Analysis

The human interactions, defined on ET or on FT level, as described earlier, will be analysed by the well known Swain-Guttman methodology in one of its simplified versions in order to fit in the time and resource limitations A more extensive investigation including Human Error Trees will be done on final stages of the study of those human interactions, found to contribute significantly to CDF

Generally, the Operator Action Trees are to be modelled for post accident operator actions, leading to sequence change and included in ETs The post accident actions in connection with back up of the automatics will be included in the FTs and investigated in combination with hardware faults as to the availability of sufficient indications for any back up actions A screening investigation is to be done for pre-accident errors leading to component or system unavailability and only those actions will be quantified that would be found to affect the whole system operation or that are not subject of multiple verification by independent personnel

3 2 5 Fire Hazard Analysis

Due to the time and resources constrains, initially only screening Fire Hazard Analysis will be done The fire locations or fire development nodes found to be important for safety in regard to their impact or their probability of occurrence, will be further analysed and quantified to provide input for modification of accident sequences modelled for independent initiators The fire related accident sequences will be modelled as combination of internal ETs and both ETs and FTs are to be modified to reflect the fire-related system and component unavailability

3.2.6. Seismic Hazard Analysis

The Seismic Hazard Analysis is to be performed in parallel with the analysis of accident sequences from internal initiators It will start with the development of the methodological basis, based on the simplified Seismic PRA procedures (NUREG/CR-4331) The earthquake-related analysis is then to be done and the results used for modification and combination of ETs developed for internal initiators The simplified procedures are to be used because of the time constrains for study completion imposed by the regulatory requirements, that in the same time require a seismic hazard to be quantified due to the public discussion over the level of seismic vulnerability of Kozloduy 3 plant

3.2.7. Results Integration

The results of accident sequence modelling and quantification from all IEs have to be processed for determinations of CDF fractions attributed to different IEs, systems, failure modes etc The results have to be presented according to recommendations of NUREG-1150, as well as in a form, that would be more suitable for the general public The importance of IEs, systems, components etc has to be evaluated, as well as uncertainties In addition, the core damage states have to be defined and categorised to prepare input for the eventual continuation of the study to level-2 PSA

3.3. Computer Codes

The available software prior to the study implementation included number of computer codes for FT processing and two public domain integrated ET/FT packages, namely PSAPACK v 4 2 , developed by a team of experts for the IAEA and IRRAS v 2 5, developed by EG&G Idaho, Inc for USNRC (NUREG/CR-2300) The use of the latter one for this study have still to be cleared with NRC The use of PSAPACK is desirable, because of some of its unique features as well as the unique way of its development through the international co-operation PSAPACK features include integrated FT/ET/Data-Base environment, SETS code as FT analyser, Boolean reduction of accident sequences' cut sets, numerous importance measures calculation and many other useful features Some problems has been encountered with the use of the package, but REL intentions are to solve the existing problems, as well as to produce a cyrillic-letters adapted version before the use of the PSAPACK in the context of this study, which is foreseen for the next year This task can be accomplished because REL have the support of PSAPACK authors

The extensive thermohydraulic analyses that have to be done, as well as the short time period, does not allow the full-scope use of RELAP5/Mod2 code, that is available This code will mainly be used for calculations with simplified models, as well as for verification of results in some cases The other available software includes MARCH-3 code, specially modified with the IAEA assistance to describe the VVER peculiarities Problems with this code are in the time-consuming user interface the over conservative results and that this code has been basically developed for level 2 calculations Anyway the MAAP code that is currently widely used for this type of PSA specific analyses up to now can not be provided for the study due to financial reasons

The specialised software for analysis of fire progression and for analysis of seismic vulnerabilities are currently not available, but an investigation is under way as to the possibility to provide such verified codes for Kozloduy-3 PSA study

4. Project Time-Table

The contract for Kozloduy-3 PSA provides only the general time frame for completion of project tasks, namely:

Task 1: preliminary investigations, information gathering and analysis of initiators;

Task 2: analysis of accident sequences from internal initiators;

Task 3: seismic hazard analysis;

Task 4: integration of results.

This time-table is graphically presented on Fig. 2, together with scheduled reviews, which are discussed later.

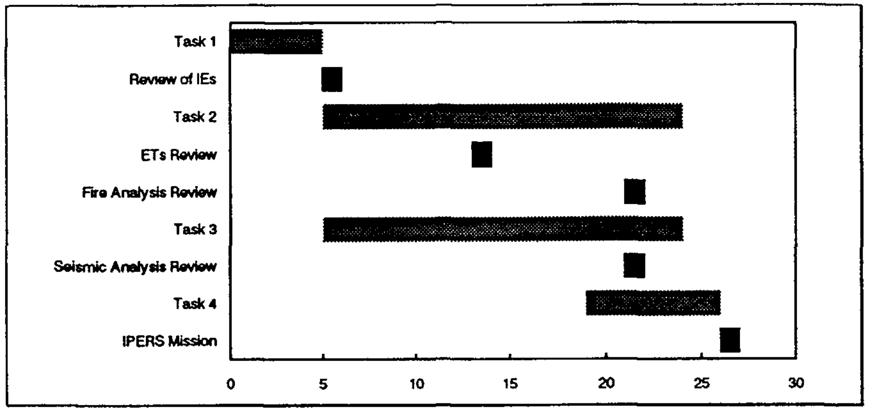


Fig. 2. General Time Frame for Kozloduy-3 PSA (months)

The exact time schedules of Tasks 2 and 3, that consist of multiple sub-tasks, will be presented to and approved by, the utility and the regulatory body upon completion of Task 1. It is only necessary to mention here, that methodological basis for Task 2 (internal initiators) is to be established during Task 1, while the fire hazard analysis methodology will be developed in the beginning of Task 2. Task 3 will also start with methodological study.

5. Project Organisation

Kozloduy-3 PSA is the first major project in the field of energy development of the post-socialist Bulgaria, that has been contracted to a local private company. This fact imposes a big responsibility upon both Risk Engineering Ltd and Kozloduy NPP management. It was agreed with the Utility, that plant personnel have to participate in the study implementation, which is also recommended by IAEA for PSAs for operating plants. The direct participation of the designer has not been planned due to difficulties in contacts with the corresponding institutions. However, REL intends to use the expertise of the Russian personnel that will stay in Kozloduy at least until the official licence is issued for full-power operation of unit 6, and will also try to establish as close as possible cooperation with Russian institutions.

Fig. 3. presents the general organizational scheme for the implementation of Kozloduy-3 PSA. It was considered appropriate that project management will be represented by the REL Managing Director and two Project Managers, responcible for PSA methodology and for plant technology, correspondingly.

The project management will be responsible for contacts with the utility, where a site team has been establish by Kozloduy-3 staff members, coordinated by Engineering Support Department and with members in all major departments of the plant. The site team is to provide the plant and systems

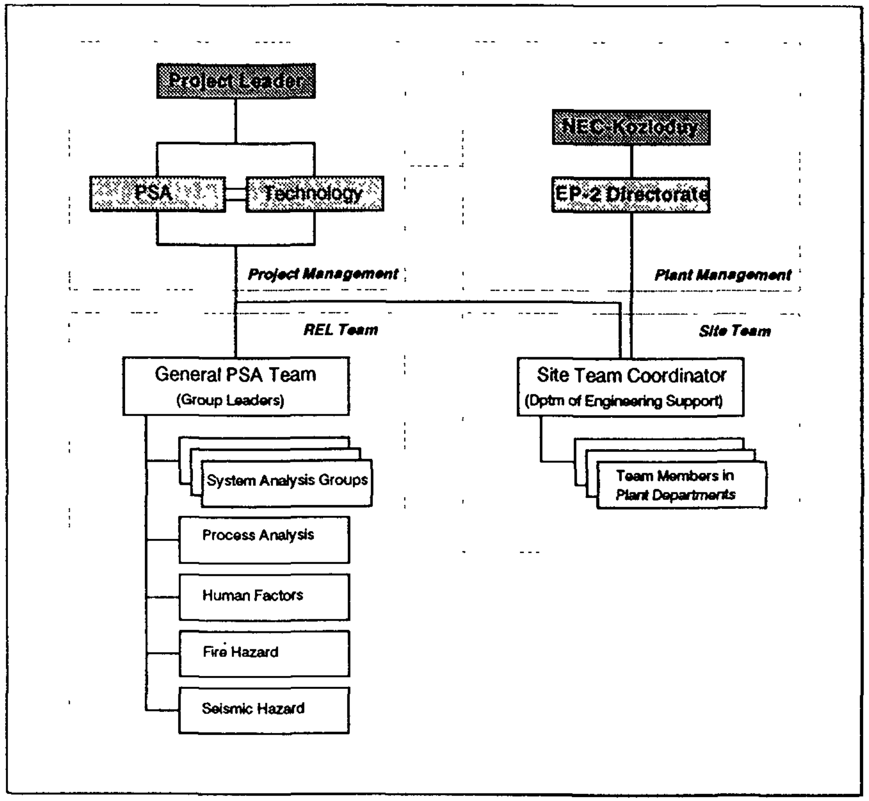


Fig. 3. Project Organization

information in the formats, suitable for PSA related system notebooks, as well as the preliminary processing of operational data on incidents and on component failures The site team is also to review the analyses being done by REL and to provide the necessary technological support

The REL team will be splitted in several subteams, so that the work will be done in parallel This subteams include 3 system modelling groups, process analysis group, as well as human reliability group and fire hazard analysis group Later a seismic hazard analysis group will be formed Each group is to consist of 2 3 engineers, with leaders of all groups forming the general PSA team whose task will be to provide ET modelling and definitions of safety functions and success criteria, as well as to assure the same modelling approaches and assumtions of all groups

Risk Engineering Ltd is the main Contractor for this study, but other organisations are to be involved as sub-contractors depending on the needs (and upon approval by the Utility) The actual organisations have not been included in the project bids because of the many organisational changes that are being currently done in Bulgaria in most state-owned institutions and companies The parts to be sub-contracted may include some thermohydraulic analysis tasks, deterministic fire progression analyses and seismic hazard analysis tasks

6. Quality Assurance

The quality assurance of Kozloduy-3 PSA project is a major issue because this is the first project of such significance that is undertaken by Risk Engineering Ltd since its foundation in 1989

The quality assurance is to be organised on several levels

- REL quality assurance procedures,
- utility participation and reviews,
- reviews by the regulatory body,
- reviews by foreign experts

The REL internal quality assurance organisation for this project includes

- use of well-established and internationally recognised methodological basis and well-known software,
- development of written methodological documents for all major tasks as well as System Analysis Manual to assure unified approach of all groups,
- reviews of all documents developed within a working group by members of another group and approval by project management, in some cases reviews by external specialists are foreseen before approval

The utility participation in the verification of initial information and modelling assumptions is considered to be important especially in cases where information about plant response is scarce or missing Expert panels are to be organised in such cases with REL specialists and utility personnel All partial reports are to be reviewed by the site team, passing through the major departments of the plant, and reports approval is planned by the Technical and Economic Expert Council of the utility

The initial technical specifications of the project tasks as well as any eventual changes are be approved by the Regulatory body In addition, regulatory personnel is to review the partial reports The regulatory body is also to organise the foreign assistance for project implementation by IAEA

The foreign assistance for the project is to consist of two separate types of activities First methodological seminars that are not directly related to the project are to assist both project staff and regulatory and utility staff in gaining deeper knowledge of the up-to-date methodological procedures and developments Second, as part of the reviewing process for each of the major task reviews are to be organised by the regulatory body and IAEA to provide foreign expertise for assurance of the international acceptance of methodological procedures and modelling approaches and assumptions The approximate time schedule of the reviewing process is included in Fig 2 The final report of the study is to underpass an IPERS (International Peer Review Service) mission organised by IAEA

7. Status of Task 1

The Kozloduy-3 Probabilistic Safety Study started at the beginning of June 1992 The Task 1 of the study is to be performed for 5 month, thus the results will be available for review in the beginning of November The status of Task 1 in the end of August 1992 is described below, as well as the results that are expected at the completion of Task 1

- site, plant, and system information formats developed and supplied to the Site Team for information gathering,
- several component information forms developed, reviewed and approved by the Site Team, then integrated in a computerised procedure and supplied to the Site Team (these are eventually to be integrated later with the plant information system that is to be developed under other projects), tasks defined for the Site Team for gathering of component failures data,
- preliminary generic list of IEs compiled, screened, adapted to Kozloduy peculiarities and presented for review to the Site Team,
- investigation of plant experience under way for IEs quantification for frequent initiators, contacts made with Russian and Ukrainian organisations for quantification of internal equipment-dependent initiators,
- investigation for LOCAs categorisation under way, tasks are defined for thermohydraulic analyses for clarification of some LOCA issues,
- logical procedure developed for grouping of transient initiators,
- development of a System Analysis Manual (to include all aspects of system analysis) under way, as well as development of documents describing general PSA methodology and defining ET analysis approaches, preliminary work started for development of methodological basis for Fire Hazard and Seismic Hazard analyses (this work is to continue at the beginning of Task 2)

The final full list of initiators will be supplied to the regulatory body for review and approval in the beginning of October By the end of October, the categories of IEs to be modelled with ETs are to be defined, as well as Methodology Overview prepared The site and plant information is to be compiled, including general system dependencies matrix and general plant success criteria as well as the system notebooks basic information, so that this documents would be extensively reviewed before the ET modelling starts

The first draft of the System Analysis Manual, which part of REL internal QA procedures, rather then of the PSA contract, is also to be completed by the end of October, so that the final version, reviewed and approved by REL and project management, will be available in the beginning of 1993

The review of Task 1 report and supporting documentation by the site team and the regulatory body will be done in the beginning of November and final approval of the report by the utility is expected in the middle of November, after that external review is planned by IAEA which is to take place presumably in the beginning of 1993

98

LIVING PSA-RISK MONITOR: CURRENT DEVELOPMENTS

P KAFKA
Gesellschaft fur Anlagen- und Reaktorsicherheit (GRS) mbH,
Garching, Germany

Abstract

The paper discusses the use of PSA model for various types of operational support A distinction between Living PSA and Risk Monitor is highlighted Some examples of such PSA applications are described Specific requirements in the area of computerization are discussed in the context of Risk Monitor tools

1. Introduction

Since the Seventies, Probabilistic Safety Assessment (PSA) has been used increasingly as an important tool in various industries PSA has made enormous strides, and it is clear to e g the nuclear industry, that it provides a beneficial framework with which an analyst can systematically identify specific event scenarios and can quantify the likelihood and consequences of these scenarios Theoretically all scenarios of interest to safety and risk will be considered and can be quantitatively ranked by various importance measures From these ranked measures designers, vendors, utilities and safety assessors are provided with a real basis to balance the different elements contributing to the two main risk components i e likelihood and consequences /1/ These insights are also essential for all type of facilities to minimize investments and operating costs and to maximize plant availability.

PSA strengths are that it is integrative and quantitative, integrative in that it has the ability to consider in one large model the whole system including design, manufacturing and operating elements and quantitative in that sense of addressing in a scientific way consequences, likelihood, and uncertainties associated with the quantification of these risk components

PSA s historical way starts from quantification of the risk level of typical NPPs (WASH 1400) In the mean time PSAs are more and more used to analyze a given plant with respect to a well balanced safety respective risk profile and if needed to eliminate by system changes and/or backfitts the identified weaknesses (NUREG 1150, /2/)

Today, there is a consistent interest to use PSAs as a tool for trending the safety and risk status during the plant operation period and to balance actions during the plant operation with respect to a minimal risk contribution /3/ Operator actions are based on tech specs and manuals which were focussed traditionally uncorrelated on safety and operating aspects only and therefore the plant operation does not follow risk-minimal strategies For these advanced utilization of PSAs additional modelings and a meaningful computerization of a plant specific PSA is needed

Convinced by these summarized benefits the US NRC has been decided to go towards to risk-based regulations In a transition phase all deterministic regulations will be revised in accordance to this new strategy /4/ /5/

2 Living PSA - Risk Monitor - How we should define these key words?

Living PSA and Risk Monitor should be differentiated regarding their objectives

Living PSA Investigation of the Safety/Risk status for a given plant after a given time interval (e g 6 month, year/s) based on an updated plant-specific PSA

Risk Monitor Investigation of the Safety/Risk impact of specific parameters for a given plant at a given time, based on an on-line recalculation of specific values of an updated plant specific PSA

The Living PSA concept does not needs necessarily a fully computerized model Traditional working procedures based on a package of advanced computer codes (e g for event tree/fault tree calculation, data treatment and handling) and an interactive step by step use of these codes can be sufficient

In contrast, the Risk Monitor concept needs definitely a fully computerized model to generate answers for questions interactively at one computer session in a few minutes Its evident, as many as questions raised, as more complex the computerized model would be

Living PSA has the potential to be used for Periodic Safety Evaluation (PSE) by the utility A Risk Monitor has the potential to support safety decisions ad-hoc by the utility and safety assessors It strength is also the potential to study the impact of parameter changes practically on-line and to use this tool as "Safety Optimizer"

For both concepts we need transparent computerized models, an accepted plant-specific PSA and agreed calculation procedures at the computer

The following graphic (Fig. 1) should illuminate the definitions

The main principles of the two concepts are shown in the Appendix, (burimo8 and burimo9)

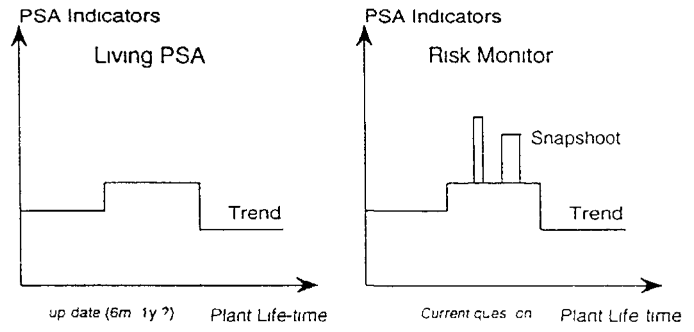


Fig 1 Basic graphic regarding Living PSA and Risk Monitor

3. Examples

3.1 Living PSA

The main aims are to support the safety assessors and the utilities in Periodic Safety Evaluation (PSE). Based on the definition, as stated in paragraph 1, the main objectives are:

Trending of:

- System changes and system improvements
- Backfitting
- Changes in operating procedures
- Changes in test, maintenance, and repair strategies
- Aging and wear-out of components

In the specification of the SAIS (Safety Analysis and Information System) System, sponsored by BMU in Germany, it is lead down that this system will be finally a tool for Living PSA application /6/. The main project runs from 1990 till 1992. A feasibility study and a test phase for a specific plant application (Brockdorf, Greifswald, WWER) showed success /7/. The generation of SAIS is supported by utilities, because a great bulk of the stored information will be used directly by the utility for general safety and operating questions at the plant. SAIS runs on a Sun Workstation including full graphic editors for text, flow diagrams, event and fault trees. Conventional programs for fault tree evaluation (e.g. RISA) are integrated.

3.2 Risk Monitor

The main aim is finally the support of plant personnel to take risk-optimal decisions /8/. Development and the initial use for prefabrication of risk-based result can be in the hands of safety analysts and assessors. As defined in paragraph 1, the main objectives are :

Monitoring of:

- Component outages
- System configuration management
- Changes of operating procedures (e.g. AOTs)
- Changes in repair and maintenance strategies (e.g. STIs)
- Aging and wear-out of components

In the framework of the so called "Störfallberatungssystem" (SBB), sponsored by BMFT, a Risk Monitor is under development at GRS. The Risk Monitor will be a stand-alone as well as an integrated module within the SBB. The development will be realized in two steps:

- Risk Monitor without PSA tool box (A)
- Risk Monitor with a PSA tool box (B)

The version (A) will be split up into a DEMO version and a full version. A commercial Expert System Shell (RT Works) on a DEC workstation is used. The development is plant specific; starting on Level 1; based on the PSA for Biblis B /2/. The PSA input should be realized as general as possible to allow the use of the monitor concept for various PSAs. Questioned output (e.g. Importance values /9/) will be calculated on three levels i.e. system function, sequence, and core damage level.

Problems are expected from the facts that the typical PSA work structure, used by PSA analysts (e.g. coding, data handling), is not as consistent as needed in good informative structures for computerization. Therefore many transcodings and interfaces are needed.

Some details coming from the developper`s workbench are shown in the Appendix, (burimo10, burimo11, burimo18)

3.3 Other Examples

Looking into literature /10/ and considering program demonstrations personally seen, one can observe a wide spectrum of activities in the mentioned field. (see also 5. Literature). Some of the available codes or the developments are multi-purpose packages and some of them are more specialized for specific users and their own purposes.

Examples focussed mainly for Living PSA applications are e.g. IRRAS /11/, LESSEPS /12/, RISKMAN /13/, Risk Spectrum /14/, SUPERNET /15/,

Examples of used Risk Monitors are PRISIM /16/ and ESSM /17/. More advanced developments are PEPSI /18/ and LIPSAS /19/.

Additional examples see /10/ and para. 5. Literature

One of the unresolved key issue for Risk Monitor development is the interactive generation of fault trees based on the flow diagram input. First examples of such tools /20/ - successful tested in-house for smaller systems (approx. 50 components) - are available. Thus, it seems to be realistic that in a few years a Risk Monitor will support also the system configuration management on-line with risk-minimal recommendation. In-depth discussion of other issues see also /21/, /19/.

4. Concluding Remarks

In this last paragraph some important issues and statements are summarized:

- For future discussions and developments a distinctions between Living PSA and Risk Monitor would be recommended
- Aims, objectives, utilization and the relevant potential user group should be clearly defined and perhaps by international organisations (e.g. IAEA) guided. It looks plausible that specific aims, e.g. Accident Management Support, need a specific computerized systems. A common basis would be the plant specific PSA

- To practice Living PSA is a consequent ongoing action to support during the whole plant life-time various decision making processes by actual PSA statements
- The strength of a Risk Monitor is the possibility to support practically on-line also plant personnel during plant operation in risk-minimal decision making. Optimization of AOTs (Allowable Outage Times,) or STIs (Surveillance Test Intervals) with respect to minimal risk impact are examples. It is evident that such optimizations can be also "prefabricated" by a Risk Monitor. Shut-down risk should be considered, if such optimizations will take place
- Two examples from Germany are described in more details and examples from other countries are referenced (see 5. Literature)
- Experiences from the ongoing Risk Monitor development show that a computerization of a PSA, performing the Risk Monitor, should go hand in hand. This procedure will be finally more efficient and of higher input quality
- Common for all computerized systems are the facts that acceptance, transparency, easy handling, guidance for input and use and a quality control system is needed.

ACKNOWLEDGEMENTS

The author is greatful to Mr. Lupas, Seel, Wu, Zimmermann wihin the Risk Monitor Team for their useful ideas supporting this paper.

REFERENCES

/1/ P. Kafka
Probabilistic Safety Assessment - Quantitative Process to Balance Design, Manufacture and Operation for Safety of Plant Structures and Systems
SMiRT- 11, Transactions, Vol. M, Tokyo, August 18-23,1991

/2/ Gesellschaft für Reaktorsicherheit (GRS) mbH
Deutsche Risikostudie Kemkraftwerke, Phase B,
Verlag TÜV Rheinland 1990

/3/ P. Kafka
Risikomanagement des Anlagenbetriebs
Atomwirtschaft, atw August/September 1991, p 421-424

/4/ H. Specter
The importance of risk-based regulations to developing nations
IAEA, TCM Meeting Budapest, 7-11 September 1992

/5/ El Bassioni
personal communications at
IAEA, TCM Meeting Budapest, 7-11 September 1992

/6/ H.-P. Balfanz, D. Böhme, S. Dinsmore, W. Musekamp
Safety analysis and information system (SAIS): a software system to support NPP - safety management
Paper, 2nd TÜV-Workshop on Living PSA application, Hamburg, 7-8 May 1990

/7/ J. Rumpf
SAIS Application to VVER Reactors
IAEA, TCM Meeting Budapest, 7-11 September 1992

/8/ G.I. Schueller
Entwicklung auf dem Gebiet rechnergestützter probabilistischer Sicherheitsanalysen
Atomwirtschaft, Februar 1989, P. 91-92

/9/ W.E. Vesely, T.C. Davis, R.S. Denning, N. Saltos
Measures of risk importance and their applications
NUREG/CR-3385, Battelle Columbus Laboratories, Columbus, 1983

/10/ D. Ilberg, D. Lederman
A Review of Computer Programs applied in Level1 Probabilistic Safety Assessment
Paper, PSA '91, Vienna, 1991

/11/ M.B. Sattison, H.J. Reilly
From PRISIM to IRRAS/SARA; Lessons Leamed in Living PSA,
Paper, 2nd TÜV-Workshop on Living PSA application, Hamburg, 7-8 May, 1990

/10/ C. Ancelin, A. Dubreuil Chambardel
From LESSEPS 1300 to the Application of Computerized PSAs to Operational Safety
Paper, PSA `91 Vienna, IAEA-SM-321/62

/13/ PLG
Riskman; The Power in PSA
PR Material, PLG, 2260 University Drive, Newport Beach, CA 92660

/14/ U. Berg
Realization of true living PSA: A challenging software development task
Paper, 2nd TÜV-Workshop on Living PSA application, Hamburg, 7-8 May, 1990

/15/ S. Hirschberg
Applications and implications of the living PSA concept
Proceedings of the 2nd TÜV-Workshop on Living PSA application, Hamburg, 7-8 May 1990

/16/ J.K. Kirkman, J.B. Fussel, D.J. Campbell
PRISIM at Arkansas Nuclear One-Unit 1: Daily in-plant use of PSA Information
Reliability Engineering and Safety System, 22 (1988), p 441-454

/17/ B.E. Horn
The Essential System Status Monitor for Heysham 2 Nuclear Power Station
TCM, IAEA, Vienna 17-21 October, 1988

/18/ K-J. Kim, J. Park
Research Activities for PSA in Korea Atomic Energy Research Institute
IAEA, TCM Meeting Budapest, 7-11 September 1992

/19/ P. Kafka, H. Kunitz
The Use of PC-based Probabilistic Safety Assessment (PSA) Models
Paper, PSA `91, Vienna, 1991

/20/ K. Gullen
PC-FTA
AECL Research, Chalk River, Canada

/21/ G. Apostolakis, P. Kafka, Edts.
The Role and Use of Personal Computers in Probabilistic Safety Assessment and Decision Making
Elsevier, 1990

/22/ C. Ancelin, M. Bouissuo, P. Le, S. De Saint-Quentin, N. Villate
A Living PSA Based on Use of Expert Systems
Paper, PSA '89, Pittsburgh, 1989

/23/ D.L. Batt, Ph.E. MacDonald, M.B. Sattison, W.E. Vesely
Organization of risk analysis codes for living evaluations (ORACLE)
Paper, PSA `87, Zurich, Vol. 2, TÜV Rheinland (1987) p 698

/24/ H.P. Balfanz
Safety information system SAIS, to support NPP safety management
Paper, TüV-Workshop on: Program Systems and Computer Codes for Living PSA Application, Hamburg, September 1988

/25/ J.A.G. Johanson, L. Gunsell, K. Laakso, P. Hellström
Safety Evaluation by use of living PSA and Safety Indicators - current Status and future Development of Models and Tools within the Nordic Project Safety Evaluation, NKS/SIK-1
Paper, PSA `91, Vienna, IAEA-SM-321/59

/26/ J. Holmberg, K. Laakso, E. Lehtinen, G. Johanson, S. Björe
Nordic Survey on Safety Evaluation by Use of Living PSA and Safety Indicators
(NKS/SIK-1), SKI Tech. Rep. 91:3, NKS/SIK-1(90)13 (1991)

/27/ C. Ancelin
An artificial intelligence-based workstation for reliability studies
Paper, 3rd Int. Conf. on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems, IEA/AIE 90, Charleston, July 1990

/28/ A. Mille, E. Niel, S. Ramet
An Expert System for Monitoring Safety of an Automated Production Cell
Paper, Reliability '92, Copenhagen, Elsevier, 1992

/29/ Esko Lehtinen, Pentti Saarelainen
Monitoring of a safety system's unavailability and maintenance performance using LOTI information system and operational safety indicators
Paper, Reliability `92, Copenhagen, Elsevier, 1992

/30/ Jan Holmberg, Gunnar Johanson
Definition of a concept for safety evaluation by use of Living PSA - the nordic project "safety evaluation, NKS/SIK-1"
Paper, Reliability `92, Copenhagen, Elsevier, 1992

/31/ U.-K Erhardsson, Y. Flodin
Momentaneous risk level. PM-project for living PSA
Report PK-79/81, NKS/SIK-1(91)30, Vattenfall, Vällingby, October 1991

/32/ R. Virolainen
Living PSA - A communication tool between regulator and utilities
Paper, 2nd TÜV-Workshop on Living PSA application, Hamburg, 7-8 May, 1990

/33/ Richard G. Parker, Stephen J. Denniss
Towards to knowledge-based support for reliability analysis: the ADVISE system
Paper, Reliability `91, London, Elsevier, 1991

/34/ F.A. Patterson-Hine, B.V. Koen
Object Oriented Fault Tree Evaluation for Quantitative Analysis
In Fourth Conference on Artificial Intelligence for Space Applications, NASA Conf. Publ. 3013

/35/ Sally J. Mennell, David P. Raymond, Alan B. Reeves
Probabilistic Safety Assessment (PSA) Applications using Knowledge Based Systems Techniques
Paper, Reliability `91, London, Elsevier, 1991

/36/ P. Christensen, L. Smith-Hansen, P. Heino, G. Fassera, A. Poucet
The use of Knowledge Bases in Advanced Computer Aided Safety Analysis
Paper, Reliability `91, London, Elsevier, 1991

/37/ A. Poucet
Knowledge Based Tools for Safety and Reliability Analysis.
Paper, Reliability Engineering and Safety System, Vol. 30, P. 379-397

/38/ J.L. Paulsen
A Continuous Decision Support System for Reliability Centered Maintenance Planning
Paper, Reliability `91 London, Elsevier, 1991

102 THE LIVING PSA CONCEPT FOR THE CERNAVODA NPP

I. TURCU, G. GEORGESCU
Institute for Nuclear Research,
Pitesti, Romania

Abstract

Beginning with 1987, in the Institute for Nuclear Research the full scope PSA activity for Cernavoda NPP, unit no. 1 was started. The final goal (the end of 1994) of the study consist of the "living PSA" implementation as an operator-aid computerized system. The system will be used by both plant operation and regulatory, and can be used also by the designer as a design checking tool. The system named COmputerized Risk Assessment system -"CORA", will be developed using expert system and management information systems techniques, the top-level design being already done. The system will be implemented on a IBM RISC 6000 workstation, UNIX environment.

I. Background

In Romania a CANDU-600 type NPP is under construction in Cernavoda, the target date for operation starting being 1994. Beginning with 1987 the PSA activity was started for the first NPP unit using the license documentation. The PSA main objectives are: early design improvements, emergency procedures development, technical specifications development and finally the "living PSA" computerized implementation as an operator aid tool.

Up to now the "limited scope PSA" is finished, e. g. 10 E/T's and about 17 F/T's, the full scope PSA being under development. The "CORA" top-level prototype design was already done, and is in our intention to use the limited scope PSA model to test it, for the beginning on a PC computer.

II. "CORA" functions

The system basic functions consist of:

- Plant risk knowledge monitoring and systematization: This function mainly consist of : accident sequence description and contributions; system, component, human error, test/maintenance and common cause failures .

- Risk-based accident management: The accident management consist of : identify and rank the success paths for the initiating event, ranking the paths according to operator requirements and success likelihood; select the success paths to define accident mitigating actions;

- Risk-based operation applications: The applications that we intend to implement in the system are:

-risk based configuration management;
-risk-focused data collection;
-precursor evaluation;
-risk-based maintenance prioritization;

III. Main features of "CORA" package

The software features include:

-user friendly interface;
-separate evaluation modules for Event/Trees, Fault/Trees, Basic Event Data;
-evaluation/ranking of contributions;
-success paths determination;
-re-evaluation of MCS;
-Event/Tree, Fault/Tree modification;
-report generation;

IV. "CORA" top-level design

Based on defined "CORA" functions and requirements the principle modules and interconnections are:

- interfaces modules with the NPP Dual Computer and Data Collection computers (a), (b) - which automatically update the Plant Status Data Base - PSDB (c) (See fig. 1).

- PSDB - contains information about the plant components that are included in the PSA model and also plant data that are used to define different plant states (pressures, temperatures, etc.).

- interface module between the PSDB and functional modules (e), initiate automatically the proper functional modules for accident management in case of plant incident.

- interface module between PSDB and PSA model - automatically update the PSA model according to the plant status (f).

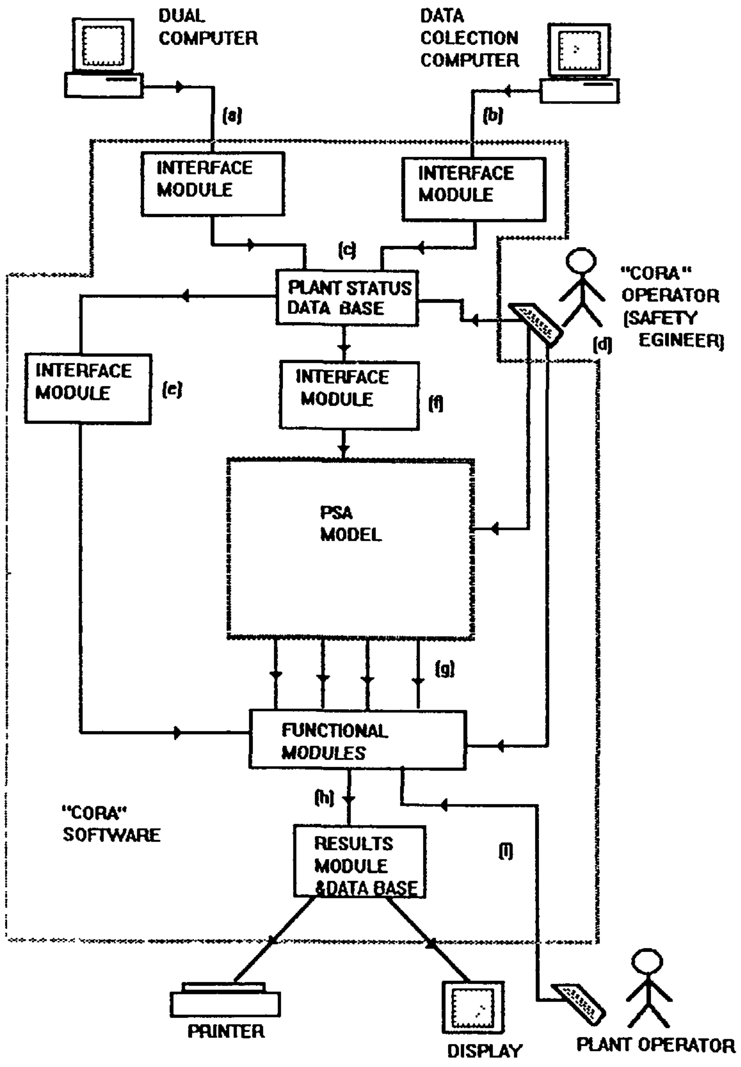


FIG. 1 "CORA" CONCEPTUAL TOP-LEVEL DESIGN

- PSA model - Data Base structure containing the PSA model, including Fult Trees model, components and human error data, accident sequences , etc.

- functional modules - modules that accomplish the "CORA" functions according with the operator requirements (i) and the plant status, using the updated PSA model (g):
  - -risk - monitoring modules;
  - -accident mitigating modules;
  - -PSA applications modules;

- interface module for "CORA" operator - provide facilities for on-line changes of PSDB, PSA model or switch the functions to be executed (d).

- Results module & Data Base - provides results and history storage, shows the processed results on the display or on the printer (h).

V. Operation

The system will be implemented on a IBM RISC 6000 workstation, UNIX environment, being used for operators guiding in plant normal state operation and in case of plant incidents. The system uses on-line data from the plant dual computers and from data colection computers, the PSDB being on-line up-dated.

In normal state, the system monitors the plant global risk and contributions and can be used for risk based configuration management, risk-focused data collection, precursor evaluation and/or risk-based maintenance prioritization.

In case of incidents the system will automatically switch on accident management functions, computing the path-sets and all derived informations, for the giving initiating event and plant status.

The plant operator will be able only to select the proper function according with his necessities, the "CORA" deep level changes being possible only from the "CORA" operator console.

VI. Development

The "CORA" development is part of the CPSE (Cernavoda Probabilistic Safety Evaluation) programme.

The main development steps are presented in fig. no. 2.

1. Principle top-level design, modules design.

2. Implementation of the "CORA" prototype on a PC.

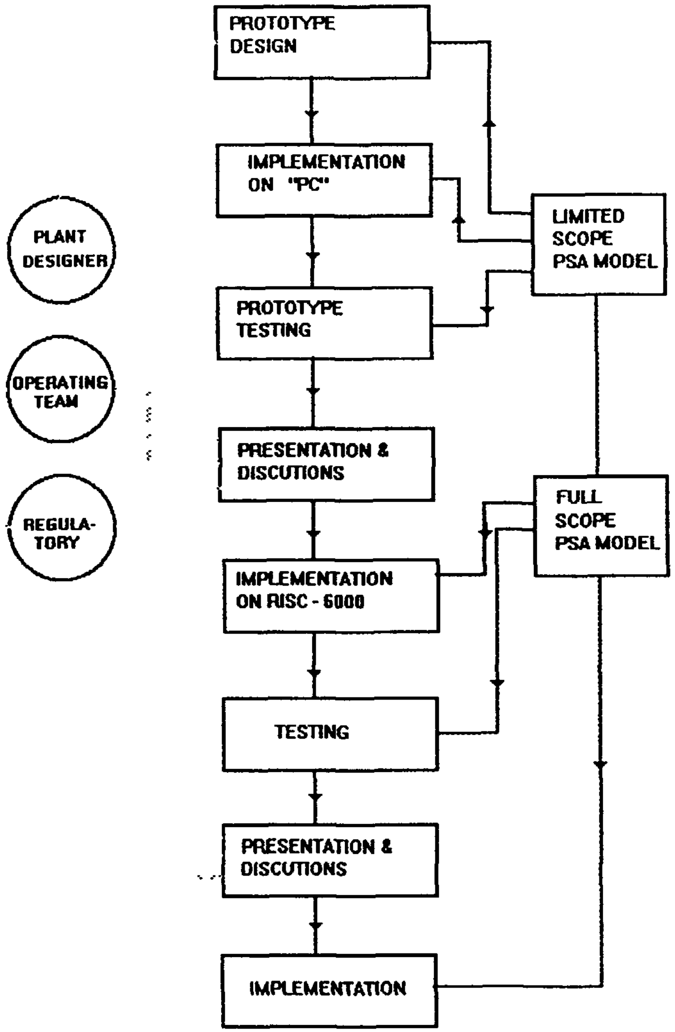


FIG. 2 "CORA" DEVELOPMENT STEPS

3 Intensive testing of the prototype using the limited scope CPSE model.

4. Presentation and discussions with the operating team, regulatory and plant designer.

5. "CORA" interfaces development using the full-scope CPSE model (defining the data necessities and the ways to provide them), final design of the system.

6. Implementation on the RISC 6000.

7. Intensive testing of the system using the full scope CPSE model.

8. Presentation and discussions with the operating team, regulatory body and plant designer.

9. Documentation, validation, operators training and plant site implementation of the system.

REFERENCES

1. *** , CERNAVODA PROBABILISTIC SAFETY EVALUATION - A LEVEL I PSA STUDY, WORKING DOCUMENT FOR IPERS EXPERTS TEAM, OCTOBER 1990.

2. ***, USE OF EXPERT SYSTEM IN NUCLEAR SAFETY, IAEA-TECDOC-542, IAEA, VIENNA, 1990.

3. ***, EXPERT SYSTEMS IN THE NUCLEAR INDUSTRY, IAEA-TECDOC-660, IAEA, JULY 1992.

PRESENTATION AND BASIC APPLICATIONS OF PSA RESULTS

V. HOJNY
Nuclear Research Institute,
Řež, Czechoslovakia

Abstract

Main, esp. graphical ways of the PSA results presentation, which make the results more user-friendly to plant personnel, are shown in the paper. There is described, namely, a utilization of different importance measures for determination of plant features which should be backfitted or maintained when seeking a decrease of the plant risk. Also the basic use of the importance measures for a risk-based improvement of technical specifications is discussed. The practical utilization of the techniques is illustrated on concrete results of the PSA Level-1 Benchmark Exercise carried out at the Nuclear Research Institute within the NPP Dukovany PSA.

1. INTRODUCTION

Probabilistic Safety Assessment (PSA) has already reached a full acknowledgement in nuclear community and there is a number of guidelines for proper conducting the PSA - e.g. [1]. Typical content of PSA reports as it is recommended in the guidelines is, however, aimed mainly at an insurance of proper documentation of the assessment process. The results presented in such a way can be sometimes understood and accepted in assessed plant with some difficulties.

Nevertheless, contemporary computer software - both PSA and general graphics oriented - enables to present the results in much more user-friendly way. The results can be, namely, presented in a form of different importance measures which makes them directly usable for considerations aimed at an improvement of plant safety. The considerations which are well supported by the importance measures include possible changes in plant design and/or procedures, and also in component technical specifications.

The paper presents some general ideas which can serve as an inspiration for ensuring better understanding of the PSA results by a plant personnel. As an illustration there are presented some results of the PSA Level-1 Benchmark Exercise (referred to as "Exercise" from here on) within which a complete assessment of the large loss of coolant accident (LLOCA) has been performed [2]. The Exercise has been carried out at the Nuclear Research Institute within a full-scope level-1 PSA of the Nuclear Power Plant Dukovany, Czechoslovakia (equipped with the VVER-440 V213-type reactors) which is currently being done.

2. MAIN RESULTS PRESENTATION

The main results of the PSA include generally plenty of raw numbers which characterize core melt frequencies for various plant emergency situations. The numbers alone are not, however, too illustrative and a graphical form of presentation is highly recommended. In addition to it, there is also an uncertainty in the absolute numbers and so some relative comparisons are more realistic.

Basic information obtained from the PSA is a comparison of contributions of different initiating events to the total core melt frequency. It is very useful for the plant as it identifies the accidents on which a special watch should be kept and for which good accident-oriented emergency procedures could be really helpful - one of the many ways how to present this information is shown in Figure 1 (the Harvard Graphics has been used to prepare this and all the following Figures). As there are no such results available for the Dukovany plant yet, Figure 1 presents instead the results of a Level 1 PSA of the Loviisa 1 nuclear power plant (also equipped with the VVER reactors) processed on the basis of the data given in [3].

Another piece of information which can be of some use for the plant is a comparison of contributions of individual sequences to the total core melt frequency for given initiating event (or to any other risk measure associated to the initiating event). A rather trivial example is given in Figure 2 where such a comparison is presented for the conditional probabilities of the core melt of the possible event sequences given the LLOCA (Figure 2 and all the following Figures are based on the results of the Exercise [2]). The comparison helps to identify accident scenarios which are especially dangerous and for which a proper training is essential.

Contributions of different types of events considered in the PSA to the risk can be also interesting to the plant personnel (and, after all, to the analysts too, as they assess the influence of some aspects of the methodology used). The event types considered may include, e.g., the influence of common cause failures (CCF) or human errors (HE). As an example, the contribution of the CCF's to the total LLOCA risk is presented in Figure 3. The same information can be derived using some importance measures as it is discussed in the next section of the paper.

The result of the PSA may depend quite substantially on the success criteria used when modeling operation of individual safety-related systems of the plant. The criteria should be determined on the basis of thermal-hydraulic calculations but a number of these calculations has not been performed yet. The problem is usually solved by using conservative assumptions in the model but this policy casts some doubts on the results which can easily over-estimate the core melt frequency. An elegant way how to address the problem is to recalculate the PSA with the conservative assumptions replaced by the opposite, optimistic ones. Hopefully, a small difference in the resulting risk in both calculations enables us to persuade the plant personnel about a low influence of the conservative assumptions used (it may also save a lot of money spent normally on the thermal-hydraulic calculations). When addressing individual assumptions separately, quite a good recognition of the situation can be reached - see Figure 4.

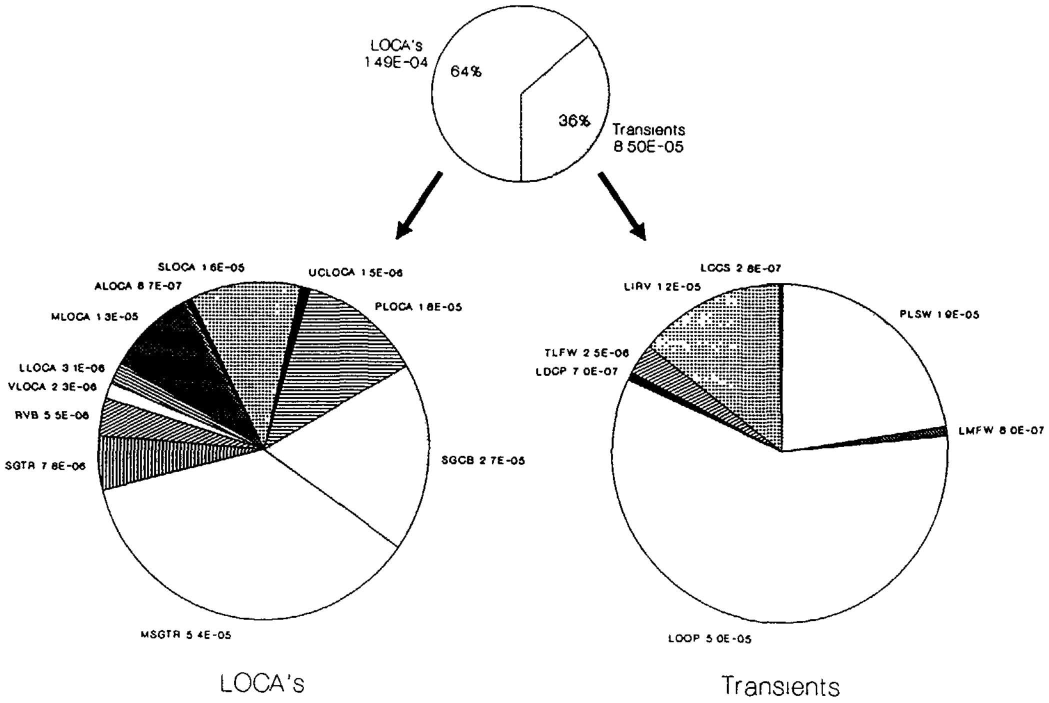


Fig. 1 - Initiating events contributions
(Loviisa PSA)
(CMF = 2.3 x10^{-4} per year)

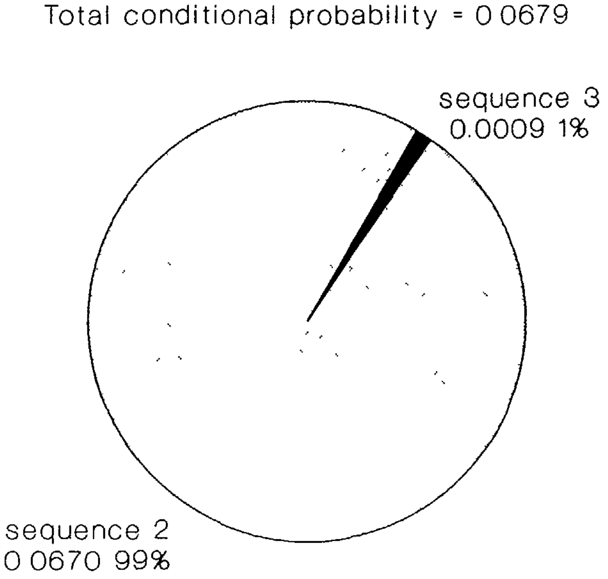
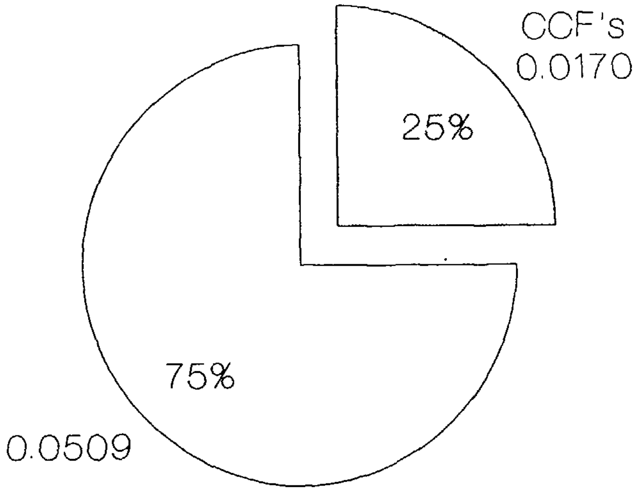


Fig. 2 - Sequence contributions
(LLOCA - Dukovany PSA)

Sequence description:

2 - failure of the low pressure ECCS
3 - failure of the core flooding system



Total conditional probability = 0.0679

Fig. 3 - CCF's contribution
(LLOCA - Dukovany PSA)

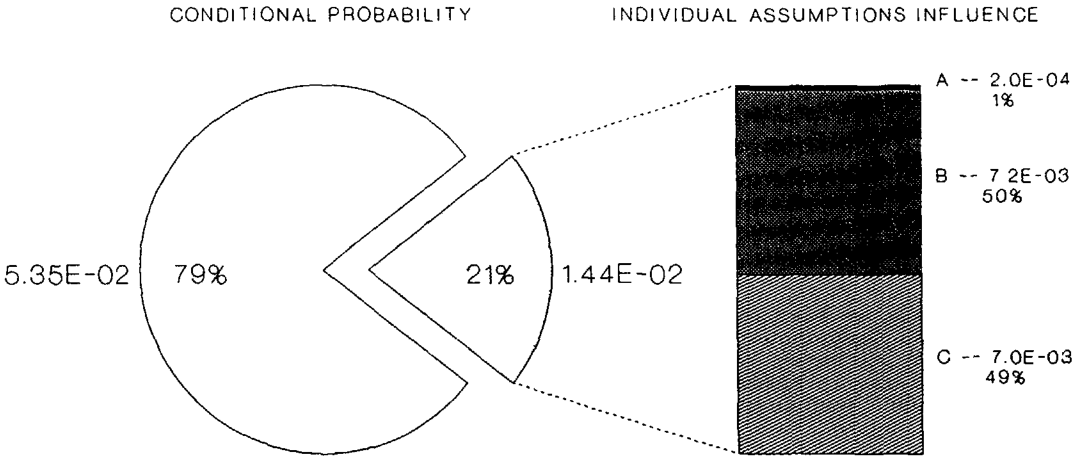


Fig. 4 - Success criteria influence
(LLOCA - Dukovany PSA)
Total conditional probability • 0.0679

A - CFS delivery to both reactor plenums
B - LPS delivery to both reactor plenums
C - closed LPS recirculation piping

3. IMPORTANCE MEASURES AND THEIR UTILIZATION

The risk importance measures are very useful tool of quantification of worth of various plant features impacting risk - as design characteristics or human actions - in both controlling and reducing risk. They can be used to help focus and prioritize efforts in backfitting, reliability assurance, inspection, and general risk management programs. Latest computer codes used for conducting the PSA commonly offer a calculation of some importance measures [4] - other measures can be usually derived quite easily from those known as they are based on the same parameters. The importance measures may be calculated not only for individual primary events but also for selected groups of events addressing thus whole systems and/or safety functions. As an example, some importance measures of the most influential component failures identified in the Exercise are given in Table 1. Besides of importance measures calculation, a sensitivity analysis can be also performed which determines the sensitivity of the results to input data used for primary event quantification; nevertheless, the importance measures and sensitivity are closely correlated and the features with a high importance also display the high sensitivity.

3.1. Risk Control Importance Measures

The risk control importance measures quantify an importance of the feature in controlling the risk level achieved; i.e. the feature with a high value of this measure are of particular interest for risk assurance programs, quality assurance programs, and inspection activities. The measure is generally calculated as the increase in plant risk level if the feature is removed.

Of the absolute measures, a Birnbaum Importance (also called Risk Importance) is widely used. The Birnbaum Importance of

Table 1 - Component importance measures

(LLOCA - Dukovany PSA)

Baseline risk = 6.79 $\times 10^{-2}$

No.	Event Name	Risk Control Imp.		Risk Reduction Imp.	
		B	RCI	FV	RRI
1	LPR3PMR-TH61D01	1.27 $\times 10^{-1}$	2.73	1.44 $\times 10^{-1}$	1.17
2	PES3KEV-LP	1.23 $\times 10^{-1}$	2.73	8.07 $\times 10^{-2}$	1.09
3	PER3DGR-QX	1.36 $\times 10^{-1}$	2.93	7.75 $\times 10^{-2}$	1.08
4	PES3DGS-QX	1.36 $\times 10^{-1}$	2.94	6.01 $\times 10^{-2}$	1.06
5	PEI3DGR-QX	1.34 $\times 10^{-1}$	2.93	4.88 $\times 10^{-2}$	1.05
6	LPS3PMS-TH61D01	1.21 $\times 10^{-1}$	2.73	4.73 $\times 10^{-2}$	1.05
7	PES3KBC-QM1	1.34 $\times 10^{-1}$	2.94	3.54 $\times 10^{-2}$	1.04
8	LP03VME-TH61S09	1.19 $\times 10^{-1}$	2.73	1.88 $\times 10^{-2}$	1.02
9	LP03VMO-TQ63S01	1.19 $\times 10^{-1}$	2.73	1.87 $\times 10^{-2}$	1.02
10	LSS3SIF-QM1	1.34 $\times 10^{-1}$	2.96	1.36 $\times 10^{-2}$	1.01

Note: The events are ranked by their Fussel-Vesely Importances

certain feature simply tells what is the difference in the risk when the feature is removed and when it is optimized, i.e. it can be expressed as:

$$B = R_1 - R_0$$

where B = Birnbaum Importance of the feature,

R_1 = risk level when the feature is removed, i.e. the risk recalculated when the unavailability of the feature is set to 1,

R_0 = risk level when the feature is optimized, i.e. the risk recalculated when the unavailability of the feature is set to 0.

The parameter R_0 can be usually replaced by a baseline risk (i.e. the original risk value) as their values are normally both much lower than the value of R_1 - it is valid especially for the features with the high Birnbaum Importances which we are interested in. In connection with the PSA calculations, the Birnbaum Importance of the feature can be directly calculated as a sum of unavailabilities of the minimal cut sets which contain events related to the feature with the unavailabilities of these events set to 1. There is an important consequence of this relation which should not be forgotten: if the feature addressed is a group of primary events, the importances of different groups cannot be normally just summed up when seeking the importance of a union of the groups because each minimal cut set may contain the events of more than one group. The Birnbaum Importance is especially useful when performing a risk-based optimization of plant technical specifications which is discussed in the next section of the paper.

Of the relative measures, a Risk Control Importance (also called Risk Achievement Worth or Risk Increase Factor) is well known:

$$RCI = \frac{R_1}{R}$$

where RCI = Risk Control Importance of the feature,

R_1 = risk level when the feature is removed, i.e. the risk recalculated when the unavailability of the feature is set to 1,

R = baseline risk, i.e. the original risk value calculated by the PSA.

The Risk Control Importance is very helpful when looking for the features which should be subject of a quality control as maintenance or testing. According to an expert opinion [5], the features with the Risk Control Importance higher than 10 are well worth being concerned about.

As the Exercise has analyzed only one initiating event, it is not a good illustration of the risk control importance measures utilization - the operation of almost all systems involved in an accident mitigation is equally necessary and so no considerable differences in the importances can be observed (cf. Table 1).

3.2. Risk Reduction Importance Measures

The risk reduction importance measures quantify the importance of the feature in further reducing of the contemporary risk level; i.e. the feature with a high value of this measure are of particular interest for risk reduction efforts. The measure is generally calculated as the decrease in the risk level if the feature is optimized.

Of the absolute measures, a Fussel-Vesely Importance (also called Fractional Contribution) is used. The Fussel-Vesely Importance of the feature tells what is a relative contribution of the feature to the total risk. It is calculated as:

$$FV = \frac{R - R_0}{R}$$

where FV = Fussel-Vesely Importance of the feature,

R = baseline risk, i.e. the original risk value calculated by the PSA,

R_0 = risk level when the feature is optimized, i.e. the risk recalculated when the unavailability of the feature is set to 0.

In connection with the PSA calculations, the Fussel-Vesely Importance of the feature can be calculated as a sum of unavailabilities of the minimal cut sets which contain events related to the feature, divided by the baseline risk value. Again, if the feature addressed is a group of primary events, the importances of different groups cannot be normally just summed up when seeking the importance of a union of the groups as the minimal cut sets may contain the events of more than one group.The Fussel-Vesely Importances are very useful when comparing the influence of different features on the total risk. Examples of some uses of the Fussel-Vesely Importance for the PSA results presentation are shown in Figures 5 through 8. Worth noticing is Figure 6 where the Fussel-Vesely Importances for individual systems involved in the accident mitigation are presented - the aggregate Fussel-Vesely Importance of each system can be divided into two parts representing the influences of single and CCF-type events respectively because the CCF's considered always cause a failure of the accident mitigation and so these two groups never overlaps.

Of the relative measures, a Risk Reduction Importance (also called Risk Reduction Worth or Risk Decrease Factor) is well known:

$$RRI = \frac{R}{R_0}$$

where RRI = Risk Reduction Importance of the feature,

R = baseline risk, i.e. the original risk value calculated by the PSA,

R_0 = risk level when the feature is optimized, i.e. the risk recalculated when the unavailability of the feature is set to 0.

The Risk Reduction Importance is generally less nice in distinguishing the importance of the features than the Fussel-Vesely Importance. It is, however, very helpful when seeking a reduction of the risk and looking for the features which should be improved; according to the expert opinion [5], the features with the Risk Reduction Importance higher than 3 are good candidates for some backfitting.

4. RISK-BASED OPTIMIZATION OF TECHNICAL SPECIFICATIONS

When a component of the plant goes down the plant risk level generally increases because of the loss of component function. To keep level of the plant risk, an allowed downtime for each plant component has to be set in plant technical specifications (Tech-Specs). The Tech-Specs control the plant risk by assuring safety-related systems reliability, namely by defining Allowed Outage Times and surveillance test strategies for their components.

4.1. Risk-Based Criteria

Using the PSA results a downtime risk associated with the component outage can be calculated. An integral risk from one downtime of the component called a Single Downtime Risk (i.e. an increase in the plant core melt probability accumulated over the single component downtime), is:

$$R_s = (R_1 - R_0) \times d = B \times d$$

where R_s = Single Downtime Risk,

R_1 = risk level when the component is down, i.e. the risk recalculated when the unavailability of the component is set to 1,

R_0 = risk level when the component is up, i.e. the risk recalculated when the unavailability of the component is set to 0,

d = component downtime,

B = Birnbaum Importance of the component.

The Single Downtime Risk calculated with the help of this equation is somewhat conservative because it includes in the calculated risk levels also the contributions from testing and maintenance of the components which cannot be tested or maintained when the component considered is down even according to the existing Tech-Specs - the error is, however, not too big and can be usually accepted similarly as in PSA studies.

In a "risk-based" approach to the Tech-Specs optimization, some limiting value/values of the Single Downtime Risk have to be set to serve as Criteria for acceptance of an additional risk from the component outage. The simplest possibility is to use a concept of the constant value of this Criterion for all components; this concept is based on the reasoning that an increase in the plant risk would be tolerable for only a limited period of time, while the higher the risk increase the less time the plant could be allowed to continue operation. The absolute value of the Criterion could be easily derived from risk-based quantitative safety goals if they are set for the plant [6]. Nevertheless, there are no such goals prescribed for any of the plants with the VVER reactors yet. A simple solution of the problem was suggested by the expert opinion [5]: to set a relative, plant-specific value of the Criterion at a 10 per cent of the baseline plant risk.

4.2. Allowed Outage Time Optimization

The Allowed Outage Time (AOT) is a maximum time during which the component can be down and its repair or maintenance can be performed. If the component is not brought back to function in the AOT then the plant must take an appropriate action defined at the Tech-Specs - usually go to a shutdown state.

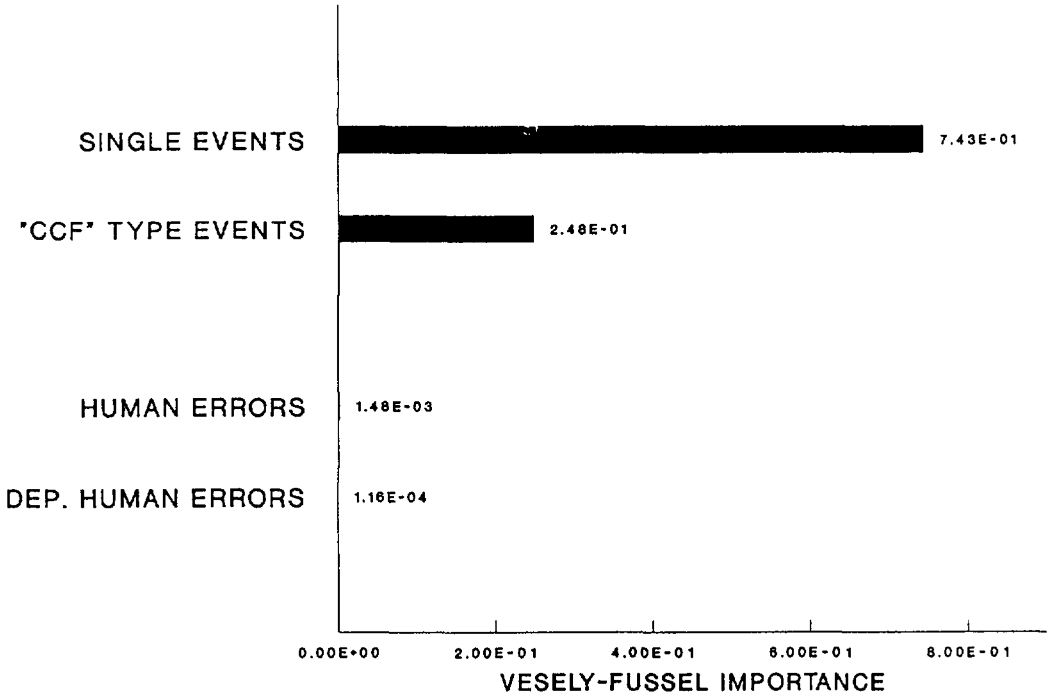


Fig. 5 - Event type importances
(LLOCA - Dukovany PSA)

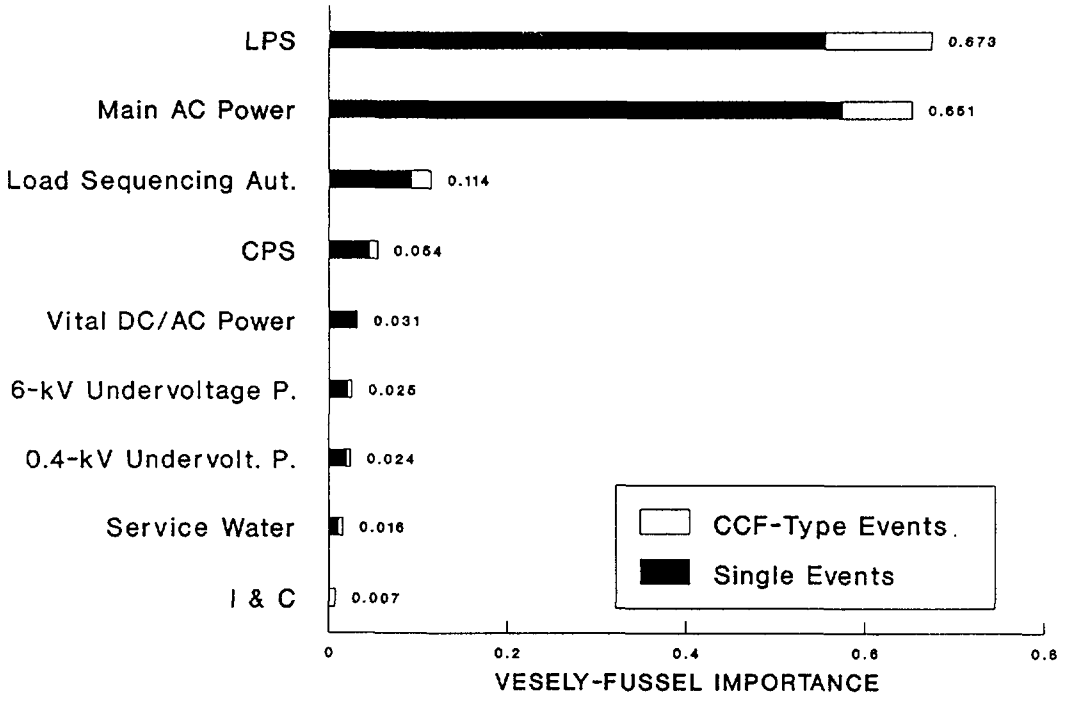


Fig. 6 - System importances
(LLOCA - Dukovany PSA)

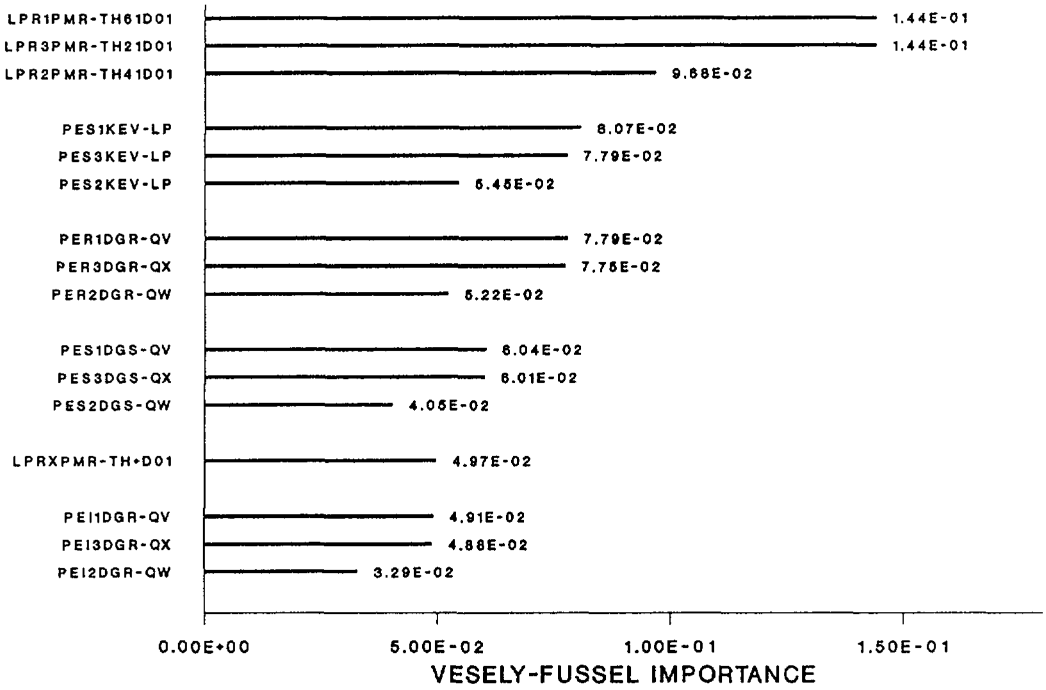


Fig. 7 - Train importances

(LLOCA - Dukovany PSA)

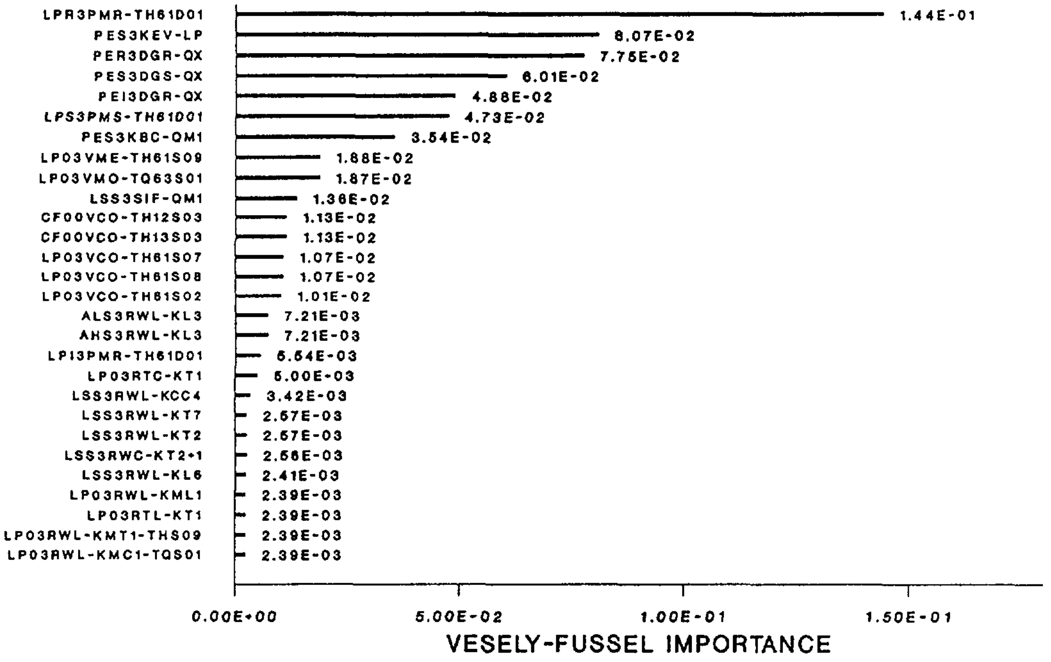


Fig. 8 - Component influences

(LLOCA - Dukovany PSA)

(components of the systems train No.3)

Using the approach described in the previous section and the relative Criterion based on the baseline plant risk, the value of the AOT can be calculated, e.g., in the following ways:

$$AOT = \frac{R}{10\ B} = \frac{1}{10\ (\ RCI - \frac{1}{RRI}\ )}$$

where AOT = Allowed Outage Time of the component,

R = baseline risk, i.e. the original risk value calculated by the PSA,

B = Birnbaum Importance of the component,

RCI = Risk Control Importance of the component,

RRI = Risk Reduction Importance of the component.

The risk-based approach makes the calculated AOT's correlated with the component importances minimizing thus the risk and burden associated to the downtimes. If the calculated AOT is longer than the original AOT set in the Tech-Specs, then there is a sufficient time for component repair. If, on the contrary, the calculated AOT is substantially shorter than the component repair time expected, some steps for improving the plant design should be taken to decrease plant's vulnerability to outages of the component. Unfortunately, as the Exercise has analyzed only one initiating event, it cannot be used as an illustration of the risk-based AOT's setting because almost all the components considered are equally important and their calculated AOT's are too short - the approach can be used effectively just when a complete PSA is performed.

4.3. Surveillance Test Interval Optimization

In order to keep the plant risk under control, the individual standby components of the plant are periodically put to surveillance tests when the plant is in operation. When the periodically tested component fails between tests, its function is lost until the next test and the plant risk increases. The size of the risk increase generally depends on the importance of the component and on the probability that the component is failed. A time period between two consecutive tests is called a Surveillance Test Interval (STI).

According to the expert opinion [5] a simplified approach can be used when determining the optimal STI for the component. The approach employs the same relative Criterion which is used for the AOT calculation; a risk increase associated with a tested component failure between the tests is compared to the Criterion. The value of the STI can be then calculated, e.g., in the following ways:

$$STI = \frac{R}{5\ \lambda\ B} = \frac{1}{5\ \lambda\ (\ RCI - \frac{1}{RRI}\ )}$$

where STI = Surveillance Test Interval of the component,

R = baseline risk, i.e. the original risk value calculated by the PSA,

λ = failure rate of the component,

B = Birnbaum Importance of the component,

RCI = Risk Control Importance of the component,

RRI = Risk Reduction Importance of the component.

The calculated STI is correlated with the component importance and minimizes the burden associated with the surveillance tests while keeping the risk on a tolerable level. The described way of the risk-based STI optimization can be, however, used only when time-dependent causes of the component failure are separated from the causes associated with component failures on demand in the PSA. Besides of the approach described here, some other approaches can be also used enabling, e.g., prioritization of the test activities according to their risk, and/or determination of a test risk-effectiveness [7].

5. CONCLUSION

Results of the PSA can be a very useful tool for the improvement of the safety of nuclear power plants. A proper processing of the results is, however, necessary to make them more ready for a direct use and/or further utilization in consequent calculations. The different importance measures appear to be especially helpful in this respect.

Besides of the simple prioritization of the control and backfitting efforts, the importances are also an essential base for the risk-based improvement of the plant technical specifications. Just the simplest ways of the technical specifications optimization are described in the paper which enable the optimization of technical specifications only for single components. In addition to them namely a risk-based configuration control is highly recommended; it enables to define configurations of component outages which are tolerable when the plant is in operation, and the Allowed Outage Times for these configurations [8]. A benefit from the risk-based approach to the technical specifications is twofold: an assurance that no risky plant state is underestimated, and a minimization of the burden associated with surveillance tests and short time windows for component repairs.

REFERENCES

[1] Safety series report; Procedures for conducting probabilistic safety assessments of nuclear power plants. IAEA, Vienna, 1992.

[2] Hojny V.: PSA level-1 benchmark exercise. Paper on the *Multilateral Symposium on Safety Research for VVER Reactors*. Cologne, Germany, July 7-9, 1992.

[3] Andsten R.S., Vaurio J.K.: Sensitivity, uncertainty and importance analysis of a risk assessment. *Nuclear Technology* 98 (1992), pp. 160-170.

[4] Computer codes for level 1 probabilistic safety assessment. IAEA-TECDOC-553, IAEA, Vienna, 1990.

[5] Vesely W.E.: Lectures at the *Workshop on the Risk-Based Optimization of Tasks and Procedures in Nuclear Power Plant Operation*. Paks, Hungary, March 9-13, 1992.

[6] Atefi B., Gallagher D.W.: Feasibility assessment of a risk-based approach to technical specifications. NUREG/CR-5742, U.S. NRC, Washington D.C., 1991.

[7] Kim I.S., Martorell S., Vesely W.E., Samanta P.K.: Quantitative evaluation of surveillance test intervals including test-caused risks. NUREG/CR-5775, U.S. NRC, Washington D.C., 1991.

[8] Samanta P.K., Vesely W.E., Kim I.S.: Toward risk-based control of nuclear power plant configurations. *Nuclear Engineering and Design* 134 (1992), pp. 355-370.

INTERNAL EVENT ANALYSIS FOR THE LAGUNA VERDE NPP: CORE VULNERABLE SEQUENCE EVALUATION, APPLICATIONS AND INTERFACE WITH CONTAINMENT ANALYSIS

A. NUÑEZ, A. HUERTA
Comisión Nacional de Seguridad Nuclear y Salvaguardias,
Mexico City, Mexico

Abstract

In this paper we present the general methodology used to carry on the Internal Event Analysis for Laguna Verde Nuclear Power Plant (LVNPP), special emphasis was put on the method used to evaluate certain accident sequences. These sequences are the so called "core vulnerable" sequences and are the result of accident sequences where core coling is working but the containment heat removal has failed. In order to preserve the containment integrity the operator is instructed by the emergency procedures to initiate the containment venting. Due to containment venting, a harsh environment will be generated in the reactor building and in some sequences in the turbine building. Simplified boolean equations were constructed for the emergency systems to evaluate the interactions between primary containment venting or failure and continued core cooling injection.

The sequences considerated in this work are the result of the internal event analysis for LVNPP that is under way by the Mexican Regulatory Agency.

We briefly present some forseeable applications for the study and finally, we stress the importance of explicity displayed and covered systems success and failure beyond successful containment venting or containment failure to more easily perform the interface between PSA level 1 and level 2, and the subsequent containment response analysis.

1. INTRODUCTION

The Mexican Regulatory Agency (CNSNS) is carrying on the Internal Event Analysis or LNVPP [1]. The objective of this study is the identification and evaluation of the accident sequences that most contribute to the total core damage frequency. The methodology employed is based on the guides developed in the accident sequences evaluation program (ASEP) as support to

NUREG-1150 [2]. The methodology is focused in areas important to risk and uses simplified techniques in other areas, however, two major expansions of previous BWR event tree work were included in the Internal Event Analysis for LVNPP. The first improvement relates to the formal analysis performed for more systems capable of core and containment cooling. Credit was given for alternate systems which can be used for long term core cooling in some accident sequences. The primary containment venting procedure was also analyzed and included at the event tree level. The second, and more important, improvement relates with the analysis of possible system success or failure paths beyond successful containment venting or containment failure. Therefore, the success or failure probabilities associated with continued core cooling were explicitly and formally analyzed rather than assumed. This second improvement trys to resolve the so called core vulnerable sequences.

In this paper we present a briefly description of Laguna Verde Nuclear Power Plant with emphasis on the safety features of the plant. We also present the major task performed for the Internal Event Analysis for Laguna Verde NPP along with the methodology used to evaluate the core vulnerable sequences. Simplified boolean equations were constructed to evaluate the survivability of injection systems to harsh environment generated in the reactor building as a result of primary containment venting or failure. Finally, we present the way the results and information from the front-end analysis are passed to the back-end analysis through the definition and evaluation of the Plant Damage States, along with the possible applications that we foresee for the Internal Event Analysis for Laguna Verde Nuclear Power Plant.

2. LAGUNA VERDE NUCLEAR POWER PLANT (LVNPP)

The Laguna Verde Nuclear Power plant has two boiling water reactor (BWR-5) units of 1931 Mwt capacity each and is located in Veracruz, México [3]. The plant has several systems capables to supply coolant injection to the core. Two independent cooling methods (flooding and spraying) are provided to cool the core. The high pressure core spray system (HPCS) and the reactor core isolation cooling system (RCIC) are designed to provide coolant to the reactor vessel during accidents in which reactor pressure remains high, on the other hand, the low pressure core spray system (LPCS) and the low pressure coolant injection system (LPCI) cool the reactor vessel when the pressure is low. The automatic depressurization system (ADS) is designed to depressurize the reactor vessel to allow the low pressure emergency core cooling systems inject water to the vessel.

The reactor is housed in a MARK II containment. The containment is a steel-lined reinforced concrete structure. During an accident, steam from the vessel is directed through the SRV's to the suppression pool and to suppress the pressure in the containment, two trains of containment spray are used. The containment spray system is one mode of residual heat removal system (RHR). In the event that RHR fails the containment can be vented.

3. METHODOLOGY USED

The Mexican Nuclear Regulatory Agency (CNSNS) is conducting the Analysis of Internal Event for LVNPP. The methodology used in this study for the estimation of the total core damage frequency is based on the guidelines developed by the Accident Sequences Evaluation Program (ASEP). The first task was the identification of the important initiating events and the plant systems required to respond to these events. The initiating events groups for LVNPP are given in the table I. The next task is the identification of the possible accident sequences for each initiator, this was done using event trees. The philosophy behind the event tree analysis for LVNPP was to depict systems success and failure until it was resolved whether or not core damage occurred, and display the status of other systems sufficiently to describe the PDS. The event tree analyzed display and cover possible systems success and failure paths beyond containment venting or containment failure

TABLE I
LAGUNA VERDE INITIATING EVENTS AND FREQUENCIES

DESCRIPTION	MEAN FREQUENCY (PER YEAR)
LARGE LOCA	1.0×10^{-4}
INTERMEDIATE LOCA	3.0×10^{-4}
SMALL LOCA	3.0×10^{-3}
INADVERTENT OPEN RELIEF VALVE	0.14
LOSS OF FEEDWATER	0.16
LOSS OF OFFSITE POWER	0.135
TRANSIENT WITH THE POWER CONVERSION SYSTEM UNAVAILABLE	4.634
TRANSIENT WITH THE POWER CONVERSION SYSTEM INITIALLY UNAVAILABLE	1.658

and evaluate the possible failures due to harsh environment generated. The success associated with continued core cooling, shutdown cooling (SDC), suppression pool cooling (SPC) and containment spray (CSC) modes of the Residual Heat Removal (RHR) were explicitly analyzed. The typical event tree for the Internal Event Analysis for LVNPP is shown in figure 1.

The next task is the systems analysis, which is used to estimate the failure probability of the front line systems identified in the event tree headings and the support systems required to operate the front line systems. For LVNPP study there are 21 systems models for front line systems and support systems. In this step the analyst selected the appropriate type of model for each system. Four different kind of models were used: detailed fault trees where the modeling was performed at the component with all possible failure modes according with the data base, simplified fault tree where the modeling was performed at the component level but the possible failure were comprised, simplified boolean expression focusing on major failure, and finally for those systems where fault trees were not constructed, actual generic data were used to represent the dominant failure of the systems. The table II shows the systems included in Laguna Verde study along with the type of model used.

Fault trees and event trees were quantified using SETS [4] and TEMAC [5] computer codes. The quantification of the accident sequences was performed using a step-by-step screening approach. Those sequences not eliminated in the screening were fully quantified. The quantification of the survive of systems after containment venting or failures is described in next section.

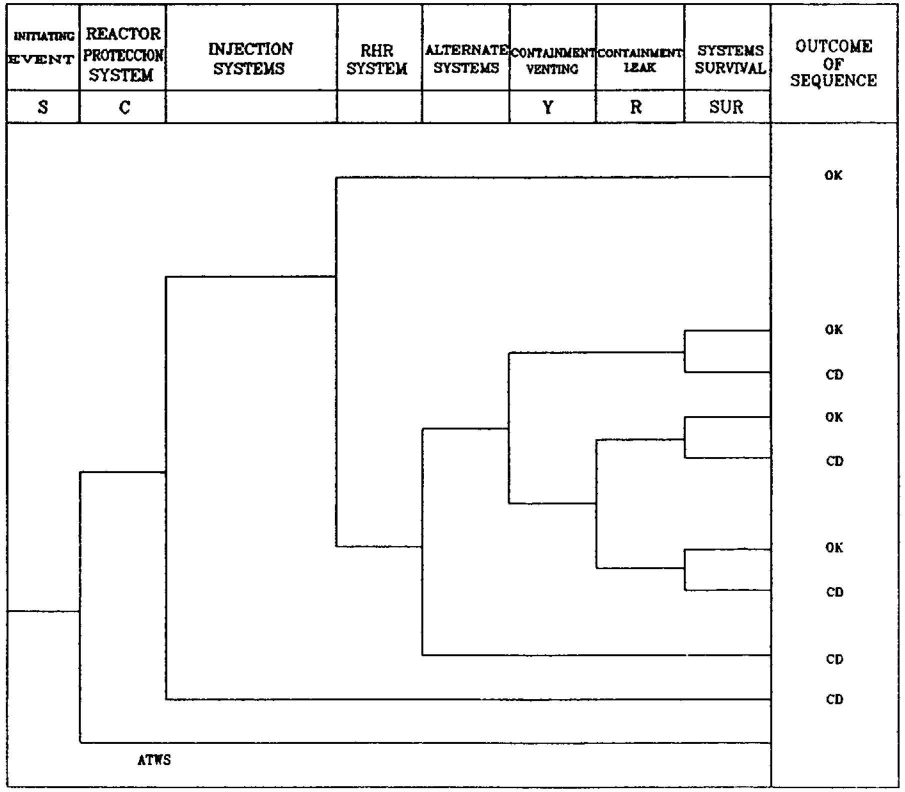


FIGURE 1 - TYPICAL EVENT TREE FOR INTERNAL EVENT ANALYSIS FOR LVNPP

TABLE II
SYSTEMS INCLUDED IN THE LVNPP STUDY

SYSTEM	TYPE OF MODEL
HIGH PRESSURE CORE SPRAY SYSTEM (HPCS)	DETAILED FAULT TREE
LOW PRESSURE CORE SPRAY SYSTEM (LPCS)	DETAILED FAULT TREE
LOW PRESSURE COOLANT INJECTION SYSTEM (LPCI)	DETAILED FAULT TREE
REACTOR CORE ISOLATION COOLING SYSTEM (LPCI)	DETAILED FAULT TREE
AUTOMATIC DESSPRESSURIZATION SYSTEM (ADS)	SIMPLIFIED FAULT TREE
SUPPRESSION POOL COOLING SYSTEM (SPC)	DETAILED FAULT TREE
SHUTDOWN COOLING SYSTEM (SDC)	DETAILED FAULT TREE
CONTAINMENT SPRAY COOLING SYSTEM (CSC)	DETAILED FAULT TREE
CONDENSATE SYSTEM (COND)	BOOLEAN EXPRESSION
FIREWATER SYSTEM (FIRE)	DETAILED FAULT TREE
STANDBY LIQUID CONTROL (SLC)	DETAILED FAULT TREE
PRIMARY CONTAINMENT VENTING SYSTEM (PCVS)	DETAILED FAULT TREE
(NSWLPCI)	
NUCLEAR SERVICE WATER CROSS TIE WITH LPCI	DETAILED FAULT TREE
AC POWER SYSTEM (AC)	DETAILED FAULT TREE
DC POWER SYSTEM (DC)	DETAILED FAULT TREE
HEATING, VENTILATION & AIR CONDITIONING SYSTEM (HVAC)	DETAILED FAULT TREE
NUCLEAR SERVICE WATER (NSW)	DETAILED FAULT TREE
NUCLEAR CLOSED COOLING WATER (NCCW)	DETAILED FAULT TREE
REACTOR PROTECTION SYSTEM (RPS)	GENERIC DATA
POWER CONVERSION SYSTEM (PCS)	GENERIC DATA
STEAM SUPPRESSION SYSTEM (SV)	GENERIC DATA

4. CORE VULNERABLE SEQUENCES EVALUATION

Those accident sequences where core cooling is working but the containment heat removal has failed are the so called "core vulnerable" sequences. The failure of the containment heat removal function results in the heat up and pressurization of the primary containment. Containment venting or failure can occur and steam may be release into reactor building and subsequently in to the turbine building. Boolean equation were constructed for the emergency systems in order to evaluate the survival probability of systems to harsh environment due to steam release. These equations were constructed by examining the systems cut sets with support systems attached, and identifying the dominant cut sets which include those components that could fail to remain operating, for example, motor operated pumps that fail to run, motor valves that fail to remain closed or open, and some associated electrical components. These equations can be used to evaluate the survival of the systems to harsh environment due to containment vented, rupture or leaked. The table III shows the containment failures probabilities, these generic values have been taken of plant whit similar design.

TABLE III

CONTAINMENT FAILURE PROBABILITIES

		PROBABILITY
WET WELL LEAKAGE ABOVE WATER	(WWLAW)	0.1094
WET WELL LEAKAGE BELOW WATER	(WWLBW)	0.0156
DRY WELL LEAKAGE	(DWL)	0.0746
DRY WELL HEAD LEAKAGE	(DWHL)	0.5487
WET WELL RUPTURE ABOUT WATER	(WWRAW)	0.1111
WET WELL RUPTURE BELOW WATER	(WWRBW)	0.0105
DRY WELL RUPTURE	(DWR)	0.0858
DRY WELL HEAD RUPTURE	(DWHR)	0.0442
LEAK TO REFUELING FLOOR	(LEAKTORF)*	0.5487
LEAK TO REACTOR BUILDING	(LEAKTORB)*	0.1996
LEAK IN THE CONTAINMENT	(LEAK)*	0.7484
RUPTURE IN THE REFUELING FLOOR	(RUPTURETORF)*	0.0442
RUTPURE IN THE REACTOR BUILDING	(RUPTURETORB)*	0.2074
RUPTURE IN THE CONTAINMENT	(RUPTURE)*	0.2515

* THESE VALUES ARE OBTAINED BY THE FOLLOWING RELATIONS.

LEAKTORF	= DWHL
LEAKTORB	= WWLAW + WWLBW + BWL
LEAK	= LEAKTORF/LEAK OR LEAKTORB/LEAK
RUPTURETORF	= DWHR
RUPTURETORB	= WWRAW + WWRBW + DWR
RUPTURE	= RUPTURETORF/RUPTURE OR RUPTURETORB/RUPTURE

In order to estimate the probability of each term in the boolean equation it is necessary to generate a set of possible environments at the reactor building, calculating the peak and average temperature in each room, containing the equipment subject to harsh environment for scenarios involving containment venting, rupture and leaked. With the temperature calculated using a reactor building model, for example with MELCOR code, and making use of expert judgment it is possible to determine the failure probability to remaining operating for equipment such as motor pumps, motor valves and associated electric components.

At the present time, we do not have the possibility to use a reactor building model, so we make use of some results for a plant with similar design for the estimation of the probability of each term in the boolean equation.

The boolean equations for the core cooling systems are the following:

FOR VENTING:

```
HPCS-SUR   = KMP004FR-SUR + HMP001FR-SUR + EFN002FR-SUR +
             HT0089FR-SUR + HT0077FR-SUR + SBU1C1FR-SUR +
             STR4C1FR-SUR + ECC002FR-SUR + TBUB18FR-SUR +
             TBU125FR-SUR .

RCIC-SUR   = RTP001FR-SUR + RCR600FR-SUR + MTR4A1FR-SUR +
             ECC004FR-SUR + NBU125FR-SUR + XBU250FR-SUR +
             NBUB30FR-SUR + NBU110FR-SUR + NBUOC5FR-SUR +
             NMC125FR-SUR .

LPCS-SUR   = LMP001FR-SUR + EFN003FR-SUR + LT0061FR-SUR +
             LT0061FR-SUR + MTR4A1FR-SUR + ECC003FR-SUR +
             NBU065FR-SUR + NBU125FR-SUR + NBUB32FR-SUR .

LPCIA-SUR = AMP01AFR-SUR + AT0004FR-SUR + EFN01AFR-SUR +
            MTR4A1FR-SUR + ECC01AFR-SUR + NBU125FR-SUR +
            NBU0C5FR-SUR + NBUB32FR-SUR .

LPCIB-SUR = BMP01BFR-SUR + BT0004FR-SUR + EFN01BFR-SUR +
            PBU1B1FR-SUR + PTR4B1FR-SUR + ECC01BFR-SUR +
            QBUB26FR-SUR + QBUB26FR-SUR + QBU125FR-SUR +
            QBU0C6FR-SUR .

LPCIC-SUR = CMP01CFR-SUR + CT0004FR-SUR + EFN01CFR-SUR +
            PBU1B1FR-SUR + PTR4B1FR-SUR + ECC01CFR-SUR +
            QBU125FR-SUR + QBUB26FR-SUR + QBUB06FR-SUR .
```

FOR RUPTURE:

```
HPCS-SUR-RUP   =  (HPCS-SUR)   * RUPTURETRB
RCIC-SUR-RUP   =  (RCIC-SUR)   * RUPTURETRB
LPCS-SUR-RUP   =  (LPCS-SUR)   * RUPTURETRB
LPCIA-SUR-RUP  =  (LPCIA-SUR)  * RUPTURETRB
LPCIB-SUR-SUP  =  (LPCIB-SUR)  * RUPTURETRB
LPCIC-SUR-SUP  =  (LPCIC-SUR)  * RUPTURETRB
```

FOR LEAK:

```
HPCS-SUR-LEAK   =  (HPCS-SUR)   * LEAKTRB
RCIC-SUR-LEAK   =  (RCIC-SUR)   * LEAKTRB
LPCS-SUR-LEAK   =  (LPCS-SUR)   * LEAKTRB
LPCIA-SUR-LEAK  =  (LPCIA-SUR)  * LEAKTRB
LPCIB-SUR-LEAK  =  (LPCIB-SUR)  * LEAKTRB
LPCIC-SUR-LEAK  =  (LPCIC-SUR)  * LEAKTRB
```

5. APPLICATIONS AND INTERFACE BETWEEN PSA LEVEL 1 AND LEVEL 2

In recent years a number of countries have successfully been using the PSA as a tool that provides guidance to safety related decision-making. As we know plant specific test and maintenance schedule, human errors and common cause failure are considered in the probabilistic models, therefore, the PSA can be applied in many areas.

Among future applications for the Internal Events Analysis for LVNPP are a review of the technical specification (TS). The TS are mostly based in deterministic analysis and engineering judgment. The experience has indicated operational and safety concerns with some of these requirements. Some elements of these requirements may be considered unnecessary or may not be conducive to the safety of the plant.

Other applications for the study will be the risk management. The Internal Event Analysis for LVNPP will provide an integrated framework effective in the evaluating the efficacy of current risk management practices at Laguna Verde. These practices include hardware improvements already made and operating procedures in place. The study also allows the treatment and evaluation of future risk management strategies.

Is important remark the the Internal Event for LVNPP will provide the initial conditions for the subsequent containment response analysis through the definition and evaluation of the plant damage state. The methodology used in the development of the event trees for Laguna Verde provide enough information of the status of the systems in order to properly define the interface of the PRA level 1 and level 2. The interface between the front-end analysis and back-end analysis is performed by grouping of the accident sequences cut sets that have similar characteristics such as vessel pressure, timing and systems availability, thus, the same containment response and radiological consequences are expected [6]. In order to perform the grouping, the back-end analysis develop questions about systems and physical parameters at the onset of core damage. The questions address certain back-end concerns, for instance, coolant make up, releases and retention.

The accident progression analysis starts with information received from the accident frequency analysis (level 1). The results of the accident progressions analysis are passed to the source term analysis (level 2), and consequences analysis (level 3), so it is very important to employ the most appropriate methodology to assure that the information and results from one analysis clarity are received in the next stage.

6. CONCLUSIONS

One of the main purposes of the Internal Event Analysis for LVNPP is to provide the initial conditions for the subsequent containment response analysis. In order to fulfill the above, the accident sequences are followed until the end state is resolved into no core damage or core damage. It is important to remark, that we can not warranty the functioning of the systems subject to harsh environment, so, it is necessary to determine the failure probability of the equipment in order to resolve the accident sequences in all the way to the core damage. In this paper we presented one way to resolve the core vulnerable sequences. The event trees for LVNPP include the feedback effects on the core heat removal systems as result of the containment phenomenology in order to predict if core damage will occur given failure of the containment heat removal systems and the subsequent containment phenomenology.

The above expansion at the event tree level provides in a natural way all the necessary information to define the interface between the front-end analysis and the back-end analysis, and also provides an integrated framework to perform PRA applications such as risk management, evaluation of plant technical specifications and limiting conditions of operations, prioritization of inspection/testing activities, evaluation of operating experience, so on and so for.

REFERENCES

[1] Huerta Alejandro, *et. al.* "Análisis de Eventos Internos para la Central Nucleoeléctrica de Laguna Verde", Comision Nacional de Seguridad Nuclear y Salvaguardias, México, to be published.

[2] U.S. Nuclear Regulatory Commission, "Severe Accident Risk: An Assessment for five U.S. Nuclear Power Plant", Final Report, NUREG-1150, January 1991.

[3] Laguna Verde Power Plant Station Final Safety Analysis Report, Comision Federal de Electricidad, México, 1989.

[4] Worrell R. B., "SETS Reference Manual", NUREG/CR-4213, SAND-2675, Sandia National Laboratories, Albuquerque NM, May 1985.

[5] Iman R. L. and Shortencarier M. J., "A user guide for the Top Event Matrix Analysis Code (TEMAC)", NUREG/CR-5498, SAND86-0960, Sandia National Laboratories, Albuquerque NM, August 1986.

[6] Payne A. C. *et. al.* "Evaluation of Severe Accident Risk: Peach Bottom, unit 2 ", NUREG/CR-4551, Vol 4, SAND86-1309, Sandia National Laboratories, Albuquerque NM, December 1990.

RELATIONSHIP BETWEEN SAFETY CULTURE AND PSA

V. JOKSIMOVICH
Accident Prevention Group,
San Diego, California,
United States of America

Abstract

A primary focus of nuclear safety is prevention of large releases of radioactivity in the case of low probability severe accidents. An analysis of the anatomy of nuclear (Chernobyl, TMI-2) and non-nuclear (Challenger, Bhopal, Piper Alpha, etc.) severe accidents yields four broad categories of root causes, or 4M (abbreviated 4M): man (operating crew response), machine (design with its basic flaws), media (natural phenomena, operational considerations, political environment, commercial pressures, etc.) providing triggering events and management (basic organization safety culture flaws). A strong management can minimize contributions of man, machine and media to the risk arising from operation of hazardous facilities. One way management can have powerful positive influence is through the establishment of a proper safety culture. The term safety culture is defined by virtue of employing IAEA's International Safety Advisory Group (INSAG) and APG's (arrived through work sponsored by the Nuclear Regulatory Commission) definitions. An example of U.S. Nuclear Utility safety culture is discussed. Like any other human endeavor, the manner in which people act is conditioned by requirements set at a top level, i.e., CEO. Policies promoted at the CEO level create the working environment and condition behavior of individuals in the trenches. A summary of the safety culture initiatives within the nuclear utility illustrates commitment to the safety culture. Other powerful examples are the existence of independent safety oversight or risk group directly reported to the CEO and a requirement for submittal of annual nuclear safety assurance reports. The paper concludes by virtue of claiming that an integrated risk management program imbedded in an effective safety culture will lead management of a nuclear utility to achieve both economic and safety goals while reducing strain on management personnel and operating budgets, primarily through an effective integration process.

INTRODUCTION

As a prelude, in setting the stage, it seems appropriate to convey two fundamental APG messages arising from some retrospective examinations; one dealing with the state-of-the-art in nuclear safety and the other dealing with lessons learned from analyses of catastrophic accidents. APG's fundamental message regarding the state-of-the-art in nuclear safety is:

- There is enough hardware in existing Western plants (the failure at TMI was not so much with hardware, as with how the hardware was used).
- The plants are well designed against natural phenomena, such as earthquakes.
- Fire protection standards are adequate in the aftermath of Browns Ferry fire.
- Since TMI accident, readiness of operating crews to handle complex accident scenarios has been greatly enhanced, although more needs to be done.

- The issue remaining is that of Safety Culture (the last frontier in nuclear power plant safety).

- Globally, in the case of Eastern Europe, the issue is how to build a safety culture. For the U.S., Western Europe and Japan, the issue is how to maintain and enhance the existing culture.

Accidents do not "just happen", but are multi-causal or composite events. They are not acts of God, but acts of people, consisting of actions, decisions or omissions. Because they are acts of people, accidents are highly preventable.. Virtually every major accident had a precursor which should have alerted the responsible parties not only with regard to the potential for recurrence, but also that the consequences may become much more serious, e.g., the Davis-Besse incident in 1978 served as a precursor for TMI-2 accident.

Analyses of catastrophic accidents (such as Chernobyl, Bhopal, Challenger, Amoco Cadiz, Piper Alpha, and Exxon Valdez) have been performed by several (e.g., papers by Carnino, Zebroski, Joksimovich presented in Risk Management [1], A.M. Jenkins, et al. [2]). By and large, the analyses led to similar conclusions regarding the accident anatomy. APG likes to classify contributions of causes to catastrophic accidents in four broad categories, abbreviated as "4M":

- Man (operating crew response),
- Machine (design with its basic flaws),
- Milieux (natural phenomena, operational considerations, political environment, commercial pressures, etc,) providing triggering events, and
- Management (basic organizational safety culture flaws).

The "Man" category to a lesser extent, and "Management" to a greater degree, played dominant roles in all of the above mentioned accidents. Some salient organizational ingredients were: lack of accident analyses, lack of risk analyses, lack of accident procedures, lack of training, procedure violations, operator errors, no operating experience feedback, no accident management training, no emergency planning, etc.

A strong management can minimize contributions of man, machine and milieux to the risk arising from operation of hazardous facilities. One way management can have this powerful positive influence is through the establishment of a proper safety culture.

NUCLEAR SAFETY CULTURE

IAEA's International Safety Advisory Group (INSAG) has used the term "Safety Culture" prolifically in its summary report related to the post-accident review meeting on the Chernobyl accident published as INSAG-1 in 1986 [3]. It was further expanded in INSAG-3 issued in 1988 [4]. Safety culture was highlighted as a fundamental management principle. In 1991 the agency issued the report titled "Safety Culture" (INSAG-4) [5] intended for use by government authorities and by the nuclear industry and its supporting organizations.

INSAG-4 offers the following definition: "Safety culture is that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance". INSAG considers that safety culture has two major components: framework created within which the individuals work and the attitude and response of individuals. Recently, with APG participation, IAEA issued guidelines when conducting an ASCOT (Assessment of Safety Culture in Organizations Team) mission.

The U.S. Nuclear Regulatory Commission (NRC) has an ongoing comprehensive program in human factors [6]. One area of research is directed towards assessing the influence of organizational factors (OFs) and management on nuclear power plant performance. APG was contracted in the Fall of 1990.

APG's research [7] corroborates the IAEA definition; however, our research leads us to conclude that safety culture is a product of a larger concept of organizational culture. What determines an organizational culture is a unique blend of policies, values, attitudes, practices, myths, history, self-image, which simply becomes: "the way things are done" or the "way business is conducted" in a particular organization. What differentiates most one organization from another is organizational culture and ability to permeate this culture down through the whole organization. Our research leads us, amongst other things, to conclude the following:

- Safety culture is predicated on a composite of key individuals which make up a nuclear utility organization.

- Within a nuclear utility there exist organizational and individual variables which interact to produce safe or, in an extreme case, accident-prone plant operation.

- External influences (i.e., Nuclear Regulatory Commission, Institute of Nuclear Power Operations, Public Utility Commissions, business climate and public relations policies) shape heavily utility corporate policies, thus as an end result, provide a powerful determinant of employee actions and management/employee relationships.

While no one openly disputes that nuclear safety issues should receive "overriding priority", it still remains a challenge to persuade some executives in the nuclear industry regarding how their actions or lack thereof influence performance at the plant and corporate level. Thirteen years of fundamentally accident-free operation in the U.S. seems to be creating complacency in some segments of the industry. As J.L. Nicolet [8] points out, men are very poor at estimating risk, even those aware of accidents that have befallen others believe it cannot happen to them or that the probability is too low to worry about. This applies not only to technical in-plant personnel, but even more so to the management decision makers. Another, and perhaps more significant, reason for organizational attitudes toward prioritization of safety is that the feedback from the corporation for achieving production goals is positive, tangible and reinforcing, while feedback from achieving safety goals appears to be somehow expected.

While in the past, primary reliance was placed upon engineered fission product transport barriers, i.e. fuel cladding, primary coolant system and containment, it is perceived that the safety culture is now probably the most effective barrier against releases of radioactivity.

A U.S. UTILITY'S SAFETY CULTURE

Safety culture, being part of the organizational culture within a utility can be broken down into corporate culture, nuclear operations culture, nuclear plant culture and employee attitudes. In the case of a strictly nuclear utility, corporate culture and nuclear operations culture are one and the same. This is of fundamental importance because there is no screen between the two.

In any human endeavor the manner in which people act is conditioned by requirements set at a top level, i.e., Chief Executive Officer (CEO). Policies promoted at a CEO level create the working environment and condition behavior of individuals in the trenches. A safety policy statement can declare a commitment and constant focus to excellent performance in all areas important for nuclear safety, making it abundantly clear to all employees that nuclear safety has the utmost priority, overriding if necessary the demands of production and schedules.

An effective way of communicating the CEO's message is via clearly defining the company's mission/objectives/core values and maintaining consistent emphasis on safety as the highest priority, and remaining constant and unchanging with time. The set of core values consisting of, say, the following components: integrity and trust, respect for nuclear technology, accountability, teamwork, cost effectiveness, respect for the individual and excellence. clearly demonstrate publicly asserted commitments and stance of corporate management in relation to the social responsibilities and willingness to be open in nuclear safety matters.

In addition to ensuring that reward system stresses safely, procuring sufficient funding for all safety related tasks such as necessary equipment, facilities, supportive technical infrastructure and creating the work environment conducive to the effective performance of safety duties, the CEO needs to explicitly endorse and be active in various safety culture initiatives.

Powerful examples of a commitment to nuclear safety are the existence of an independent safety oversight or risk management group directly reporting to the CEO, and a requirement for submittal of annual nuclear safety assurance reports. Such a report typically consists of three parts:

1) Nuclear safety performance indicators,
2) Each corporate division's assessment of operations, including organization, people, design configuration, operational features, operating experience and human performance.
3) Independent safety oversight group assessment of the affairs and scrutiny of division reports from the standpoint of both positive and negative trends, coupled with their assessment of plant and corporate performance from a human, equipment and organizational perspective.

EVOLUTION OF PSA

Pioneering contributions in the late 'Sixties and large generic studies conducted in the 'Seventies (e.g., Wash-1400, AIPA, DRS)[9] focused primarily on modeling and quantification of the plant hardware configurations aspects. This could be characterized as Phase I, or the machine phase in the evolution of PSA. AIPA study led the field in realistic modeling of HTGR severe accidents.

A profound impact of dependent failures, and in particular major common cause initiators such as earthquakes and fires, was recognized but not adequately dealt with until Phase II, or the milieux phase in the evolution of PSA, which took place primarily in the early 'Eighties, (e.g., Shoreham Study [10]). Realistic modeling of LWR degraded core accidents was accomplished in this phase as well.

A second profound innovation was explicit modeling of operating crew actions in accident sequences. This was primarily accomplished in the decade of the 'Eighties and constitutes the Phase III, Human Reliability or the man phase, in the evolution of PSA.

Human reliability is a complex subject, which does not lend itself to relatively straightforward models like those for component and system reliability. Typically, every accident sequence consists of an initiating event, plant hardware response(s) and human action(s) required to terminate a sequence. In order to perform a credible HRA, one needs hard data on human contributions to the frequency of initiating events, plant system unavailabilities and operating crew responses to a spectrum of accident scenarios. For the first two items sufficient statistical information is typically available, while the data and insights on operating crew responses can only be obtained through simulator exercises. The ORE (Operator Reliability Experiments) project [11], jointly sponsored by EPRI and six U.S. nuclear utilities, and executed by APG, NUS and General Physics, collected data at six full-scope control room simulators. The project encompassed simulation of 43 plant-specific accident scenarios, involved 93 operating crews, focused on 117 human interactions, and resulted in more than 1,000 data points. Subsequently, EPRI sponsored development of an application of ORE methodology for plant-specific PSAs or IPEs [12].

In order to facilitate simulator data collection, a tool named OPERAS (Operator Reliability Assessment System)[13], was developed. OPERAS represents automation of the ORE project developed simulator data collection and interpretation methodology. It should be noted that in parallel, a tool named COPAS was developed at the PAKS training center in Hungary, showing a commonality of need. COPAS is currently being used for operating crew data collection responding to VVER 440 model 213 accident scenarios.

Phase IV, or the management phase, in the evolution of PSA is underway, with the NRC-sponsored research into organizational factors currently leading the field. Figure 1 illustrates how organization factors (OFs) connect to PSA and HRA analyses. The left-hand portion of the chart represents the areas where organizational factors (behavioral science) come into play in the complex interactions of organizational units and people (organizational variables and individual variables). External influences of regulatory pressures and business climate on a nuclear utility

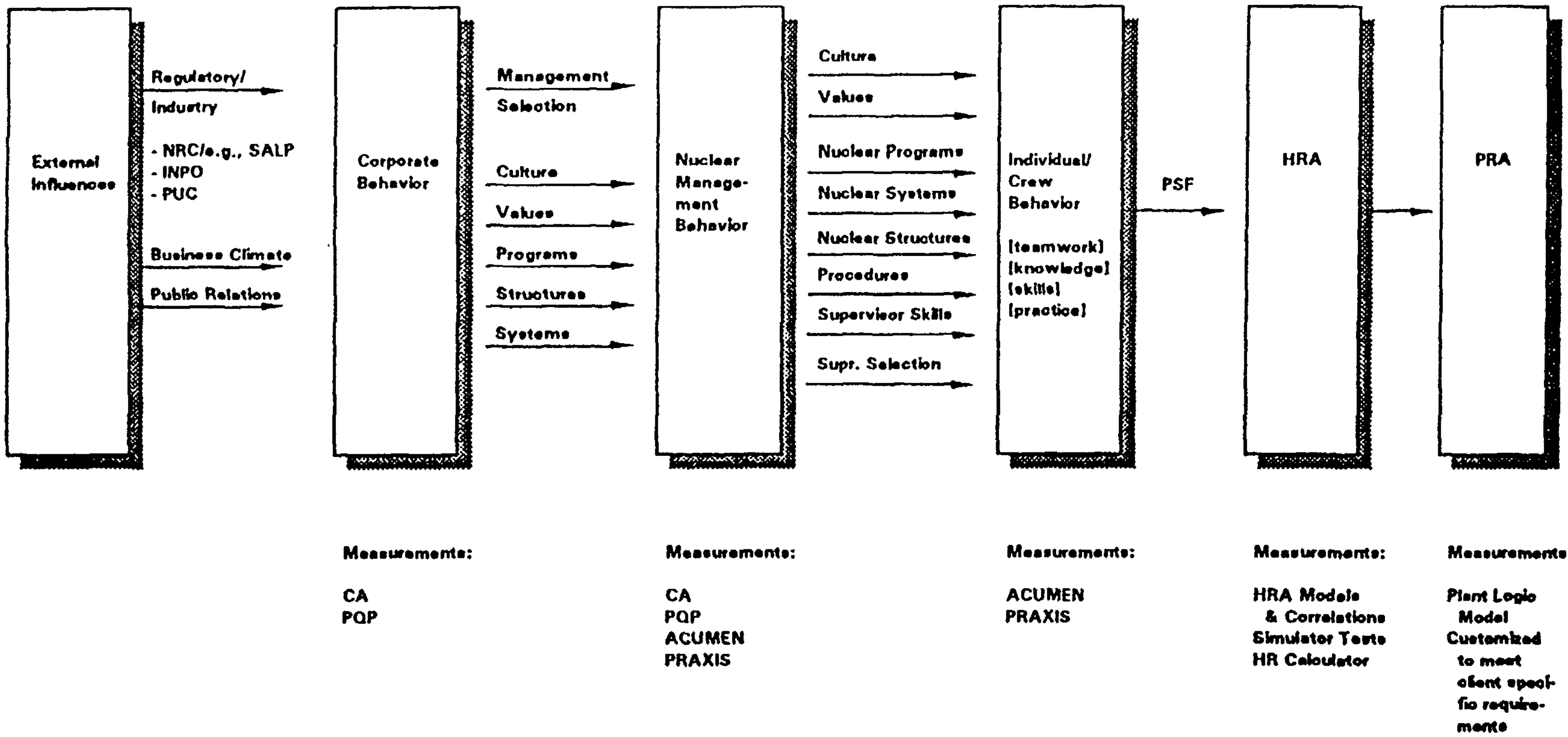


Figure 1. Link between OFs and PSA/HRA

as well as internal corporate culture affect the policies and practices of the organizations including its ability to foster an effective safety culture. The right-hand side of the chart illustrates how the organizational factors influence the reliability of plant personnel (HRA), with respect to safe operations and maintenance, which in turn factors into components of plant safety and reliability (PSA).

RISK MANAGEMENT AND IPE's

PSA or PRA is the process for identifying potential losses, either in terms of human health consequences or financial losses and estimating their likelihood due to accidents or forced outages. Risk management is defined as the decision making process to minimize these potential losses. Typically, risk management is accomplished by virtue of exercising a safety and reliability model of a specific plant and weighing the costs, benefits and risks of available options for achieving risk control.

PSA is now becoming "main stream" within the USNRC. Risk-based regulation has gradually supplemented conservative and qualitative single failure/design-basis-accident types of safety assessments. The NRC's generic letter 88-20 requested all utilities to perform a plant-specific PSA or an Individual Plant Examination (IPE). A number of IPEs, containing the Level 1 (Internal events core damage frequency) and the Level 2 (containment performance) have already been submitted.

Conduct of PSAs/IPEs, and living ones in particular, relies heavily on the existence of efficient computer tools. Advances in the field of personal computers have led to the development of PSA workstations [14] which have been used invariably in the IPE process. As an example, EPRI, Texas Utilities and APG sponsored development of a Human Reliability Calculator [15] for inclusion into the workstations such as CAFTA [16]. TU Electric has not only applied the EPRI-sponsored HRA methodology, but has made full use of the Calculator in the development of the Comanche Peak IPE just submitted to the NRC.

Nuclear utilities appear to be mixed in their views on the usefulness of PSA as a risk management tool. Enlightened utilities find many practical uses of PSA and have developed risk management programs. To our knowledge, Yankee Atomic has probably the most advanced program in the industry [17]. The referenced report was written to describe numerous applications of PSA techniques beyond those typically found in PSAs/IPEs as a sample of benefits. A striking example is its use in closure of NRC's severe accident policy issues, i.e., IPE, IPE for External Events (IPEEE), Containment Performance Improvements (CPI) and Accident Management (AM). The report concludes with the following statement: "By pursuing a proactive program in risk assessment, a utility can influence the NRC process for issue resolution. By proposing an integrated solution that meets the intent of the NRC's multi-element program, a utility may be able to avoid need for costly responses to the individual elements".

Some utilities seem to be performing IPEs purely as a licensing necessity. As a consequence, IPEs are not being used as a powerful risk management tool to ferret out not only potential plant configuration vulnerabilities, but also to address the operational issues. Some of these IPEs end up modeling the plant configuration adequately, leading to proper identification of plant hardware vulnerabilities, but do not adequately account for the plant operational history. Nor do they account for the actual measured readiness of plant specific operating crews to handle analyzed accident scenarios. The treatment of human reliability by "handbook" methodology fails to capture actual operating crew performance.

INTEGRATED RISK MANAGEMENT

Risk management process is incomplete unless it accounts for organizational factors; therefore APG has developed the concept of Integrated Risk Management (IRM). It represents a fusing of 1) engineering technology including a) probabilistic risk assessment (PRA) and its sub-discipline of human reliability analysis (HRA) and associated engineering disciplines of reliability, availability and maintainability and b) nuclear power operations, maintenance and engineering support with 2) the science of organizational factors which embraces elements of modern management theory and behavioral science. Figure 1 represents the framework for IRM.

Once properly identified, incorporating organizational influences into PSA as a category is relatively straightforward! On examination of constituents of core damage sequences, one notes cutsets made up of: a) initiating event frequency and one or more of terms representing a) unavailability of hardware and b) reliability of various human actions. Since an NPP is operated and maintained by humans who are influenced by the organization for which they work, good or bad organizational factors should be represented in the quantification of each term in the sequence cutsets. Similar to the treatment of "performance shaping factors" in HRA or "environmental factors" in reliability engineering, organizational influences may be treated as multiplicative factors for each cutset term, e.g., on equipment failure rates and human failure rates. However, a very important aspect of treating organizational influences is their importance as common-cause factors; i.e., a given organizational influence may adversely affect several terms in the same or other cutsets.

The difficult part of the analysis is to a) identify the specific organizational factors that have significant influence on the various cutset events and their interdependence and b) quantify the effect of each factor on cutset probabilities. For example, APG is pursuing research to extract factors for organizational influences on operator reliability i.e., operator reliability factors from simulator measurements at various NPPs can be correlated to measures of organizational factors (based on suitable instruments of behavioral and management sciences) to derive the appropriate factors.

There are several programs in effect at every nuclear utility that have a direct or indirect influence on plant safety and productivity. Several of the programs are the result of regulatory imperatives and others are the result of "good practice". Our experience in working with many nuclear utilities is that there is a tremendous degree of fragmentation among such programs with a lack of appreciation of the interrelation of one program to the other, especially with respect to nuclear safety. A good example being a lack of integration between PSA, human factors and training activities. In our strong view, the IRM concept represents the best safety assurance program the contemporary state-of-the-art risk assessment technology provides. An IRM program imbedded in an effective safety culture, will lead management to achieve both economic and safety goals while reducing strain on management personnel and operating budgets primarily through an effective integration process.

ACKNOWLEDGEMENT

The author wishes to acknowledge the contributions of his colleagues at APG; Doug Orvis and Tony Spurgin, in particular.

REFERENCES

[1] Ronald A. Knief, Editor, Risk Management: Expanding Horizons in Nuclear Power and Other Industries, Symposium of September 6th, 1989, sponsored by GPU Nuclear Corporation, Hemisphere Publishing Corporation, New York, 1991.

[2] A.M. Jenkins, et al., Management at Risk, RDA-R3, 1992.

[3] International Nuclear Safety Advisory Group, Summary Report on the Post-Accident Review Meeting on the Chernobyl Accident, Safety Series No. 75-INSAG-1, IAEA, Vienna, 1986.

[4] International Nuclear Safety Advisory Group, Basic Safety Principles for Nuclear Power Plants, Safety Series No. 75-INSAG-3, IAEA, Vienna, 1988.

[5] International Nuclear Safety Advisory Group, Safety Culture, Safety Series No. 75-INSAG-4, IAEA, Vienna, 1991

[6] F. Coffman, et al., Human Factors Regulatory Research Program Plan, NUREG-1384, U.S. Nuclear Regulatory Commission, Washington, D.C., 1989.

[7] V. Joksimovich, P. Moieni and D. Orvis, Organizational and Management Influences on Safety of Nuclear Power Plants: Modeling Hypotheses Using PRA Techniques, U.S. Nuclear Regulatory Commission, Draft NUREG/CR-5752, 1991

[8] A. Carnino, J.L. Nicolet and J.C. Wanner, Man and Risks: Technological and Human Risk Prevention, Marcel Dekker, Inc., New York, 1990.

[9] V. Joksimovich, "An Overview of Insights Gained and Lessons Learned From U.S. Plant-Specific PRA Studies" Nuclear Safety, Volume 27, No. 1, Jan-March, 1986.

[10] V. Joksimovich, R. Paccioni, "Overview of Results and Perspectives From Shoreham Major Common Cause Initiating Events Study", ANS/ENS Topical Meeting on Nuclear Reactor Safety, San Diego, 1986.

[11] A.J. Spurgin, et.al., Operator Reliability Approach Using Power Plant Simulators, Volumes 1, 2 and 3, EPRI NP-6937 and NP-6937L, Electric Power Research Institute, 1990 and 1991.

[12] A.J. Spurgin, P. Moieni, and G.W. Parry, A Human Reliability Approach Using Measurements for Individual Plant Examinations, EPRI NP-6560L, Electric Power Research Institute, 1989.

[13] A.J. Spurgin, J. Hallam and J.P. Spurgin, Operator Reliability Assessment System (OPERAS), Volumes 1, 2, and 3, EPRI RP-3082-01, Electric Power Research Institute, 1992.

[14] "The Role and Use of Personal Computers in Probabilistic Safety Assessment and Decision Making", Journal of Reliability Engineering or Systems Safety, Volume 30, Nos. 1-3, 1990.

[15] P. Moieni, et.al., "A PC-Based Human Reliability Analysis (HRA) Calculator", prepared for American Nuclear Society Probabilistic Safety Assessment International Topical Meeting, PSA '93, Clearwater, Florida, January 26-29, 1993.

[16] Science Applications International Corporation, CAFTA: A Fault Tree Development Work Station, Los Altos, CA 9189.

[17] Yankee Atomic Electric Company, "Applications of Probabilistic Risk Assessment", Electric Power Research Institute, NP-7315, 1991.

RESEARCH ACTIVITIES FOR PROBABILISTIC SAFETY ASSESSMENT AT THE KOREA ATOMIC ENERGY RESEARCH INSTITUTE

Kil-Yoo KIM, Chang K. PARK
Reactor Safety Assessment Department,
Korea Atomic Energy Research Institute,
Daeduk, Republic of Korea

Abstract

In Korea Atomic Energy Research Institute (KAERI), there are two kinds of activities in probabilistic safety assessment (PSA) area. One of them is PSA for Nuclear Power Plants (NPPs). Several Probabilistic Safety Assessments (PSAs) for NPPs under construction or in operation are carried out. The other activity is PSA methodology development. In this paper, the PSA methodology development activity is mainly introduced, especially for Level-1 PSA.

1. INTRODUCTION

In KAERI, there are two kinds of activities in PSA area. One of them is PSA for Nuclear Power Plants NPPs. Several PSAs for NPPs under construction or in operation are carried out, and more PSA projects for new NPPs and for the remaining plants in operation will continue. There are two major organizations which can perform PSA for NPPs in Korea which are KAERI and KOPEC (Korea Power Engineering Company). Each organiztion specialized in different field. For example, KAERI is performing internal Level I PSA and most part of Level II. On the other hand, KOPEC is performing external Level I PSA.

The other activity of KAERI is PSA methodology development, which again can be classified as PSA tool development and PSA technique application. As a PSA tool development, KIRAP-II computer code was developed. As PSA technique applications, PEPSI, ROMAS and COSMOS were developed. In the following sections, those computer codes are described. Also, future research areas which KAERI is going to study are described.

2. PSA for NPPs

KAERI has finished or is performing several PSAs for NPPs. Table 1 is a list of PSA projects in which KAERI is involved. In Table 1, PSA for Wolsung 3,4 is not mentioned, but the project will start next year. In every PSA project, KAERI always uses KIRAP code for level I PSA.

Table 1. List of PSA Projects Performed by KAERI

PLANT NAME	PERIOD	SCOPE	REMARK
Kori 3.4 & Yonggwang 1,2	'89.9 - '92.8	Level I	Indep't Peer Review
Yonggwang 3,4	'87.8 - '89.3	Level I	Preliminary
	'90.7 - '92.12	Level I	Final
	'91.4 - '94.2	Level II	IPE
Wolsung 2	'91 4 - '95.3	Level I	AECL/KAERI
Ulchin 3,4	'91.7 - '97.10	Level I, II	KAERI

3. KIRAP-II

A PC-based Level-1 PSA Code Package, KIRAP-II (KAERI Integrated Reliability Analysis Code Package II), was developed and is used in PSAs for NPPs. KIRAP-II provides functions that range from graphical fault tree and event tree construction to cut set generation and quantification. It also can do importance, uncertainty and sensitivity analyses.

KIRAP-II consists of two parts. One is KIRAP-I and the other is reliability data analysis part. As shown in Figure 1, KIRAP-I consists of 7 independent computer codes : namely KIRAP-TREE (fault tree editor), KIRAP-ET (event tree editor), KIRAP-TDBEDIT (event data manager), KIRAP-CUT (cut set generator), KIRAP-UNCERT (uncertainty analysis module), and KIRAP-CONVERT (fault tree data conversion utility). Fault trees are constructed interactively on a character-based graphic screen by using KIRAP-TREE. KIRAP-TREE generates the fault tree in the form of Boolean equations, which are stored in the CUT file Event trees are built interactively on a graphic screen using KIRAP-ET and Boolean equations for event sequences are stored on USR files. These files are automatically transferred to KIRAP-CUT or KIRAP-RESULT. KIRAP-TDBEDIT collects events data of several system fault trees and build a total event data base. It supports reliability data for KIRAP-CUT, RESULT, and UNCERT codes Cut sets are generated using KIRAP-CUT or RESULT KIRAP-CUT runs in the batch mode like the old computer codes, and can run on IBM-PCs and workstations. KIRAP-CUT for workstations would be used to generate cut sets for large fault trees and event sequences. KIRAP-RESULT can generate cut sets and edit cut sets in an interactive mode on PCs. Cut sets generated by KIRAP-CUT or KIRAP-RESULT are stored in files and can be reused in another run. Uncertainty analysis can be done using KIRAP-UNCERT code. Fault trees and event trees can be plotted on HP-GL compatible plotter or HP Laser Jet III printer.

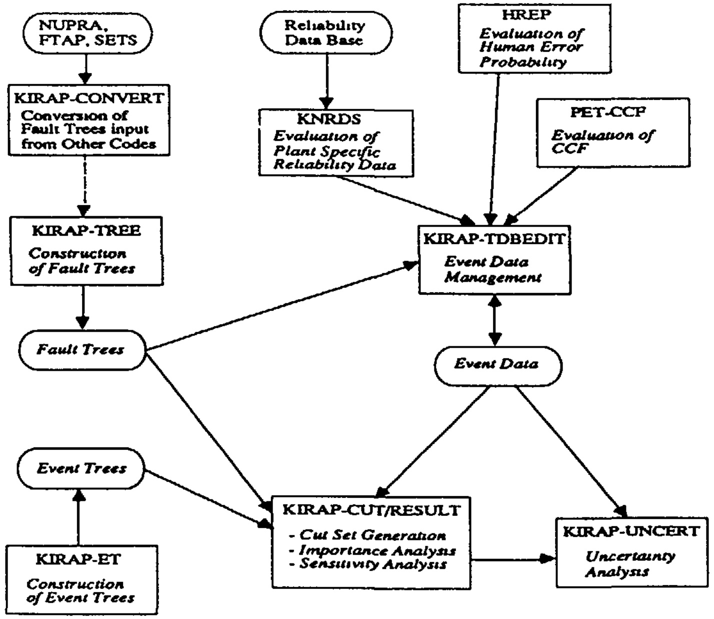


Figure 1. Overview of KIRAP-II

The reliability data analysis part consists of 3 programs HREP, PET-CCF, and KNRDS HREP (Human Reliability Evaluation Program) is developed to evaluate human error probabilities It provides simplicity in HRA (Human Reliability Analysis) and consistency in the obtained results.

PET-CCF is developed to provide parameters of common cause failure (CCF) based on the MGL (Multiple Greek Letter) or the Alpha Factor model

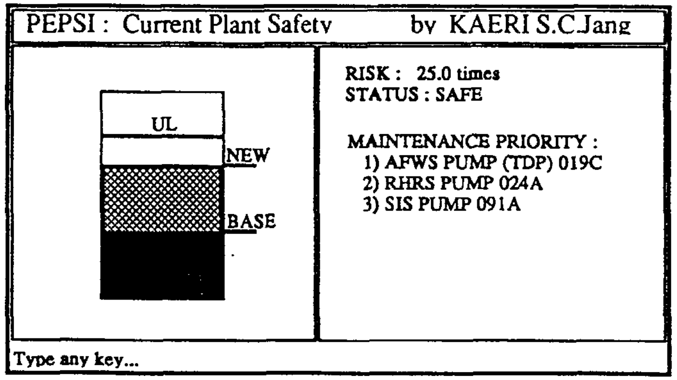
KNRDS is developed to generate reliability data for Korean nuclear power plant (NPP). In KNRDS, the data analysis is performed by using Two-Stage Bayesian (TSB) procedure to incorporate the foreign generic data and similar plant's data. This KNRDS system is used to provide hardware failure rates and initiating event frequencies reflecting Korean specific experience.

The KIRAP-II will be modified to be used in X-Window and in MS- Window environment to provide better user interface and to avoid memory limitation problem.

4. PEPSI

As a "living" PSA application tool for operation, a code, called PEPSI (Probabilistic Evaluated Plant Safety Indicator), was developed.

PEPSI can updates the plant risk continuously according to the change of system/component configuration. As shown in Figure 2 , whenever plant configuration changes, PEPSI re-evaluate the plant risk based on the PSA results of a baseline plant configuration. And it shows new plant risk relative to baseline risk level. The basic purpose of PEPSI is to help to identify the early signals of deteriorating plant safety and to trace relative changes of plant risk. In the case of multiple component outage, PEPSI suggests maintenance priorities according to the importance of each component from the viewpoint of the plant safety.



PEPSI : Current Plant Safetv by KAERI S.CJang

RISK : 25.0 times
STATUS : SAFE

MAINTENANCE PRIORITY :
1) AFWS PUMP (TDP) 019C
2) RHRS PUMP 024A
3) SIS PUMP 091A

Type any key...

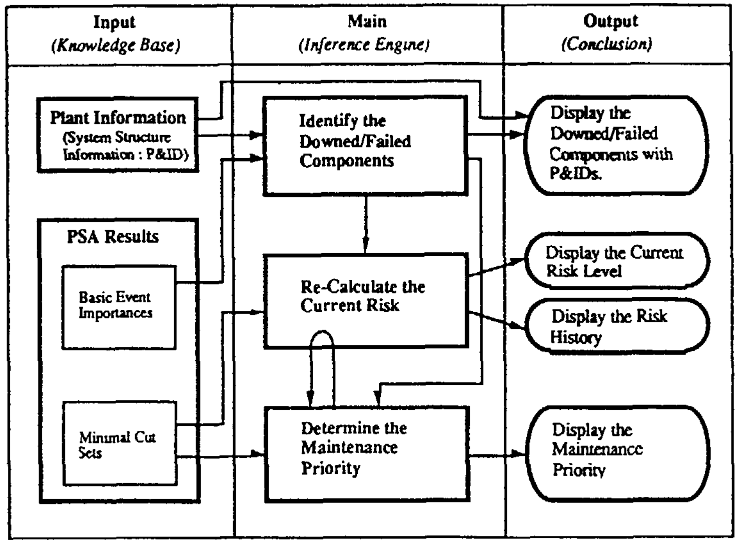
Figure 2 Display of Current Plant Safety

5. ROMAS

As a "living" PSA application tool for maintenance, a code, called ROMAS (Reliability Oriented Maintenance Advisory System) was developed. If a component is selected on a P & ID shown on a computer screen, and if an input such as "fail to start", or "fail to open", etc., is entered, then an increased core melt frequency shows up.

Actually, ROMAS is similar to PEPSI, since ROMAS was developed based on PEPSI. The big differences between two are the user interface and the purpose of usage. In ROMAS, component status can be inputted on the P&ID shown on the computer screen. Also, ROMAS is intended to be used mainly in maintenance work. The other functions and concepts are borrowed from PEPSI.

In ROMAS, the plant CDF is used as a measure for the plant risk level which is calculated dynamically from the present component reliability. The current risk level is calculated from the minimal cut sets (MCSs) with the consideration of the component status at that time. The ROMAS can also suggest the maintenance priorities for failed components so as to minimize the risk level. The overall structure of the ROMAS is shown in Figure 3 with the information flow.



Input
(Knowledge Base)
Main
(Inference Engine)
Output
(Conclusion)
Plant Information
(System Structure Information : P&ID)
PSA Results
Basic Event Importances
Minimal Cut Sets
Identify the Downed/Failed Components
Re-Calculate the Current Risk
Determine the Maintenance Priority
Display the Downed/Failed Components with P&IDs.
Display the Current Risk Level
Display the Risk History
Display the Maintenance Priority

Figure 3. Information Flow of ROMAS

Finally, the history of risk level change is stored as the proposed system is used for many times This history is also used to retrieve the plant operation experience, and this can help the operator for grasping the operating history ROMAS is written in PROLOG language and is built in a workstation with color display

Since ROMAS is based on the change of component status, it can be used as a tool for indicating the current risk level and an advisory system for the risk management and the component maintenance policy In addition, it can be utilized for the study on flexible technical specification monitoring

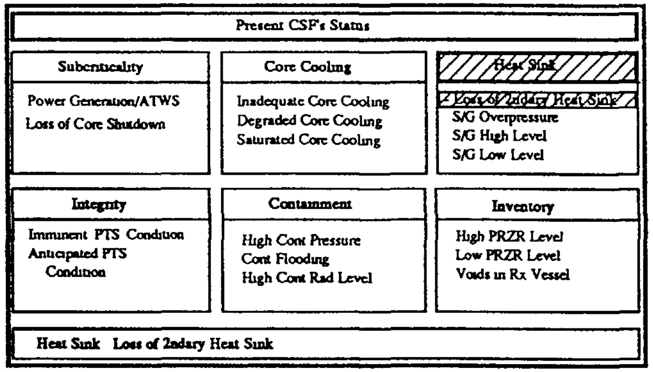
6 COSMOS

COSMOS (Computerized Success path Monitoring System) was developed by KAERI in order to support emergency operation of nuclear power plants

COSMOS assists operators by providing the present status of critical safety functions (CSFs), and by suggesting necessary operator's action items to restore challenged CSFs COSMOS consists of two parts one is to identify CSF's status and to determine the overall response strategy and the other to generate the success path which restores the challenged CSFs The CSF's status is identified by the rule based reasoning The rules are derived from the CSF's Status Tree provided in ERG's (Emergency Response Guidelines) The overall response strategy is inferred according to the identified CSF's status The knowledge base for this part is based on the analyzed results of FRG s (Functional Restoration Guidelines) The actions of FRG s are classified and standardized according to their functions Based on the current plant state, appropriate response actions are inferred.

Success paths are generated by the given structure descriptions and the general generation algorithm The structure descriptions of systems are based on the piping and instrument diagrams (P&IDs) Generated success paths are ranked according to either its respective reliability or the number of manual operator's actions required to complete each success path A prototype COSMOS was built on a workstation

To test COSMOS, a hypothetical scenario is assumed for Loss of Secondary Heat Sink At first, it is assumed that Loss of Secondary Heat Sink" occurs due to 'Loss of Main Feedwater,' and then a CSF, i e , Heat Sink is assumed to be challenged The status of CSF's is displayed as shown in Figure 4 In this case, the level 1 action item, Establish Secondary Heat Sink," and the level 2 action item with the highest priority, "Establish AFW Flow" are inferred Hence, the auxiliary feedwater system (AFWS) is selected as an appropriate safety system for this situation Among the generated success paths, the most operable success path is displayed as shown in Figure 5, and all the operator's action items of the three levels are also displayed

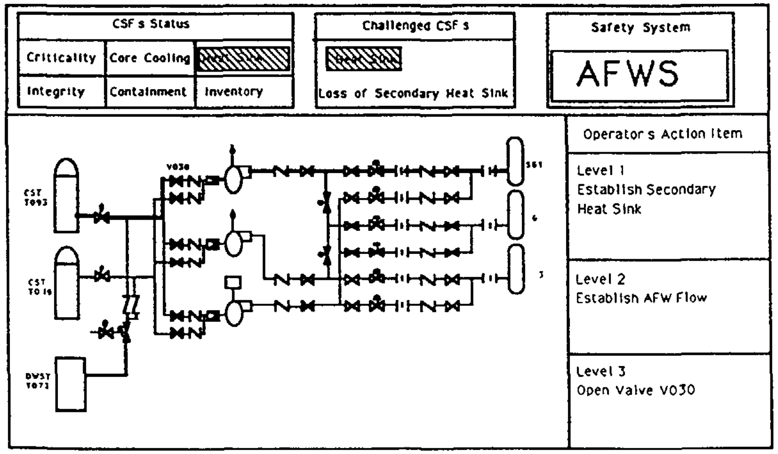


Present CSF's Status

Subcriticality	Core Cooling	Heat Sink
Power Generation/ATWS Loss of Core Shutdown	Inadequate Core Cooling Degraded Core Cooling Saturated Core Cooling	Loss of 2ndary Heat Sink S/G Overpressure S/G High Level S/G Low Level
Integrity	**Containment**	**Inventory**
Imminent PTS Condition Anticipated PTS Condition	High Cont Pressure Cont Flooding High Cont Rad Level	High PRZR Level Low PRZR Level Voids in Rx Vessel

Heat Sink Loss of 2ndary Heat Sink

Figure 4 Display of CSF's status



CSF s Status

Criticality	Core Cooling	▨
Integrity	Containment	Inventory

Challenged CSF s

▨

Loss of Secondary Heat Sink

Safety System

AFWS

Operator s Action Item

Level 1
Establish Secondary Heat Sink

Level 2
Establish AFW Flow

Level 3
Open Valve V030

Figure 5 Success path display for AFWS

The intended function by an initially selected level 2 action item may not be achieved due to various reasons. When a selected item cannot perform its function, an alternative level 2 action item will be suggested. The status of CSF's can be changed by the actuated success path(s). If the status of CSFs are still challenged, a new appropriate system is chosen. For instance, if it is confirmed that AFWS does not perform its function, then "Establish Bleed and Feed (PORV and HPSI)" will be suggested as an alternative level 2 action item by the rules for level 2 and a new set of success paths to complete this action item will be generated for the respective safety systems.

7. FUTURE RESEARCH AREAS

From the next year, several new projects will begin. One of them is to develop a PSA tool using artificial intelligence, which can automatically generate fault tree and event tree, and can manage the whole PSA work to do a "living" PSA.

Another one is to develop an accident management expert system, which will be used to monitor and evaluate the status of the containment during a severe reactor accident. The system will also provide information on the time, rate, and magnitude of release of important radioactive isotopes given a loss of containment integrity.

IPAM(Integrated Plant Analysis and Management System) also will be developed. IPAM consists of 3 modules : 1) knowledge base module which is a collection of commonly used knowledge organized in object libraries, 2) generic problem solver module which can be used repeatedly in solving certain generic type problems, and 3) integrated user interface module. The object-oriented reusable architecture of IPAM will make the development of many computer application programs manageable, expandable and modifiable easily. Since the capability of personal computer (PC) increases, PC is a target platform of IPAM, and MS-Window NT and C++ will be used.

Also, the following research areas will be emphasized in KAERI :

1) level III PSA methodology and its computer codes
2) level II PSA methodology including containment event tree.

ACKNOWLEDGEMENT

The authors wish to acknowledge the contribution of Dr. J. O. Yang, Y. Choi, K.S. Chung, S.H. Han, S.C. Chang, and Dr. J.J. Ha of Reactor Safety Assessment Department, KAERI in preparing this paper.

THE IMPORTANCE OF RISK-BASED REGULATION TO DEVELOPING NATIONS

H. SPECTER
New York Power Authority,
White Plains, N.Y.,
United States of America

Abstract

The paper discussed the present status of risk-based regulation (RBR) in the United States. RBR potential of both improving NPP safety while reducing plant operating costs and the workload of the regulatory staff has been pointed out. Recent efforts involving both utilities and regulatory organizations are briefly described.

RBR can be particularly valuable to developing nations, since it assures more economic way of achieving high level of nuclear safety.

Introduction

This paper discusses the present status of risk-based regulation in the United States. It then describes the special importance this emerging regulatory process can have to developing nations.

Background

Nuclear power plants in the United States are regulated today on the basis of demonstrating that they can meet a number of very conservative deterministic criteria. A number of design basis accidents are postulated and it must be shown that a plant's design must be able to place the plant into a safe condition for each of these design basis accidents. While such an approach has been quite effective in the past, i.e., no member of the U. S. public has ever been subject to fatal doses of radiation from any plant operation or accident, the present regulatory process is not an economically efficient one.

Further, some potentially serious events, which may occur more frequently than some design basis accidents, appear to have been overlooked.

An alternative way of evaluating the adequacy of a plant's design and operation is to use Probabilistic Safety Assessment [PSA] techniques. Although such methodologies have been available since the mid-1970's, the use of PSA as a regulatory tool has dramatically advanced in the recent past. Not only has the technology evolved over the past twenty years, as well as the operational data base, a major turning point occurred when virtually all U.S. operating commercial nuclear power plants committed to producing plant-specific PSAs. This greatly expanded the body of plant-specific knowledge and set the stage for even further developments. Increasingly, PSA considerations have been incorporated into the regulatory process as these studies advanced to their level one [core melt frequency] and level two [containment failure frequency, source terms] results.

Another milestone in the utilization of PSA technology occurred on March 10, 1992. On that date three members of the U.S. nuclear industry* came before all five NRC Commissioners in a public briefing to recommend that major portions of the present deterministic regulatory process be replaced, over time, with a risk-based approach. A transition strategy to bring about this change in the regulatory process was offered at this presentation.

Risk-based regulation [RBR] is the utilization of a modern technology, PSA, to better distribute the resources of both the regulator and the nuclear industry. More specifically, resources would be distributed according to risk significance. Those items or events that have high risk significance would receive the most attention, while those with little risk content would command fewer resources.

RBR has the potential of <u>both</u> improving nuclear power plant safety while reducing plant operating costs and the workload of the regulatory staff. If applied, the public could then receive a double benefit: safer nuclear plants <u>and</u> lower nuclear generated electricity costs. This modern form of regulation could be applied to present operating plants and to advanced designs. In fact, it would help quantify the safety improvements of advanced designs.

It is anticipated that even should application of the RBR process expand over time, that a deterministic approach to certain portions of the overall regulatory process could still be of value. For example, various on-site normal operations such as the handling and storage of nuclear fuel and wastes, ALARA activities and routine plant emissions may be efficiently regulated by a deterministic process. Characteristically, such deterministically regulated processes would not lead to exceeding offsite PAG (Protective Action Guides) levels, if there were some type of failure. RBR lends itself more to severe accident situations where core damage or loss of containment integrity is possible. Thus an appropriate blend of deterministic normal

*Messrs. John C. Brons and Herschel Specter of the New York Power Authority and Mr. William Rasin of NUMARC.

operations regulation and risk-based severe accident regulation could yield an optimum overall regulatory process.

Present Status

RBR is developing at a rapid rate. In industry, the New York Power Authority (NYPA) has offered to fund an RBR pilot program using its J. A. FitzPatrick plant. Interest in this NYPA activity is growing. The Empire State Electric Energy Research Company, ESEERCO, is now sponsoring a portion of the NYPA program. About eight utilities within the New York area comprise ESEERCO and a number of other utilities outside of New York are also associated. This ESEERCO effort started in August, 1992. EPRI, the Electric Power Research Institute is conducting RBR research and its utility members recently overwhelmingly voted to support a multimillion dollar effort. The BWROG, the Boiling Water Reactor Owner's Group, established an ad hoc committee on RBR in early 1992. The long term scope and funding level of this BWROG Committee is now under review. The B&W Owner's group and the Edison Electric Institute conducted meetings on this regulatory concept in June, 1992. Both of these groups see great potential in RBR. Presentations on RBR are also planned for INPO in the near future.

The American Nuclear Society has also been active in advancing RBR. Of most significance is a June, 1992 decision by the ANS Public Policy Committee to develop a public policy statement in support of RBR. Several RBR technical papers have already been presented at ANS conferences and a technical session devoted to RBR is planned for the June, 1993 ANS annual meeting. RBR will also be a key topic at the ANS Executive Conference to be held in October, 1992.

In March, 1993 the Second International Conference on Nuclear Engineering, ICONE-2, will have a technical session on RBR. This conference is co-sponsored by the American Society of Mechanical Engineers and the Japan Society of Mechanical Engineers.

NUMARC, the Nuclear Management and Resources Council, who with NYPA, participated in the March 10, 1992 Commission presentation, has offered to take a leadership role in this modernization of the regulatory process if a similar level of activity is demonstrated by the NRC. NUMARC recently created an Ad Hoc Advisory Committee on RBR to guide its activities on this subject. NUMARC and NYPA have also worked together to address a number of Commission questions that arose after the March 10, 1992 presentation.

The NRC is in the process of putting a staff team together to respond to this industry initiative. Interest on the part of the NRC Commissioners is high. It is expected that a number of NRC/industry meetings will take place in 1992 to define a transition strategy more precisely.

Lastly, the International Atomic Energy Agency (IAEA) is quite interested in RBR. This subject was discussed at the Laguna Verde Plant in Mexico in November, 1991 and again at an IAEA sponsored PSA training course at Argonne National Laboratory last February. Our meeting today shows this continuing IAEA interest and an IAEA document on RBR will be drafted in November, 1992.

RBR and Developing Nations

RBR can be especially valuable to developing nations, particularly those with regulatory processes which are in their formative stages. Two reasons for this are improved safety and the best use of national resources.

With regard to improved safety, a number of important observations have already been made. As discussed during the March, 1992 NRC briefing, analyses show that significant variations in risk levels can occur during actual plant operation as plant configurations change from time-to-time (see Figure One)*. Operational risk levels can, at times, be orders of magnitude higher than typical time-averaged PSA results. Additionally, certain combinations of components, simultaneously unavailable, can result in core melt frequency "spikes" [See Figure Two]*. Even more important, analyses indicate that there is a strong correlation between such "spikes" and precursor events, i.e., situations approaching a severe accident. Since all of the high risk configurations shown in these figures were allowed by present plant technical specifications, there is a clear need to improve these specifications. This can be accomplished by using RBR to minimize such operational risks. RBR efforts now underway, e.g. the ESEERCO program, would identify high risk plant configurations for NYPA's FitzPatrick plant and would develop strategies to minimize such risks. Results of these ESEERCO efforts will be published.

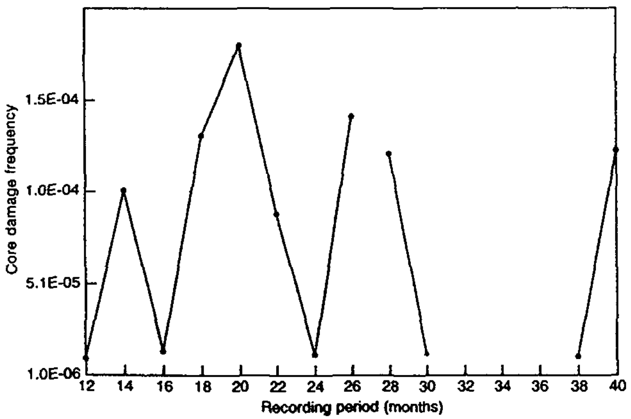


FIG. 1. Core damage frequency versus time.

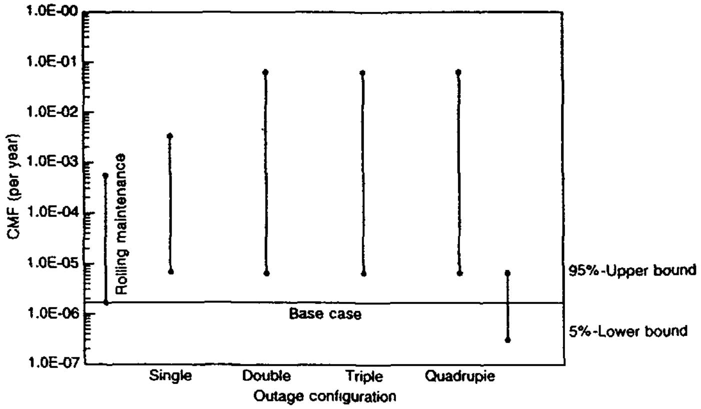


FIG. 2. Range of CMF levels.

*The author wishes to acknowledge to very valuable work of Dr. William Vesely in producing these figures.

Other observations, based on recent PSA studies are now surfacing. For example, in one boiling water reactor analysis it was shown that should certain plant systems fail, it would be safer to continue power operation than to shutdown, as called for by the plant's present technical specifications. Observations, such as this, means that a more sophisticated approach to plant operation is needed than is presently employed. RBR, which emphasizes such operational risk issues, as compared to traditional,static "bottom line" PSA results, will lead to these safety improvements.

On a broader scale of considerations, should RBR be used on an international basis, safety technology could be more readily exchanged among nations, even though design and operational practices differences may exist. Simply stated, the mathematical basis of RBR lends itself to all nations, since mathematics knows no borders. The exchange of safety technology among nations enhances safety for all. RBR facilitates this exchange process.

There are also profound resource benefits for developing nations which use RBR technology. First, if a developing nation wishes to purchase a new nuclear power plant, it may choose to establish design requirements, expressed in RBR or PSA language, that all reactor vendors would have to meet. For example, maximum mean core melt frequencies and maximum mean severe release frequencies might be established as design requirements for all reactor vendors bidding on a contract. By using such requirements, an importing nation would be able to judge if a proposed plant achieves an adequate level of protection for a given financial investment.

With regard to the actual plant design and construction, RBR teaches us that only a select few systems, structures, and components (SSCs) are truly important to the public's radiological safety. If a typical nuclear plant contains 100,000 SSCs ± 20%, then a rule-of-thumb is that only about 1/2 to 1% of these components are risk relevant. One major implication of this observation is that since a great number of the plant components are not safety related, their initial purchase costs and later, replacement costs, will be much lower than typical safety related components are today. Furthermore, it may be possible to manufacture many of these non-safety related components within the country that purchased the nuclear plant. Some importing developing nations today may not be able to locally manufacture safety related components, and are forced to import expensive equipment. Much of this could change as the list of safety related SSCs is minimized through RBR. By careful labeling of which components are safety significant and which are not, precious national currency could be conserved while supporting domestic industries that manufacture components for the nuclear plants.

Further savings, both to the developing nation's regulator and to the plant operator, would occur over the lifetime of a plant if its license is based on RBR. We already know today that many of the surveillance tests, maintenance actions, limiting conditions of operation that exist in present technical specifications are not risk significant. Their removal would greatly reduce costs, as well as inadvertent reactor scrams introduced by human error during such actions. RBR leads to more cost effective regulatory inspections, tests, and operator training programs. Perhaps most important, it encourages the regulator and the plant operator to make safety decisions on a more technically justified basis. RBR technology also permits a risk ranking of SSCs. Once such rankings are established, resources could be expended more efficiently by concentrating on the highly ranked SSCs.

Conclusion

Nuclear power is a necessary part of the energy future of many nations. However, a modern technology needs a modern regulatory process. RBR is well suited to this task. It can be particularly valuable to developing nations who can chose to "leap frog" over the present deterministic regulatory methodology used elsewhere, to enjoy both higher levels of nuclear safety and much more economical nuclear power.

THE ROLE OF PROBABILISTIC SAFETY ASSESSMENT IN THE LICENSING OF ANGRA-I NUCLEAR POWER PLANT

S.M. ORLANDO GIBELLI
Division of Safety Assessment,
Comissão Nacional de Energia Nuclear,
Rio de Janeiro, Brazil

Abstract

The Licensing of Nuclear Power Plants, in Brazil, is carried out by the Regulatory Body, the National Nuclear Energy Commission (CNEN), and it has been based on deterministic approach.

However, aiming the issuance of the Authorization for Permanent Operation to Angra-I Nuclear Power Plant, which is expected to occur after the next refueling, the Regulatory Body decided to include, in the terms of the Authorization, requirements related to the most important aspects of the use of Probabilistic Safety Assessment (PSA) as a complementary tool to enhance plant safety.

In order to accomplish those measures and enable their implementation, the Regulatory Body will request the Utility (FURNAS) to provide a PSA of Angra-I to be used as a reference study.

Taking into account that a PSA level 1 of Angra-I was performed in Brazil, from 1982 to 1985, under an IAEA Research Contract, the Utility has shown the intention to consider this original study as a starting point on which a rigorous review will be conducted.

The objective of the present paper is to describe the Brazilian Regulatory Body position concerning the Role of the Probabilistic Safety Assessment in the Licensing of Angra-I NPP. The main PSA related topics to be potentially implemented by the Utility are also presented.

1. INTRODUCTION

The Licensing of Nuclear Power Plants, in Brazil, is carried out by the Regulatory Body, the National Nuclear Energy Commission (CNEN), and has been based on deterministic approach. Nevertheless, with a view to issue the Authorization for Permanent Operation of Angra-I, which is expected to occur after the next refueling outage time, the Regulatory Body decided to include in the terms of the Authorization, the main aspects of the use of PSA as a complementary tool to enhance plant safety, mostly concerning the possibility of occurrence of events beyond design basis. In order to accomplish those measures and enable their implementation, CNEN will request the Utility (FURNAS) to provide a Probabilistic Safety Analysis (PSA) of Angra-I to be used as a reference study.

Basic principles of safety point out to design and operational relevant aspects which need to be considered and are not necessarily included in a conventional deterministic safety assessment as, for instance, questions related to accidents beyond design basis and severe accidents. These accidents can be identified through a systematic analysis of the accident sequences resulting from a PSA. Additionally, PSA provides qualitative and quantitative information and insights into plant design, which can help to improve operational practices and conditions. Therefore, the Probabilistic Safety Assessment plays a complementary role to the Deterministic Assessment.

Nowadays, the development of a plant specific PSA is an international trend, either from Utility initiative or from Regulatory Body requirement. The relevance of these studies is directly connected to the utilization of plant specific data base in their elaboration in order to obtain reliable results which could be put into practice.

The objective of the present paper is to present and discuss the relevant aspects of the possible uses of PSA [1] which should be taken as starting points to the formulation of a programme to be implemented by the Utility to enhance Angra-I NPP safety.

Due to resource limitations in the Brazilian nuclear field, the establishment of a prioritization of potential uses for the above mentioned aspects is also discussed.

2. ANGRA-I BACKGROUND INFORMATION

The Brazilian Nuclear Power Plant Angra-I, a two-loop pressurized water reactor of 626 MWe, Westinghouse design, turn key contract, has been in operation from 1981 to 1987 under an Authorization for Provisory Operation. The Authorization for Initial Operation was issued in 1987, by CNEN.

The safety assessment for the issuance of the Angra-I License has been performed according to Brazilian standards [2] and based on the U.S. NRC 10CFR [3], which considers deterministic assumptions to preserve plant integrity and public health during the different operational conditions and in case of occurrence of a set of postulated accidents, the most severe being the design basis Loss of Primary Coolant Accident (LOCA).

In order to accumulate more experience concerning the use of probabilistic techniques and to produce a probabilistic model of Angra-I to be used by CNEN and FURNAS in the safety and operational plant analysis, a Probabilistic Safety Study (PSS) Level 1 [4] was carried out. This was the first work of the PSA type performed in Brazil, from 1982 to 1985, under an IAEA Research Contract.

The methodology used in the study was one of those recommended in the PRA Procedures Guide [5], called small fault tree/large event tree approach. In addition, to reduce event tree complexity and processing effort, the impact vector concept was adopted. Due to limited plant specific failure data available, in most of the cases, a generic data base was used to quantify system unavailabilities and the likelihood of accident scenarios.

Sixteen dominant accident sequences were selected, representing a contribution of 83% to the total core melt frequency, whose final value was 1.18E-03/year. It is important to remark that those PSS results should be carefully utilized, for this study has many limitations mostly due to the fact that it did neither adopt a plant specific failure data base nor perform an adequate data uncertainty treatment. Furthermore, this study no longer reflects the real plant design, since Angra-I was submitted later to many design modifications. Additionally, the last report version of the study was presented in a very draft form. Nevertheless, it represents a source of information on plant behavior in case of occurrence of a beyond design basis accident, as far as its results constitute if not quantitative, at least qualitative indicators of plant safety level.

In april 1992, the Utility submitted a report to CNEN as an addendum to the Angra-I PSS [6], in which a decrease in the core melt frequency was claimed (3.8E-05/year).

This addendum was examined by CNEN and considered very limited, since an adequate PSA review should follow a systematic process on assumptions and models adopting, as far as possible, plant specific data base and being presented as a report following a PSA standard format as recommended by a PRA Procedures Guide.

The existence of a limited version of Angra-I PSS report, led the Utility to consider it as a starting point on which a rigorous and complete review should be conducted, instead developing a new study.

Progress reports on the Angra-I PSA study review, as well as its expected final version, will be submitted to CNEN for further evaluation in the future.

To initially accomplish those activities, CNEN will be supported by an IAEA technical assistance mission covering, basically, the following items:

- to review the Regulatory Body position concerning the use of PSA in the Licensing of Angra-I NPP.
- to advise CNEN on the formulation of the regulatory requirements for the Authorization for Permanent Operation of Angra-I NPP, concerning PSA.
- to establish priorities with respect to a proposal of a complete review for the Angra-I PSS.

3. USING PSA TO ENHANCE ANGRA-I SAFETY

In Angra-I, the assessment of proposed backfits has been carried out without taking into account any probabilistic aspect, such as, for instance, system or function reliability calculation.

After a review of the PSS level 1 is completed, CNEN shall request the Utility to consider the use of PSA methods in the analysis of future design backfittings [7], which will help to justify the selected alternative, mostly concerning the achievement of the desired plant safety level.

As a consequence of the Angra-I PSS level 1 results, CNEN has already requested the Utility to perform supplementary safety analysis. Additionally to requirements established in the US 10CFR part 50.62, related to protection against Anticipated Transients Without Scram (ATWS) for Westinghouse type PWR reactors, CNEN requested the Utility to carry out the analysis of Angra-I response to the most limiting ATWS case, namely Total Loss of Feedwater [8]. According to the Angra-I PSS results, scenarios obtained from initiating events involving ATWS are the major contributors to the total core damage frequency (31.4%). The request of this study had the intention to verify whether the generic recommendations were sufficient to cover the specific case of Angra-I. As soon as the reviewed PSA version is finalized, the same treatment should be recommend by CNEN to similar cases, if they arise.

Concerning safety assessment, one of the most frequent tasks within the Regulatory Body is the evaluation of Utility requirements of AOT's (Allowed Outage Time) extensions/exemptions and STI's (Surveillance Test Interval) modifications to be implemented on the already approved Technical Specifications.

Angra-I Technical Specifications [9] present a lack of completeness in the formulation of some of the technical basis as well as some inadequate specifications.

Due to this fact, various specifications have very often been modified, but without following any uniform criterion or standard procedure. The justification for some of AOT's extensions/exemptions or STI's modification requirements presented by the Utility either makes use of the weakness associated with the technical basis or evokes a comparison with the Westinghouse Standard Technical Specifications [10], in case the latter is less restrictive.

Technical Specification modification requirements have been submitted to CNEN based on either engineering judgment or quantitative and qualitative considerations without taking into account any probabilistic aspect. Yet, PSA methods can be utilized to improve AOT's and STI's [11]. After adopting a PSA as a reference study, CNEN shall include PSA techniques in the assessment of Technical Specification modification requirements presented by the Utility.

Another application of PSA techniques is the identification of the most important precursors of significant accident sequences associated with incident reporting analysis [12]. The basic objective is to obtain, starting from the occurrence of an incident, a probability value which represents how close has the plant been to a core melt situation. In this sense, a work has been carried out by the Regulatory Body [13] to identify the most important precursors of significant accident sequences through a systematic analysis of the operational incidents which occurred in Angra-I during the years of 1984 and 1985. This was performed utilizing the dominant accident sequences obtained in the already mentioned PSS of Angra-I.

As a consequence of this work, the weaknesses of the current reporting criteria as well as the incompletenesses of the report contents appeared. The incident reporting criterion follows a CNEN standard [14], which is expected to be reviewed to include concepts of the root cause methodology. Within the Regulatory Body the systematic evaluation of incident report has just been modified to incorporate concepts of the methodology proposed by the IAEA (ASSET) [15], which recommends the use of PSA to assess the potential significance to safety of occurrences related to the event under analysis. Concerning this matter, no PSA application has been performed to the present date.

Regarding Accident Management, within the Regulatory Body, no plan to address severe accident issues for Angra-I has been developed up till now. However, the adoption of concepts from the U.S. NRC document on "Policy Statement on Severe Reactor Accidents", is under discussion. If those concepts are adopted, their implementation should follow guidelines of NUREG-1335 [16] and an Individual Plant Examination for Angra-I, using PSA methodology, should be performed by the Utility and submitted to be reviewed and evaluated by CNEN.

The current Angra-I emergency operating procedures are based on an WOG (Westinghouse Owners Group) programme [17], which includes a systematic evaluation of generic event sequences using Probabilistic Risk Assessment techniques. The results of this evaluation, presented in WCAP-9691 [18], indicate that the proposed Emergency Operating Instructions fully cover the generic Westinghouse type design basis events. Moreover, those Emergency Operating Instructions address a number of events beyond design basis. Therefore, plant-specific accident sequences, as results of an Angra-I PSA, shall be considered by the Utility to review the current status of the emergency operating procedures, to verify whether they cover the actual Angra-I response to severe accident.

The current Angra-I Emergency Plan follows US NRC Criteria [19]. Although the adopted planning basis is independent of specific accident sequences, a number of accident descriptions are considered, including the core melt accident release categories of the Reactor Safety Study [20].

The regulatory position is being reviewed within CNEN [21], concerning the definition of intervention levels and the corresponding protective measures, following IAEA recommendations [22], which requires a coherent revaluation of the considered release categories and associated risks.

The results of an Angra-I PSA shall be used to improve the current off-site emergency planning. Recommendations of corresponding protective actions to different emergency type situations should consider plant specific accident scenarios and consequences.

3. CONCLUSIONS

Although the relevance of the use of PSA concepts to enhance plant safety is internationally recognized, due to limited available resources to carry out this matter, a prioritization of the implementation of those measures should be considered.

A great effort is needed to perform the implementation of all possible PSA applications. Concerning the difficulties faced by the nuclear field in Brazil, it is expected that a long time will be necessary until a final version of a full scope PSA study is completed. However, some of the presented PSA uses can be put into practice by having only results of a PSA level 1.

Considering that Angra-I is under operation for more than ten years, priorities should stay with the implementation of matters related to the operational uses of PSA. Moreover, to support operational decisions, PSA level 1 is already sufficient, since it provides system and function information.

Among the priorities related to the use of PSA to improve operational issues, a complete review of the current Angra-I Technical Specifications should be carried out the first place. Some technical basis and surveillance requirements of Angra-I Technical Specifications were developed using concepts from generic Westinghouse operational experience. Moreover, some of the specifications have been modified, mostly after TMI-2 accident, but without following any systematic procedures or criteria to produce a coherent set of specifications. The way to implement a programme to improve the review of Technical Specifications is expected to be included in the terms of the Authorization for Permanent Operation of Angra-I, to be issued by CNEN.

Secondly, the priorities should be concentrated on the review of the emergency operational procedures to verify whether the existing Angra-I strategies of accident management are consistent with the plant specific response to severe accidents.

The use of PSA in the assessment of accident sequence precursors is dependent on the improvement of the incident reporting criteria. To accomplish that, CNEN intends to perform a review on the concerning regulation to obtain more accuracy and completeness in the reports presented by FURNAS.

Lower priority is given to the use of PSA to improve Angra-I emergency planning, mostly due to the fact that a complete PSA is required to conduct a review of the considered release categories and associated risks.

Safety related design changes, which are internationally recommended, have been incorporated to Angra-I without the help of PSA techniques (with the exception of the ATWS case), nor utilizing any probabilistic criterion for the decision making process. However, since Angra-I design is a very typical standard Westinghouse two-loop PWR, from the point of view of safety, design modifications take no priority to the above mentioned operational applications.

REFERENCES

[1]. INTERNATIONAL ATOMIC ENERGY AGENCY, The role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Power Plant Safety, Safety Series No. 106, IAEA, Vienna 1992.

[2]. COMISSÃO NACIONAL DE ENERGIA NUCLEAR, Licenciamento de Instalações Nucleares, CNEN-NE-1.04, Outubro 1984.

[3]. USA, Code of Federal Regulations, Title 10: Energy, Part 50 - 10 CFR 50, Office of Federal Register, January 1989.

[4]. COMISSÃO NACIONAL DE ENERGIA NUCLEAR, Estudo Probabilístico de Segurança da Central Nuclear Almirante Álvaro Alberto, Unidade I, Fase A, CNEN, DR-127/85, GAS-01/85, Rio de Janeiro, Abril 1985.

[5]. U.S. NUCLEAR REGULATORY COMMISSION, PRA Procedures Guide, NUREG/CR-2300, January 1983.

[6]. FURNAS CENTRAIS ELÉTRICAS S.A., Revisão da Análise Probabilística de Segurança da Angra-I - Nível 1, R-DEN.N.0003.92/R-DNTC.N.0028.91, Rio de Janeiro, Fevereiro 1992.

[7]. INTERNATIONAL ATOMIC ENERGY AGENCY, Case study on the use of PSA methods: Backfitting decisions, IAEA-TECDOC-591, Vienna, April 1991.

[8]. FURNAS CENTRAIS ELÉTRICAS S.A., Análise de Transitórios sem Desarme do Reator (ATWS) para Angra-I, Nota Técnica DCS.N.0026.86, Setembro 1986.

[9]. FURNAS CENTRAIS ELÉTRICAS S.A., Final Safety Analysis Report, Central Almirante Álvaro Alberto, Chapter 16, Technical Specifications.

[10]. U.S. NUCLEAR REGULATORY COMMISSION, Standard Technical Specifications for Westinghouse Pressurized Water Reactors, Draft, NUREG-0452, Revision 5, October 1984.

[11]. INTERNATIONAL ATOMIC ENERGY AGENCY, Use of probabilistic Safety Assessment to evaluate Nuclear Power Plant Technical Specifications, IAEA-TECDOC-599, Vienna, April 1991.

[12]. INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Plant Specific PSA to evaluate Incidents at Nuclear Power Plants, IAEA-TECDOC-611, Vienna, June 1991.

[13]. FERNANDES FILHO T. L., GIBELLI S.M.O., Angra-I Probabilistic Safety Study, Phase B, CNEN, DR-NT-GAPS-Nº02/88, Rio de Janeiro, Maio 1988.

[14]. COMISSÃO NACIONAL DE ENERGIA NUCLEAR, Relatórios de Operação de Usinas Nucleoelétricas, CNEN-NE.1.14, Janeiro 1983.

[15]. INTERNATIONAL ATOMIC ENERGY AGENCY, ASSET Guidelines Revised 1991 Edition, IAEA-TECDOC-632, Vienna, December 1991.

[16]. U.S. NUCLEAR REGULATORY COMMISSION, Individual Plant Examination: Submittal Guidance, Final Report, NUREG-1335, August 1989.

[17]. WESTINGHOUSE OWNERS GROUP, Emergency Response Guidelines, September 1983.

[18]. WESTINGHOUSE ELETRIC CORPORATION, Transient and Accident Analysis, (NUREG-0578 2.1.9.c), WCAP-9691, March 1980.

[19]. U.S. NUCLEAR REGULATORY COMMISSION, Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants, NUREG-0654, FEMA-REP-1, Rev. 1, October 1980.

[20]. U.S. NUCLEAR REGULATORY COMMISSION, Reactor Safety Study, An Assessment of Accident Risks in The U.S. Commercial Nuclear Power Plants, WASH-1400, NUREG-75/014, October 1975.

[21]. COMMISSÃO NACIONAL DE ENERGIA NUCLEAR, Diretrizes para Registro e Atendimento a Emergências Radiológicas ou Acidentes Nucleares.

[22]. INTERNATIONAL ATOMIC ENERGY AGENCY, Techniques and Decision Making in the Assessment of Off-Site Consequences of an Accident in a Nuclear Facility, Safety Series No. 86, Vienna, 1987.

SURVEY OF GERMAN PSA INVESTIGATIONS FOR NUCLEAR POWER PLANTS

H.P. BERG
Bundesamt für Strahlenschutz,
Salzgitter

U. HAUPTMANNS, P.M. HERTTRICH
Gesellschaft für Anlagen- und Reaktorsicherheit,
Köln

Germany

Abstract

One major topic of the Nuclear Regulatory Research Programme established by the supreme regulating authority is the probabilistic safety assessment (PSA) which constitutes at present an indispensible tool in the German nuclear safety work. Hence, for the further development of PSA a comprehensive research programme has been defined by BfS and BMU in 1991. The main issues of these activities are discussed, in particular the actual state of the German PSA-guideline and the supplementary chapters on special topics like human factors.

1. INTRODUCTION

In the Federal Republic of Germany both the construction and the operation of nuclear power plants are subject to comprehensive licensing and supervising procedures enforced by the respective Federal State Authority on behalf of the Federation. The prime responsibility for the safe nuclear power plant operation is assigned to the operating organisation. All necessary procedures are determined in the operating license in order to ensure the safe control of the plant under all conditions including investigations into operational experiences and systematic evaluation of advances in research and development for further safety improvements.

Because nuclear regulatory procedures must be tied as closely as possible to the actual state of scientific and technological knowledge, the Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (Federal Ministry for the Environment, Nature Protection and Nuclear Safety - BMU) has established in its responsibility as the supreme regulating authority a comprehensive Nuclear Regulatory Research Programme. This programme is in its main part now implemented at the Bundesamt für Strahlenschutz (Federal Office for Radiation Protection - BfS) which was founded in November 1989 as an autonomous Superior Federal Authority within the portfolio of the BMU.

One major topic of this programme is the probabilistic safety assessment (PSA) which constitutes at present an indispensible tool in the German nuclear safety work. Hence, for the further development of PSA a major investigative programme has been defined by BfS and BMU which has started at the end of 1991 and the beginning of 1992. The main issues of these activities are discussed in the following.

Because of the German approach - in analogy to the international understanding and development of PSA - towards a high standard of PSA, the creation of a PSA guideline for narrower analysis justification and its acceptibility has appeared to be adequate and recommendable. This guide should, in particular, contribute to the use of uniform analyses as a working tool. A first version of such a PSA procedure guide - developed by a group of experts - has been published in 1990 by the supreme regulatory authority. Additional guidance on human factors, common cause failures, and data collection is supplemented. The main aspects of these additional subjects are presented.

2. ACTUAL RESEARCH PROJECTS ON PSA

The complexity of nuclear power plants, the requirements for their efficient and safe operations, the occurrence of major accidents, and the resulting attention of the public to the safety of these facilities have accelerated the development and use of models that accurately represent these plants. The developed PSA-procedure has made it very clear that the events of interest are rare and any decision-making process that involves these events must account for the large uncertainties that are associated with their analysis.

Therefore, at national and international level comprehensive investigations have been performed concerning the PSA methodology. Nevertheless, the potential of PSA in practice is still far from being exhausted and the methodology is subject to continued development as well as promotion in various fields of application. The extension of PSA application - for example in the context of reevaluating and optimizing surveillance and test procedures - requires additional or new methods, models and, in particular, a different kind of data base.

For the further development of PSA in the Federal Republic of Germany, a major regulatory research programme has been defined by BfS and BMU. Main topics of this programme are:

- comparison of different international PSA studies with respect to methodology, models and results in order to gain insights for further investigations and developments in the Federal Republic of Germany; this comparison takes into account - among others - initiating events, plant status, event sequence analysis, and accident management procedures,

- characterisations of the state of safety technology by using qualitative and quantitative PSA results,

- improvement of methods for special issues like human factor dependencies, low power and shutdown operation as well as uncertainties,

- development of a proposal for a periodical precursor report system taking into account international experiences,

- PSA for fire events including a proposal for a guideline for this specific type of PSA,

- containment performance related to severe accidents,

- evaluation of existing computer codes based on explicit event sequences and fault trees of real plants comparing the results, calculation rules, input parameters and techniques to determine the cut-sets; development of a procedure for the qualification of PSA-codes,

- evaluation of existing PSA applications for passive and inherent safety features; resulting proposals shall be checked on the basis of examples,

- contribution to an integral risk management approach investigating different energy supplying systems,

- further investigations for providing a living PSA tool,

- improvements and further development of the PSA guideline based on experiences of the users and new scientific knowledge as well as

- a first approach to a guideline for the review of PSAs which are performed within the framework of periodic safety reassessments.

As recommended by the German Reactor Safety Commission in November 1988, every nuclear power plant would be made subject to at least three complete safety reviews during their lifetime. In practice, this recommendation leads to a periodic safety reassessment of nuclear power plants in operation about every ten years.

Essential elements of this periodic safety reassessment are the analysis and evaluation of the overall status including the operational experience of the respective plant and a probabilistic safety assessment.

Concerning the probabilistic safety assessments, an examination of balance of the safety concept of the plant is planned using probabilistic methods.

3. MOTIVATION OF A PSA GUIDELINE FOR NUCLEAR POWER PLANTS

The safety concept of nuclear power plants in the Federal Republic of Germany is at present mainly based on deterministic principles like

- safety features to prevent or control operational disturbances and incidents,
- reactor containment as a passive barrier against radioactivity releases in case of an incident,
- redundant and diverse safety systems to ensure high system reliability.

Safety decision making during design and licensing is essentially reduced to a verification of compliance with predescribed technical requirements as laid down in the standards.

However, these safety principles have steadily been improved and made more precise by the increase of conventional safety analyses and, in particular, of systematic PSAs which are supported to a large extent by plant-operational experience.

Using the analytical tool of a PSA, the safety design of a plant could be better balanced preventing both over and underdesign of safety features.

Such plant-specific PSAs offer an additional and different tool for evaluating a safety concept of a plant based on deterministic principles. Furthermore PSA delivers explicit results on the actual safety standard of a plant.

The use of PSA for designing a new nuclear power plant is a reasonable way to optimize - for example - mitigation measures for beyond design accidents during the planning phase of the respective plant. At the moment, this aspect of PSA is of minor importance in the Federal Republic of Germany because at present there is no application of a new nuclear power plant in Germany. The only important activity is the common project NPI of Germany and France where deterministic and probabilistic aspects form the basis for the design.

Until now, PSA in Germany is developed and mainly used for evaluating all system safety functions with respect to a spectrum of possible incidents resulting in sequences of a core-melt accident (level-1 analysis).

The broad application of level-1 PSAs justifies the exact definition of the PSA tool in a guideline.

Setting up such a guideline corresponds to German safety standards where in several regulations statements are given referring on the necessity of highly reliable safety systems.

For plants in operation such a PSA guideline can be applied for

- evaluating desired plant and system modifications,
- optimizing backfitting measures,
- reevaluating and optimizing surveillance and test procedures and safety related operational procedures,
- evaluating actual operational experience.

Moreover, as described above, a level 1+ PSA (level 1 plus active containment related systems) is required as one part of the periodic safety reassessment of nuclear power plants in operation.

A first version of a PSA procedure guide has been published in 1990 by the supreme regulatory authority, developed by a group of experts and taking into account the statements of the federal states. This version has been discussed in the Reactor Safety Commission and its application has been recommended.

The contents of the PSA guideline and the structure of the documentation of a PSA are shown in Table 1 and 2 respectively.

4. ADDITIONAL ISSUES OF THE PSA.GUIDELINE

The PSA guideline of 1990 only contains short statements on human factors, common cause failures and reliability data collection for technical systems. Therefore, additional guidance on these topics shall be supplemented; drafts of the amendments concerning human factors, reliability data acquisition and evaluation and common cause failures exist as proposals of a technical committee which have to be discussed with the federal state authorities. This procedure may start at the end of this year.

Table 1: Structure of the German PSA-guideline

1. Place and objective of the Guideline
2. Overview of the probabilistic safety analysis (PSA)
3. Input information for the PSA
4. Probabilistic Analysis
5. Data for quantifying event sequence diagrams and fault trees
6. Quantification of fault trees
7. Valuation and review
8. Documentation of the results of the analysis

Table 2: Requirements on the documentation of the PSA results

- list of documents used
- description of the events and event sequences analysed
- success criteria used
- fault and event trees elaborated
- reliability data used including their sources
- indication of the component models for independent and common cause failures
- indication of fault tree simplifications made before their evaluation (e.g. modularization, super-components etc.)
- indication of the method used for evaluating the fault trees (analytical or simulation) including parameters characterizing the quality of the final result
- indication of the type of documentation used for the results of the analysis (e.g. storage of computer output, microfiche etc.) including an appropriate codification
- results and their valuation

4.1 Approach to human factors

The general procedure is based on the well-known Swain and Guttman reliability handbook including ASEP for screening and as final result for less important human interventions.

Types of interventions which have to be treated are for example actions during stand-by, actions during an incident as prescribed by the operational manual or accident management actions. Acts like sabotage are excluded.

Data for rule-based and skill-based behaviour can be taken - as far as available - from the above mentioned handbook while data for knowledge-based behaviour have to be estimated. The use of plant-specific data would be very helpful.

Uncertainties are described by log-normal distributions, but the uncertainty factors recommended are larger compared with the data of the handbook (cf. Table 3).

4.2 Approach to the treatment of common cause failures

The basis of the evaluation of common cause failures are the relevant national (for example BEVOR data bank of the Gesellschaft für Anlagen- und Reaktorsicherheit) and international (for example IRS data bank of the OECD) data banks.

Concerning the relevance of observed failures engineering judgement is required. In order to give a guideline for this procedure, some criteria for the engineering judgement are developed like comparability of systems or distinction between immediate and underlying cause of failure. An observed failure shall be considered as a relevant failure if the immediate cause is applicable to the investigated system.

Table 3: Recommended uncertainty factors for human factors evaluation

Uncertainty factor of Swain	Uncertainty factor in German PSA-guideline
2	5
3	6,2
5	8,7
10	15,2
30	40,4

The probability assessment is based on a modified binomial-failure-rate model (BFR-model) as used in the German Risk Study Phase B with estimated error bounds; nevertheless, the need for an improved method of evaluation going beyond the BFR-model is recognized.

4.3 Approach to reliability data collection

Concerning the reliability data collection for technical components, main emphasis is laid on the use of plant-specific reliability data.

The detailed plant inventory, incident reports, maintenance records and records on time of operation or number of demands form the basis for such a reliability data collection.

Types of events which have to be taken into account are for example instantaneous failures, failures in the long term and unavailabilities. Important aspects are the type of repair and the way of discovery.

Systems which must be included are all safety systems, safety relevant operational systems and additionally operational systems which are part of the plant model.

For the evaluation of failure rates and unavailabilities the Bayesian approach is recommended. The results are approximated by log-normal distribution and multplied with a corrective distribution taking into account uncertainties due to extrapolation into the future or/and to other plants.

5. THE STATUS OF THE PSA GUIDELINE

The PSA guideline is, in particular, useful as a description of an accepted methodology including both methods and boundary conditions.

An example of methods is the use of the THERP method for human error quantification.

Examples of boundary conditions are the list of initiating events contained in the PSA guideline - which must, of course, be modified taking into account the respective plant-specific design - and the considerations of test and maintenance activities before an initiating event.

If the methodology of the PSA guideline is used in a specific PSA, the guideline can be referred to. If other methods or boundary conditions are used, they have to be described in detail in the documentation of the PSA.

Since an important goal is to have comparable PSAs as far as possible, a common source of guidance is desirable as to how to perform a PSA and how to obtain results with a comparable quality level. This is necessary due to the fact that different utilities, different authorities depending on the Federal State where the nuclear power plant is located and different expert institutions are involved in performing and reviewing the respective PSA.

On the other hand, the possibility to address special situations or use newer techniques is, however, also desirable. If these deviations prove generally useful and acceptable, their documentation could eventually support the inclusion of the new methods or new boundary conditions in the guideline.

This procedure implies the fact that the PSA-guideline is a living document. This is, indeed, planned and depends on results of the further development of PSA-methodology at national and international level on the one hand side and on experiences of the users of the PSA guideline and their suggestions for improvements.

Due to the fact that different institutions are involved in the review process of the PSAs provided by the utilities, a concept for a unified procedure of reviewing PSAs shall be performed. First results are expected by the end of this year.

6. CONCLUSION AND OUTLOOK

PSA is a very powerful tool to investigate, verify and improve safety practices. Therefore, the regulatory authorities are increasingly making use of PSA in safety evaluations of nuclear power plants and other kinds of nuclear facilities.

The results of the ongoing PSA projects in the Federal Republic of Germany described above should provide deeper insight into PSA methods. They will be evaluated with respect to their importance in order to prepare a basis for the decision if certain results should be implemented in a further version of the PSA-guideline.

There is an important linkage between PSA and deterministic criteria which are described in an annex of the PSA guideline called "probabilistic requirements in the regulatory framework". It is an impressive collection which appears as though it could indeed serve as a basis for setting analysis boundary conditions and identifying a large number of potential quantitative safety goals.

Nevertheless, for the time being, the deterministic and probabilistic methodologies have to be kept separately. It is in a first step necessary to interpret all the deterministic rules from a PSA point of view. In a further step, the results have to be integrated into a consistent and realistic framework. This is certainly a major task (involving a large number of judgements) which may be started in the future.

Considerations on possible probabilistic (i.e. quantitative) safety goals are not performed with high emphasis at the present

moment, but they may become more important with the further progress of the NPI project.

In particular, a risk-based procedure in the regulatory framework of the Federal Republic of Germany as envisaged by the USNRC is not part of the planned revision of the German Atomic Energy Act or relevant existing ordinances and safety criteria in near future.

USE OF PSA IN A REGULATORY FRAMEWORK

P.J. ROSS
Nuclear Electric plc,
Knutsford, Cheshire,
United Kingdom

Abstract

The paper will briefly describe the use of PSA in the licensing process for the Sizewell 'B' PWR Power Station currently under construction in the U.K. There are two distinct phases in the licensing process -

(i) A PSA has been performed to support the application to construct Sizewell 'B'. At that stage the PSA was used as a design tool (along with deterministic design requirements) for Sizewell 'B' and as such lead to a number of significant design changes in the early design process.

(ii) A PSA is currently being performed to support the application to operate Sizewell 'B'. The PSA is required to support the claim that the design has included all reasonably practicable measures to prevent and mitigate accidents.

The comprehensive PSA being produced for the second phase of the licensing process will be described.

The way the regulators/designers/analysts have interacted over the years has affected the scope, complexity, detail and bias of the comprehensive PSA. The paper will discuss these issues and highlight some of the more significant ones. The benefits and drawbacks of providing a PSA in a regulatory framework will be discussed.

One of the conclusions of the paper is that the use of true "best-estimates" in the PSA is difficult to achieve in a regulatory framework where persistent bias to the conservative side is apparent in the designers, analysts and regulators judgements. The usefulness of the PSA is therefore, potentially, compromised by giving misleading outputs or diverting resources to unnecessary areas.

1. INTRODUCTION

In the late 70's, the Central Electricity Generating Board (CEGB), Nuclear Electric's predecessor, set itself probabilistic targets for new nuclear power plants for the frequency of various levels of radiological release. These targets were to be used by designers to help in the preliminary and detailed design phases of new nuclear reactors. This meant that a Probabilistic Safety Assessment (PSA) was required to be performed even at the preliminary design stage for the Sizewell 'B' PWR power station. Although this was a self imposed requirement of the utility it was discussed with the regulator the Nuclear Installations Inspectorate (NII). The NII ultimately adopted the CEGB's presentation of these targets.

As a consequence, the licensing of Sizewell 'B' has been linked to the PSA for the plant. This is performed in two fundamental stages - i) clearance for construction of Sizewell 'B' and ii) having constructed Sizewell 'B' clearance to operate it - consequently there have been two significantly different PSAs performed.

The Pre-Construction Safety Report (PCSR) was first issued in 1982 and contained a preliminary level 1 PSA. This was sent to the NII in support of the application to begin construction of Sizewell 'B'. At that time, however, the Secretary of State for Energy called for a Public Inquiry to be held into the application to build a PWR Power Station at Sizewell. The Public Inquiry which ran from late 1982 to early 1985 (the longest ever in the UK history) dealt with all aspects of the application including safety and the PSA. Consequently throughout 1982-1985 the preliminary PSA was discussed and addressed with both the regulator and at the Public Inquiry.

In 1986, the Inspector published his report that gave the go ahead for Sizewell 'B' subject to the normal licensing process and requirements of the NII. A licence to construct Sizewell 'B' was given in 1987 based on the information in the Pre-Construction Safety Report and supporting references. However, as the detailed design was not finalised and following discussions with NII, CEGB entered into a number of additional committments to be addressed within a subsequent PSA to be performed for the Pre-Operational Safety Report (POSR).

This paper goes on to discuss the PSA performed for the PCSR and the commitments for further more detailed work referred to above. This led to the highly detailed, complex and comprehensive analysis, currently nearing completion, that is being carried out for the POSR. Having been through this process it is clear there are many lessons to be learnt in attempting to develop a highly complex and comprehensive PSA; this paper attempts to highlight the more significant ones.

Although a large part of the PSAs performed addressed the large releases (in our case this translates not to a core melt but to a release equivalent to a whole body dose of 100 mSv or greater at the site fence) there are also targets for smaller releases. The targets set were as follows:

Dose Band	Summated Frequency for all Faults
0.1 - 1.0 mSv	10^{-2}/year
1.0 - 10 mSv	10^{-3}/year
10 - 100 mSv	10^{-4}/year
> 100 mSv	10^{-6}/year

Note that these were set as targets to be aimed for <u>not</u> acceptance criteria.

The following sections go on to discuss the preliminary PSA performed for the construction licence, the regulators review of that preliminary PSA, the final PSA and the overall impact of using PSA in a regulatory environment.

2. PSA FOR THE PRE-CONSTRUCTION SAFETY REPORT

i) Releases leading to doses < 100 mSv

To determine the release frequencies for releases leading to a dose < 100 mSv the fault schedule was reviewed to identify faults which could lead to a potential increase in radioactivity released to the environment (e.g. would the fault lead to failed fuel; would the fault lead to relief valves opening). Then the barriers between that increased release and the environment were reviewed to estimate the failure probability of the barriers and thus produce an estimate of the frequency of releases to the environment. The actual releases were then assessed to determine which dose band each release should belong to.

Specific, more detailed, analyses were performed for certain significant faults such as Loss of Coolant Accidents (LOCA) and Steam Generator Tube Ruptures (SGTR).

The results of this preliminary analysis showed the targets to be met. It was recognised that the analysis was not "complete" but it did give confidence that the basic design was acceptable and that no significant design changes would be required.

ii) Releases leading to doses > 100 mSv

Because the analysis was addressing releases leading to doses of greater than 100 mSv the analysis was required to address two sets of conditions:

Degraded Core

Conditions arising, for example due to the failure of decay heat removal systems, such that coolable geometry of the core may not be maintained.

Containment Bypass

The uncontrolled discharge of RCS inventory into the containment due to an initiating or consequential LOCA, with failure of the containment systems to maintain the containment within design basis conditions, or failure of the isolation valves to close to prevent leakage to the environment. This covers non-degraded core conditions.

Fault Tree Analysis was performed to derive the probability of each of the above conditions given an initiating fault. In principle such fault trees are required for each initiating fault however, for this analysis the initiating faults were grouped together on a judgemental basis; thus reducing the amount of analysis necessary.

A functional fault tree was drawn for each initiating fault group. The functional fault tree modelled the way in which safeguards system failures combined to produce one of the conditions defined above. System fault trees were drawn for each of the systems that appeared on the functional fault trees. The system fault trees modelled the way in which component failures combine to produce system failure. The system fault trees included inputs from the service systems on which operation of the system is dependent e.g. electrical and cooling water supplies.

For each initiating fault, the functional fault tree and associated system fault trees were combined to produce one overall fault tree which was then analysed to derive the failure probability.

The results of this preliminary analysis showed for the faults analysed the frequency of releases greater than 100 mSv was about 5 x 10^{-6}/year. There were some significant omissions from the analysis which are discussed below.

iii) Omissions from the analysis

The preliminary analysis described above was not a "complete" analysis and areas which had not been addressed were identified, these included:

- Faults during shutdown and refuelling
- Modelling of failures in the Reactor Protection System (reactor trip and safeguards actuation)
- Modelling control systems
- Internal and External Hazards (e.g. seismic, fire, turbine disintegration etc.).
- Operator Errors
- Beyond Design Basis Initiating Faults (BDBIFs)

Work was put in hand to address these areas for the PSA in support of the POSR.

iv) Overall Conclusions from the Preliminary PSA

Judgements were made that for the releases <100 mSv the preliminary analysis had shown the targets could be met.

For the releases >100 mSv the fault tree analysis performed had shown a frequency of about 5 x 10^{-6}/year. Furthermore, judgements were made that the omissions from the analysis would contribute about 2 x 10^{-6}/year thus leading to an estimated frequency for releases >100 mSv of 7 x 10^{-6}/year.

Numerous pessimisms in the analysis were noted and the conclusion made that the 10^{-6}/year target could be met. However, the analysis performed (and the judgements about the analysis not performed) had confirmed that a target frequency for releases >100 mSv was very stringent. Consequently in presenting the case to the regulators it was stated that if this target was not met the analysis would be extended to ensure that the risk of death to any individual member of the public was less than 10^{-6}/year. This was the fundamental criterion that had led to the setting of the targets discussed in the introduction.

3. THE REGULATORS REVIEW OF THE PRELIMINARY PSA

The review of the Preliminary PSA was a part of the review of the PCSR as a whole. Consequently as with the rest of the safety case there was a reluctance to accept judgements of a best-estimate nature without justification. The emphasis required from the NII was to demonstrate and justify the completeness and acceptability of the safety case (including the PSA).

The NII did however welcome the considerable effort which had been devoted to producing the PSA in support of the safety case and the attempt made to show that the design met the probabilistic targets. They commented that the analysis had made a valuable contribution to the safety case, but that the analysis also had limitations in that it excluded many contributors.

Taking into account the reviews of the preliminary PSA the CEGB recognised the need to develop the PSA in a number of areas and the following are significant in relation to this paper:

- The identification of all sequences leading to releases <100mSv and the demonstration of consistency with the transient analysis performed.
- The inclusion of greater detail in the PSA, i.e. address all initiating faults, all operating states.

- The identification of contributors from other sources (e.g. External Hazards, Beyond Design Basis Initiating Faults).

These commitments have led to a greatly increased scope of the PSA for the POSR. The next section briefly reviews the effect of these commitments on the scope of the work performed.

4. PSA FOR THE PRE-OPERATIONAL SAFETY REPORT

i) Releases leading to doses < 100 mSv

The requirement to identify all sequences leading to releases <100mSv was of itself quite onerous. It led to the use of large event trees to model post-trip behaviour of the pressuriser relief system, condensers, turbine trip, secondary circuit relief system and other ancillaries (the event trees do not model the success or failure of decay heat removal). These event trees led to many hundreds of sequences for each event tree analysed which had to be shown to be within the design basis and lead to doses <100mSv. The requirement to demonstrate consistency with the transient analysis led to an even greater complication.

The transient analysis that had been performed was based on the design transients and contained generic pessimistic assumptions throughout the data sets and in the modelling (i.e. in the computer analysis codes). Also the structural integrity limits for the plant had been conservatively set. The aim of the use of pessimistic assumptions was originally conceived for the deterministic transient analysis work to allow for margins associated with other unknown effects. However, the output from the event tree analysis was a list of thousands of very specific sequences and their associated frequencies. To allow for transient analysis of these sequences, they were reduced to a set of Limiting sequences for each event tree analysed. They were then further reduced to a set of Bounding Limiting sequences covering a number of event trees. Consequently the type of sequence analysed by transient analysis had a large number of failures included in it. (Note: at this stage successful operation of Auxiliary feedwater, safety injection etc. is based on the minimum safeguards requirements; typically one pump out of 4 only is assumed to work successfully). An example of a bounding limiting sequence is:

Unisolated Feed Line Break:

+ Blowdown of water at zero quality

+ RCS over pressure transient, up to 4 pressuriser relief valves fail to open.

+ Failure of the Primary Protection System

+ Loss of off-site power.

  - Condensers assumed unavailable

  - Loss of Reactor Coolant Pumps at any time in transient (including pre-trip).

  - Loss of main feed.

+ Loss of auxiliary feed control.

+ Failure of 2 RCCAs to insert on reactor trip.

+ SG overpressure on more than 1 SG.

The failures noted above are largely independent events and an estimate of the sequence frequency suggests a value less than 10^{-15}/year! Because of the way all sequences bounded by this are included in the bounding sequence frequency the above is associated with a sequence frequency of 2.9 x 10^{-4}/year. The above is then shown by (pessimistic) transient and radiological analysis to lead to releases <100 mSv.

The amount by which the pessimisms are compounded at each stage of the analysis is apparent.

The analysis involved in the generation of the event tree sequences was further compounded by the large number of initiating faults (~170) on the fault schedule and the need to address all operating states.

ii) Releases leading to doses >100 mSv

The commitment to include greater detail in the PSA led to an extensive fault schedule and an even more extensive safeguard schedule (i.e. the list of success criteria for feedwater, safety injection, boration etc.) because the failures from the event tree analysis could affect the safeguard system requirements.

This allied with the requirement for more detail in the fault tree support system modelling and the need to address all operating states, has led to an enormously complex fault tree analysis(the fault tree analysis primarily addresses the failure of decay heat removal). Although faults have been bounded to reduce the amount of analysis required (and therefore introduced the sort of conservatisms discussed above) there are still some

61 fault trees to be analysed
58 systems modelled in the fault trees

each fault tree typically consists of

1500 components
900 gates
10 inputs from event trees to fault trees

With cut-off frequencies set very low ($\sim 10^{-10}$/year) there are typically 5000 cut-sets per fault tree.

Because of the complexity of the analysis it became apparent that many bounding assumptions and the associated success criteria were grossly pessimising the results from the fault tree analysis. For example the Feed Line Break fault described above is assessed as requiring 3 oo4 Emergency Boration Tanks injecting boron into the RCS. This requirement is, however, associated with the Feed Line Break fault with no further failures; but the sequence frequency from which the 3 oo4 requirement came from is already less than 10^{-15}/year! The real requirement is probably 0oo4 (no other PWR plant has an Emergency Boration system).

As the data derived for the probabilistic analysis was being derived in a regulatory framework claims of data being "best-estimate" were often questioned. This led to a generic bias in the data to the pessimistic side because such data could be more readily justified in a licensing submission. Likewise the modelling was also biassed to the pessimistic side by counting failures in the data base which the modelling would assume to lead to loss of functionality whereas the actual failure recorded in the data did not lead to total loss of functionality.

The complexity of the analysis makes it less flexible than we would have liked. However, to remove the worst of the pessimisms we are currently reviewing the individual cut-sets to identify and correct the types of gross pessimism noted above.

iii) Contributions not previously assessed

Following the commitment to identify all possible sources which may contribute to releases >100 mSv the following have been included in the analysis.

- Beyond Design Basis Initiating Faults (BDBIFs)

  BDBIFs are faults where no specific protection has been designed into the plant (these include the *incredible initiating faults* such as Reactor Pressure Vessel and Steam Generator Failures). This does not mean, however, that a BDBIF would always lead to plant damage. A list of BDBIFs has been produced (about 80 such faults have been identified) and case by case assessments made of the likelihood of plant damage (if any) and the frequency of each fault.

- Operator Errors (not covered elsewhere)

  It was recognised during the analysis that there may be contributions (albeit few) from operator errors that could lead to plant damage which had not been included in the event tree or fault tree or other analyses. Therefore a further route for the inclusion of other significant operator errors has been incorporated into the analysis. This 'direct estimation' route (largely based on reviews of Operating Instructions) extends the coverage of the quantification of operator errors beyond the normal coverage of a fault tree analysis.

- Internal and External Hazards

  Hazards have been addressed by various combinations of techniques such as event and fault trees and the extensive use of engineering judgement. In outline the analysis consisted of a three stage process:

  i) Production of a comprehensive list of possible hazards (about 60 such hazards were identified).

  ii) Use of a screening process to eliminate hazards not possible at Sizewell, or of very low frequency or bounded by another fault or hazard being analysed.

  iii) Quantification of the hazards not screened out.

  Contributions to the frequency of plant damage are being incorporated in the PSA.

- Non-reactor Core Sources of Radioactivity

  These include contributions from the radwaste plant and the fuel building/handling faults. These faults have generally been addressed using event tree and fault tree techniques, although simpler analyses were performed than those performed for the faults associated with the reactor core. These contributions are being incorporated in the PSA.

5. IMPACT OF THE USE OF PSA IN A REGULATORY FRAMEWORK

The previous section has highlighted the way the PSA has been greatly increased in scope to provide as complete a PSA as practicable. The highly complex and exhaustive analysis now nearing completion has led Nuclear Electric to think about the benefits and drawbacks of such a highly complex PSA. This section tries to highlight such lessons learnt.

i) Benefits

The detailed review of the results of the PSA, which is primarily aimed at removing the worst of the pessimisms, has also led to a much greater understanding of the types of failure sequence that can lead to a significant release. Indeed the reviews of individual cut-sets has led Nuclear Electric to identify (among other things) :

- The types of sequences that are leading to releases >100 mSv and hence if a particular type is dominant
- If there are any other safeguards systems which could be used (whether in it's intended role or in an off-normal role) to prevent the damage occurring
- Any further Operator actions that may prevent the damage occurring
- If more frequent testing of equipment could significantly reduce the frequency of releases >100 mSv

The use of detailed analysis overcomes the uncertainty associated with gross judgements. For example at the PCSR stage the effects of Shutdown conditions and Hazards were presumed to be secondary to the "traditional" internal plant faults at power. The complex analysis is now beginning to show (once gross pessimisms are removed) that the shutdown conditions and hazards are significant; indeed hazards occurring while at shutdown may provide the largest contribution to the results.

The need to systematically identify and consider, in some way, all possible routes to a release greater than 100 mSv means that failures other than core melt have to be considered. One significant contributor to risk comes from a series of isolated 'V' sequence LOCAs (i.e. where the Operators have successfully closed an isolation valve within 1 hour). These types of sequences would be missed if an analysis was based on core melt only.

The analysis performed has put Nuclear Electric into a position where it has an unprecedented understanding of the Sizewell 'B' design and the way the systems interact. This places us in an excellent position for any future work in assessing the potential benefits and limitations of future designs.

ii) Drawbacks

The driving aim behind the commitments entered into by the CEGB was to demonstrate completeness and to quantify contributions wherever possible. This has been a major reason for the extremely complex analysis performed. That analysis is so complex that even simple re-runs of it are a major resource undertaking. It would have been far better to qualitatively review the fault schedule and safeguard schedule to identify the potentially significant initiating faults and their associated success criteria. Only the reduced set of such potentially significant faults need be analysed.

In a similar manner, the extensive analysis for releases <100 mSv could be dramatically curtailed. More importantly the use of detailed event tree analysis to derive hundreds of sequences for each event tree which are then reduced to Bounding Limiting sequences which in turn are addressed by pessimistic transient analysis is not necessary for a PSA. The potentially significant sequences should be identified and analysed using best estimate data and modelling. Pessimistic transient analysis should be reserved for deterministic analysis of design transients where it has a useful role to play. The use of conservative transient analysis of the Bounding Limiting sequences to justify the success criteria leads to a blurring of the distinction between the deterministic design basis analysis and the "best estimate" probabilistic analysis (as well as introducing excessive conservatism in the latter).

The success criteria to prevent releases > 100 mSv should be based on best estimate transient analysis data and modelling. The use of pessimistic analysis had directly led to gross over-complication of the analysis. Also it is clear that many of the failures identified are not real failures; the reviews of cut-sets currently being undertaken highlight the potentially misleading results from such pessimistically set success criteria. Similarly the use of pessimistic data in the probabilistic modelling should be avoided. The way the pessimistic analysis could distort the results and lead a utility into expending resource unnecessarily concerns the regulators as well as the utilities.

6. CONCLUSIONS

This paper has discussed the impact of the use of PSA in the regulatory framework for Sizewell 'B'. As one of the most complex and comprehensive PSAs currently being performed there are many lessons to be learnt. There have been many benefits and drawbacks that have been identified from the analysis. this paper has tried to highlight the more significant ones.

The analysis performed has put Nuclear Electric into a position where it has an unprecedented understanding of the Sizewell 'B' design and the way the systems interact. This places us in an excellent position for any future work in assessing the potential benefits and limitations of future designs.

In summary, an ideal PSA will:

- consider, but not quantify, all possible routes to a radioactive release.
- consider, but not quantify all, possible ways of leading to a core melt.
- identify those faults and fault sequences which are potentially major contributors and quantify those.
- use best estimate analyses at all stages (probabilistic, transient and radiological analyses).
- keep the resultant logical models small enough to allow simple re-runs of the analysis; this is how many significant insights into the reactors safety characteristics can be gained.

STATUS AND FUTURE PROSPECTS OF REGULATORY ISSUES OF PSA APPLICATION IN THE UKRAINE

G. GROMOV
Ukrainian State Committee for Nuclear and Radiation Safety,
Kiev, Ukraine

Abstract

From the regulatory point of view safety assessment means the safety analysis that should be submitted to the licensing authority for review and getting relevant license. That implies existence of a comprehensive system of regulatory criteria and requirements in compliance to which the submitted safety case should be assessed.

Nowadays the Probabilistic Safety Assessment (PSA) is becoming one of the obligatory components of the safety substantiating materials to be submitted to the regulatory body for review within standard licensing procedure. So it requires a definite and sophisticated system of regulatory requirements and PSA acceptance criteria to be elaborated and established within the general safety assessment regulatory framework.

The paper briefly outlines probabilistic and quantitative criteria elaborated earlier in the USSR, which now are included in the safety regulations and standards in force in the Ukraine. Those regulations are valid until introduction of a new nuclear legislation and safety regulations in the Ukraine.

General principles of DANU standpoint concerning future prospects of PSA regulation in the Ukraine are following:

1. Probabilistic techniques and approaches should be used to determine and demonstrate the sufficiency of established deterministic safety requirements.
2. Mostly appreciated are optimizational applications of PSA concerning safety:
   - achieving a smooth risk profile across the plant level;
   - expansion of a radiation protection principles to the risk-oriented criteria (e.g. application of ALARA principle to the calculated risk characteristics of the plant at the design stage).
3. The regulatory body decision making criteria should be differed for every definite kind of PSA application.
4. As for absolute quantitative probabilistic criteria, it is intended to replace the only core melt and RPV destruction frequencies for risk acceptance criteria/correlations for whole range of possible radiological consequences of PIEs, thus giving classification base for different modes of operations.

Taking into account the need for clear correlation and inter-connection of regulatory deterministic and probabilistic criteria, initial revisions of the upper level safety regulations is intended to avoid the postulation of any absolute quantitative risk-oriented criteria. Such definite regulatory requirements is reasonable to place into special PSA guidelines.

An important aspect of risk-oriented safety assessment approaches regulation is an appropriate organizational structure of the regulatory body and its sub-divisions. So the paper also describes the relevant functional distribution between different laboratories of the Scientific & Research Center of the Ukrainian State Committee for Nuclear & Radiation Safety.

In present in Ukraine 12 units are in operation on five NPPs. These are 10 units VVER-1000/320 and 2 units VVER-440/213 and the other 3 units of the type VVER-1000/320 are now under construction and they will be put into operation soon.

The three units of Chernobyl NPP are to be put out of operation on the decision of Ukrainian Goverment in the year 1993.

In the nearest future we plan to run operation of the existing NPPs only and we do not plan to build new NPPs. In this respect it is interesting to have a closer look at the NPPs of the type VVER-1000/320 and VVER-440/213.

Chernobyl NPP and "Ukrytiye" (Shelter) construction constitute another specific problem that needs further investigation, because there has not been complete understanding and no programme of investigation has been adopted yet.

Dershatomnagliad as an independent organization exists just a little more than half a year therefore it is quite understandable that we have to use at this stage the sets of regulations that were in use in the former USSR.

That is first of all the set of regulations OPB-88 (General Safety Regulations-88) and a number of other regulations on the lower level. These regulations specify probabilistic safety techniques and in OPB-88, in particular, required safety criteria are presented, that is: frequensy of core melting and the probabitity of out of design releases of radionuclides.

In the new set of regulations that are being developed now the stress would evidently shift to the deterministic approach, that is, besides probabilistic parameters, deterministic principles would be taken into account.

First of all it can be ascribed to the fact that the existing database for probabilistic analysis is not thorough and reliable becanse no integral approach for data collection and for processing of the primary information on NPP operation, especially for common failures and operators failures has been adopted. These shortages in the database are coped with the help of foreign sources.

The existing database (table 1) does not tale into account the specifics of the equipment and its operational conditions for different NPPs it is one and the same for all NPPs. Thus the results of the probabilistic analysis, for example, for VVER-1000/320 of different units and plants are practically equivalent. Therefore the existing probabilistic analysis carried out for VVER-1000/320 and VVER-440/213 do not reflect life cycle changes in the equipment.

I would like to dwell upon PSA for VVER-1000/320.

In the analysis several variants has been considered, one of them corresponds to the existing technological regulations and design, in the rest of the variants there are variations in organization of the operation of the safety systems during capacity operation of the unit and some insignificant changes in the design have been proposed. The aim of these changes is to cope with design safety drawbacks.

The analysis has been done for practically all initial internal events of the accident:

- small leakage (dia 30) of the first circuit;
- medium leakage (dia 150) of the first circuit;
- large leakage (dia 800) of the first circuit;
- leakage from the first circuit to the second dia.100 (blowing up of the lig of the steam generator);
- leakage of the second circuit in the dumping part;
- leakage of the second circuit in the nondumping part;
- disruption of normal heat removal in the second circuit without loss of integrity;
- power failure for up to 1 hour and 72 hour,

and with taking into account common failures and human errors.

We stick to conservative assumption in the analysis. The essence of this assumption is the following: when the fuel reaches the second design threshold, that is, the temperature of the fuel surface increases up to 1200 C, further destruction of the core with the subsequent destruction of the containment takes plase as the result of its melting through with the maximum radionuclides release.

The results of this analysis are given in the table 2. The weak point of this project is low reliability of the function of continuous heat removal from the core.

The proposed measure is the following: regeneration of the function on account of minor design changes in the safety systems of the second circuit, permits to significantly increase reliability of the unit. It allowed us to give recommendations on operation directed at "liberalization" of periodicity and the strategy of control of some safety systems which are not critical in this project.

TABLE I

NN n/n	Denomination	Type of failure	Intensivity of failure 1/hour			Time of restoration
			Medium	Maximum	Minimum .	
1	2	3	4	5	6	7
01	Emergency feed-water pump (ЦН-150-90)	Failure to start Failure to run Damage	3.0E-6 30.0E-6 21.0E-6	9.0E-6 90.0E-6 84.0E-6	0.9E-6/H 7.5E-6 3.0E-6	36 36 11
02	High pressure injection (ЦН-150-110) Low pressure injection (ЦНР-800-230)	Failure to start Failure to run Damage	8.3E-6 50.0E-6 46.0E-6	25.0E-6 150.0E-6 77.0E-6	1.7E-6 - 24.0E-6	36 36 5
03	Tank	leakage	0.01E-6	0.1E-6	-	24
04	Fan, cooling air	Failure to start Failure to run Damage	10.0E-6 10.0E-6 130.0E-6	30.0E-6 30.0E-6 300.0E-6	- - -	- - -
05	Motor	Failure to start Failure to run	9.0E-7 5.0E-6	20.0E-7 25.0E-6	0.6E-7 1.0E-6	2 2
06	Air operated valve	Failure to open Failure to close	3.0E-6 3.0E-6	11.0E-6 9.0E-6	1.4E-6 1.4E-6	- -
07	Motor operated valve	Failure to open Failure to close Failure to close Failure to remain in position	5.0E-6 5.0E-6 3.0E-3/D	13.0E-6 13.0E-6 6.0E-3/D	1.0E-6 1.0E-6 -	- - -
08	Safety valve	Failure to open Failure to close Failure to remain in position	6.0E-7 1.0E-2/D	36.0E-7 3.0E-2/D	0.9E-7 2.3E-3/D	- -
09	Heat exchanger	Leakage	1.0E-6	5.0E-6	-	-
10	Check valve	Failure to open Failure to close	0.3E-6 3.0E-6	3.0E-6 9.0E-6	0.06E-6 0.6E-6	10
11	Relief valve	Failure to open Failure to close Failure to remain in position	9.0E-6 2.0E-2/D	90.0E-6 4.0E-2/D	0.9E-6 0.2E-2/D	24
12	Diesel generator	Failure to start 1 Failure to run 2 Failure to run Damage	5.8E-5 1.5E-3 1.5E-3 1.3E-4	9.1E-5 4.5E-3 4.5E-3 1.5E-4	3.3E-5 5.0E-4 5.0E-4 0.7E-4	16 2 30 6
13	Battery	Failure to function	1.0E-6	3.0E-6	0.1E-6	-
14		Failure to function	1.0E-6	5.0E-6	0.3E-6	-
15	Distributing electric circuit	Failure to function	5.0E-6	15.0E-6	-	10
16		Failure to function	1.0E-5	8.0E-5	0.25E-5	-
17	Rectifier	Failure to function	1.0E-6	6.0E-6	0.5E-6	-
18		Failure to run	1.0E-7	20.0E-7	0.02E-7	-
19	Transformer	Failure to function	6.0E-7	30.0E-7	1.5E-7	-
20	Switch (all types)	Failure to function	8.0E-6	24.0E-6	0.8E-6	24
21	System of proper needs provision	Failure to function	5.0E-6	11.4E-6	-	10
22	Main steam line isolation valve	Failure to open	1.0E-6	-	-	-

TABLE II.

NN n/n	Initial events of the accident	Probability of IFA	Probability of core damage									
			Var. 1		Var. 2		Var. 3		Var. 4		Var. 5	
		1/year	abs. 1/year	relat. %	abs. 1/year	relat. %	abs. 1/year	relat. %	abs. 1/year	relat. %	abs. 1/year	relat. %
1	Leakage of the second circuit in the nondumping part	1.00E-4	8.47E-7	<1	8.42E-7	<1	8.51E-7	<1	8.42E-7	<1	8.42E-7	1
2	Leakage of the second circuit in the dumping part	1.00E-3	1.45E-5	3.67	1.35E-5	3.99	1.65E-5	4.02	1.35E-5	3.94	4.56E-6	5.7
3	Disruption of normal heat removal in the second circuit without loss of integrity and technol. condenser (TC)	7.00E-2	5.46E-6	1.38	4.76E-6	1.41	5.78E-6	1.41	4.76E-6	1.39	9.99E-7	1.2
4	Disruption of normal heat removal in the second circuit without loss of integrity and with of TC	3.00E-2	2.37E-4	60.00	2.05E-4	60.65	2.51E-4	61.21	2.05E-4	59.9	3.44E-5	43
5	Large leakage of the first circuit	3.20E-4	8.60E-7	<1	9.00E-7	<1	1.80E-6	<1	9.00E-7	<1	9.00E-7	1.12
6	Medium leakage of the first circuit	1.00E-3	4.50E-8	<1	4.70E-8	<1	1.30E-7	<1	1.32E-7	<1	1.32E-7	<1
7	Small leakage of the first circuit	3.20E-3	2.06E-6	0.52	1.88E-6	0.56	2.43E-6	0.59	2.22E-6	0.6	2.22E-6	2.77
8	Leakage from the first circuit to the second	1.00E-3	6.37E-6	1.61	6.50E-6	1.92	1.05E-5	2.56	1.09E-5	3.18	1.09E-5	13.6
9	Power failure for up to 72 hour	7.00E-3	1.25E-4	31.65	1.02E-4	30.18	1.18E-4	28.78	1.02E-4	29.8	2.39E-5	30
10	Power failure for up to 720 hour	1.00E-4	2.97E-6	0.75	2.64E-6	0.78	2.88E-6	0.70	2.64E-6	0.77	1.21E-6	1.5
	Total		3.95E-4	100	3.38E-4	100	4.10E-4	100	3.42E-4	100	8.00E-5	100

ROLE OF PSA IN LICENSING, REGULATION AND DESIGN AS APPLIED IN THE NETHERLANDS

M.F. VERSTEEG
Nuclear Safety Department,
The Hague, Netherlands

Abstract

A historical perspective of PSA applications in the Netherlands is provided in the paper. PSA programmes for existing NPPs are briefly overviewed. An information concerning future PSA activities is also provided. Regulatory guidance and pre-conditions related to PSA applications are discussed. Regulatory use of PSAs in licensing process is briefly described. Current PSA activities for new and advanced NPPs are also presented.

I. PSA APPLICATIONS IN THE NETHERLANDS; A HISTORICAL PERSPECTIVE.

Although, there are only two operating nuclear power plants (NPP's) in the Netherlands and a further expansion of this small program is still undecided, Probabilistic Safety Assessments (PSA's) play a major role in NPP licensing and regulation. PSA's are necessary for obtaining a construction license for a new NPP, as well as in the required periodic safety review of an existing NPP. It is evident that in both cases the results will have design implications.

Before Chernobyl two new nuclear power plants were foreseen in the Netherlands. To show compliance with the at that time newly postulated environmental safety goals for new hazardous installations, a level-3 PSA was foreseen to be part of the siting and licensing procedure. Such a PSA should aim at a more global/integrated assessment of the plant safety. It should contain an element of overall adequacy, in that it is deemed desirable to be able to compare the assessed safety-related capabilities of a NPP against the probabilistic safety criteria and objectives (PSC)[1, 2] which were formulated by the Dutch government at that time.

In the mid-eighties the Dutch government had adopted a more general and integrated safety policy regarding potential hazardous industries and activities (not only nuclear). This 'external' safety policy explicitly referred to the safety of each single individual in the vicinity of a hazardous plant and of the population as a whole. Explicitly a verification step in relation to pre-set probabilistic risk criteria was included in this policy.

Because of the aforesaid 'external' safety policy, a PSA would not only play a role in identification of weak spots in the prevention and mitigation of severe accidents, but also a leading role in a verification process. Although these probabilistic safety criteria have been developed to create a yardstick for proper assessing the risk of new hazardous industries, these criteria have recently been declared to be applicable to existing NPPs as well.

One application would be the use of the PSA for siting. It can be used to judge the acceptability of a proposed site or to compare the alternatives in this respect.

After Chernobyl the decision to expand the nuclear power capability was postponed. The government decided to reconsider the nuclear option. Several studies were initiated to help them with this decision-making process. A major part of these studies was devoted to safety related issues of the existing Dutch NPP's. One of these studies was about the possible accident management measures of the nuclear power plants Borssele and Dodewaard. This study, performed by GRS, recommended to perform at least a level-1 PSA for both these plants with the purpose to optimize plant improvements. Thus, identification of the 'weaknesses' and 'imbalance' in the design and operation features that could be improved (e.g. by backfitting, accident management or changes in the conceptual design). In other words, the PSA should give a clear picture of the various scenarios leading to core melt, the relative frequency contribution to the core melt frequency of each initiating event group, and the spectrum of resulting plant damage states. The PSA's had to give guidance to the development of possible risk reducing measures for preventing and/or reducing accident scenarios as well as for mitigating the consequences of accidents.

Recently both utilities have been asked to extend their PSA's to a full scope level-3 PSA. A comparison of the results with the aforesaid PSC will be inevitable. Also in this case results may lead to design changes.

Although, the present policy of the Dutch government is not to expand the nuclear option during the current governmental period, there is an incentive to keep the nuclear option open for the future. This incentive caused the start of a four-year research program with two supplementary objectives. The first objective is to intensify the nuclear know-how and skills in the Netherlands, whilst the second objective is to look if the licensing of any evolutionary light water reactor and/or advanced reactor is feasible in the Netherlands. PSA tasks were envisaged to be an integral part of this research program.

II. PSA's FOR EXISTING NPP's.

II.1 PROGRAMMES OF PLANT SPECIFIC PSAs.

After Chernobyl the decision to expand the nuclear power capacity was postponed. The government decided to reconsider the nuclear option. Several studies were initiated to help them with this decision-making process. One of these studies was about the possible accident management measures of the nuclear power plants Borssele and Dodewaard. This study, performed by GRS, recommended to perform at least a level-1 PSA for both plants with the purpose to optimize plant improvements.

For Borssele, a 472 MWe KWU-PWR, both the licensee and the licensing authorities agreed with this proposal. This resulted in a bid specification for a level-2 minus PSA. This PSA-project was awarded to the combination KWU and NUS.

Early 1990 bid specifications for a level 2 minus PSA of the Dodewaard plant (58 MWe BWR) were send out by GKN (utility which operates the

Dodewaard nuclear power plant) and KEMA. The study was awarded to Science Applications International Corp. (SAIC) from the USA.

II.2. OBJECTIVES.

After Chernobyl the Dutch regulatory body asked in 1988 both nuclear power plants to perform a level-1^{+} PSA. This means a level-1 analysis plus containment analysis. In formal discussions with the licensee some guidance was given regarding the objectives, scope and boundary conditions of these PSAs.

As indicated above, the main objectives of the PSAs should be the assessment of the relative weaker points in the design and operation of the power plants, in order to support the design of accident management measures, and to support backfitting. An assessment of source terms, public health risks, etc., was regarded as unnecessary at that time. Mainly, because it was feared that the focus would only be on the final number(s). But even without these additional source term and level-3 analyses, the tendency to produce only numbers for whatever political reasons, and no insights, had to be avoided.

Although, these PSA's will be used to identify those safety issues with some significance, their resolution will be based on more conservative and deterministic assessments.

Recently, this one-time ad hoc request for a PSA has even got a more official and legal basis by the requirement of a periodic 10-year safety review. This requirement is included in the operating permits of both plants. On basis of this periodic 10-year safety reviews (including a PSA) backfitting is required if safety can be improved significantly at reasonable costs, and the design of the measure fits in the total existing design and/or operation. The reasonableness of the costs should be viewed in relation to the next 'long' period of operation (10-years). However, design or operational features which are regarded as shortcomings or violations with respect to the original safety level as assumed during granting the current license for operation, need to be resolved immediately.

The regulatory requirements as well as the wishes of the licensees themselves regarding the objectives of the PSAs were translated by the licensees in their respective bid specifications:

- To identify and analyze accident sequences, initiated by internal and area events, that may contribute to core damage and quantify the frequency of core damage.
- To identify those components or plant systems whose unavailability most significantly contribute to core damage and to isolate the underlying causes for their significance.
- To identify weak spots in the operating, test, maintenance and emergency procedures which contribute significantly to the core damage frequency.
- To identify any functional, spatial and human induced dependencies within the plant configuration which contribute significantly to the core damage frequency.
- To rank the weak spots according their relative importance and to easily determine the effectiveness of potential plant modifications. (both backfitting and accident management)
- To provide a computerized level -1 PSA to support other living PSA activities like optimization of Tech Specs, Maintenance Planning, etc.
- To transfer technology and expertise to the licensee to make them fully capable to evaluate future changes in system design, operating procedures and to incorporate these changes in the 'Living' PSA.

II.3 CURRENT STATUS OF PLANT SPECIFIC PSAs.

The actual PSA-work for the Borssele Nuclear Power Plant started 1 september 1989. The study was finished in february 1992 after most of the comments and remarks of the last out of a series IAEA reviews(IPERS-review) were processed by the contractors.

In april 1990 SAIC started with the analyses for the Dodewaard Nuclear Power Plant. The study was finished in april 1992 after processing the remarks and comments of an IPERS-review.

II.4 ADDITIONAL FORTHCOMING STUDIES.

During the first IAEA IPERS review of the Borssele PSA several suggestions were made for inclusion in the PSA, or as an extra additional study afterwards. Because, the main purpose of this IAEA IPERS review was to look if the bid specification, contract proposal and regulatory wishes were, more or less, in good agreement, the recommendations being made were very important for the follow up of the studies and for getting a better feeling of the state-of-the-art. The review emphasized the need to pay attention to the so called human errors of commission, to include shut-down states and transition states in the operating states being analyzed. These recommendations were translated by the regulatory body as a requirement for later additional studies.

Recently these requirements were expanded by asking for an analysis of the non-power states. Apart from this expansion, the Dutch government asked to expand these studies to a full scope level-3 PSA. That a comparison with the aforesaid probabilistic risk criteria will be made is obvious.

Also, recently a requirement for a periodic 10-year safety review is included in the operating permits of both plants. On basis of this periodic 10-year safety reviews (including a PSA) backfitting is required if safety can be improved significantly at reasonable costs, and the design of the measure fits in the total existing design and/or operation. The reasonableness of the costs should be viewed in relation to the next 'long' period of operation (10-years). However, design or operational features which are regarded as shortcomings or violations with respect to the original safety level as assumed during granting the current license for operation, need to be resolved immediately.

II.5 REGULATORY GUIDANCE AND PRECONDITIONS.

Primarily the PSAs should be state-of-the-art and in broad accordance with NUREG/CR-2300 "PRA Procedures Guide" (ch. 3 to 6) and NUREG/CR-2815 "PSA Procedures Guide". For the containment analysis the restriction was given that the computer code MAAP would be unacceptable as the prime analyzing tool, due to the discussions between the US-NRC and EPRI at that time (1988). However, for sensitivity studies and interpolation between results from other codes, like the Source Term Code Package (STCP) or MELPROG, no objections remained for the use of MAAP. In the human reliability analysis emphasis should be put on the so called cognitive errors.

It was also communicated to the licensees that the assumptions being made must be realistic, state-of-the-art and traceable. This means that CCF limits must be realistic (ß-factors < 10^{-4} are unrealistic!), that operator recovery actions can only be claimed when written procedures exist, that available time-scales for performing human actions must be large enough to be realistic. This means also that the data being used must be plant specific as much as possible. The assumptions being made (e.g. system success criteria) should be based on plausible and consensus assumptions. These assumptions however, should be backed up by uncertainty and sensitivity analyses for a more confident interpretation of the significance of the results.

A FMEA was recommended, but not required. However for the Borssele PSA FMEAs have been carried out for the system modeling of the support systems (e.g. instrument air or component cooling water).

II.6 PSA REVIEW PRACTISES.

Both PSAs were characterised by a large involvement of plant staff. An important aspect of this involvement was the review by the licensees together with the research institute of the electric utilities, KEMA. Apart from these reviews, the regulatory body monitored and reviewed the PSA activities. Last but not least, the IAEA reviewed both PSAs via the so called IPERS program (International Peer Review Service).

For Borssele the first phase of a peer review by the IAEA took place in the last week of August 1989. This review involved the scope of the project and how this scope was translated into a project proposal by the contractor. The review was conducted by a team of PSA specialists under the IAEA's recently initiated International Peer Review Services (IPERS). The peer review was split into three phases. A second review was conducted in June '90, approximately halfway the project. The last review took place in October 1991 after 95% completion of the PSA. In combination with the first peer review a training course on the review of PSA's was given by the team members of the IPERS-team for staff and consultants of the Dutch regulatory authorities.

For Dodewaard the first phase of an IPERS Peer Review took place in May '91 after approximately 60% completion. The second and last review took place in February '92 after 100% completion.

III. PSA's FOR NEW NPP's.

III.1 LICENSING; SHOWING COMPLIANCE WITH PSC.

Because PSA's play an essential and central role in the aforesaid 'external' safety policy, a PSA is nowadays part of the licensing procedure. Before the construction licence can be granted, compliance has to be shown with the aforesaid risk criteria[3]. This means that the calculated risk should be well below the criteria for both individual fatality risk and societal prompt fatality risk. During the construction phase this pre-construction PSA has to be updated with more precise data and detailed design information to obtain the commissioning and operation permit.

In case of comparison with probabilistic safety criteria/objectives, one should keep in mind that the criteria and objectives are only meaningful if there is a consistency between the PSC and the scope, definitions, assumptions being made and the boundary conditions of the PSA.

III.2 LIMITATIONS OF "SHOWING COMPLIANCE".

However, a warning must be given here. It may look that 'best estimates' remove some of the uncertainties involved by using consensus for what is hoped to be the most likely combination of inputs and phenomenology. But, even 'best estimate' assumptions, are sometimes subjective. Best estimate risk values may be the most likely outcomes for the consensus assumptions, but may at the same time present an overly false picture of the risk. Also the assessment of the associated uncertainties is subjective. What one analyst might consider quite reasonable as representing the range of uncertainties, might be totally unreasonable to others. But an uncertainty analysis, as well as a sensitivity analysis based on consensus and plausible assumptions are highly valuable for identification of the most sensitive contributors to the risk and to provide a plausible guess of their likelihood. There is no guarantee that a true answer will lie within the band of uncertainty which has been assessed.

In practice all internal and external events and all operating states which are safety relevant are to be included in the PSA. This is because in this case the PSA is an integral assessment of the nuclear power plant (NPP) as it is located in its environment. On the other hand there are still a lot of problems in showing compliance with the aforementioned risk criteria and goals. In assessing the risk of a nuclear power plant one should be aware of these difficulties.

The most important insights provided by a PSA ate engineering ones, i.e. those related to identification of potential plant vulnerabilities. Such results of PSA's are usually not undermined by the uncertainties involved, given that the PSA has a relevant scope, uses state-of-the-art approaches to modelling topics and has been subject to an adequate review process. As such, PSA's constitute a necessary supplement to traditional deterministic studies. In addition to the quantitative perspective on plant safety, the PSA's provide in many cases a more balanced and realistic picture than the predominately conservative deterministic analyses. Both types of analyses are subject to uncertainties, but the PSA approach makes them in, a certain extend visible. However, incompleteness as well as some elusive contributors to risk cannot be quantified. Therefore, the most appropriate way to use the quantitative results of a PSA is in a relative sense and not as an absolute yardstick, as this is less sensitive to the uncertainties involved. This fact has been recognized by both experts in the nuclear community as by experts which can be characterized as critical opponents of nuclear energy. They both agree[4, 5, 6] that PSA techniques are not yet developed to the point that it can be used as a definitive means of determining whether the numerical target has been met. The range of uncertainty is still too large for use of PSA in 'bottom line' evaluation. Both parties agree that

PSA - if its limitations are kept in mind - has a number of useful applications. However, to what extend PSA's are useful is strongly disputed between the two groups.

III.3 OTHER PSA REQUIREMENTS IN LICENSING.

Also in the more traditional deterministic licensing approach some implicit probabilistic aspects play a major role. Since several years the Netherlands have adopted the IAEA safety codes (as well as the underlying safety guides) as a legal basis for their regulatory work. Especially the Safety Code for Nuclear Power Plant Design (IAEA Safety Series 50-C-D) has to be mentioned here. In this safety code the postulated iniating events (PIEs) play a central role. These PIEs are those postulated and/or identified anomalous but credible events (or combination of events) with a potential for serious consequences which have to be accommodated by the design. It is in the selection of the PIEs that implicitly probabilities are used to decide if an event (or combination of events) is credible.

The design basis of a NPP needs to specify those safety requirements for the plant design that, by an adequate implementation of these requirements, the sensitivity to PIEs will be reasonably low, and that the resulting accident conditions will fulfil the defined radiation protection requirements. To confirm the design both traditional safety analysis and PSA are required. The selection as well as the consequences of event sequences resulting from a PIE have to be analyzed and evaluated in a conservative and deterministic way to check if those consequences fall within the radiological acceptance criteria. On the other hand a PSA is required to demonstrate that the NPP is designed against PIEs that the probability of a large release is not greater than 10^{-6}/reactor-year, and that there is no sharp increase of risk just below the probability of 10^{-6}/reactoryear. Traditionally PSAs were used to provide better insights in the risks associated with the beyond design basis area of a NPP. However, the undeniable offspin as well as the powerful potential for assissing the design basis area have been recognized. Therefore, a PSA will increasingly be used as a tool for design confirmation.

III.4 STUDIES; CURRENT PSA ACTIVITIES FOR NEW AND ADVANCED NPP's.

The aforesaid four-year governmental sponsored research program was divided in several sub-programs. The first sub-program was carried out jointly by the Netherlands Energy Research Foundation (ECN), the research laboratory of the electric utilities (KEMA) and a Dutch engineering and contracting company NUCON. It started with an extensive review of the SBWR, AP600, SIR and Candu3 reactor designs. This review included an analysis of PSA results and insights as far as these were available. Also the possibility if the results could be used for comparison with the Dutch PSC was part of this review. Because at the time of the project initiation only preliminary PSA's were performed for all four reactors due to their early design stage, the outcomes could only be used in a very limited and indicative manner regarding a comparison with PSC. The third stage reactor-designs (sometimes referred to as inherently safe) MHTGR, PRISM, SAFR and PIUS were reviewed last year. For these latter reactor designs no preliminary PSA's were available.

The second sub-program is structured around a participation of the above mentioned institutions in the development of the SBWR design. A special cooperation agreement with General Electric was signed, whereby these institutions were allotted tasks in accordance with their specific capabilities and GE's need for support. In this sub-program PSA activities form an important part of the total Dutch input. Because the SBWR is still in the design stage, an interaction between PSA and design might be expected.

Especially, the assessment of transiënt process behaviour inside the reactor coolant system as well as the containment with RELAP-SCDAP (ECN), MELCOR (ECN) and TRAC (KEMA) has to be mentioned, as well as the assessment of some containment issues. These assessments will undoubdly be used for the resolution of some severe accident issues for the SBWR. Especially the structural analysis of the RPV and RPV internals (ECN) under core degradation conditions will benefit from these analyses. Where GE uses MAAP, uses ECN MELCOR. The resulting different insights, e.g. in MELCOR is the debris not always coolable, highlight the uncertainties regarding the specific SBWR safety issues. Also a consequence analysis based on the afore-mentioned containment analyses and some generic core melt scenario's will be performed within the scope of this sub-program by means of the COSYMA code to assess the consequenses of large releases.

IV. REGULATORY USE OF PSA's

The regulatory body uses the current PSA as a common basis of understanding in discussions regarding plant modifications, backfitting, etc. In this case the PSA is not a replacement of regulatory work; it only assesses and guides this work.

Another use is to provide staff personnel of the regulatory body an alternative and complementary look on safety issues and safety decisions. Because, traditionally many safety decisions were made solely on the basis of deterministic studies and/or engineering judgement, the probabilistic aspects were often overlooked. But the PSA offers an extensive set of deterministic analyses as well.

The PSA can also optimise the various areas for attention within the regulatory body regarding safety issues, and indicating priorities within these areas for attention.

Because, the regulatory body has besides the traditional controlling and inspection tasks, a stimulating and initiating role as well, an important task of the regulatory body is to promote the use of the PSA as an operational tool for the licensee. Because a PSA has so many potentials for helping to improve the safety of a plant, that it would be a waste if the operating organization would not make use of the full range of capabilities of a PSA. Optimization of Techspecs, maintenance strategies, test intervals, etc. are possibilities to think of.

For future PSA activities PSA-guidelines are in preparation. The guidelines will be structured around the drafted IAEA PSA guidelines "Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants". An introductory document has been written by the regulatory body. The possible objectives, scopes and their relation is given in this document. Because, in the Netherlands risk criteria have been formulated and will be used for reasons of comparison in the external safety policy of the Dutch government, this document describe some pitfalls in comparing PSA results with these risk criteria and objectives. Therefore some guidance is given in how to deal with uncertainties and very low probability numbers. Especially, in which circumstances it is allowed to cutoff the frequencies of accident sequences and single events in the extreme low probability domain without causing a significant underestimation of the risk, and how to do it.

REFERENCES

1. M.F.VERSTEEG, External Safety Policy in the Netherlands; an Approach to Risk Management, *Journal of Hazardous Materials 17*, page 215-222, 1988.

2. M.F.VERSTEEG, The Practice of Zoning; how PSA's can be used as a Decision-making Tool in City and Regional Planning, *Reliability Engineering and System Safety 26*, page 107-118, 1989.

3. M.F.VERSTEEG, Showing compliance with probabilistic safety criteria and objectives, *Reliability Engineering and System Safety 35*, page 39-48, 1992.

4. OECD-NEA, Applications and Limitations of Probabilistic Assessment; Note on the Outcome of a Workshop held in Santa Fe, New Mexico, USA, 4-6 September 1990, *NEA/CSNI/R(91)2*, Paris, 1991.

5. GREENPEACE, IAEA Safety Targets and Probabilistic Risk Assessment; State of the Art, Merits and Shortcomings of Probabilistic Risk Assessment, *A Report prepared for Greenpeace International by the Gesellschaft Für Ökologische Forschung und Beratung mbH*, Hannover, 1989.

6. INSAG, A Review of the Report "IAEA Safety Targets and Probabilistic Risk Assessment, prepared for Greenpeace International, A Report by the International Nuclear Safety Advisory Group, *INSAG Technical Note No. 3*, IAEA, Vienna, 1991.

PSA SOFTWARE AND UTILIZATION EXPERIENCE IN REACTOR PLANT DESIGN

O.B. SAMOILOV, E.V. FROLOV, A.M. BAKHMETIEV
OKB Mechanical Engineering,
Nizhny Novgorod, Russian Federation

Abstract

The report presents information concerning methodology and computer software used in PSA in the area of reactor plant design in OKB Mechanical Engineering, Russian Federation Basic elements of PSA modelling are described, including unacceptable plant state criteria, system reliability techniques, data assessment, dependency analysis and human reliability analysis Information is also provided on computer software used in accident model quantification

Some practical PSA results related to AST-500 district heating plant are briefly presented

INTRODUCTION

Methodology, software and experience of probabilistic safety analysis (PSA) utilization in practice of the designing by OKB Mechanical Engineering of enhanced safety WWERs for nuclear district heating plants (NDHP) and nuclear power plants (NPP) are discussed in the report.

At the designing stages PSA is used for the attainment of the following goals:

- choice and optimization of the basic engineering decisions on systems important for safety;
- provision of safety design decisions balance due to the revealing and exclusion of "weak points" in the design ;
- working out of accident control procedures ;
- corroboration of the reached in the project safety level of the plant, basing on the core damage probability assessment.

Probabilistic safety analysis is based on deterministic analysis of thermophysical processes in all the emergencies and accidents with the loss of normal heat removal, primary circuit loss-of-tightness and inadvertent positive reactivity insertion.

To perform PSA in OKB Mechanical Engineering a software system TREES was developed which allows to analyze safety systems reliability, to construct and analyze event trees in accordance with the recommended by IAEA methods of PSA performance.

Main PSA results are presented for AST-500 reactor - a new generation nuclear district heating plant developed in OKB Mechanical Engineering.

1. UNFAVOURABLE STATES CRITERIA

In course of the analysis was evaluated the probability of unfavourable reactor states, aggravation of which can lead to the core damage. The following criteria of unfavourable states were used :

- coolant level reaches the upper core boundary in course of its leakage from the reactor ;
- primary circuit pressure rises up to the values, corresponding to the pressure of reactor vessel break down at realization of hypothetic defect, the size of which is 0,25 from the wall thickness and the worst characteristics of the material.

It is obvious that the aforementioned criteria are conservative enough for the following reason. Coolant level decrease in the reactor do not sure lead to unfavourable consequences with the core damage. Even at partial core uncovering the fuel element's cooling by steam is kept which prevents from their overheating. Timely coolant level recovering excludes fuel elements failure. The second criterion is also conservative because the realization of the given size defect and of the worst mechanical characteristics is low probable; for defect-free vessel the ultimate pressure is considerably higher than the value chosen by the stated criterion. Nevertheless, direction of attention toward more strict criteria at the development of balanced design decisions on safety, utilization of which gives the upper assessment for the core failure probability, is justified in the opinion of the reactor plant designers.

2. SAFETY SYSTEMS RELIABILITY ASSESSMENT

When analyzing safety systems reliability, elements' independent failures, common-cause failures of the same type equipment and personnel errors were considered.Systems elements were controlled and non-controlled at reactor power operation. Cotrolled elements had apparent and latent failures. Latent failures are revealed at periodic control of system's serviceability. Apparent failures are revealed at the moment of their emergence or at the instruments readings control by personnel.

It was assumed that the element's time to failure was distributed by exponential law in the calculations of safety systems reliability.

System's serviceability success criteria condition was presented as sequential-parallel logical diagram. Analogous to the fault tree in the logical diagram are shown different combinations of the failed elements leading to the system's failure. Calculations of safety systems failure probability were made using known method of minimal cut-sets.

3. DATA BASES ON EQUIPMENT RELIABILITY

As data on equipment reliability are used statistic data on the analogs operation experience on NPPs with WWER reactors and on nuclear ice-breakers. If there were no national data on separate elements, data from IAEA/1/data bank were used. When choosing equipment reliability characteristics basing on IAEA data bank, conservative approach was used, which allowed to obtain assessments in design margin.

The aforementioned approach is:

- if in the bank are given different values of reliability for one and the same element, the worst value was used for calculations;
- if there is one val of failure rate or probability of failure on demand. for the calculations is used value increased by a factor of three (characteristic value of error factor).

4. COMMON-CAUSE FAILURES

When evaluating safety systems reliability and determining emergency sequences probability, all types of potentially possible dependences between the elements, channels and systems are analyzed :

- dependence upon initial event ;
- structural-functional dependence, conditioned by presence of common structural elements or auxiliary systems ;
- dependence, conditioned by equipment design uniformity including due to the personnel errors.

Two first types of dependences were taken into account when making emergency sequences and determining safety systems serviceability conditions basing on the deterministic account of the existing dependences between systems and elements.

To take into account the dependences, conditioned by equipment design uniformity and personnel errors, together with the elements of qualitative, deterministic analysis was used the probabilistic model of binominal failure rate (BFR-model) .

For the system, consisting of "m" uniform elements in accordance with BFR-model three types of failures are considered :

- independent elements failures with rate λ ;
- failures because of non-lethal shock, if its appearance rate is μ , each of the elements independently of others can fail with P probability;
- failure because of lethal shock, if it's appearance rate is ω , all systems elements fail by common cause.

In reliability calculations conservative assessment is used for common-cause failure probability $Q_{\geqslant k}$ (t) of "k" or more elements in the system, consisting of "m" elements in (0,t) interval

$$Q_{\geqslant k}(t) < \mu \cdot t \cdot \binom{m}{k} \left[(q\lambda t + P)^k - (q\lambda t)^k \right] + \omega t , \quad q = 1 - P$$

Models parameters were determined basing on data on national experience of analogs operation, from literature /2,3/ and some other sources

The given approach to common-cause failures taking into account is conservative enough especially for the elements, actuation of which do not need any external power sources and is performed due to potential spring energy or its own weight

5 PERSONNEL ERRORS

When performing probabilistic safety analysis the following personnel errors types were taken into account

- personnel errors, made before accident beginning ,
- personnel errors,initiating the emergency situation ,
- personnel errors at the emergency control of the plant

Errors of the first group were analyzed in course of safety systems reliability assessment and personnel error was considered as an arbitrary element of logical diagram, which is able by himself or together with equipment failures to form minimal cut-sets

Errors of the second group were taken into account at the assessment of the considered initial events occurence rate. Personnel errors of the third group were taken into account at event trees making and analysis.

When analyzing errors, made by personnel after the initial event occurence, the stages of the emergency situation detection and diagnosis setting up as well as operator actions trees were analyzed. Personnel's reliability was determined using models of personnel error probability dependence on available time realized within THERP method /4/. Utilization of these dependences allowed to realize multiparameter dependence model "time-personnel reliability", taking into account the following factors

- relationship between available and necessary time for action performance,
- personnel qualification;
- stress level;
- means for processes and systems state control,
- type of the problem under solving

Operator actions undertaken by him in accordance with the chosen method of situation control were analyzed using operator actions trees and home and foreign data banks on errors probability.

6 SOFTWARE TREES

To perform probabilistic safety analysis of the designed plants in OKBM was developed software system TREES.

It consists of two independent programs, one of which is intended for safety systems reliability analysis, the other one - for the event tree making and analysis (Fig 1)

Software allows to analyze large failure trees, including safety systems combinations, forming emergency sequences in the event tree

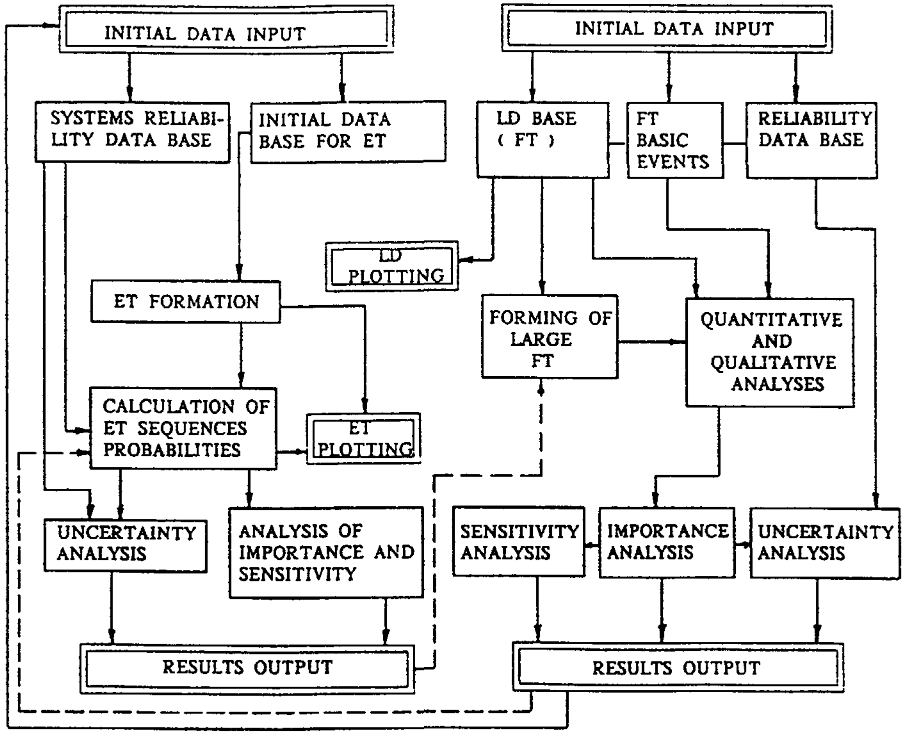


FIG 1 TREES code block diagram

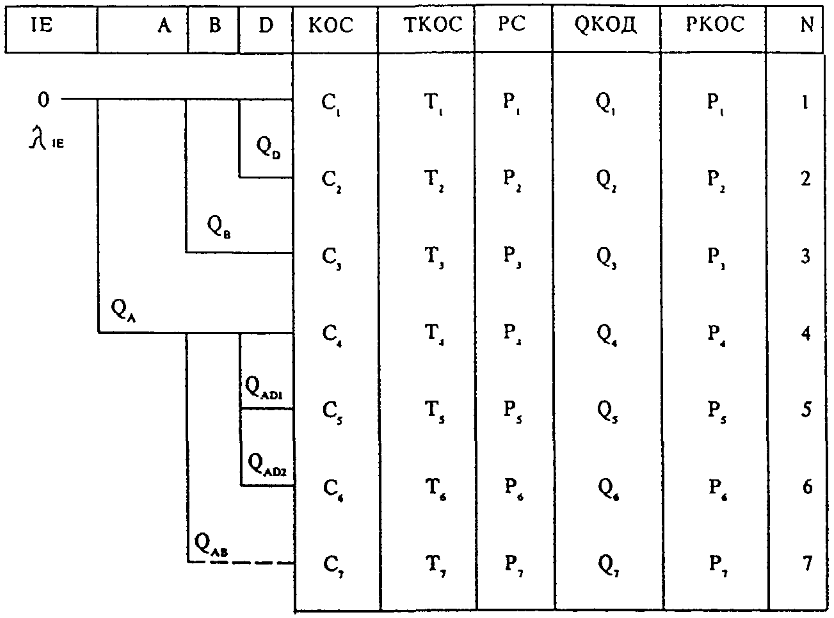
Failure tree can include up to 2000 base events and up to 1000 logic operators Different methods for provision of high effectiveness of minimal cut-sets generation algorithm for failure tree are: modularization, convolution of cut-sets sifting out by probabilistic criterion To perform safety systems reliability calculations with the account of common-cause failures BFR-model and - factor model were realized

System event tree is constructed basing on

- matrix of dependences between safety systems ;
- consequences matrixes for emergency sequences

Software allows to analyze up to 30 event trees, each of which may include up to 1000 emergency sequences

Fig 2 gives event tree structure and includes initial event, safety systems set influencing the accident's development together with their reliability assessment accident's development ways and the results table


IE
A
B
D
KOC
TKOC
PC
QKOД
PKOC
N
0
λ IE
Q_D
Q_B
Q_A
Q_{AD1}
Q_{AD2}
Q_{AB}
C_1 T_1 P_1 Q_1 P_1 1
C_2 T_2 P_2 Q_2 P_2 2
C_3 T_3 P_3 Q_3 P_3 3
C_4 T_4 P_4 Q_4 P_4 4
C_5 T_5 P_5 Q_5 P_5 5
C_6 T_6 P_6 Q_6 P_6 6
C_7 T_7 P_7 Q_7 P_7 7

IE - initial event

A, B, D - systems, influencing emergency situation development; solid line is without branching-system's states do not influence the cousequences for the given chain; dotted line - dependent failure of the system due to the failure of preceding systems.

Q - probability of partial or complete system's failure

KOC - classes of the determined states

TKOC - time for corresponding states reaching

QKOД - probability of correcting personnel actions non-execution

PKOC and PC - rate of chains of accidents realization with the account or without the account of correcting personnel actions

N - chain number (event tree branches)

FIG 2 Structure of event tree

In the conditions of separate systems failure, the designed enhanced safety plants (especially NDHP) are characterized by relatively large time reserves for the accidents control TKOC parameter, characterizing these time reserves is included in the resulting table of the event tree (see Fig. 2)

Software's capabilities allow to analyze importance, sensitivity and uncertainty To analyze uncertainty Monte Carlo method is used.

Software TREES system was developed as applied to the computer of EC type using mode of dialog with user

7. AST-500 PLANT PROBABILISTIC SAFETY ANALYSIS RESULTS

AST-500 reactor plant has been developed in OKB Mechanical Engineering for nuclear district heating plants proceeding from the requirements of the enhanced safety provision of such plants in comparison with nuclear power plant.

Fundamental engineering decisions of AST-500 (see Fig. 3) were published widely enough /5/. High level of the reactor plant's safety is conditioned by the following main design decisions (Fig.4) :

- integral layout of the reactor with low coolant parameters (temperature - 200 °C, pressure - 2,0 MPa) and its large inventory over the core ;
- absence of large diameter primary circuit pipelines ;
- use of the reactor guard vessel as localizing and protective system ;
- all-conditions natural circulation of primary coolant ;
- low fuel rating of the core, possessing the property of fission chain reaction self-suppression at high circuits accumulating ability ;
- organization of the emergency heat removal from the core at natural coolant circulation over all circuits up to the ultimate heat sink;
- low fluence on the reactor vessel ;
- redundancy, physical channels separation and safety systems passivity, use of self-actuating devices.

Within the performed PSA for AST-500 plant the reliability of systems, important for safety, was analyzed. Table 1 gives reliability assessments for some reactor systems, obtained using conservative models of taking into account of common-cause failures of the same type elements.

AST-500 probabilistic safety analysis has been performed conformably to the internal initial events. Unfavourable core states probability was estimated basing on fault trees making and on the analysis of numerous emergency sequences (ES). Calculation results of some most important ESs probability are given in Table 2.

It is important to note, that the base of NDHP safety concept is self-protectiveness, which is provided by inherent reactor properties, thereby large time reserves are formed for taking correcting actions on the accident's control by personnel. As appears from the analysis the majority of determining ESs, time reserves for personnel corrective actions (grace period) exceed 14 hours (see Table 2)

Table 3 gives concluding results of PSA for AST-500 plant. Point assessement of probability of unfavoured core states realization (for internal initial events)

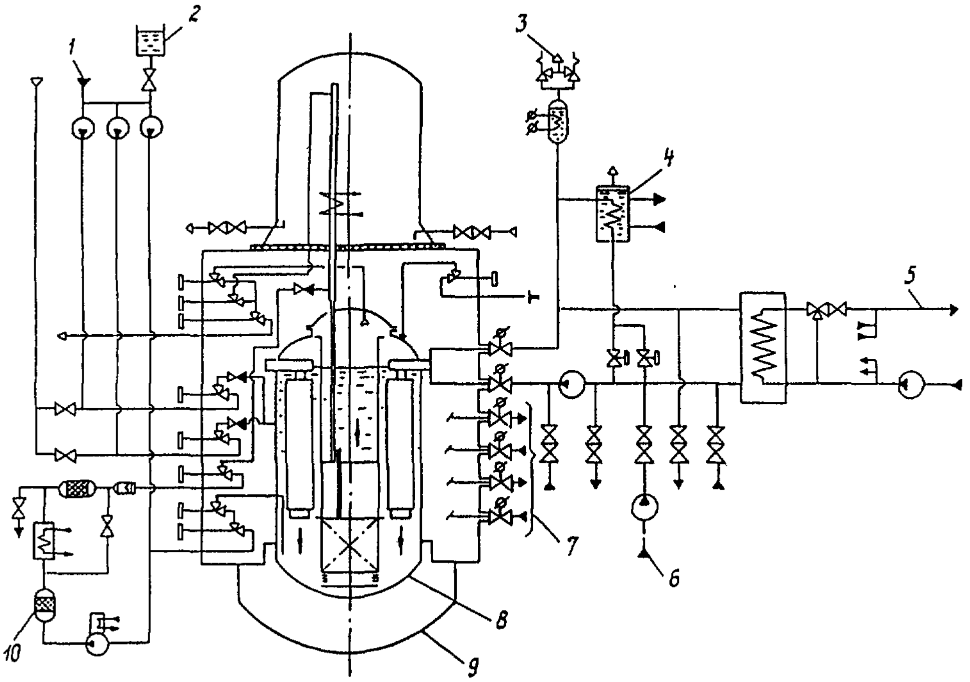


FIG. 3. Schematic diagram of the ACT-500 reactor plant. 1 – primary circuit make-up system; 2 – boron solution tank; 3 – safety valve; 4 – emergency residual heat removal system tank; 5 – district heating circuit; 6 – secondary circuit make-up system; 7 – secondary circuit loops; 8 – reactor; 9 – guard vessel; 10 – primary circuit purification system.

Low power potential, no boron injection	Integral reactor lay-out	Natural reactor coolant circulation	Passive and self-actuated safety-related devices	Safety systems reliability
*low coolant parameters (T=200°C, P=2.0 MPa) *low core power density (27 kw/l) *power self-regulation *no accidents with boron dilution	*no large diameter piping *high accumulating capacity *low RV fluence *no transients with rapid RV cooldown	*no accidents with pump's failure *self regulation of coolant flowrate	*guard vessel *emergency heat removal under natural circulation *insertion of EP control rods under gravity *opening of ERHRS valves under spring action *closing of localization valves under spring action	*redundancy *diversity *separation *principle of safe failure

FIG. 4. Key decisions used to provide ACT-500 safety.

TABLE 1.

RELIABILITY ANALYSIS RESULTS FOR SOME SYSTEMS. IMPORTANT FOR SAFETY

System	Probability of failure on demand
ERHRS (3 channels failure)	6,6•E-4
IAC	5,6•E-2
PORD (failure of 5 from 6)	7•E-4
MS 2 (3 channels failure)	1,05•E-4
EP (failure of 12 rods or more)	2•E-6
EBIS (2 channels failure)	2,1•E-2
RPSS (2 channels failure)	3,9•E-3
EBDS (1 channels failure)	4,4•E-2
RVJ	1•E-2

ERHRS - emergency residual heat removal system

IAC - intermediate auxiliary circuit

PORD - power operated relief device

MS 2 - secondary circuit make-up system

EP - emergency protection system of the reactor (control members)

EBIS - emergency boron injection system

RPSS - reliable power supply system (diesel)

EBDS - emergency blow-down system

RVJ - reactor vessel joint

TABLE 2.

REALIZATION PROBABILITY AND TIME RESERVES FOR SOME MOST IMPORTANT EMERGENCY SEQUENCES

N	Emergency Sequence	Probability (point evaluation) 1/year	Time reserve (grace-period) hours
1.	"Stop-grid" + 3 channels of ERHRS + IAC + (5-6) PORD	0,4•E-9	17
2.	"Stop-grid" + 3 channels of ERHRS + IAC + 3 channels of MS 2 + 1 channel of EBDS + RVJ	0,1•E-9	15
3.	"Stop-drid" + EP + 2 channels of EBIS + 3 channels of MS 2	0,5•E-10	14
4.	LOSPS + 3 channels of ERHRS + IAC + (5-6) PORD	0,15•E-9	17
5.	LOSPS + EP + 3 RPSS	0,1•E-9	14

"Stop-grid" - loss of heat removal to district heating grid

LOSPS - loss off-site power suplay

TABLE 3.

PROBABILITY OF UNFAVOURABLE REACTOR STATES

TYPE OF ACCIDENT	INITIAL EVENT RATE, 1/R-YEAR	ACCIDENT PROBABILITY PER R-YEAR	RELATIVE CONTRIBUTION, %
LOCA			
* PIPING RUPTURE	$< 10^{-3}$	$< 10^{-11}$	0,3
* REACTOR VESSEL LOSS -OF -INTEGRITY	$< 10^{-7}$	$< 2*10^{-10}$	6,2
MAIN HEAT EXCHANGER LEAKAGE			
* HEADER RUPTURE	$3*10^{-4}$	$4*10^{-10}$	12,5
* PIPE RUPTURE	$< 10^{-2}$	$< 10^{-10}$	3
LOSS OF HEAT REMOVAL TO GRID CIRCUIT	3,5	10^{-9}	31
LOSS OF OFF-SITE POWER	0,13	$0,73*10^{-9}$	23
ATWS	$0,8*10^{-5}$	$0,74*10^{-9}$	23
INADVERTENT CONTROL RODS WITHDRAWAL	$< 10^{-2}$	$< 3*10^{-11}$	1
FOR ALL ACCIDENTS		$3,2*10^{-9}$	100

is $\sim 0,3 \cdot 10^{-8}$ 1/year and is a conservative assessment of the core damage probability.

Basing on uncertainty analysis assessments of 5% and 95% boundary for the given safety index, which are $2 \cdot 10^{-12}$ and $0,6 \cdot 10^{-8}$ 1/year respectively, have been obtained.

CONCLUSION

1. Probabilistic safety analysis is used widely enough together with deterministic analysis in the design works on the development of enhanced safety reactor plants.

At early stages of the designing the probabilistic analysis is used for engineering decisions choice and optimization and at final stages of NPPs construction in confirmation of the achieved safety level.

2. To perform probabilistic analysis methodology is used which takes into account IAEA recommendations on all aspects, determining PSA results, such as choice and classification of initial events, choice of initial data on equipment reliability, taking into account common cause failures and personnel errors. Direction of attention toward "strict", conservative approach as for some methodic aspects allows to obtain the upper estimate of the core damage probability.

3. The results of the performed PSA of AST-500 reactor plant for the nuclear district heating plants are presented here. The obtained results are evidence of the fact, that due to the developed self-protectiveness properties and use of passive safety systems, the probability of serious core damage over the whole range of initial events is not higher than 10^{-8} per reactor year.

REFERENCES

1. Component Reliability Data for Use in Probabilistic Safety Assessment. IAEA-TECDOC -478, Vienna, 1988.

2. Atwood C.l.and Steverson J.A. Common Cause Fault Rates for Valves.NUREG/CR - 1770, February 1983.

3. Meachum T.R. and Atwood C.L. Common Cause Fault Rates for Instrumentation and Control Assemblies. NUREG/CR - 3289, May 1983.

4. Swain A.D. and Guttmann H.E. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR - 1278, August 1983.

5. Mitenkov F.M., Egorov V.V.,Kuul V.S. and others. Safety Concept of District Heating Plant Reactor. - Nuclear Energy, 1988, volume 64, N 4, pp 267-275.

INFLUENCE OF PSA METHODOLOGY ON NPP DATA COLLECTION

I. ČILLÍK, B. MARKECH
Nuclear Power Plant Research Institute,
Trnava, Czechoslovakia

Abstract

Present activities in the field of PSA in the CSFR lead to improvement of the reliability information system (RIS) of all NPP equipment. The creation of a suitable specific reliability database for each NPP with WWER on the basis of existing databases focussing on specific topics is one of the main tasks on NPPs to solve the basis problems of safety improvements.

The first part of the article describes the basis aspects and description of the RIS in the innovated version which involved following collection of primary data from the NPP:

- record about the equipment failure;
- record about the equipment defect;
- record about the equipment maintenance;
- record about the safety system tests;
- record about the operation and outages of the unit and turbo generators;
- record about the operation and outages of the systems.

This data are filled on the NPP by its staff and are elaborated by software "Complex programme of the following and evaluation of the operational reliability and lifetime of the NPP with WWER selected systems and components".

In the second part of the presented article is showed the preparation and the way of elaborating the Data Base of the Reliability Characteristics for the specific NPP during the PSA project for NPP Dukovany. It is the presentation of the interesting progressive steps of the creation of a Data Base for the PSA project according to the requirements of the safety analytic staff on the basis of present situation in the data collection by the operational staff on an NPP. In the end there is the positive backward influence of PSA project upon practical approach of the operational staff to the operational and maintenance data collection on NPP.

1. INTRODUCTION

In this paper I would like to demonstrate the positive influence of the performance of PSA Level 1 on the problem of the collection, registration, keeping, elaboration and evaluation of operation data for the creation of sufficient reliability information system.

The basic assumption for a systematic assuring of the necessary level of the NPP technological equipment reliability is the existence of a suitable operational reliability information system (RIS).

The first system of such a kind in the field of energy implanted in the seventies in CSFR for the follcwing and evaluation of the conventional power plant operating reliability - Electric Power System Rules No. 4 "Unit evidence, reporting and evaluation of exploatation reliability of conventional power plants", IX. 1972 was elaborated, which was than modified for following of the operational reliability of the NPP with WWER reactors.

On the basis of requirements of the equipment manufacturers designers, research institutes and other organizations, the problems of the innovation proposal of the given RIS was performing in the Nuclear Power Plants Research Institute (NPPRI). A basic aspect of the innovation was the requirement of a wide use of the personal computers for the collection, registration, keeping, elaboration and evaluation of the NPP equipment reliability data. A proposal of this innovated RIS (IRIS) considered a unified way of designation of the equipment in the power plant project documentation and provisions of the Czecho-Slovak state norms, of INTERATOMENERGO and also of IAEA.

The IRIS proposal principally issued from the above mentioned RIS which was valid up to this time. All data comparised in this RIS were included also in the proposed IRIS, even though IRIS uses the data gained from the NPP operation substantially broadly.

2. BASIC ASPECTS OF IRIS

In the NPP operation it is necessary to keep a lot or data because of the various reasons resulting from fulling of the NPP own activity and from keeping of its operation. These data are followed and kept in a diverse operational documentation. It is a fact that only a small part of these interesting and from the point of view of the equipment reliability also useful data have been used for the purpose of the creation of RIS up to now.

For instant, there were some different types of data bases which were used for different purposes. One of them was automatic system of the C & I equipment maintenance on NPP V-1 and V-2 in J. Bohunice (in the function from year 1980) and on NPP Dukovany (in the function from year 1988), which was used for establishing and keeping of the sufficient maintenance strategy and reliability of C & I equipments on NPP's. Other type of the collection of the exploatation and reliability data was used for the creation of data base according to "Rules No. 4" to give requested information for governmental organization, electric utilities and different international organizations. Both types of data base had the similar background of the collection of data to give the sufficient information to creat data base of reliability characteristics of operational equipment for system modelling analysis. The specific type of data of stand-by state, common cause failures and human errors had to be found in the corresponding records of tests, maintenance, training and so on.

It means, that the operational data collected on NPP's, such as
- failures
- maintenance (planned, unplanned, preventive)
- repairs
- tests (especially of the most important NPP systems)
- operational loads of the main NPP components
- destructive and non-destructive tests
- chemical regimes

and data gained from the diagnostic systems, could not be directly used for PSA and reliability analysis and had to be elaborated carefully.

The given informations, which have already been followed and kept in the NPP operation - it must be emphasized - mostly unsystematically and non-uniformly, provide sources of the most current input data used in the calculations of reliability parameters as follows:
- failure rate (of the particular followed systems and components)
- frequency of the tests and maintenance
- duration of the tests and maintenance, etc.

By using all data from the NPP which the operation can offer, it is possible to gain information which is very interesting from the point of view of reliability for all organization which participate on the design, construction, operation, supervision and research in the field of the production and supply of electric power.

RIS was first experiment to establish serviceable data base and was focused namely on data collection about the equipment failures, to provide detail evaluation of the equipment maintenance strategy and to prepare some data for the equipment manufacturers. Primary data were collected and kept in six so called reliability reports. The filled reports were further checked and elaborated. In the RIS used to now, elements of the equipment were encoded by a five figure code while some data were repeated in the reports and on the other hand many interesting data was not appeared. The said RIS reports are as follows:

Report No. 1 - Monthly survey of the NPP equipment failures
Report No. 2 - Analysis of NPP equipment failures
Report No. 3 - Monthly survey of operation and outage of particular NPP units
Report No. 4 - Monthly survey of operation and outage of the namely followed NPP equipments
Report No. 5 - Monthly survey of the NPP supplementary data - - part A
Report No. 6 - Monthly survey of the NPP supplementary data - - part B

3. DESCRIPTION OF THE IRIS

The IRIS proposal contains 10 forms for the collection of primary data from the NPP operation and maintenance.

Form No. 1 - "Record of the equipment failures", which serves for following the failure and repairs of the NPP equipment with WWER 440 reactors which:

a) caused loss or decrease of the electrical energy and heat production
b) are significant from the point of safety
c) were performed in the frame of preventive power decrease or in the frame of preventive outage required by the operating organization to prevent a failure occurence.

The form serves as the basis for:

- elaboration of the separated specialized analyses of the NPP technological equipment failure rates
- proposals of the most convenient correction measures for increasing the operational reliability of the NPP equipment which are performed by suppliers
- analysis elaboration of the NPP events significant from the point of view of safety.

Data of the equipment failures during the whole period of operation of the NPP with WWER reactors are available in the NPPRI.

Form No. 2 - "Record of the equipment defects", which serves as the basis for following and evaluation of the NPP equipment faults or defects which did not cause loss of the energy production and which are not significant from the point of view of safety and are not kept in the form No. 1.

The data of defects or faults kept and elaborated at the particular NPP. Partially elaborated data are provided to the NPPRI central reliability data base. There is only a part of these data from the NPP V-1 and V-2 Bohunice in the NPPRI.

Form No. 3 - "Record of the equipment maintenance", which serves as the basis for following, keeping and evaluation of the equipment maintenance data. The data are elaborated at the particular NPP. Partially elaborated data are provided to the central reliability data base. "Working order" serves as the basis for filling this form. Working order is filled in before beginning of the work and it is completed after finishing of the work.

Considering that the working orders have not been registered, kept and evaluated by computers up to now, these data are not suitable for using at the reliability parameter calculations.

Form No. 4 - "Record of the safety system tests", which serves for following of the safety system tests, which are not permanently under operation, but their operating ability is verified in the regular intervals. The data serve for determination of the testing optimum intervals. Part of these data from NPP V-1, V-2 Bohunice and NPP Dukovany is elaborated in the NPPRI.

Form No. 5 - "Record of the operation and outage of unit and turbogenerators", which serves as the basis for following of the periods of particular modes of operation and of particular modes of outage of units and turbogenerators. The electric energy production, heat production, losses of the electric energy and heat production caused by the equipment failures, by the equipment maintenance, by the electric network failures and so on are followed by this form. The data necessary for calculation of the unit technico-economic parameters are provided by this form. Part of these data is in the NPPRI in the elaborated form.

Form No. 6 - "Record of the operation and outage of systems", which serves for keeping of the periods of equipment operation and outage which are the most important from the point of view of the NPP reliability. The fail-safe operation, preventive outage, maintenance outage and failure outage are followed. Part of these data is in the NPPRI in the elaborated form.

Considering that the data, which are kept the aid of the forms No. 7÷10, have relation to the equipment lifetime, they are not comparised in this paper.

All mentioned forms are filled on the NPP by operational staff of NPP. Staff of NPP is responsibile for the data correctness, for complying with the terms of filling and for their storage on the computer media.

It was necessary to create a computer programme which would comprise all necessary activities and mutual links-up for a permanent following and evaluation of the equipment reliability parameters, to provide valide reliability and safety analysis for NPP's.

Such software was elaborated by the NPPRI: "Complex programme of the following and evaluation of the operational reliability and lifetime of the NPP (with WWER reactors) selected systems and components" according to the agreements with utilities CEZ and SEP so that, this guiding provision for a systematic following and evaluation of the NPP equipment operational reliability must be improved into live.

4. THE PREPARATION AND THE WAY OF ELABORATION OF THE "DATA BASE OF THE RELIABILITY CHARACTERISTICS FOR THE NPP WITH WWER 440/V 213 REACTORS" (FURTHER ONLY DATA BASE)

There was given a task to performed the Data Base of the reliability characteristics in January 1991 with assumption to use all available information and experience.

As the preliminary draft, the survey of the most important elements of the safety systems (emergency high pressure injection system, emergency low pressure injection system, spray system, service water system, auxiliary and emergency feedwater system and intermediate cooling circuits of safety systems) with given types of failures and their reliability characteristics (failure rate and time of the repair) was elaborated. The survey was complemented with a brief description of the electric equipment failures (transformers, diesel generators, cables, connections, penetrations, invertors, rectifiers, breakers and switchboards) including given causes and consequences of failures. Data were taken especially from IRIS in the NPPRI (failure reports of the NPP Bohunice, Dukovany) and consulted with the operational staff.

It is necessary to emphasize some substantial facts which considerably influenced and in many cases still influence on the quality of reached characteristics:

a) Data collection, registration and keeping system of there failures and faults of the NPP systems and equipment was unsufficient to cover fully the requirements of the reliability analyses.
b) The menace of a possible penalty for contingent mistakes or non-professional manipulations of NPP's personnel considerably influenced on true clarifying of the causes and courses of the failures and therefore some failures from this reason were not mentioned.
c) Regarding to the fact of (in some cases) the individual filling of the forms (the long period of activity without using the personal computers) as an unnecessary work and the work over labour duties, the staff did not realize a common way of failure registration and in some case they even refused way of information record proposed in IRIS.
d) IRIS did not take advantage of a full use and it was not fully realized in the nuclear power plants. On the basis of this situation only failure report forms were followed and elaborated.Failures and faults which were significant from the point of view of safety and the ones which led to a production

decrease or loss, were only registered in these failure report forms. It was necessary to gain information from the operational notebooks and records. Regarding to the extent and amount of the necessary information this possibility was continually reduced. It means that only the information from failure reports are completely registered and elaborated.

Except these essential lacks there were inaccuracies in the creating of information files from the following causes:

- activities and reports leading to a system readiness increase are performed mainly during examinations, tests and maintenance and these activities are not registered in the IRIS and there are only a few available information of this kind for the stand-by and safety systems which are in a waiting regime
- inaccurate registration of the real time of repair, mainly during general maintenance and overhaulting is relevant lack at the mean time of repair. In many cases the time of repair was given by the value of some days (regarding to the maximum allowed outage time), although a real repair activity lasted only some hours
- during examinations and tests some unsuccessful starts of the systems were not registered as failures. The examination or test lasted until a successful start. This occured mainly in the past, present situation is a little better. There are some discussible questions in this area too. Tests of the systems and equipment must be performed after each bigger maintenance and outage. It is truth that these tests were unsuccessful in many cases because of a non-professional manipulation or activity which caused an unsuccessful tests.

From these facts result simple conclusions that if we require high-quality information for reliability analyses responding to a real state of the operation, it is necessary to gain or consult a big part of information with the operational staff and to provide the verification of the quality of elaborated data.

The following presentation presents as the main steps for the creation of the Data Base for PSA according to the requests and needs of the analysts participated in this study.

DATA BASE - FIRST DRAFT

As a base of the first draft was taken "the preliminary Data Base draft", complemented by the information from the Soviet data base and research report and informations of EGU Prague, which dealt with the evaluation of some elements and systems data collected on NPP Dukovany - EDU.

The Data Base was arranged in the table form and contained the technological designation, name and types of failures of the particular equipments, data scurces and reliability characteristics (the demand failure probability, failure rate and a mean time of repair). Types of the failures were selected from real failures of the given equipments and some failures did not take into account the need of the analyst for the reliability analyses and probabilistic safety assessment.

The most of the comments dealt with detailed specification of the failure types where the equivocations concerning of some terms occured. The relevant comment was said to the determination of the element boundaries and conditions. Other comments concerned of the data base incompleteness. It was necessary to complement especially electric elements (fuses, elements of the load sequencing system, of the quick reactor protection system and so on) to divide circuit breakers and relays into more types, to disinguish cables into power cables and control cables and to make more accurate the failure types at armatures, relays, contactors and circuit breakers.

DATA BASE - SECOND DRAFT

The second draft of the Data Base was performed by incorporating most of comments of the particular organizations, which participate on PSA Level 1 for NPP Dukovany. The basic structure of this draft was not changed in comparison with the first draft. Number of the elements was substantially extended and complemented by missing elements according to the comments of the particular organizations (elements of the load sequencing system, emergency protection, safety systems, safety valves and so on). Control circuits were separated and inserted just behind an element to which they belong. Only the elements which directly participate on the control were included into the control circuit group. Electric elements (relays, circuit breakers, contactors, pickups,...) were divided into the concrete types according to real state on the NPP Bohunice and NPP Dukovany. Commencing with the second draft of the Data Base type designation of the electric elements (relays, circuit breakers, contactors and so on) is without to their function in the electric scheme. The same types of elements with different reliability characteristics, regarding to their placement in a diverse working environment (control circuits, emergency protections, load sequencing system and so on), were considered. Data from the Soviet Data Base were not clear and substantiated and therefore they were continually substituted by data from our NPP's.

DATA BASE - THIRD DRAFT

The effort of the organizations participating on PSA Dukovany was to incorporate their opposers' comments and to create the accepted system of event designations in this third draft of the Data Base. This structure of the Data Base was conceptionally different from the second draft. Information and reliability characteristics were ranked in the following way:

- identification code (accepted system of the primary event designations)
- name of an element (name and type of an element)
- kind of an element (way of verifying its functional ability, where PK means periodically checked, M - monitored, N - - unrepairable during the operation)
- the demand failure probability
- failure rate
- time till the failure revealing (for periodically checked elements of the stand-by and safety systems which are in a waiting regime-testing interval)
- time of maintenance/operation (mean repair time, resp. required time of operation during the service of an element).

We assumed that there would be enough high-quality data for the particular systems in future,so that it would not be necessary to determine a value of one system as an average value of several subsystems, but every subsystem would have another value given by unique working conditions and material properties of each element.

During selection of the failure types of single elements, such failure types, which would be necessary for analysts during reliablity system analysis were emphasized. Codes of failure types of the single elements took into account possible failures according to the kind of an element (PK, M, N) in the dependence on a regime (waiting regime of the stand-by and safety systems, operation, injection and recirculation phase) in which they can occured. Technological systems, which are periodically checked, have an enumerated total contribution to the unpreparedness of a given subsystem for a test with a given duration of test.

The third draft of the Data Base need some comments. Sources of data are not mentioned for each element, a manual for using of the Data Base misses, some data of identic system are uselessly repeated. Unaccuracies of the designation of some electric elements in the operation of the NPP Dukovany 1st unit was pointed out.

The problem of element boundaries was open again, it was pointed out that there are not disconnectors in the control circuits which were mentioned in another part of the Data Base.

Tables in the Data Base are incomplete, mean times of repairs miss at many elements. Used failure types of relays and circuit breakers are incomplete. The models and ways of gaining of the total unpreparedness from the tables, together with giving model examples, are not mentioned in this draft.

Error coefficients, numerical values of the initial events and common cause failures miss in the third draft. Components of the emergency protections (neutron pickups, pressure and power relays, units BKU and BKV) and data for cable contacts are missing. The possible types of failures are simple defined for the circuit breakers.

PROPOSAL OF THE DATA BASE STRUCTURAL CHANGE

All drafts of the Data Base have been performed by unsuitable way up to now, which requires a tremendous mass of work and time. It would be necessary to come through the whole NPP, each system and all important components with necessary information in this way. It is also necessary to determine the component boundaries.

The consequences of the neglecting of component boundaries are confusing in construction of the fault trees and also in evaluation of specific values.

After evaluation of all these facts we elaborated "Proposal of a structural change of the Data Base of reliability characteristics of the NPP's with WWER 440 reactors type V 213", where all requirements of analyst of PSA Dukovany and operational staff of NPP's and some IAEA materials were taken into account. Content of the Proposal is divided into particular components (pumps, armatures, tanks, heat exchangers and so on). For each component the regime which can be found and the responding reliability characteristics are distinguished. The proposal is aimed at component types on NPP and an appurtenances of a certain technological or electric systems are not presented. The use of the error coefficients, differences of the component data for various working environment and various ways of the appropriate system operation, will be presented. The important fact is that the table in this proposal contains determination of the component boundaries and all presented parts of the components, concerning the data in table, will be defined. The first responses of the organizations on this submitted Proposal were favourable.

During the further work (fourth draft) we assume re-elaboration of third draft according to a new approved proposal:

1. Overtaking the information from the third draft and their re-evaluation
2. Complementing the missing informations, determination of the component boundary, completing the so called "background" of the presented characteristics
3. By validisation and use of the information and experience gained up to now, to elaborate the Data Base for the NPP's with WWER 440 reators type V 213.

It is possible that so as reliability system modelling in PSA is in evolution and knowledgies of analysts about the component modelling will not be final, the modelling of suitable Data Base will be also particulary modified according to their requirements. But the main problem is to find the compromise between the PSA requirements on reliability characteristics and "status quo" on NPP, where on the first place are operational aimes. Than it is necessary to show the positive influence of PSA not only on exploatation reliability and safety, but also on operational economy and only really positive results can you open "door" of NPP to meet the operational staff to help you to find this compromise.

VVER SEVERE ACCIDENT MODELING WITH MAAP4

M.G. PLYS
Fauske and Associates, Inc.,
c/o Westinghouse Electric Nuclear Energy Systems,
Brussels, Belgium

Abstract

The MAAP 4 code for integrated severe accident analysis, its modifications for VVER plants, and its applications to PSA are described here. MAAP 4 contains thermal-hydraulic and fission product models to simulate plant response including operator actions and time dependent availability of equipment throughout a severe accident. MAAP 4 can be used to determine which accidents lead to fuel damage and which accidents are successfully terminated, as well as the potential for mitigation of consequences via actions. It is easy to run hundreds of cases with MAAP 4 for a PSA to quantify plant damage states, fission product release, recovery potential, and operating conditions for equipment, and to observe the impact of current or proposed plant design features, systems and setpoints, and procedures. MAAP 4 is the newest version of MAAP offered by the Electric Power Research Institute (EPRI) and developed by Fauske and Associates, Inc. (FAI).

1.0 INTRODUCTION

1.1 Purpose

MAAP 4 is a general tool for light water reactor Probabalistic Safety Assessment (PSA). It can be used for Level 1 analyses to determine core damage frequency (given initiating event specification) and Level 2 analyses to determine containment response and fission product release. This paper describes the general content of MAAP 4 and how it can be used for PSA's. Further applications for simulating the impact of current and proposed plant design features, systems and setpoints, and operating procedures are discussed.

This paper also introduces the VVER capability of MAAP 4, which provides a vital link in PSA between the accident frequency and overall risk evaluations.

1.2 Background

MAAP 4 is an advanced and improved code in the Modular Accident Analysis (MAAP) family of codes. MAAP was originally developed during the Industry Degraded Core Rulemaking (IDCOR) program in the early 1980's, and it is now property of the Electric Power Research Institute (EPRI). Fauske and Associates, Inc. (FAI) has been the prime contractor for all versions of MAAP. MAAP is licensed to utilities and other organizations by EPRI.

Currently, MAAP 3.0B is the practically exclusive tool of choice for Individual Plant Analyses (IPE's) and PSA's performed by utilities. It is favored over alternative codes or code systems because of its rapid simulation time (about 2 to 4 hours on a PC are required for a 40 hour accident), its ability to consider operator actions, its capacity for sensitivity studies, and general ease of use.

Interest in severe accident management (SAM), the recovery of plants before and after core damage, the study of operator actions, and general advances in our understanding of severe accident phenomena have motivated the development of MAAP 4. Its capabilities make it much better suited to VVER analyses than MAAP 3.0B.

1.3 Philosophy

MAAP 4 combines in one package models for heat transfer, fluid flow, fission product release and transport, plant system operation and performance, and operator actions. Physical models exist for processes that are important during transients that lead to and go beyond fuel damage, and all models are coupled at every timestep. This concept of model integration is essential because of the strong influence of processes on one another or on plant systems, and the strong role that operators can have on the outcome of an accident.

The level of model detail is sufficient to acceptably match experimental data but simple enough to allow rapid simulation on ordinary computers. It is therefore inexpensive and easy to make hundreds of MAAP runs for a PSA, and the Level 1 analyses benefit greatly from information concerning conditions that affect equipment and the overall sequence and timing of events.

The models are validated against experimental data and evaluated by a Design Review Group of experts independently convened by EPRI; these topics are beyond the present paper scope.

2.0 GENERAL CODE FEATURES

2.1 Architecture

Plant simulation is a dynamic process which begins with a picture of the plant state and then predicts the time evolution of the state. Real state variables are masses and energies in control volumes plus equipment status, while observable quantities such as pressure, temperature, and water level are derived. To begin the prediction of the evolution, conditions for automatic equipment function (or impairment) and operator actions are scanned, and the appropriate equipment and operator response is taken. Then, rates of change due to individual processes are evaluated and summed for each state quantity. For example, the water mass in a VVER vessel lower plenum may be influenced by heat transfer to structures, decay power of movable control assemblies, flashing, inflow, etc. Last, total rates are integrated over a timestep to yield the next state, and its observable quantities are derived. This process is repeated until the end of the simulation.

2.2 Plant Representation

The entire plant is divided into control volumes for conservation of mass and energy. Core nodalization is flexible (up to 7 radial and 25 axial nodes), while primary system nodalization is fixed per reactor type (18 nodes for the PWR and VVER including the steam generators and 8 for the BWR including the recirculation piping, if any). The containment/accident localization regions and any auxiliary and turbine rooms are simulated by the user with up to 30 nodes that may be arbitrarily connected. The connections can include normal openings, leakage paths, ventilation ducts, and failures.

MAAP uses "smart nodes" that contain gradients or "sub-node physics" to simulate certain processes in otherwise well-mixed control volumes. For example, fluid-structure heat transfer in the hot leg and steam generator piping considers gradients in temperature along the flowpath.

Typical plant equipment is represented with standard input for system setpoints and performance curves. In addition, users may partly or completely redefine system logic. VVER systems are easily represented within this framework. Generalized injection and spray systems including suction locations, pumps and heat exchanger characteristics, and destinations may be specified.

2.3 Core Models

Each core node has separate temperatures for the fuel, cladding, control material, and fuel channel, if any. Heat transfer to water and gases, hydrogen generation, core-upper plenum natural circulation, clad ballooning and failure, fission product release, and radiative energy transport are modeled. The U-Zr-O phase diagram is used for fuel-cladding interactions and melt progression, and a molten pool model is used for highly degraded geometry. Recovery of a damaged core considers the effects of porosity and critical heat flux.

2.4 Primary System Models

BWR natural circulation and PWR phase separation are considered, though the primary system models are most detailed for cases with limited water inventories. Gas phase natural circulation and countercurrent circulation, reflux condensation, and stratification of noncondensible gases are allowed. Fission product transport, deposition, and revaporization occur.

Also considered are the temperature response of the vessel, piping, and components, including creep rupture at elevated temperatures, insulation, heat losses to containment, possible vessel submergence, and interactions of core debris in the lower plenum.

2.5 Containment and Auxiliary Building Models

Pressure-driven gas flows, counter-current flows induced by temperature gradients, flow of water and core debris, and entrainment of water and core debris are allowed between nodes. Debris-water interactions, debris-concrete interactions, fission product release, transport, deposition, and revaporization, flammability and combustion of general H2-CO-air-H2O-CO2-N2 mixtures, and direct containment heating phenomena are considered. Structures with temperature gradients (walls), lumped heat capacities (cable trays, etc.), and engineered safeguards like sprays, fan coolers, simple fans, and fire suppression are included.

2.6 User Interface

A "parameter file" is constructed that contains a complete plant description independent of any accident. The parameter file contains containment geometry and topology, primary system and core geometry, equipment logic and performance data, and initial conditions. Special "model parameters" for sensitivity analysis are grouped together in the parameter file, such as aerosol shape factors or the choice of fission product release correlations.

An "input deck" is used to describe an accident and control a simulation. The input deck considers accident initiators such as pipe breaks, loss of power, or equipment failures, and degraded system response such as revised pump curves.

"Intervention conditions" can be specified to represent plant states that will lead to either operator actions, equipment automatic function, or some other equipment status change. "Action blocks" are linked to the conditions and contain the commands for equipment operation and performance.

Detailed system logic, operator procedures, and event trees can be easily represented and understood using the Intervention/Action structure. Interventions may occur for reasons (equipment automatic setpoints or operating limits may be reached, or the operator may notice a combination of containment and primary system conditions that cause him to enter a procedure) or arbitrarily (a failure is defined at a time or upon transition between system modes). Actions basically consist of turning equipment on or off, controlling pumps or valves, or adjusting performance curves. Sets of these conditions and actions may be logically linked to describe entire systems or procedures.

3.0 VVER FEATURES

MAAP 4 represents the VVER core like a Western PWR but with fuel channels and borated steel absorber. Movable control assemblies that are partly below the normal bottom of active fuel are considered in the lower plenum control volume. The displacement of water, production of decay power, heat transfer to lower plenum water (and gas when present), and melting are included.

The water level calculation in the horizontal steam generators considers the circular cross section and structures such as the primary headers, tubes, and supports. Appropriate correlations are used for horizontal tube heat transfer. No countercurrent gas exchanges with the vessel are possible due to the hot leg loop seal. Hydrogen preferentially fills the primary side from the top down and thus reduces heat transfer area for reflux condensation.

The bubble tower is represented by placing the inlet structure and trays in separate control volumes linked by a junction that is normally submerged in the tray water. MAAP considers vent clearing of any junction based on the difference in pressures across the junction compared to the static head required for uncovery. Condensation may be degraded for shallow pools or high pool temperature.

4.0 CODE APPLICATION

4.1 Single Accidents

A simple MAAP simulation can be made by specification of systems that are unavailable or impaired at the beginning of an accident. The end time for the simulation, a title, and print control are the only other essential input. MAAP will then simulate plant response. A "success" is typically defined as a plant state at the end of the simulation in which temperatures, pressures, and water levels are steady, and decay heat is being removed. Success cases may also have unsteady levels, but either the core is still covered, or at least no fuel damage has been sustained during the defined time interval. Otherwise, either some fuel damage has already occurred, or this damage may be presumed inevitable. Success may also be defined as recovery of a safe, stable state after fuel damage.

The simple simulation described above is a typical PSA application of MAAP in which equipment availability is predefined and we seek to determine a resulting plant damage state. A related simulation could be made using additional input that redefines some plant characteristics, such as an increased flow capacity of an emergency system or the existence of a containment heat removal system qualified for LOCA environments. In this case the simulation is part of a study to determine the most effective and economical plant modifications.

When a simple simulation is run for every sequence specified in all the event trees of a Level 1 PSA, the results constitute a simple Level 2 study. Such simulations may include input that control specific phenomena models to consider sensitivity.

4.2 Operator Actions

A simple simulation may be extended by specification of pairs of intervention conditions and operator actions. As far as the code is concerned, "conditions" may be either observable plant variables such as water levels, or they may be quantities used during a simulation such as the amount of hydrogen evolved by clad reaction. "Actions" may either be actions taken by an operator, equipment functions that are normally automatic, or input changes redefining the operating characteristics of equipment.

A typical application of these intervention/action inputs is the determination of the recovery potential when operators take actions at specified times, after specified plant conditions are known, or after some postulated delay. This input structure also allows equipment availability to be determined naturally by the evolution of the transient itself instead of being specified in advance (and possible incorrectly) by a Level 1 study.

More generally, this application tests the effectiveness of procedures. Finally, and most important for a PSA, this application can demonstrate the reduction in core damage frequency achievable by considering operator actions.

A thorough Level 2 study should use operator actions in this manner for the event trees specified in a Level 1 study in order to more realistically assess overall frequency of plant damage states and release categories.

4.3 Event Trees and Accident Groups

When pairs of intervention conditions and actions are placed in the input, it is often unknown whether the conditions will actually be achieved and the actions taken. The power of conditional execution of actions lies in this fact. Enough conditions and actions may be input to simulate an entire set of operator procedures. This may remain a constant input for a large number of transient simulations in which only the initially unavailable systems are varied. A single input deck, with only minor changes, then can be used to test the impact of current or revised procedures for a variety of sequences.

Similarly, input may be created so that some conditions are never achieved, on purpose, during a simulation. Any number of such condition/action pairs may be input with no impact on a simulation. These conditions may be choices for equipment availability or phenomena paths which taken together constitute an event tree for a given accident initiator. Simple changes to the input deck can "activate" and "deactivate" conditions from being physically achievable. In this manner, all the sequences represented by a single event tree may be entered into a single input deck. Minor variations on this input deck cause specific paths of the event tree to be followed. Alternately, groups of accidents with similar initiating conditions or time dependent availability histories may be grouped into the same input deck.

The beauty of this input structure is that there may be a true one-to-one correspondence between Level 1 and Level 2 studies in which the Level 1 event trees or accident sequence categories are correctly converted to MAAP input.

4.4 Accident Management

Accident management applications of MAAP 4 include: Training of operators, support staff, engineering staff and upper management, accident management planning support, and support of personnel in the Emergency Offsite Facility (EOF), Technical Support Center (TSC), and Regulatory Emergency Response Centers during drills or emergencies. The emergency response application is enhanced by the additional use of the MAAP Accident Response System (MARS), as described below.

The MARS software (developed by FAI) uses the MAAP codes as its basis to calculate the thermal-hydraulic and fission product response under accident conditions, and adds the following features, beyond those available in MAAP: 1) The ability to use actual on-line plant data to initialize MAAP under accident conditions; 2) The ability to diagnose incoming plant data to validate plant instrumentation readings and to determine the plant status; 3) The ability to assess a root cause of the accident; 4) The ability to track the evolving plant status; and 5) The ability to perform predictions of potential future plant states based upon no operator actions, operator actions based upon procedures, and operator actions that employ accident management guidelines.

5.0 CONCLUDING REMARKS

A VVER Level 2 PSA may be conducted using MAAP 4 as the tool for quantification of plant response to prescribed system failures. Existing and proposed VVER systems and operator procedures may be evaluated. MAAP 4 can be used to determine which accidents lead to fuel damage and which accidents are successfully terminated, as well as the potential for mitigation of consequences via actions.

178 RECENT ADVANCES IN PSA-ORIENTED THERMAL-HYDRAULIC ANALYSES FOR WWER-440 NPPs

M KULIG
Central Laboratory for Radiological Protection,
Warsaw, Poland

J SZCZUREK
Institute of Atomic Energy,
Świerk, Poland

W. KOWALIK
Central Laboratory for Radiological Protection,
Warsaw, Poland

Z. BAZSO
Nuclear Power Plant Research Institute,
Trnava, Czechoslovakia

Abstract

The paper is concentrated on PSA-oriented thermal-hydraulic analysis of WWER-440/V213 NPP Analyses are limited to LOCA initiating events, excluding LOCAs within the steam generator. The most important results of the work recently undertaken in the Central Laboratory for Radiological Protection (Warsaw), Institute of Atomic Energy (Świerk), and Nuclear Power Plant Research Institute (Trnava) are discussed in the paper

The main objective of the study was to provide quantitative evidence for PSA accident sequence modeling The study was devoted to identification of minimal safety system requirements and grouping LOCA initiators with the same safety system success criteria

This work was motivated by unsatisfactory status of PSA-oriented WWER plant response evidence The main shortcoming is unsufficient number of accident scenarios covered by existing analyses, as well as limited confidence related to thermal-hydraulic computer codes that had been used in the past

The study included several tasks

1 Categorization of LOCAs according to minimal safety system requirements based on existing results
2 Selection of accident scenarios for computer analysis to verify qualitative assessment
3 Performing computer analyses with RELAP/MOD2 for the selected scenarios
4 Reassessment of LOCA categorization and verification of minimal safety system requirements

Preliminary categorization of LOCAs was performed basing on available thermal-hydraulic analyses supported by engineering judgment Existing PSA-related plant response evidence has been reviewed Several sources available in CSFR, Russian Federation and Poland were taken into account Conclusions formulated during the workshop on 'Plant Response for WWER-440 NPPs" held in Trnava, CSFR were also considered

LOCA categories were selected according to system success criteria - each LOCA category was defined to have the same system configuration logic and the same system capabilities

Accident scenarios for computer analysis were selected in such a way that all important limits for LOCA categories were bracketed In this way both success scenarios and failure sequences were selected for further investigations

Selected cases were investigated with RELAP5/MOD2 code (version for PCPPS workstation provided by RMA, Albuquerque) Simulation time was adjusted to achieve stable core cooling conditions (for successful scenarios) or the beginning of core overheating/uncovering

Calculations were performed using actual version of input data prepared for WWER-440/V213 within the frame of IAEA Regional Programme RER/9/004 More than 20 accident scenarios were analysed within the study, covering the break size range 60 - 300 mm D and various configurations of safety systems

These calculations provided great amount of information needed to verify existing analyses (performed previously with RELAP4 and SLAP) Both LOCA group limits and allowable time margins for the operator actions were addresed Smaller sizes were not very well covered, due to high CPU-time requirements

Results of RELAP calculations were used to re-assess the preliminary categorization The paper summarizes current state of plant response evidence and discusses stil existing gaps in PSA-oriented T/H analysis

Background and Objectives

Evaluation of PSA results obtained within the frame of Regional Programme RER/9/005 during the first three years of programme activities identified plant response evidence as one of the most important issues that determine the quality of accident sequence model. This subject was not considered with appropriate attention in the past, due to limited manpower capabilities in the area of thermal-hydraulic analysis

PSA-oriented thermal-hydraulic WWER-440 plant response evidence was recently discussed during the workshop held in Rez, 3-7 Feb 1992, where current status of plant response analysis was reviewed

More detailed review of plant response evidence was made during the next project workshop held in Trnava, CSFR, 4-7 May 1992 [1]. Discussion was devoted to primary circuit LOCA with exception of LOCAs within the steam generator.

PSA-related plant response evidence currently available in CSFR, Russian Federation and Poland was compiled. Existing Event Tree models developed in CSFR (VUPEC, Bratislava and UJV, Rez) and Poland (CLRP, Warsaw) were reviewed. Some differences in ET models were identified and discussed. Rationale behind the models was explained by the PSA analysts.

Taking into account available thermal-hydraulic analyses and using engineering judgment provided by thermal-hydraulic experts, new LOCA categorization supplemented with system success criteria was proposed. This categorization reflected current state of T/H plant response evidence.

It was found that current state of PSA-oriented WWER-440 plant response evidence is still not satisfactory. The main shortcoming was insufficient number of accident scenarios covered by the analyses, as well as limited confidence related to T/H computer codes that had been used in the past. The most important issues that required refinement were identified and documented.

Trnava meeting was an important milestone that stimulated further activities in this area. Intensive investigations were undertaken in the National Inspectorate for Radiation and Nuclear Safety, Warsaw and the Institute of Atomic Energy, Swierk in cooperation with Nuclear Power Plant Research Institute (VUJE) Trnava. This study, fully financed by VUJE, was directed to cover existing gaps in PSA-oriented T/H analysis. The study was devoted to identification of minimal safety system requirements and grouping LOCA initiators with the same safety system success criteria. The most important findings of the study are reported in this paper.

Preliminary Categorization of LOCA Initiating Events

Preliminary categorization of LOCAs was performed basing on available thermal-hydraulic analyses supported by engineering judgment. Conclusions formulated during the workshop on "Plant Response for WWER-440 NPPs" held in Trnava, CSFR (4-7 May 1992) were taken into account.

LOCA categories were defined according to system success criteria - each LOCA category was defined to have the same system configuration logic and the same system requirements. Table I summarizes essential information concerning successful system configurations. Fig.1 explains the basic logic applied in LOCA categorization process.

Six categories were selected for LOCA initiating events, with the following features.

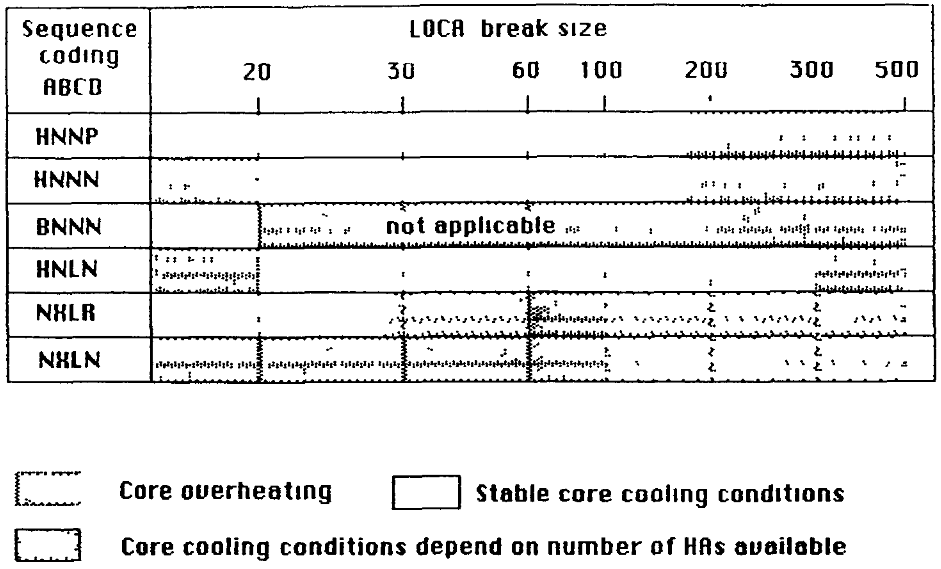
LOCA L1 covers the smallest break size range considered in LOCA PSA. Unique feature of this initiating event is the necessity of secondary side cooling. For this break size energy removed by coolant flow through the break and by injection coolant heating is insufficient to ensure system depressurization if secondary side cooling is not provided. System configuration HNNN is not successful.

Table 1. Successful configurations of safety systems for various LOCA categories.

LOCA Category	Coding identifier [1]								Sequence coding[2]
	A			B	C		D		
	HPI	HPR	PRV	CFS	LPI	LPR	EFS	SCS	ABCD
L1	●	●				●	●	P	HNLP
	●	●					●	P	HNNP
				●	●	●	●	R	NXLR
	●	●	●						BNNN
L2	●	●				●		P	HNLN
	●	●						P	HNNN
				●	●	●	●	R	NHLR
L3	●	●				●		P	HNLN
	●	●						P	HNNN
L4	●					●		P	HNLN
	●	●						P	HNNN
				●	●	●		P	NHLN
L5	●					●		P	HNLN
				●	●	●		P	NXLN
L6				●	●	●		P	NXLN

[1]) System identifiers:
HPI - High Pressure Injection System
HPR - High Pressure Recirculation System
PRV - Pressurizer Safety Relieve Valve
CFS - Core Flooding System
LPI - Low Pressue Injection System
LPR - Low Pressure Recirculation System
EFS - Emergency/Auxiliary Feedwater System
SCS - Secondary Pressure Control System
P - Pressure maintenance mode
R - Heat removal mode (30 K/h)

[2]) Sequences designated with bold style determine LOCA category limits



System configuration coding - ABCD

A - High Pressure Injection/Recirculation System
N - system unavailable, H - single HPS train available
B - Primary Feed and Bleed (HPI/HPR + PSRV)

B - Core Flooding System
N - system unavailable, X - number of HAs available

C - Low Pressure Injection/ Recirculation System
N - system unavailable, L - single train available

D - Secondary Side Cooling System
P - Pressure maintenance mode (single EFW train + single dumper)
R - Heat removal mode -30 K/h (single EFW train + single dumper)
N - EFW unavailable, single dumper operable

Fig.1. Logic used in LOCA categorization process.

Lower limit for this group was estimated as the largest break size compensated by normal make up system

Preferable mitigation measures for this accident include High Pressure Injection/Recirculation System (HPI/HPR) for the initial phase of accident and Low Pressure Recirculation System (LPR) for long-term cooling In case of LPS failure HPS may be used alternatively for long-term cooling, but it involves some manual operator actions to control the process In both cases secondary cooling is required in addition to ECCS

For scenarios with HPS operable and failure of secondary side cooling, primary feed and bleed is the only mean of accident mitigation Primary feed and bleed requires operation of HPS and Pressurizer Safety Relief Valves (controlled manually)

For scenarios with HPS failure in the very early phase of accident depressurization of RCS by the use of secondary feed and bleed and LPS for long-term cooling is acceptable mean of accident mitigation Time margin for the operator to initiate depressurization (manually) depends on availability of Core Flooding System (Hydro-accumulators) If CFS is operable this time margin is proved to be relatively large for this LOCA category

Lower limit for this LOCA category was estimated as 10 mm D, upper limit was assessed as 20 mmm D

Lower limit for **LOCA L2** category is related to secondary side cooling requirements For break sizes larger than this limiting value HPS is sufficient to achieve stable core cooling conditions, even if secondary side cooling is not established

Upper limit for LOCA L2 is related to practical acceptability of secondary feed and bleed, followed by LPS operation for long-term cooling, as an alternative way to HPI operation Limiting value is selected in such a way that sufficient time margin for correct plant state diagnosis and for manual alignment of secondary side cooling system is assured One hour is considered as practically acceptable time margin to allow correct operator behaviour

Mitigation of the accident is similar to L1 except that secondary side cooling is not needed, if HPS is operable Preferable mitigation measure for this accident is operation of High Pressure Injection/Recirculation System (HPI/HPR) for the initial phase of accident and Low Pressure Recirculation System (LPR) for long-term cooling In case of LPS failure HPS may be used alternatively for long term cooling

Respective upper limit for this LOCA category was estimated as 50-70 mm D It depends on success criterion adopted in ET model for CFS

For **LOCA L3** category the HPS is the only mean to establish stable core cooling conditions in the initial phase of accident and to depressurize RCS below LPS operational limit If only CFS (Hydro-Accumulators) is available core uncovering and overheating occur at the RCS pressure exceeding the LPS operational limit Depressurization of RCS by the use of secondary feed and bleed is not practically achievable, because of timing requirements

Mitigation of the accident is similar to L2 except that in case of HPS failure, secondary feed and bleed (with subsequent use of LPS) is not taken into account

Upper limit for this LOCA category was estimated as 120-150 mm D

For **LOCA L4** category operation of CFS and LPS is an alternative way to assure successful mitigation of accident in addition to mitigation measures applicable to LOCA L3. For the break size range considered, depressurization of the RCS occurs at such a rate that long term cooling may be taken over by LPS, and HPS is not needed.

For this LOCA category operation of HPS followed by LPS is preferable mitigation measure (similarly to LOCAs L1-L3). HPS is also acceptable mitigation measure for long term cooling in case of LPS failure.

Upper limit for this LOCA category was estimated as 200 mm D.

For **LOCA L5** category CFS or HPS are required for early phase of the accident and LPR for long term-cooling. For the break size range considered the HPS alone is not sufficient, as it is the case for LOCA L4.

Upper limit for this LOCA category was estimated as 300 mm D .

For **LOCA L6** category simultaneous operation of CFS and LPS is the only measure for successful mitigation of accident. Operation of HPS followed by LPS is not sufficient to prevent core uncovering and subsequent overheating.

All breaks larger than 300 mm D are covered by this category (up to double-sided break of primary loop piping).

Selection of Accident Scenarios for Computer Analysis

Selection of accident scenarios to be investigated by computer analysis was based on the results of preliminary categorization. Selected scenarios differed by system configuration and break size. Localization of the break size was not investigated. In all calculations cold leg break was selected as the basic case.

The main effort was concentrated on verification of LOCA grouping ranges. The most important system configurations that determine limits for LOCA groups were identified, as shown in Fig.1. For each system configuration at least two LOCA break sizes were selected in such a way that all important limits for LOCa categories were bracketed.

LOCA categories L1 and L2 were not well covered by he analyses, due to very high CPU-time requirements. However, some attempt has been made to verify the existing results, obtained for this LOCA categories in the past with RELAP4, SLAP and other less sophisticated codes. For scenarios with HPI/HPR system operable (HNNP, HNNN, HNLP) three break sizes were investigated - 160, 200, 300 mm D. For scenarios with HPI/HPR unavailable (scenarios NXLR, NXLN) smaller sizes were included - 60, 90, 120, 160 mm.

In all calculations capability of High Pressure Injection/Recirculation system was limited to single train (not degraded). In majority of cases that involve Low Pressure Injection/Recirculation System, its capability was assumed to be limited to single train (degraded to 50% and supplying coolant to upper plenum of the RPV).

In the whole break size range considered in the study (60-300 mmD) the secondary circuit was assumed to operate in its automatic mode (pressure maintenance mode) with single EFS pump and single steam dumper (BRU-A).

For scenarios NXLN various numbers of Hydro-Accumulators (designated in the coding system as "X") were considered (in the range 0-3). In case of X=3 two HA were connected to down-comer (DC) and one HA to upper plenum (UP). For X=2, two cases were considered - two HA connected to DC, as well as one HA connected to DC and one connected to UP. In case of X=1 both cases - HA connected to UP and HA connected to DC - were analysed.

Detailed specification of calculational cases is given in graphical form in Fig.2.

RELAP5 Calculations

Calculations were performed using RELAP5/MOD2 code (version for PCPPS workstation supplied by Risk Management Associates Co., Albuquerque, USA) and present version of input data prepared for WWER-440/V213 within the frame of IAEA Regional Programme RER/9/004.

Simulation time was adjusted to achieve stable core cooling conditions (for successful scenarios) or the beginning of core overheating/uncovering. In case of successful scenarios simulation was terminated when ECCS flow was higher than leak flow, the RCS inventory acceptably high and core temperatures stabilized or decreasing. In case of failure sequences maximum cladding temperature in average channel equal to 1200 K was adopted as termination criterion.

The results obtained from RELAP5 calculations provided some new evidence for re-assessing the categorization of LOCA and related success criteria. In addition, relatively detailed information on timing of accident progression was accumulated, particularly for sequences with degraded Core Flood System (3-1 Hydro-accumulators) and for sequences with no ECCS at all.

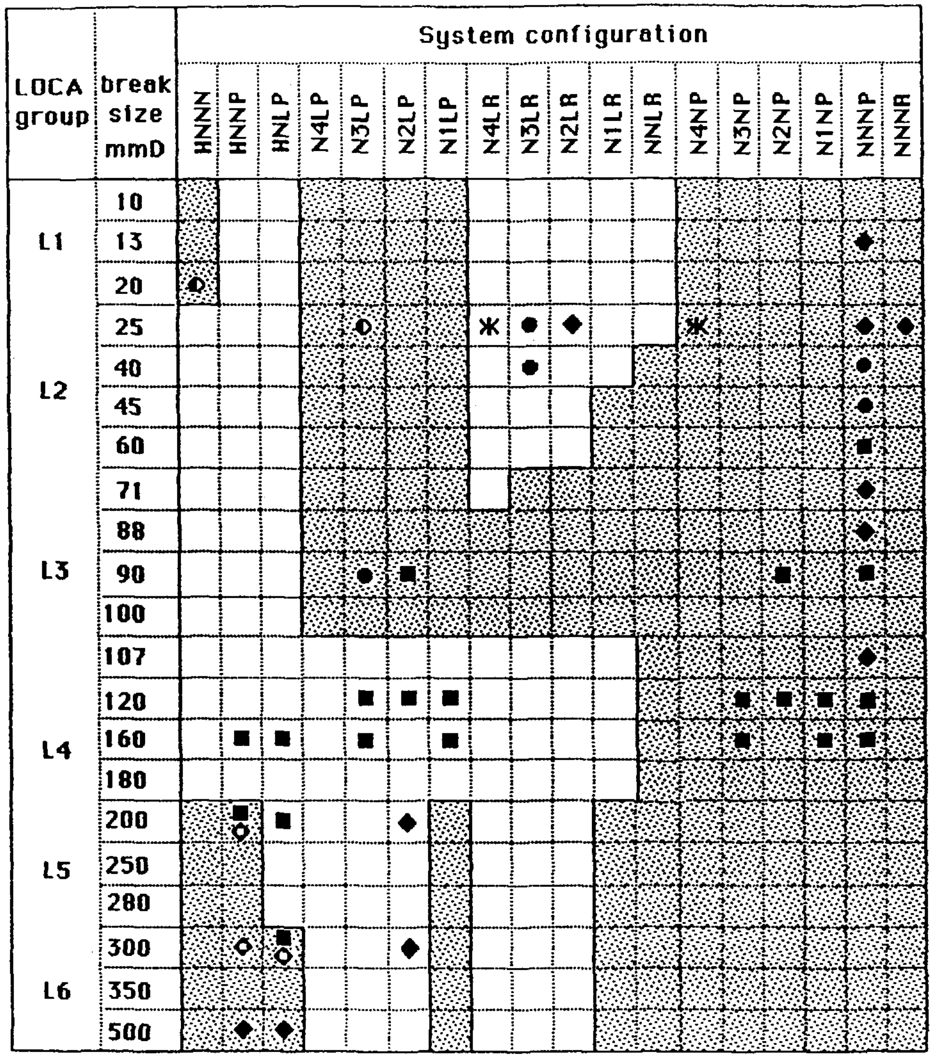
To large extent the new results are in good agreement with previous calculations. However, in some cases slight re-evaluation of LOCA category limits was needed.

The results of calculations are briefly disscussed below with respect to each of the six categories mentioned above. More detailed information is given in [3].

Refinement of LOCA Categorization

LOCA L1

This category was not investigated within the study and no new evidence was brought up to verify previous assumptions. The calculations for this break size range are very CPU-time consumming. From the point of view of LOCA PSA these investigations are not the highest priority tasks. In some WWER-440 PSAs [2], it was found that dominant contributors for LOCA category L1 are very close to those for category L2.



LOCA group	break size mmD	System configuration																	
		HNNN	HNNP	HNLP	N4LP	N3LP	N2LP	N1LP	N4LR	N3LR	N2LR	N1LR	NNLR	N4NP	N3NP	N2NP	N1NP	NNNP	NNNR
L1	10	▨			▨	▨	▨	▨						▨	▨	▨	▨	▨	▨
	13	▨			▨	▨	▨	▨						▨	▨	▨	▨	▨ ◆	▨
	20	▨ ◐			▨	▨	▨	▨						▨	▨	▨	▨	▨	▨
L2	25				▨	▨ ◐	▨	▨	✱	●	◆			▨ ✱	▨	▨	▨	▨ ◆	▨ ◆
	40				▨	▨	▨	▨		●			▨	▨	▨	▨	▨	▨ ●	▨
	45				▨	▨	▨	▨				▨	▨	▨	▨	▨	▨	▨ ●	▨
	60				▨	▨	▨	▨				▨	▨	▨	▨	▨	▨	▨ ■	▨
L3	71				▨	▨	▨	▨		▨	▨	▨	▨	▨	▨	▨	▨	▨ ◆	▨
	88				▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨ ◆	▨
	90				▨	▨ ●	▨ ■	▨	▨	▨	▨	▨	▨	▨	▨	▨ ■	▨	▨ ■	▨
	100				▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
L4	107												▨	▨	▨	▨	▨	▨ ◆	▨
	120					■	■	■					▨	▨	▨ ■	▨ ■	▨ ■	▨ ■	▨
	160		■	■		■		■					▨	▨	▨ ■	▨	▨ ■	▨ ■	▨
	180												▨	▨	▨	▨	▨	▨	▨
L5	200	▨	▨ ■ ◇	■			◆	▨				▨	▨	▨	▨	▨	▨	▨	▨
	250	▨	▨					▨				▨	▨	▨	▨	▨	▨	▨	▨
	280	▨	▨					▨				▨	▨	▨	▨	▨	▨	▨	▨
L6	300	▨	▨ ◇	▨ ■ ◇			◆	▨				▨	▨	▨	▨	▨	▨	▨	▨
	350	▨	▨	▨				▨				▨	▨	▨	▨	▨	▨	▨	▨
	500	▨	▨ ◆	▨ ◆				▨				▨	▨	▨	▨	▨	▨	▨	▨

✱	SECNPS, Moscow (several cases)
◆ ◇	VUJE, Trnava, SLAP code
● ◐	IEA, Swierk, RELAP4/MOD6
■	Recent analyses, RELAP5/MOD2

Fig. 2. Current status of PSA-oriented thermal-hydraulic analyses (Sep. 1992).

LOCA L2

Estimation of the time margin for the operator to initiate system depressurization by the use of secondary feed and bleed for scenarios without HPS was the most important issue to be clarified. This time margin determines the upper bound for LOCA category L2.

Relatively limited calculations were performed for this LOCA range. However, the results obtained for larger break size range (60-160 mm) seem to be in good agreement with the results obtained previously with SLAP and RELAP4/MOD6. This agreement allows some extrapolation of results to cover the range below 90 mm D. Summary of these results is presented in Fig. 3.

The following observations can be made in relation to timing of LOCA accidents with HPS unoperable (NXNN/ NXNP scenarios).

- Time margin to core overheating depends strongly on break size and on availability of Hydro-accumulators. For 90 mm D this time margin varies from 1240 s (for scenario with all HAs unoperable) to 4420 s (for scenarios with 2 HAs injecting to down comer). For 160 mm break the time margin is reduced to 626 s (the case NNNP 90 without HAs) and 1444 s (the case N3NP09D with 3 HAs).
- Time period between the end of HAs discharge and the core overheating is a considerable part of the total time margin (in the range investigated it varied from 50 to 65%).
- Interesting observation is that time margins for scenarios with 2 HAs injecting to down comer (DC) are very similar to those obtained for scenarios with 3 HAs (2 HAs injecting to DC and 1 HA to UP). This result is related to loop seal phenomena induced by UP injection. Apparently, in this case primary coolant mass distribution in the RCS is much more unfavorable than that in case of pure DC injection.

Basing on existing results, the upper break size limit for LOCA L2 is finally estimated as 60 mm D. This value is derived from extrapolated value of time margin. Time margin to core overheating for this break size is expected to be in the range 7000-8000 s (for 2 or 3 HAs). It is expected that even with limited availability of CFS (2-3 HAs), the LPS operational limit (0.75 MPa) may be reached before the core is uncovered and overheated, provided that secondary feed and bleed is initiated within the period of 1 hr. Confirmation of this result is required by performing calculation with RELAP5 code.

LOCA L3

Upper limit for this LOCA category (lower limit for LOCA L4) was to be estimated in the study as the smallest break size that allows for successful mitigation of accident by the use of Core Flooding System (HAs) and LPS only. The HPS was assumed to be unavailable and no operator actions were taken into account. Two break sizes were investigated with respect to this limiting value - 120 and 90 mm.

The results may be summarized as follows:

- The scenario with break size 120 mm appeared to be successful both for 3 HAs (2 HA injecting to DC and 1 HA to UP) and 2 HAs (both injecting to DC). In both cases the core temperatures were relatively low. The case with single HA injecting to UP has also been proved to be successful.

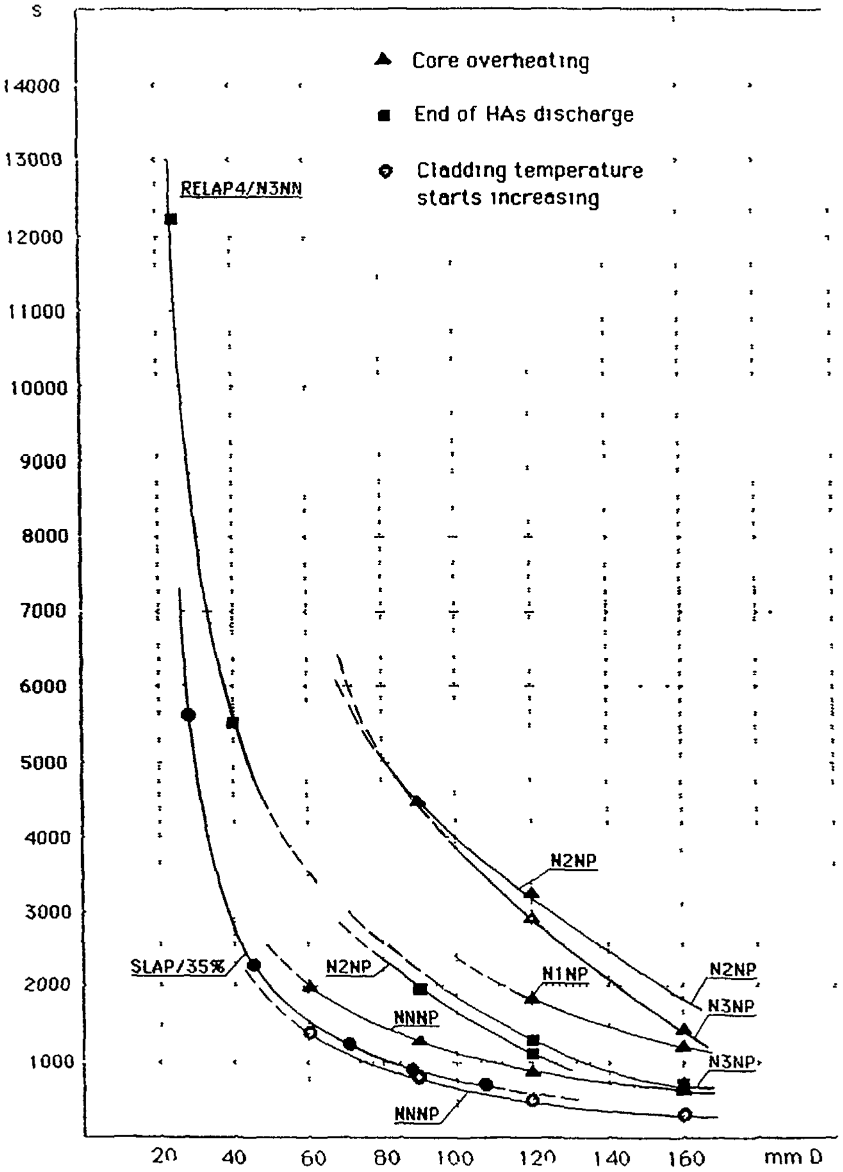


Fig.3. Timing characteristics for accident sequences NHLP

- The scenarios with break size 90 mm should be considered as limiting for this LOCA category The RCS pressure was decreased to the LPS operational level (in 4000 s) and the LPS started to inject coolant Operation of the LPS was found to be periodical The RPS pressure oscillated at the level of LPS initiation (0 75 MPa) up to 4900 s (the end of simulation period) It also appeared that at the beginning of LPS initiation the RCS was relatively close to core overheating (without LPS initiation the core overheating occured in ~420 s)

- Taking into account these results it seems reasonable to increase limiting value for this LOCA category to 100 mm D (as intermediate value in the range 90-120 mm)

- Success criterion for CFS may be relaxed to a single HA, if this limiting value is increased to 120 mm Accident scenario NNNP 120 mm, with no HAs available, appeared to be very close to reach the LPS operational limit (0 75 MPa) before the core overheating In these conditions operation of a single HA is sufficient (this was proved for both 120 mm as well as 160 mm break)

LOCA L4

Upper limit for this LOCA category (lower limit for LOCA L5) was to be estimated as the largest break size that allows successful mitigation of accident by the use of HPS only Two break sizes were investigated with respect to this limiting value - 200 mm and 160 mm D The results may be summarized as follows

The break size 200 mm D, previously considered as the limiting value for LOCA L4, appeared to lead to core overheating The break size 160 mm D permits successful mitigation of the accident Taking into account a/m results intermediate break size 180 mm seems to be reasonable limiting value for this group

LOCA L5

Upper limit for this LOCA category was to be estimated as the highest break size that allows successful mitigation of the accident by the use of HPS and LPS only (without operation of HAs) Scenarios HNLP 300 and HNLP 200 were investigated for this LOCA category Calculations were performed for partial capability of LPS (50%, injecting to UP through HA-1 surge line)

The results may be summarized as follows

- The accident scenario with 300 mm break should be classified as leading to core damage Maximum cladding temperature in hot channel (1518 K) exceeds 1200 °C considered as a limit for zirconium cladding oxidation Maximum cladding temperature in average channel reached maximum 1080 K Slightly lower temperature may be expected for the case with full LPS capacity, however, this scenario was not investigated Basing on previous result obtained by VUJE with SLAP code this scenario was assumed as successful

- Maximum cladding temperatures reached in the core for the scenario HNLP 200 (covered by the LOCA L5 category) are considerably lower - 833 K in average channel and ~1100 K in the hot channel

- Taking into account the results for 300 mm break slightly lower limit is proposed for LOCA L4 The limiting value 280 mm is adopted basing on engineering judgment Success criteria for this category may be relaxed to partial capability of the LPS (50%)

LOCA L6

Very limited investigations were carried out for this LOCA category Analyses covered lower limiting break size 300 mm D No investigation was undertaken to verify success criterion for CFS (the number and location of HAs)

Issues for further investigation

- Thc smallcst sizc LOCA catcgory L1 should bc invcstigated, particularly with the respect to upper limit for this category

- Some additional calculations would be advisable to investigate timing of accident scenarios NXNN in the break size range 40-90 mm Extrapolations made for 40 and 60 mm breaks should be verified Some additional cases with a single hydro-accumulator should also be included for the range 40 - 90 mm D

- Scenario NXLR for 60 mm break should be calculated to investigate allowable time margin for starting the operator actions (initiating secondary feed and bleed) and to confirm assumption related to selection of this break size as the upper limit for LOCA L2

- Relaxation of success criteria for HPS for LOCAs L1-L3 is very likely (capability of HPS train reduced to 50-60%) Some investigations with respect to this issue would be valuable in PSA modeling

- Relaxation of success criteria for LOCA L4 scenarios, with LPS and CFS only, is likely (capability of CFS train reduced to single HA)

- Scenario HNLN 300 should be investigated for full capability of LPS

- Necessity to supply coolant from HAs and LPS to both lower and upper plenum of the RPV should be investigated for large LOCAs (L6)

- Some analyses would be needed to investigate effect of different break locations LOCAs within the steam generator comprises the separate category that should also be covered

References

[1] "Workshop on Plant Response for WWER-440 NPPs", Trnava, CSFR, 4-5 May 1992, IAEA, TC Project RER/9/005, Consultant Report

[2] M Kulig, W Stępień Rudzka, R Guzik - "LOCA PSA for WWER-440 NPPs", RER/9/005 Final Report, Central Laboratory for Radiological Protection, Warsaw, January 1992

[3] M Kulig, J Szczurek, W Kowalik, Z Bazso - "PSA-Oriented Thermal-Hydraulic Analyses for LOCA Accident in WWER-440 V213 NPP", work under the contract for VUJE, Science and Engineering International Ltd, June 1992

LESSONS LEARNED IN APPLYING PSA METHODS TO TECHNICAL SPECIFICATION OPTIMIZATION

K N FLEMING
PLG, Inc.,
Newport Beach, California

R P MURPHY
Houston Lighting & Power Company,
Wadsworth, Texas

United States of America

Abstract

The paper presents some results of PSA application in the evaluation of Technical Specifications Two plant-specific studies are addressed in relation to Seabrook NPP and South Texas Project plants Technical approach to TS evaluation is highlighted Some insights and lessons learned are presented

1. INTRODUCTION

PLG has been involved in a number of projects in which probabilistic safety assessment (PSA) techniques were used to address Technical Specification issues These projects have addressed a range of applications including proposals to make permanent changes to specifications regarding surveillance testing and allowed outage times for equipment maintenance as well as one-time proposals to gain temporary relief on specific occasions In a few cases, use was made of completed PSA models to support a comprehensive set of revisions to the plant Technical Specifications The object of such plant-level evaluations is to determine the full plant-level risk impacts of proposed changes to conditions under which component testing and maintenance are performed during plant operations In this paper, some of the results and lessons learned from such applications of PSA on the Seabrook and South Texas Project plants in the United States are highlighted

2. SEABROOK STATION

The first full plant level assessment of Technical Specification changes that was performed by PLG was performed for the Seabrook plant (Reference 1) following the completion of a full-scope Level 3 PSA for that plant (Reference 2) In this study proposed changes to allowed outage times and surveillance test intervals were evaluated for several systems including the component cooling, service water emergency feedwater electric power and emergency core cooling systems In addition changes to the amount of time that the containment purge isolation valves are permitted to be open with the plant in operation were also evaluated The proposed changes were evaluated with respect to their impact on system unavailability, average annual core damage frequency, and conditional core damage frequency given selected action statements within limiting conditions of operation (LCO)

Of all of the proposed changes to the Technical Specifications that were evaluated, only the proposed change to the allowed outage time of the diesel generators from 3 days to 7 days was found to have significant impacts to the average annual core damage frequency, and this impact was small The greatest impact of taking equipment out of service for maintenance was observed for the component cooling water system whose conditional frequency of core damage, given that one of its two trains is out of service for maintenance, was found to be about a factor of 25 above the baseline average annual core damage frequency value of 2 7 X 10^{4} per year

One of the most significant results of the Seabrook study was that the relationship between Technical Specification changes and plant-level risk as measured by core damage frequency was established This required two features of the risk model One was the explicit modeling of the impact of allowed outage times (AOT) and surveillance test intervals (STI) on system performance, and the other was the modeling of the impact of system-level changes brought about by AOT and STI changes on the core damage frequency The latter was addressed by using the full plant PSA models that were available from the completed PSA The former was addressed using the modeling approaches described in the next section

The Seabrook study was submitted for review by the U S Nuclear Regulatory Commission (NRC), and a limited number of the proposed Technical Specification changes were accepted However, the utility and NRC resources that were originally assigned to this issue were subsequently diverted to address the emergency planning issues that greatly delayed the licensing of that plant Currently, as part of the Seabrook Station living PSA program, the effort to pursue a risk-based approach to optimizing Technical Specifications at Seabrook Station is being reexamined

3. SOUTH TEXAS PROJECT

The most ambitious project that PLG has supported in the area of risk-based Technical Specification optimization was a major study performed for the South Texas Project PWR Plant in Bay City, Texas, that proposed substantial changes to the AOTs and STIs (Reference 3) of that plant Like the case with Seabrook, the owners of the South Texas plant had made a unilateral decision to perform a PSA as the initiation of a risk management program The PSA was performed by a team from HL&P and PLG, and the transfer of PSA technology to HL&P was given a heavy emphasis The South Texas PSA was completed in 1989 as a full-scope Level 1 PSA with external events and a full treatment of plant damage state bins (Reference 4) This particular PSA scope is sometimes referred to as a Level 1 5 PSA because all active systems needed to support the containment safety functions were included as well as those needed to protect the reactor core

The mean core damage frequency obtained in the PSA was 1 7 X 10^{4} per year, with large contributions to CDF from support systems needed to protect the reactor coolant pump seals and to maintain adequate core cooling A number of significant design and operational features of the plant were changed as a result of the PSA including a change of containment isolation valves in the containment purge system from motor-operated to air-operated valves to reduce the likelihood of containment isolation failure a similar change in the primary coolant letdown isolation system to reduce the likelihood of loss of coolant during a station blackout a new capability to provide reactor coolant pump (RCP) seal injection cooling that is independent of the need for safety-grade electric power, and new procedures and training to reduce the likelihood of critical damage to electrical switchgear following a loss of electrical auxiliary building ventilation

While the PSA was in progress, HL&P notified the NRC that it intended to propose changes to the Technical Specifications based on an evaluation using the models that were developed during the PSA There were a number of motivations for this request that made this a particularly important issue for the South Texas plant These motivations included

- There was no definitive basis for the original Technical Specifications that were generically developed for Westinghouse pressurized water reactor (PWR) plants
- The original generic Technical Specifications were developed for a plant with two redundant trains for safety-related systems South Texas has at least three redundant trains for all safety-related equipment With a few and only rarely occurring exceptions, only one train is needed to provide basic safety functions
- As a three-train plant, the frequency of events requiring maintenance or testing is at least 50% greater at South Texas compared with a two-train plant
- There was a desire to achieve a better balance in the maintenance program between the conflicting goals of reducing the frequency of component failures via preventative maintenance and the undesirable consequences of maintenance unavailability Similarly, there was a desire to obtain a stronger payoff from the heavy investment into plant maintenance
- There was the usual desire to reduce operation and maintenance costs and to reduce the amount of lost electrical generation due to unfavorable interactions between test and maintenance activities and plant operations

NRC agreed to proceed with the review of the requested changes following an in-depth review of the original PSA in which the baseline core damage frequency and the PSA models that would be used in the Technical Specification evaluation could be approved by the NRC as a valid basis for the acceptability of the Technical Specification changes The Technical Specification evaluation was performed by HL&P personnel who provided a real demonstration of the skills in PSA technology that they acquired in the PSA such that only a modest amount of consultant support was needed The NRC review of the original PSA was performed and was supported by its contractors, Sandia National Laboratories, and the results of that review were published in a safety evaluation report (Reference 5) To summarize the results of its review the NRC found the STP PSA to be a state-of-the-art study and accepted the estimated core damage frequency and the PSA models to be a valid basis for completing its review of the Technical Specification study According to current U S law, the NRC review of the PSA and the Technical Specification evaluation, albeit independent, was paid for by the plant owner, HL&P The results of the Technical Specification evaluation that was performed after the PSA are discussed in Section 5

4. TECHNICAL APPROACH TO EVALUATION

4.1 OVERALL APPROACH

The technical approach to evaluation of Technical Specifications in the South Texas study was patterned after the approach pioneered for Seabrook and included the basic elements listed in Figure 1 Following the formation of proposed changes to AOTs and STIs with input from the operations and maintenance departments, the impacts of these changes were evaluated in two stages to determine the impact of the changes on core damage frequency This two stage process was natural because of the particular PSA methodology that was employed in the original PSA, which features the use of large linked and modularized event trees In this approach, the event trees are quantified numerically with input provided by the results of system fault tree analyses separately performed Rather than using a single event tree, a set of modularized and linked event trees was used, as illustrated in Figure 2 In the current form of the models, the entire risk modeling effort is performed within the PC-based risk analysis and risk management software system known as RISKMAN® (References 6 and 7)

To understand the way in which changes in AOTs and STIs were evaluated within the RISKMAN technology, it is useful to review the basic steps employed in this methodology for event sequence quantification

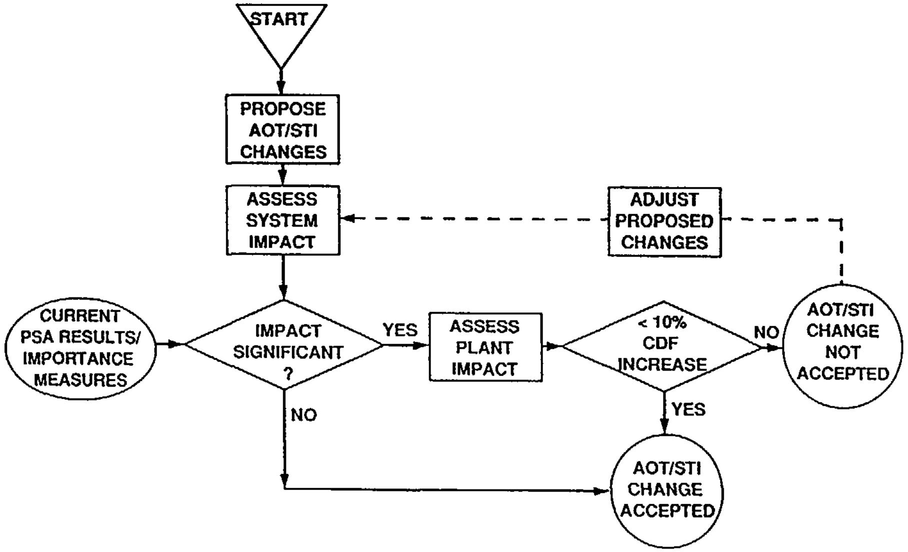


Figure 1. Two-Stage Process for Evaluating AOT and STI Changes

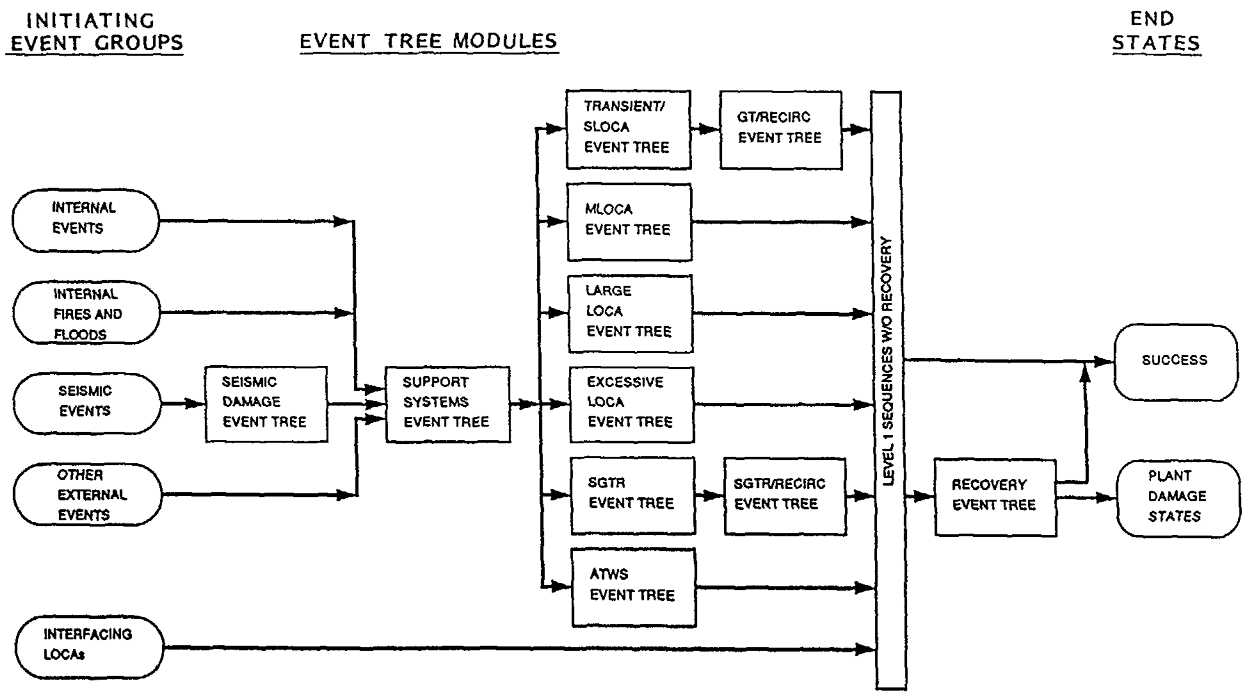


Figure 2. Modularized Event Tree Structure for South Texas Level 1 PSA

1 Event sequences are constructed via computer software and logic rules that transform the set of event tree modules into a set of large event trees that trace sequence progression from initiating events to sequence end states including successful termination and plant damage states

2 Event sequences are quantified in terms of initiating event frequencies and branching frequencies for each event tree node These event tree branching ratios are referred to as *split fractions* The numerical values of those split fractions associated with system performance are developed from the results of systems analysis models that include explicit treatment of initial system alignments, fault tree minimal cutsets, common cause failure models, and simple probability models that relate the fault tree basic event probabilities to parameters whose values are estimated from data

3 Each split fraction related to system performance along an accident sequence is expanded to consider any number of initial system alignments according to the following equation

$$F(SF_i) = \sum_{1}^{N} F(A_j)\text{*}F(SF_i|A_j)$$

where

$F(A_j)$ = fraction of time that the system is in alignment A_j

$F(SF_i|A_j)$ = conditional *frequency of split fraction* SF_i, given that the system is in alignment A_j

N = total number of different alignments

Equation (1) is exact as long as the set of alignments considered is both mutually exclusive and complete The approach to implementing the alignment concept in the RISKMAN software is to first develop a *fault tree* for the "normal alignment" in which no *test or maintenance is in progress* Then, the models for the separate alignments are developed as special cases of the *fault tree*, and each one is analyzed separately through Boolean reduction and quantification The separate models are integrated automatically by RISKMAN which applies Equation (1) to construct the *split fraction* model from the individual alignment models

This equation is extremely important in modeling of the impact of Technical Specification changes on risk for the following reasons Separate system alignments are normally specified for testing and maintenance Using this approach, basic events associated with unavailability for test or maintenance are removed from the fault tree and used to quantify the terms F(Aj) As a result, dependencies created by the Technical Specifications that prohibit maintenance of one train of equipment while a redundant counterpart train is also being maintained can be handled without the problem of introducing "complement events" or NOT gates into the fault trees There are no valid fault tree solution schemes that can properly handle such fault trees Any alignment that could result from a combination of possible concurrent maintenance or test activities is simply treated by enumerating the proper set of alignments

4 *The impacts of each alignment on the performance of the system are modeled by* applying a "house" event to the fault tree to model the resulting functional unavailabilities introduced by the alignment conditions Separate Boolean reductions must be made of the fault tree for each alignment Common cause events are applied to the system fault tree prior to Boolean reduction to take care of the concerns flagged in the common cause analysis procedures guide in Reference 8 regarding the impacts that common cause events have on the determination of minimal cutsets

5 The initial alignment probabilities F(A) and the fault tree basic event probabilities are quantified using probability models that are derived in terms of parameters that are quantified from available data These probability models account for the following causes of degradations to system performance

- Initial unavailability due to being removed from service for testing or maintenance
- Misalignment due to human errors following test or maintenance
- Independent or common cause failures to start on demand
- Independent or common cause failures to continue operation during the system mission

6 Bayesian updating is employed to synthesize data from other plants and other sources of data to produce generic uncertainty distributions for model parameters such as failure rates maintenance frequencies and durations, and common cause failures parameters Bayesian updating is also used to incorporate plant specific data from the plant being evaluated using the generic distribution as priors

4 2 MODELING ALLOWED OUTAGE TIMES

As with many issues that are modeled in a PSA the treatment of AOTs uses the principle of using models that make the most effective use of the available data In the treatment of AOTs at Seabrook and South Texas use was made of the PSA database at PLG that includes the plant specific databases that have been developed in 22 plants in the U S and in Europe that had accumulated at least 5 years of experience (Reference 9) This database includes sufficient experience to be able to estimate reasonably well the relationship between AOTs and maintenance unavailability

With reference to Equation (1), each unavailability of equipment in a system due to maintenance is modeled by defining an appropriate set of maintenance alignments, one for each unique system configuration created during the maintenance of equipment For example, suppose the one such alignment is defined for maintenance of a pump train within a system

Let A_j = alignment for pump maintenance

$F(A\ ) = F\ ?\ T \leftarrow F_{mp} \cdot T_{mp}$

where F_{mp} = frequency of pump maintenance (per hour)

T_{mp} = duration of pump maintenance (hours) while the plant is operating at full-power for a full power PSA, or while the plant is in an alternate mode for an alternate mode PSA

The maintenance frequency can include contributions from both preventive or corrective maintenance, or, alternatively, separate alignments may be specified for each if the separate maintenance frequencies are known Note that neither the total maintenance frequency nor the corrective maintenance frequency should be confused with the failure rate because there are many examples of corrective maintenance being performed when actual failures have not occurred Please also note that maintenance duration is the total time that the component is *out of service for maintenance and not equivalent to the so called mean time to repair* which may be a small fraction of the actual out of service time

Upon careful review of actual plant data from the above mentioned 22 plants 2 observations have been made that have guided our approach to modeling the impact of AOTs on system performance One observation is that the database includes many generic components that are subjected to widely varying AOTs in their respective plants Thus, we can actually measure the impact of the AOTs The second is that the principal way in which the AOT comes into play is to determine the possible range of maintenance durations By sorting the generic database on maintenance durations by AOT at the respective plants, a clear correlation is observed, as illustrated quite graphically in Figure 3 for pumps

As can be seen in Figure 3, which presents the values of the maintenance duration in the form of an uncertainty distribution that accounts for data sparsity and plant-to-plant variability, the duration of maintenance distributions is bounded at levels that are slightly higher than the AOT values This figure is derived from operating plant data none of which were ever in violation of the given Technical Specifications or exceeded their limits The upper tails of the distributions that lie in the regions outside the limiting conditions are an artifact of using a lognormal model for the prior These upper bounds however are not completely erroneous but reflect the fact that the respective Technical Specifications normally provide a few hours after the AOT has expired to affect the appropriate shutdown procedure These results reflect not only the impact of the AOT in constraining the operation of the plant when an action statement is entered but also the fact that the level of AOT will influence the priority given to when the actual repair activity will begin

In the case of the South Texas Project study the generic maintenance frequency and duration distributions were adjusted to reflect the preventive maintenance program of that plant as well as its equipment tag out procedures which set a lower bound on the durations to permit administrative processing of the tag out

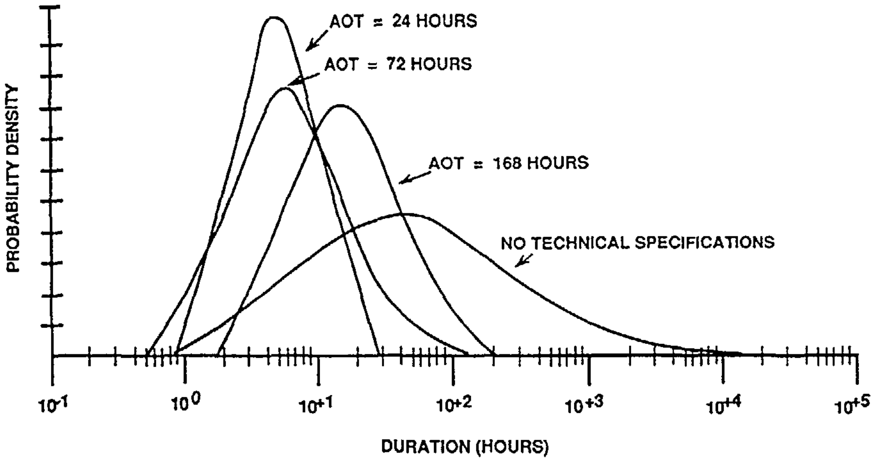


Figure 3. Impact of Allowed Outage Time on Maintenance Duration of Pumps

4.3 MODELING SURVEILLANCE TEST INTERVALS

As with the AOTs, the approach to modeling the STIs is rooted in a firm understanding of the characteristics of the underlying PSA database From elementary reliability modeling, it is well known that periodic testing of standby equipment helps to reduce the probability that the equipment would be unavailable at some random point in time when a demand for operation occurs due to some latent condition from a failure in standby that occurred and remained undetected since the last test In addition to these standby failures, standby components can also be subject to failures that occur at the time of demand due to the stress of bringing the component into service from the standby state This is especially important for mechanical components such as diesel generators

Unfortunately, in putting together the current PSA database, the data for standby components are only segregated to the extent that failures to operate on demand are distinguished from failures that occur during operation The demand failures had not been broken down into separate contributions from undetected standby failures and stress-related failures

Moreover, even if the need to address this issue had been foreseen when the data were originally collected, in most cases, plant records were inadequate to be able to distinguish the two failure types for particular component types

To treat the question of STI changes the failure rates for standby equipment for failure to operate on demand are decomposed according to the following simple formula

$$Q_{NEW} \quad - \quad \underbrace{(1 \;\; f_s)\, Q_d}_{\text{Shock Induced Failures}} \quad + \quad \underbrace{f_s \left(\frac{T_{NEW}}{T_{ref}} \right) Q_d}_{\text{Standby Failures}}$$

Q_d = failure rate per demand from data

f_s = fraction of demand failures that occur in standby

T_{ref} = effective or average STI for demand failures in database

T_{NEW} = proposed new STI for Technical Specification changes

Then, special studies were performed to estimate the values of the factor f_s for generic component types For example, the mean value of f_s for standby diesel generators was estimated to be about 57, i e , 57% of the failures on demand were estimated to be truly standby failures, and the remaining 43% were determined to be stress induced

Equation (2) permits the prediction of changes to the effective standby failure rate due to changes in the test interval that only impact the true standby failure contribution There is an important implication of the stress-induced failures that sheds light on the dubious wisdom of another frequently encountered facet of the Technical Specifications Plants such as Seabrook and South Texas have a Technical Specification requirement to perform confirmatory tests on components in a system when a redundant component is taken out of service and a corresponding action statement is entered To the extent that the parameter f_s is less than 1 0, such testing would increase the likelihood of multiple component unavailabilities from the test itself It was found in the Seabrook study that by replacing such a confirmatory test for the diesel generators with an alternative requirement for a visual inspection to ensure proper lineup of the redundant diesel generator that a net reduction in core damage frequency would result

A final implication of the stress-induced component to the demand failure rate is that, unless the value of f_s is known, it is not possible to know the optimum testing frequency There is introduced a tradeoff that occurs when testing frequency is increased in that the reduction in the unavailability due to undetected standby failures is offset by the increase in the likelihood of a failure caused by the test itself

5. RESULTS OF SOUTH TEXAS EVALUATION

The Technical Specification evaluation of Reference 3 is currently being reviewed by the NRC In this evaluation, Technical Specifications covering AOTs and STIs in 22 different systems are proposed For 5 of these systems, changes were proposed for both the AOTs and STIs, for 4 systems, only the STI was changed, and, for the remaining 13 systems only the AOT was proposed for a change Although the evaluation showed that most proposed changes have little or no impact on either system performance or core damage frequency the proposed changes that were found to have the relatively greatest impact are summarized in Table 1 As can be seen in this table in many cases the AOT of 3 days was evaluated for extension to 10 days and in a few cases, monthly or bimonthly testing was evaluated for extension to quarterly testing In general, changes were only proposed when considered to be beneficial from an operations or maintenance point of view

The 22 changes that were proposed for consideration by the NRC were evaluated both individually and in combinations, including the combination where all 22 changes are accepted The results of the evaluation for the changes listed in Table 1, analyzed individually, and the collective results for all 22 changes are illustrated in Figure 4 The remaining 12 changes that were evaluated were found to have essentially no impact on either system-level or plant-level performance The individual results are not additive because individual sequences contributing to core damage frequency may contain split fractions from any number of different systems The results in terms of core damage frequency for individual systems ranged from essentially no increase to less than 30% increase, with the combined effect of all 22 changes found to have about 70% increase in core damage frequency At the system level, the changes are seen to be amplified because no single system really dominates core damage frequency

Based on preliminary discussions with the NRC, there has been an indication that core damage frequency impacts of more than 10% for individual changes may not be accepted, and, conversely, that changes less than this value are acceptably low There were three systems whose changes were found to individually increase the CDF by more than the suggested 10% criterion auxiliary feedwater, essential raw cooling (service) water, and emergency diesel generators

Table 1 Technical Specification Changes with Greatest Risk Impact

System	Allowed Outage, Time	Surveillance Test Interval (Days)
Reactor Protection	No Change	62 → 92
Accumulators	1 Hour → 6 Hours	No Change
ECCS	3 Days → 10 Days	No Change
Auxiliary Feedwater	3 Days → 10 Days	31 → 92
Component Cooling Water	3 Days → 10 Days	No Change
Essential Cooling Water	3 Days → 10 Days	No Change
Control Room HVAC	First Train 7 Days → 10 Days Second Train 1 Day → 3 Days	31 → 92
Essential Chilled Water	3 Days → 10 Days	No Change
Diesel Generators	First Train 3 Days → 10 Days Second Train 2 Hours → 12 Hours	No Change
DC Power Batteries Channel I IV Chargers Channel II IV Chargers	 2 Hours → 24 Hours 24 Hours → 72 Hours 2 Hours → 72 Hours	 No Change

Recently, HL&P and PLG performed an update of the PSA as it was extended to Level 2 for the purpose of meeting the individual plant examination requirements that have been imposed for U S plants The Level 1 portion of the PSA was updated to match up the models with recent upgrades to the RISKMAN software and to incorporate system changes, plant-specific operating experience, and PSA modeling refinements As a result of these changes and the mutual desire to keep the proposed changes within the unofficial 10% criterion, the NRC and HL&P are currently evaluating the implications on the Technical Specification evaluation Thus, it is not unlikely that there may be a revision to the actual Technical Specification changes that will be proposed and accepted To support this effort, NRC and its contractors at Brookhaven National Laboratories are planning to perform independent analyses using the PSA models developed by HL&P and the RISKMAN software developed by PLG

6. INSIGHTS AND LESSONS LEARNED

The applied PSA studies for Seabrook and South Texas Project have provided a number of important insights and lessons learned regarding the use of PSA techniques to address the impact of changes to the plant Technical Specifications These insights and lessons learned include

- The importance of modeling the maintenance unavailability in sufficient detail so that the effects of varying maintenance durations can be addressed
- The need to distinguish between the mean time to repair and the actual duration of a maintenance outage
- The need to identify the impact of Technical Specifications on the observed generic data for maintenance duration
- The important need to distinguish between standby failures and failures induced by the shock of putting a standby component into service and the implications that this has on conclusions regarding the optimum testing interval and confirmatory testing
- The need to be able to view the relationship between Technical Specifications and plant level risk and the misleading conclusions that can be reached from system level evaluations
- The importance of a full scenario perspective on the risk significance of a change in Technical Specifications and the fact that a given change may increase the risk of one class of sequences while decreasing the risk of others
- The use and interpretation of risk importance measures to guide decisions regarding testing and maintenance

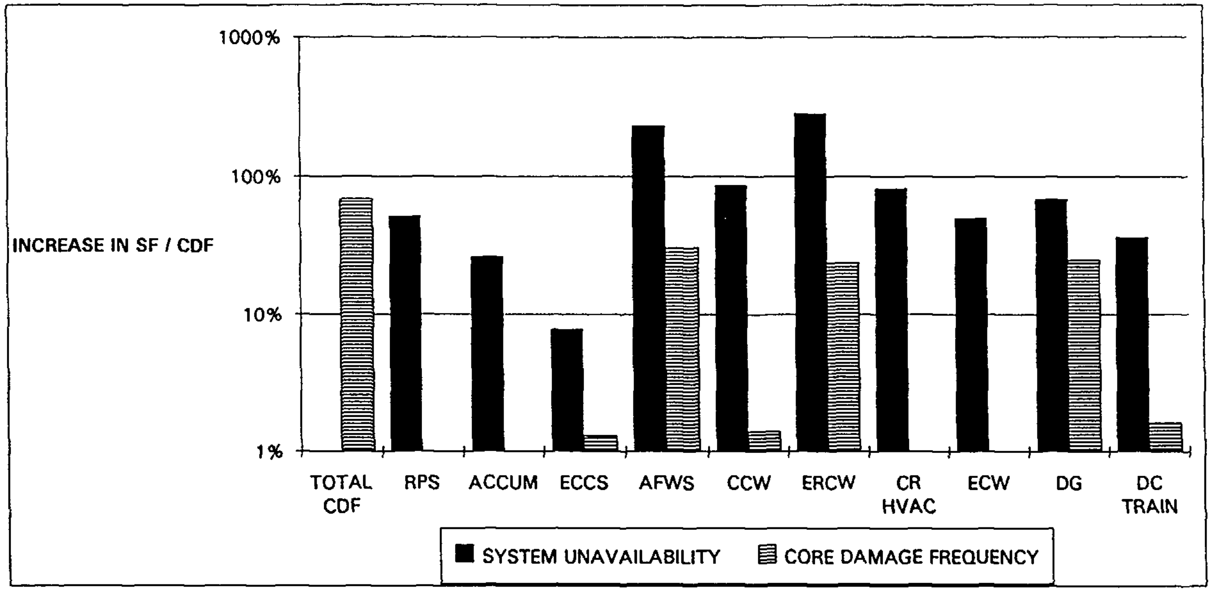


Figure 4. Comparison of System and Plant Level Impacts of Technical Specification Changes at STP

REFERENCES

1 Fleming, K N et al , "Risk-Based Evaluation of Technical Specifications for Seabrook Station," prepared for New Hampshire Yankee by Pickard, Lowe and Garrick, Inc , PLG 0431, August 1985

2 Pickard, Lowe and Garrick, Inc , "Seabrook Station Probabilistic Safety Assessment," prepared for Public Service Company of New Hampshire, PLG-0300, December 1983

3 Houston Lighting & Power Company, "Proposed Amendment to the Unit 1 and Unit 2 Technical Specifications Based on Probabilistic Risk Analyses—South Texas Project Electric Generating Station, Docket Nos STN 50-498 and STN 50-499," Letter from G E Vaughn to USNRC, ST-HL-AE-3283, February 1, 1990

4 Pickard, Lowe and Garrick, Inc , "South Texas Project Probabilistic Safety Assessment," prepared for Houston Lighting & Power Company, PLG-0675, May 1989

5 Dick, G F , U S Nuclear Regulatory Commission letter to D P Hall, Houston Lighting & Power Company, "Safety Evaluation by the Office of Nuclear Regulation Related to the Probabilistic Safety Analysis Evaluation, South Texas Project, Units I and E," (Docket Nos 50-498 and 40 499), January 21, 1992

6 PLG, Inc , "RISKMAN—PRA Workstation Software," User Manuals I-IV, Version 3 0 (Proprietary), 1992

7 Epstein, S A , RISKMAN® A System for PSA," presented at Third Workshop on Living PSA Applications, Hamburg, Federal Republic of Germany, May 11 and 12, 1992

8 Mosleh, A , et al , "Procedures for Treating Common Cause Failures in Safety and Reliability Studies," Pickard, Lowe and Garrick, Inc , prepared for U S Nuclear Regulatory Commission and Electric Power Research Institute, NUREG/CR-4780, EPRI NP-5613, PLG-0547, Vols 1 and 2, January 1988

9 PLG, Inc Database for Probabilistic Risk Assessment of Light Water Nuclear Power Plants," PLG 0500 (Proprietary) Volumes 1-9, 1991

TEST STRATEGIES FOR STANDBY DIESEL GENERATORS*

T MANKAMO
Avaplan Oy,
Espoo, Finland

Abstract

Diesel generators (DG) have been selected as the object for a pilot study, with the aim to address plant specific defensive measures against CCFs, and to generate representative CCF data which take into account such defences . As a part of this venture, the surveillance test arrangements were considered with special emphasis on the detection and removal of latent CCF mechanisms.

A comprehensive data base for the DGs of the Swedish plants and TVO I/II plant was collected and analysed in regard to the CCF mechanisms. 418 DG years were covered, including 49 monitored critical (shortly revealed), and 83 latent critical faults detected at startup from standby and 40 during DG operation. This data base was further supplemented with a closer interpretation of failure mode, and detectability by different test methods. The information provided a good basis in order to draw conclusions about the efficiency of different test types, and to evaluate test interval influence and to compare alternative test strategies for a group of redundant DGs.

1 INTRODUCTION

These considerations for test strategies constitute a part of the joint effort, conducted by ABB Atom AB and Avaplan Oy, within the research program of the Swedish Nuclear Power Inspectorate (SKI), with the aim to address plant-specific defensive measures against CCFs and to generate representative CCF data which properly take into account such defences [RPC 89-60].

Diesel generators have been selected as the object for the pilot study. A comprehensive data base for the diesel generators of the Swedish plants and TVO I/II plant, covering the years 1980-89, was collected and analysed in regard to CCF mechanisms [RPC 91-76] This data base was further supplemented with a closer interpretation of the failure mode and detectability by different test methods [NDGDB_LC] This information base covers 418 DG years and includes 172 critical failures of mode

49 monitored critical (shortly revealed)

83 latent critical faults detected at startup from standby

40 critical failures during DG operation,

providing useful input to investigate the test efficiency, with special emphasis on an early capture of CCF mechanisms The test interval and test scheme, i.e. relative placing of tests in redundant subsystems, varies among the plants, which gives a good possibility to investigate their influence as well.

This work builds upon the earlier related work, specially the earlier DG studies [FS_DG82, F12_DGS], as well as on the more general developments for test arrangement considerations [NKA/RAS-450].

The main results and new insights from the test strategy considerations will be summarised in this paper. A more complete technical documentation can be obtained from the SKI [NDGDB_LC, DG_TestS].

2 FAILURE MODES OF A STANDBY DIESEL GENERATOR

For a standby safety component like a DG, the failure modes which are relevant for the operability of the component when called upon from the standby state, divide up into two main categories

- so called monitored faults, which are promptly or shortly revealed, although being in standby state, by instrumentation, alarms or frequent walk-arounds
- latent faults, or more generally hidden faults, revealed only at a demand and required mission period, or by an effective test

A proper distinction shall be done between these categories due to the principally different unavailability contributions, as already discussed in more detail in Ref.[TI_Opt88]. It should be noted, that the monitored critical failures contribute only during the repair downtime, while the latent/hidden critical failures have a more extensive contribution through the standby unavailability

The latent/hidden faults shall still be divided up in regard to whether they are revealed at start or during mission period Failures affecting a DG after a long load running period may have own characteristics· they may be correlated only to cumulative running time but not to time being in standby state or test properties. In this context this kind of further classification is not implemented, because mean load operation time is only about one hour per pest. The failure modes detected at startup and during test running time, are classified separately in the data analysis, but lumped together in unavailability modelling

Faults can be either critical in regard to safety function, or so called noncritical faults, which do not directly imply

* Work performed under the auspices of the Swedish Nuclear Power Inspectorate (SKI) The views expressed are those by the author and do not reflect any position or policy of the SKI

unavailability, but need to be repaired in order to prevent their escalation into critical state, and impose unavailability during the active repair time.

A definition scheme of failure modes, following the above principles, is presented in Table 1, specifically applicable to DGs. Table 1 also shows the number of events for the failure modes according to the updated DG data base

3 TEST TYPES, DETECTION OF FAILURES

The detection methods of failure mechanisms can be structured in the way presented in Table 2. These detection methods are arranged according to the expected efficiency in the detection of latent faults. They are specific to DG, but still reflect the difference in test/demand efficiency for standby equipment in general. The content of the different test/demand types are discussed in more detail in Refs.[F12_DGS, DG_TestS]

For diesel generators, the continuously monitored parameters include start air pressure, lube oil and cooling water level/temperature/pressure, and base state of various components. The monitored variables or properties sum up to about one hundred per DG aggregate. About half of these are monitored continuously or at frequent time points during the standby time, while the other half are relevant for the startup and loading phases. As a net effect, a relatively large part of faults fall into the category of monitored ones, Table 1. This reduces the standby unavailability.

4 TEST SCHEMES, CCF DETECTABILITY

The detection of a latent CCF depends on the test method but also on the relative placement of test times in the redundant DGs.

4.1 Basic test schemes

The periodic tests ST/LT are performed with intervals varying from one to four weeks per DG aggregate. Different type of schemes are used to place these tests in redundant aggregates Selected standard schemes are illustrated in Fig.1, for the case of four redundant DGs, and preserving the frequency of LTs as once per four weeks per DG aggregate, while varying the frequency of STs as well as the relative placement of ST/LTs There are included

- two sequential schemes SEQ1 and SEQ2, with ST/LT interval of 1 and 2 weeks, respectively
- pairwise staggered scheme PST2, where ST and LT are performed alternately
- evenly staggered scheme EST4, including mere LTs

These schemes were considered as alternatives in the earlier test arrangement study [F12_DGS], and their comparison will be discussed in Section 6, based on updated data

Table 1 Definition of functional failure modes for a standby diesel generator Division of the experienced faults for failure modes, Swedish NPPs and TVO I/II, 1980-89 [NDGDB_LC].

	FUNCTIONAL CONSEQUENCE			
Component state at fault occurrence/detection	NONCRITICAL Prevents operation only during active repair		CRITICAL Component inoperable directly	
MONITORED IN STANDBY Detected via instrumentation, walkarounds, etc	MN Monitored noncritical 67	51%	MC Monitored critical 49	28%
LATENT IN STANDBY Detected at startup from standby or at initial loading	LN Latent noncritical 59	45%	LC Latent critical 83	48%
FAILURE DURING OPERATION Fault occurs after startup	FN Fault during operation, noncritical 6	5%	FC Failure to run, critical 40	23%
HIDDEN IN STANDBY Hx = Lx + Fx	HN Fault at startup or during running period 65	49%	HC Failure to start/run, critical 123	72%
Number of events altogether Ax = Mx + Hx = Mx + Lx + Fx	132	100%	172	100%

Relative contribution

Number of events

Table 2 Detection methods of faults in a standby DG, arranged in the general order of efficiency [DG_TestS].

MO	Monitoring measures	Detection by instrumentation, alarms, visual inspections at walk-arounds etc
PM	Preventive maintenance	Includes post-maintenance tests prior to reconnection
ST	Start test	Starting and running over about half an hour without load
LT	Load test	In addition to start test, the generator is phased with and loaded to power bus, with load running over 1-2 hours. Also more detailed controls and checks are carried out as compared to a start test.
AT	Annual subsystem test	The loss of voltage is simulated in one bus at a time.
DE	Demand event	The loss of voltage occurs at a random time point, and loading is controlled by automation. Also isolation transients, where DGs are automatically started but not necessarily loaded are included in this category.

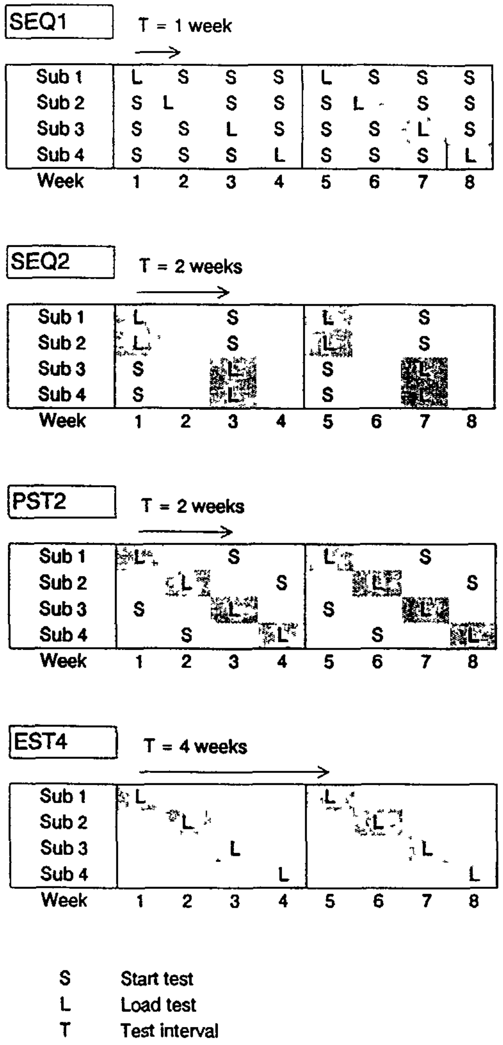
The current schemes at the Swedish plants and TVO I/II plant closely follow the basic schemes in Fig.1. At some plants, all periodic test include loading, i.e. no mere STs are performed. Main part of periodic tests utilise so called soft starting, where fuel injection is reduced in the first beginning resulting on a slower, and less stressing startup of the engine. In part of the tests, cold rush starts are performed.

4.2 CCF detection

The sequential scheme is clear with regard to CCF detection as the redundant aggregates are tested consecutively by the same persons (mostly).

In pairwise and evenly staggered test schemes, the CCF detection depends further on whether in case of fault detection, additional tests are done for the other redundant aggregates:

- if no additional tests are done, the multiple unavailability situation may be revealed only afterwards; nevertheless, it is beneficial that part of the faults are repaired due to the first detection, because after the completed repair, the unavailability of the repaired aggregates is independent from the possible remaining CCF in the other aggregates



SEQ1 T = 1 week

Sub 1	L	S	S	S	L	S	S	S
Sub 2	S	L	S	S	S	L	S	S
Sub 3	S	S	L	S	S	S	L	S
Sub 4	S	S	S	L	S	S	S	L
Week	1	2	3	4	5	6	7	8

SEQ2 T = 2 weeks

Sub 1	L		S		L		S	
Sub 2	L		S		L		S	
Sub 3	S		L		S		L	
Sub 4	S		L		S		L	
Week	1	2	3	4	5	6	7	8

PST2 T = 2 weeks

Sub 1	L		S		L		S	
Sub 2		L		S		L		S
Sub 3	S		L		S		L	
Sub 4		S		L		S		L
Week	1	2	3	4	5	6	7	8

EST4 T = 4 weeks

Sub 1	L				L			
Sub 2		L				L		
Sub 3			L				L	
Sub 4				L				L
Week	1	2	3	4	5	6	7	8

S	Start test
L	Load test
T	Test interval

Figure 1. Basic test schemes for a group of four DGs.

- if additional tests are done in staggered scheme in fault detection situation, this scheme as a whole becomes most efficient with regard to high order CCF detection, because there are shorter intervals of detection possibilities as compared to sequential scheme (with equal test interval per subsystem, compare with Fig.1).

There are additional influences of the test scheme. In staggered scheme, the risk of systematic errors introduced in test, and test related maintenance actions may be significantly lower as compared to sequential scheme, where the actions are consecutively done by the same persons on the same day. In the opposite direction, in staggered scheme, it is more difficult to get an alert from early symptoms of developing CCF in redundant aggregates, specially if the consecutive test actions in the redundant subsystem are done by different shifts (as usual).

5 COMPONENT UNAVAILABILITY AND CCF MODEL

This chapter shortly summarises main concepts of the unavailability and CCF model for a standby component. The more detailed presentation can be found in Ref.[TI_Opt88].

5.1 Simple $q+\lambda t$ model

The main characteristics of the latent failures of a standby component is that their presence is not known during the standby state. They are described by a probability, called instantaneous unavailability. The following simple model is usually applied:

$$u(t) = q + \lambda\,(t - t_{LastTest}) \qquad (5\ 1)$$

where

q = Timeindependent part of the unavailability

λ = Standby failure rate (timedependent part)

$t_{LastTest}$ = Last test/demand time point

The timeindependent part constitutes of failures introduced in tests and remaining unnoticed up to next test or demand, and failure mechanisms progressing merely in test/demand operations but being "frozen" during standby time. The timedependent part describes generally failure mechanisms progressing during standby state

Part of the latent faults may not be detected in normal component tests, but only in annual system tests or actual demands The $q+\lambda t$ model can be extended to these cases by modelling the failure mechanisms distinctly by different test/demand schemes and specific unavailability parts This will be done for DGs in regard to faults detectable in ST, LT and AT/DE, respectively, will be discussed in the following sections

4.2 Modelling approach to CCF mechanisms

The CCF mechanisms can in the first approximation, be described in a similar fashion as component failure mechanisms above: the CCF basic events affecting different combinations of redundant components are modelled by a simple linear model constituting of timeindependent and timedependent part as in Eq (4.1) The point of last test/demand is associated to the time point where some of the components in a given combination have been tested or demanded last time (i.e. the last possibility to reveal a common fault) The modelling of CCF mechanisms, and their interference with tests are of central importance for the consideration of test schemes for redundant components. A more detailed treatment of this area is presented in Ref.[TDep_CCF].

6 RESULTS ON TEST EFFICIENCY, TEST INTERVAL INFLUENCE

6.1 Relative contribution of failure modes

The number of events (NE) when classified according to the fault detectability are summarised in Table 3, and the fractional contributions illustrated in Fig.2. In addition, there are shown the corresponding contributions in the mean unavailability (Un) of a single DG aggregate with 1 week test interval, every 4th test being LT, while other tests during power operation are mere STs.

About the efficiency of the test methods, the results show that the role of mere STs is limited. Although the number on faults revealed only by ATs is small, their unavailability contribution is significant due to the long latent time. Thus, ATs have an important role to complete ST/LTs, which are not 100% efficient.

Table 3 The number of events (NE), classified according to the fault detectability, and the corresponding contributions in the mean unavailability (Un) of a single DG aggregate. Swedish plants and Finnish TVO I/II plant 1980-90.

Failure mode/Detectability		Class	NE		q	f [1/h]	Un		
Latent	AT/DE	HC D	3	1%		8 2E-7	0 0026	20%	td=0 4 a
critical	LT	HC L	37	12%	3 0E-3	4 6E-6	0 0049	38%	T=4 w
	ST	HC S	83	27%	2 3E-3	1 3E-5	0 0043	33%	T=1 w
Monitored critical		MC	49	16%		1 3E-5	0 0003	2%	a=20 h
Noncritical, all modes		AN	132	43%		3 6E 5	0 0009	7%	a=24 h
			304				0 0129		

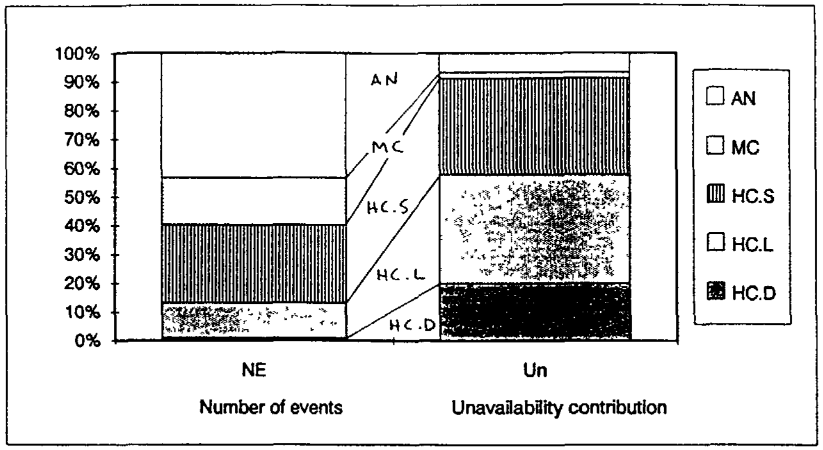


Figure 2 Relative fractional contributions from Table 3.

The contribution of HC.D is nevertheless smaller than what can be inferred from foreign data [CCF_DGRD]. This is presumably related mainly to an enhanced physical and process separation of DGs and their supports systems, as well as of the AC/DC buses for safety systems, at the plants of ABB Atom AB design (valid also for Ringhals 2-4 units, Westinghouse PWRs).

It should be pointed out, that the unavailability estimates presented here lack the downtime contribution of preventive maintenance, which is usually about 1E-2 per DG aggregate, i.e. at the same level as the contribution of random faults/repairs.

6.2 Aggregate part versus failure mode

It was of interest to investigate, where the different failure modes are localised in respect to DG aggregate parts, in order to see, how this information compares with the statistical consideration of test efficiency. The following conclusions can be drawn [DG_TestS]:

- noncritical faults (AN) concentrate on cooling system and fuel oil system, being mostly leakage events
- Monitored critical faults (MC) are quite evenly distributed, being most frequent in engine, cooling system and lube oil system: continuous monitoring is mainly focused in these subsystems
- Latent/hidden critical faults, detectable by starting (HC.S) are dominant for start system and governor, as well as important to engine and fuel oil system: this is natural as these subsystems play major role in startup
- Latent/hidden critical faults, detectable by loading (HC.L) concentrate on exciter/voltage regulator; they are important also to cooling system, being detected only after running some time under load, which is also natural; but the other half of this failure type is quite evenly distributed over other aggregate parts indicating the more challenging nature of LT as compared to ST
- Latent/hidden critical faults, detectable by annual test or actual demand (HC.D) affected start system (1 event) and auto-start equipment (2 events), all being components, which are actually tested only in AT/DE

6.3 Timedependence of latent faults

The reactor units in the data base fall in different categories in respect to ST/LT interval per DG train. The correlation of expected number of latent critical faults per ST/LT, i.e. HC.S and HC.L failure modes respectively, is presented in Fig.4. It shows a clear linear relationship, which means that the latent failure mechanisms are to a part of timedependent type. It is of special importance to notice, that lumping failure modes together produces a distorted correlation, because then for the joined 1 week interval category about 75% periodic tests are STs, but for 2 week interval category the opposite holds, as about 75% tests are there more efficient LTs. (The joined class of failure modes HC.S and HC.L is denoted by postfix "P", standing for periodic test during power cycle.) Generally, the result is compatible with earlier investigations about the relative portions of timeindependent and timedepedent parts of the q + λ.t -model, compare with Section 5.

6.4 General influence of the start/load test interval

The standard consideration of the test interval influence, such as presented in Refs.[TI_Opt88, F12_DGS], is shown in Fig.5. Also with the updated data, the optimum is rather broad, confirming the earlier conclusions, that the test interval can be decided, in the range of 1-4 weeks, by technical/operational factors.

7 RESULTS ON TEST STAGGERING, CCF DEFENCES

The data base included several latent CCF mechanisms giving valuable insight about their development and detectability characteristics. Model comparisons of the alternative test schemes proved, that the staggered scheme is strongly recommendable as compared with sequential. By staggering, the test frequency per DG aggregate can be reduced while still maintaining control over CCF mechanisms. Also other means of breaking the operational symmetry and simultaneous ageing should be used whenever feasible, for example, in preventive maintenance and advance replacement of ageing components.

7.1 Test scheme sensitivity model

The consideration made earlier for Forsmark 1/2 [F12_DGS], for the alternative test schemes shown in Fig.1, were updated according to the new data. The results are shown ın Fig.6.

To this aim, a sensitivıty analysis model was constructed at the core damage frequency level by using the importance measure information from Forsmark 1/2 PSA study. The sensitivity consideration could be confined to the sequences initiated by the loss of external grid (ATE), because the DGs were primarily

Point estimate of parameters

qs_S	2.30E-3	qs_L	2.96E-3	qs_P	7.77E-4
fs_S	1.33E-5 /h	fs_L	4.63E-6 /h	fs_P	2.96E-5 /h

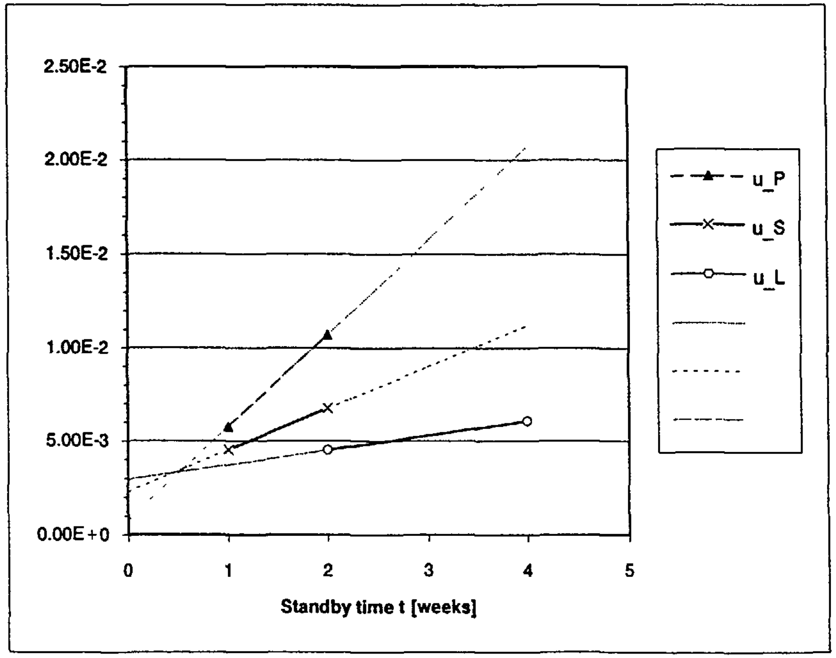
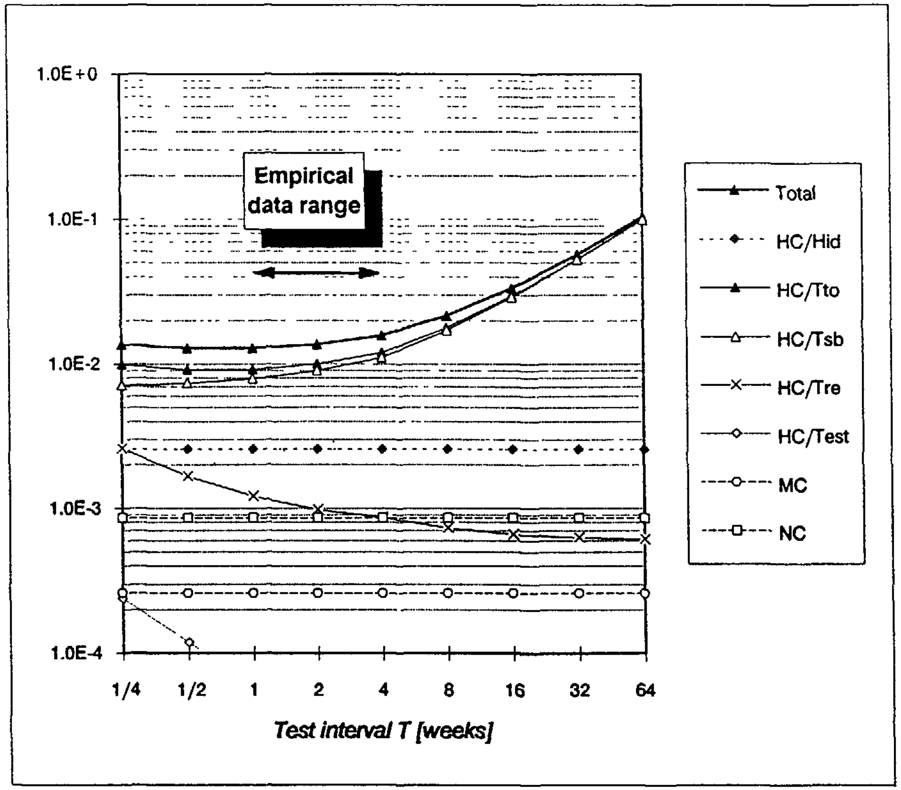


Figure 4 Fıtting tımedependent model to HC.S and HC.L failure modes separately, and as lumped together into class "P".

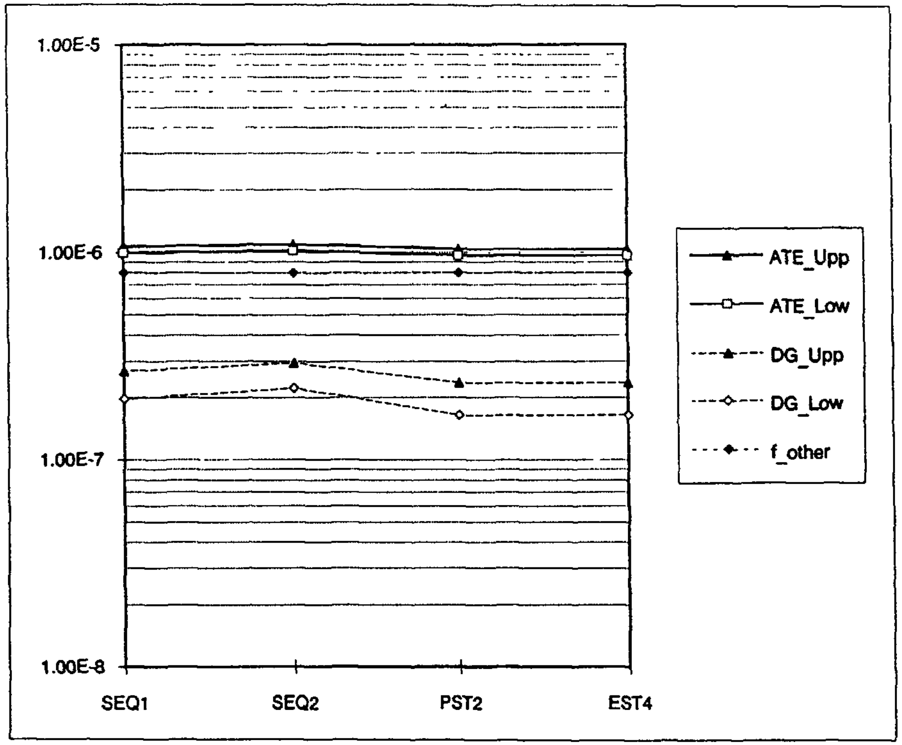


Unavailability contributions

Total	All contributions in total
HC/Hid	Latent and operation critical, detected only in annual test/actual demand
HC/TTo	Latent and operation critical, detected in ST/LT, sum contribution
HC/Tsb	Latent and operation critical, detected in ST/LT, standby period
HC/Tre	Latent and operation critical, detected in ST/LT, repair period
HC/Test	Latent and operation critical, detected in ST/LT, test contribution
MC	Monitored critical, repair period
NC	Noncritical, repair/disconnection period

Figure 5 Influence of the start/load test interval on the mean unavailability of a DG. With overall test interval less than 4 weeks, load test is done once in 4 weeks, other tests are start tests. With longer test ıntervals all tests are load tests.

T_INT	U_TT	f_other	DG_Low	DG_Upp	ATE_Low	ATE_Upp
SEQ1	7.01E-3	7.98E-7	1.97E-7	2.69E-7	9.95E-7	1.07E-6
SEQ2	7.92E-3	7.98E-7	2.22E-7	2.94E-7	1.02E-6	1.09E-6
PST2	5.86E-3	7.98E-7	1.64E-7	2.36E-7	9.62E-7	1.03E-6
EST4	5.86E-3	7.98E-7	1.64E-7	2.36E-7	9.62E-7	1.03E-6



Contributions

ATE_Upp	LoEPS sequences in total	HC/Hid included
ATE_Low	-"-	HC/Hid excluded
DG_Upp	DG failure sequences	HC/Hid included
DG_Low	-"-	HC/Hid excluded
f_other	Sequences not including DG failures	

Figure 6 Influence of the alternative test schemes, as applied to Forsmark 1/2, core damage frequency contribution of loss of external power supply sequences [F12_DGS].

important only for that scenario. The ATE frequency was divided up into two parts

$$f_{ATE} = f_{MCS(DG)} + f_{Other} \qquad (7.1)$$

The DG influences are collected in the first term covering the contribution of just those MCS, which contain multiple DG failures at demand (effectively this term is composed of the mean unavailability of the DG function and its importance measure in regard to ATE end event frequency). This term is shown in Fig.6 by the band DG_Low/Upp. In the upper bound case, the LC.D contribution is based on three, somewhat conservatively interpreted events, as discussed earlier. In the lower bound case all latent faults are assumed to be detected in LT, i.e. LC.D term is effectively neglected. The sensitivity band thus shows the influence of the latent unavailability, which is hidden in normal periodic tests ST/LT.

The influences in ATE frequency is presented by the corresponding sensitivity band ATE_Low/Upp in Fig.6. The influences are masked by the other MCS not containig multiple DG failure at demand. These are collected in term f_Other, and they include failures to disconnect secondary loads from buses at loss of offsite power, and also the contribution of DG failures to run after 30 min from the startup, which is considered independent from ST/LT interval and scheme. (The DG failures during the first 30 min running time are combined with the demand unavailability. Effectively, this means that only the early phase failures of the running time are assumed detectable in the periodic tests ST/LT.)

7.2 Comparing alternative test schemes

The sensitivity study results show that scheme SEQ2 is somewhat disadvantageous in comparison with scheme SEQ1, the base scheme for Forsmark 1/2. This is explained by the increasing contribution of the latent critical faults with the longer ST/LT interval, other factors being same.

The pairwise staggered scheme PST2 is somewhat advantageous compared with the base scheme SEQ1, although the ST interval is increased. Due to staggering, two DGs are still tested every week in scheme PST2. The latent time of CCFs of order 3 and 4, which dominate the DG system unavailability, is at most 1 week as in the base scheme SEQ1. On the other hand, staggering of both ST and LT on different weeks is estimated to decrease the likelihood of systematic errors in test actions and test related maintenance, which as a net effect results in a slightly lower total unavailability for scheme PST2 as compared to the base scheme SEQ1.

The evenly staggered scheme EST4, with only LT preserved, is near to scheme PST2, because the quadruple CCFs are the main contributor, and one DG is still tested every week in scheme EST4. (The maximum latent time of the quadruple CCFs is same in schemes SEQ1, PST2 and EST4, therefore they are so close to each other in regard to the plant level influence.)

The influences are rather small at the plant level, especially if other initiating events than ATE are also considered. Due to the small calculated risk significance, even, when taking into account the identified uncertainties, the final recommendations can primarily be based on technical arguments

The earlier conclusions of Forsmark 1/2 test arrangement study seem to be valid in light of the updated and extended data base The alternative scheme PST2 was then proposed as an optimal resolution. The pairwise staggered scheme was believed to decrease the risk of systematic errors in testing/maintenance actions compared to the base scheme SEQ1, where all DGs are subject to actions by the same persons(s) on the same day. In the proposed scheme PST2, two DGs are still tested every week, which gives a reasonable control over the risk of latent multiple CCFs. There are many other technical factors like soot buildup in ST, oil film dryout during standby time etc., which were deemed to be in proper balance in the proposed scheme [F12_DGS]. Based on the results, the relaxation of STs is currently under trial in one subsystem at the Forsmark plant, in order to verify the technical influences prior to a final implementation for all redundancies.

8 SUMMARIZING CONCLUSIONS

The reliability of DGs were found relatively good, and the frequency of CCF mechanisms rather low. The considerations about test strategies resulted in the following conclusions and suggestions for maintaining the current status, and towards further improvements:

1) Staggered test scheme is strongly recommendable as compared to sequential; by staggering the test frequency per aggregate can be reduced, while still maintaining control over CCF mechanisms.
2) The frequency of the mere start tests without loading could be relaxed, specially in the case of weekly testing.
3) Leading DG rule should be implemented; desirable operation time overhead is in the range of 500 hours.
4) Other means for breaking symmetry and simultaneous ageing should be used whenever feasible (in preventive maintenance, advance replacement of ageing components etc.).
5) Interface of DG aggregates with support systems, electrical buses and auto-start/sequencing equipment should be checked in regard to coverage and efficiency of surveillance tests, and with respect to integral functions.
6) Improvements towards more efficient root cause elimination should be encouraged; specially with staggered test scheme and reduced test frequency, proper emphasis should be paid on the synthesis of test outcomes, evaluation of symptoms and trend followup over the redundant aggregates' status

In conclusion, the thorough analysis of the operating experiences of the diesel generators produced a very useful information base, both in qualitative and quantitative terms

ACKNOWLEDGEMENTS

This study is conducted within the research program of the Swedish Nuclear Power Inspectorate (SKI), subsponsored by the power utilities The author will express the contribution of the reference group for generating ideas and guiding the work, as well as for providing input information from the plants Specially, the contributions by Gunnar Johansson (SKI project coordinator), Staffan Bjore (ABB Atom AB) and Fritiof Schwartz (OKG power company) are acknowledged

References

CCFD_DGP Bjore, S. et.al., Defences against CCFs and generation of CCF data, a pilot study for diesel generators. SKI Technical report, under preparation by ABB Atom AB and Avaplan Oy, Draft 20 March 1992.

DG_TestS Mankamo, T., Test strategies for standby diesel generators. Work report under preparation within SKI/CCF/DG pilot study, Draft 17 February 1992.

RPC 91-76 Qualitative CCF analysis and Cause-Defence matrices, pilot study for diesel generators. Technical report prepared by Lennart Bons, RPC 91-76, ABB Atom AB, October 1991 (in Swedish)

RPC 91-57 Defences against CCFs and generating CCF data, pilot study for DGs, quantitative analysis. Technical report prepared by Staffan Björe, RPC 91-57, ABB Atom AB, October 1991 (in Swedish).

NDGDB_LC DG data base: latent critical faults, Swedish and TVO I/II experience 1980-89. SKI/CCF/DG pilot study, Work report, prepared by T. Mankamo, Avaplan Oy, 5 June 1992.

CCF_DGRD Specific CCF mechanisms of DGs at real demands. SKI/CCF/DG pilot study, Work report, prepared by T. Mankamo, Avaplan Oy, 29 May 1991.

FS_DG82 Pulkkinen, U., Huovinen, T., Mankamo, T., Norros, L. & Vanhala, J., Reliability of diesel generators in the Finnish and Swedish nuclear power plants. Technical Research Centre of Finland, Report SÄH 7/82, June 1982. (Enhanced version published as VTT Research Notes 1070, 1989)

F12_DGS Engqvist, A. & Mankamo, T., Test scheme rearrangement for diesel generators at Forsmark 1/2. PSA 89 Interna-tional Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, April 2-7, 1989.

NKA/RAS-450 Optimization of technical specifications by use of probabilistic methods - a Nordic perspective Final report of the NKA project RAS-450. Ed K Laakso. Prepared by a team consisting of K Laakso, M Knochenhauer, T. Mankamo & K.Porn. Nord Series 1990:33, May 1990

TI_Opt88 Mankamo, T. & Pulkkinen, U , Test interval optimization of standby equipment, Technical Research Centre of Finland, Research notes 892, September 1988

TDep_CCF Mankamo, T , A timedependent model of dependent failures - Application to a pairwise symmetric structure of four components Report manuscript NKS/SIK-1(92)13, 30 March 1992.

200 STEPWISE APPROACH TO RISK-BASED TECHNICAL SPECIFICATIONS

J.A. BECERRA, J.L. DELGADO
Comisión Nacional de Seguridad Nuclear y Salvaguardias,
Mexico City, Mexico

Abstract

A PSA application program is being developed by the mexican regulatory body (CNSNS) and the national utility (CFE) for the Laguna Verde NPP. Several alternatives have been selected for PSA application among them: importance prioritization, assessment of technical specifications, maintenance assessment and prioritization, risk configuration management and reliability focused maintenance.

In this paper a number of specific applications are described by present examples of modifications on Laguna Verde Technical Specifications in allowed outage time (AOT'S) and surveillance test intervals (STI'S).

The risk based allowed outage time and surveillance test intervals have been calculated for most important contributors to core melt frequency and categorized in three risk importance classes. Risk Class 1 contributors are significant risk contributors; Risk Class 2 contributors are moderate to marginal risk contributors and Risk Class 3 contributors are marginal to insignificant risk contributors.

After categorizing contributors by risk classes, several issues on safety and operation are being discussed from probabilistic and deterministic point of view. Among these issues are; probabilistic safety criteria for risk classification; condition for granting extended AOT's; surveillance frequency, wear-out and operational burden; shutdown as an option and risk increase; cumulative risk; and unbalance safety design.

Implementation of risk based surveillance test intervals and allowed outage times are not direct, but a structured program to review and potentially to modify current regulations and Technical Specifications.

I. INTRODUCTION.

For the Laguna Verde Nuclear Power Plant, a Probabilistic Safety Assessment (level 1) was developed and after that the national utility (CFE) and the regulatory body (CNSNS), have been engaged in a PSA application program, as well as a review and update of the Laguna Verde PSA original effort.

At Laguna Verde, probabilistic risk evaluations are being used to develop deterministic criteria for applications to operations and Technical Specifications. The Laguna Verde implementations of risk based evaluations are interesting and are important since they show how Probabilistic Safety Analysis (PSA Results) can be used to obtain workable, deterministic guidelines and deterministic regulations for implementations.

Inside the PSA study it was developed a risk importance prioritization for components, front line systems, and some support systems after the review and update. If is expected to improve the risk importance prioritization.

Importance models used in the PSA were,

Vesely-Fussell Importance ;

$$I^{VF}{}_{I} = (\partial R/\partial P_I)P_I/R$$

Birnbaum Importance ;

$$I^{B} = \partial R\,/\partial P_I$$

Risk Achievement Worth Increment

$$I^{AI} = R^{+} - R.,$$

Risk Reduction Worth Increment

$$I^{RI} = R - R^{-}$$

At present, a Risk-Importance prioritizations for optional activities, is in process in order to optimize resources. For the regulatory body point of view, regulations are expected to be risk-optimized in correlation with the risk importance of the contributors.

A risk-based regulations would redirect resources from the risk unimportant to the risk important contributors, and the resources would be thus, most effectively utilized. Some other benefits would be a total risk reduction by focusing control on the risk important contributors. A burden reduction is expected by relaxing control on the risk unimportant contributors; optimizing resources for test and maintenance activities during operation for the utility point of view and during inspection and enforcement activities.

A risk-based regulation is expected to address the regulatory and utility concerns in an objective manner, identify effective risk reductions and burden reductions, and provide an objective basis for communication and interfacing between the utility and the regulatory body.

Three risk importance classes are defined: Risk Class 1 for risk importance significant contributors, Risk Class 2 for moderate to marginal risk contributors and Risk Class 3 for marginal to insignificant risk contributors.

The risk classes have been defined as a fraction of the Baseline Risk for Laguna Verde, the point value for the core damage frequency is reported as 1.97E-04.

A criteria for determining risk important failures and component going down have been selected; as those components with significant risk impact (risk increase). Significant risk increase RI, it is defined to be 10 times baseline of core damage frequency, for Laguna Verde risk significant or risk critical failures are those which have a risk increase R > 1.0 E-03 / yr.

RISK BASED TECHNICAL SPECIFICATIONS

The Operational Technical Specifications (OTE s) are considered, most of the time, as to restrictive nevertheless, the objective of OTE's is to minimize the total risk during plant operation by setting the lowest functional capability level of equipment required for safe operation of the nuclear power plant, by the Limiting Conditions for Operation, which do not allow the plant to be placed in an unsafe condition

The OTE's control the risk of the plant by assuring that required safety function should be fulfilled by the required safety systems availability, through controlling the timely repair, detection of failures and determination of operability and the action requirements to reduce risk vulnerability

General problems with technical specifications are, the lack of adequate technical bases, difficult to be changed, unnecessary restriction, and there is no credit for risk-effective practices

Engineering judgment and common sense have been used most of the time for implementing changes in allowed outage times (AOT's) and Surveillance Test Intervals (STI'S) and operability requirements

Allowed outage time (AOT'S) and Surveillance Test Intervals (STI'S) are problems in Technical Specifications For AOT'S the risk is not explicitly considered, as a result, inadequate outage times are assigned, and their stringency it is not consistent with their risk importance On Surveillance Test Intervals (STI'S) also, the risk is not explicitly considered and unnecessary surveillance are required, and their stringency it is not consistent with their risk importance

RISK-BASED AOT'S

The allowed outage times (AOTs) are defined at the standard technical specifications for all the safety systems Components may be inoperable because is failed and is under repair, or the component is taken out of service for scheduled testing or maintenance When a component is down, during a AOT, the risk level increases due to loss of function of the component, and the increased risk level depends on the risk importance of the component

At Laguna Verde NPP, as any other plant, extensions to AOT's, are request and are evaluated case-by-case Traditional assessment of AOTs extensions were hard to implement otherwise risk-based AOTs and risk importance prioritization can be used during the optimization process

The down time risk associated with a component outage can be calculated by a probabilistic safety analysis The component is assumed to be down and the new core damage frequency is calculated by using the risk increase (RI) importance The new core melt frequency is then multiplied by the downtime or AOT and the single downtime is determined

AOT RISK METHODOLOGY FOR LAGUNA VERDE

Using the Laguna Verde, level 1, Probabilistic Safety Assessment (PSA), all components related with AOT s in the technical specifications and used in the PSA models are identified

For each component identified is determined the present AOT and converted to units of years, d (YEARS) = TR / 8760, and using the risk increase (RI) , RI = R $^{+}$- R, and the contribution associated with the AOT (ACd) is calculated ACd = d * RI

The risk-based AOTs are calculated by assuming the risk contributor (ACd) as 1% of the base line,

$$\Delta C_d\ ^{*} = 1\ \%\ of\ \ 1\ 0E-04$$

$$\Delta C_d\ ^{*} = 1\ 0E-06$$

$$d\ ^{*}(YEARS) = \frac{1\ 0E-06}{RI}$$

$$d\ ^{*}(hrs) = d\ ^{*}(YEARS) * 8760$$

These process has been carry out for almost 600 components out of a thousand identified in the 300,000 most significant minimal cut sets (94% of the total CMF) for the Laguna Verde PSA

At table 1, a sample of the results can be found, the component in the table have been ranked according to the maximum permissible, risk-based, AOT (HR)

It should be pointed out that critical components are arised for risk increase (RI) values greater than 1 OE-03 and risk contributions associated with the AOT (Cd) greater than 1 OE-06

Three risk importance of downed component are defined fig 1

a) Class 1, are risk significant contributors and focus AOT control is required Suggested options for these components would be, tightened AOT, accident recovery plan, additional test requirement and a reliability program

b) Class 2, contributors are moderate to marginal risk contributors, the AOTs optimization process should aim to increase risk Class 2 and decrease any other Class For Laguna Verde Class 2 contributors are defined between 1 0 E-08 to 1 0E-06, with 271 contributors out of a thousand

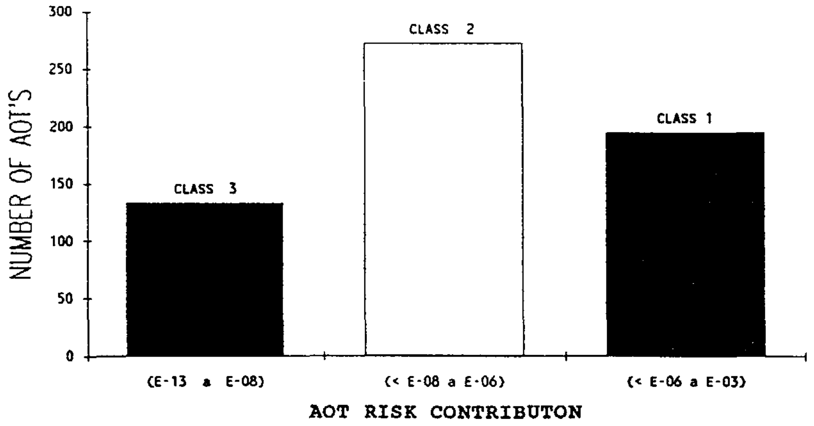


FIG. 1. Risk contributors.

TABLE 1

Component	Description	Unavailability	Downtime length	Risk Increase	AOT Risk Cont	Risk-Based AOT
ACV49AMA	RHR-V Check valv	1.0E-01	4	4.4E-10	2.0E-13	19909091
KXV23-MA	SLC-V Manual valv	3.0E-05	4	2.4E-09	1.1E-12	3650000
DSVA3LOB	S-RV Obstructed valv	1.4E-03	336	2.5E-08	9.6E-10	350400
EBCR2-NF	Battery Charger	4.1E-03	336	3.1E-08	1.2E-09	282581
BXV--5PC	HR-V Failed keep clos	1.3E-05	168	3.2E-07	6.1E-09	27375
IMV100AA	CIC-MV Failed keep ope	3.7E-03	336	1.3E-06	5.0E-08	6738
APV225MA	R-PCV Failed keep op	2.2E-02	8	1.5E-06	1.4E-09	5840
DPVP4BPA	IA-PCV Failed keep ope	5.7E-01	336	1.6E-05	6.1E-07	548
EBU4B1CC	AC-BUS Short Circuit	2.4E-07	8	8.5E-04	7.8E-07	10
BMV202AA	RHR-MV Fail to open	3.3E-03	168	1.1E-03	2.1E-05	8
BCV13BAA	RHR-V Fail to open	2.5E-04	168	1.1E-03	2.1E-05	8
AHX001MI	R Heat Exchanger Main	4.7E-03	168	1.6E-03	3.1E-05	5
BHX001MI	R Heat Exchanger Main	4.7E-03	168	1.7E-03	3.3E-05	5
HMV184MA	HPCS-MV Motovalv open	2.1E-04	4	1.8E-03	8.2E-07	5
HMV177MI	HPCS-MV Motovalv Maint	2.1E-04	4	1.8E-03	8.2E-07	5

c) Class 3 are marginal to insignificant risk contributors. Unneeded Burden can be reduced by loosening AOT control.

Risk-Based AOT Conclusions

Significant risk variations exist for contributor of the same system, present AOTs are not correlated with their risk importance, PSA/PRAs can be easily used to determinerisk-based AOTs, risk -based AOTs control dowtime , and are correlated with risk importance and burden can be minimized.Some risk-based AOTs are dificult to appply because they are uncorrelated with present AOT,as the operational experience; that ids the case of the AOT for the RHR heat exchanger (AHXOO1MI); some other components could be from the Technical Specifications and verified at shutdown like the manual valve, XV23, for the standby liquid control systems.

RISK-BASED STI'S

Surveillance tests are required to detect failures in standby equipments as a mean of assuring their availability and satisfies manufacturer recommendations to prevent degradation. A total Risk assessment associated with the test (R_T) it is the sum of risk contribution that is detected by the test (R_D) and the risk contribution that is caused by the test (R_C). For an effective test $R_D > R_C$ or $R_D / R_C > 1$.

Among the adverse risk impacts caused by the test are: (1) Trips caused by the test; (2) Equipment wear-out.

The risk associated with a surveillance test is caused when the component fails between tests, when the component fails, the component's function is lost until recovered at the next test and the loss of the component function causes a subsequent risk increase.

The surveillance test risk is standardly calculated as a contribution in a PSA/PRA, and the surveillance test risk can be extracted for every test carried out and included in the PSA. To evaluate the risk from different intervals, component failure rates per hour must be used in the PSA. For the Laguna Verde PSA; a failure rate model was implement in the data base.

STI's RISK METHODOLOGY FOR LAGUNA VERDE.

For every test carry out and included in the Laguna Verde PSA line standby periodically tested failure modes, and unavailability for miscalibration.

The risk contribution associated with the test can be calculated by considering; a) risk from test-caused trips, b) risk from test-caused equipment wears, c) risk from test misconfigurations, and d) risk associated with test down time in carrying out the test.

By using the Laguna Verde PSA, all components related with STIs in the technical Specifications and used in the PSA models are identified. The document importance for the component tested is calculated (RI) and the risk contribution associated with the test (C_t) is calculated.

$$RI = R^{+} - R$$

$$\Delta C_t = \frac{\lambda\, T_S\, RI}{2}$$

T_S = actual downtime; Surveillance Test Interval

λ = component failure rate

Finally, the risk-base STI is calculated by assuming 1% of the base line.

$$C_t = 1\%\text{ OF BASE LINE} \quad ; \quad Ct = 1.OE\text{-}06$$

$$T^{*} = \frac{2.0\,E-06}{\lambda\, RI}$$

This process has been carry out for 262 contributors of risk from significant events identified in 300,000 most significant cut sets for de (94% of the total CMF) of Laguna Verde PSA.

In table 2, a sample are shown, and the components in the table have been ranked according to the maximum permissible, risk based, STI.

Three risk importance for document components are also defined;

TABLE 2

Component	Description	Actual Lambda	STI	Risk Based STI		STI Risk
				HR	YEAR	
ACV208A	RHR-AV Fail to open	2.0E-07	4,380	666,666,666,667	7.61E+07	6.6E-15
AXV-3AP	RHR-V Fail keep open	2.0E-07	12,960	666,666,666,667	7.61E+07	1.9E-14
AMV209A	RHR-MV Fail to open	2.6E-06	4,380	48,076,923,077	5.49E+06	9.1E-14
AMV200P	HR-MV Fail keep clos	1.0E-07	2,208	14,285,714,286	1.63E+06	1.5E-13
AMV221A	RHR-MV Fail to open	2.6E-06	2,208	3,496,503,497	3.99E+05	6.3E-13
AMV210A	HR-MV Fail keep clos	2.6E-06	2,208	1,831,501,832	2.09E+05	1.2E-12
HMV187A	HPCS Fail keep close	2.6E-06	2,208	274,725,275	3.14E+04	8.0E-12
AMV255P	HR-MV Fail keep clos	1.0E-07	2,208	208,333,333	2.38E+04	1.1E-11
EBCR2-N	attery Charger Faile	6.0E-07	12,960	107,526,882	1.23E+04	1.2E-10
ARO217N	RHR-ROOrifice Obstrc	1.0E-07	12,960	15,384,615	1.76E+03	8.4E-10
HAS001N	HPCS Sprinkler Failed	1.0E-10	12,960	11,111,111	1.27E+03	1.2E-09
DCV18AA	CIA-V Fail keep close	2.0E-06	350,400	3,571,429	4.08E+02	9.8E-08
IOV100P	RCIC Fail let open	4.6E-04	744	7,199	8.22E-01	1.0E-07
BPV225P	RHR Fail keep close	9.5E-06	12,960	13,158	1.50E+00	9.8E-07
PRV13CN	Valve Neumatic Fail	7.7E-06	1,250	1,237	1.41E-01	1.0E-06
DAV22-P	CIA Fail keep open	1.0E-05	3,754	1,111	1.27E-01	3.4E-06
HMV189A	HPCS Fail to open	2.6E-06	4,380	405	4.62E-02	1.1E-05
ITB001A	RCIC Bomb Failed	2.4E-05	2,208	97	1.11E-02	2.3E-05
KOV--9A	SLC Manual Valve	1.3E-03	744	22	2.47E-03	3.4E-05

a) STI risk Class 1, are high contributors to risk, some alternatives are; focus on Quality Assurance program, review recovery procedures, reliability focused maintenance, and root cause analysis.

b) STIs, risk Class 2 are moderate to marginal contributors and the STIs optimization process should aim to increase risk Class 2 and decrease any other class. At Laguna Verde they are 48% of all STI contributors to risk.

c) STIs, Risk Class 3 are contributors to risk which are candidates to be removed for test and they should be in observation.

RISK-BASED STI CONCLUSIONS

Significant risk variations exist in present STIs for Laguna Verde Technical Specifications. Present STIs are not correlated with their risk importance and it has been shown that a PSA/PRA can be used to determine risk based STIs. Risk-based STIs, control the test risk and are correlated with risk importance, and can minimize burden.

REFERENCES

1. W. E. Vesely, T. C. Davis; evaluations and Utilizations of risk importances, NUREG/CR-4377, U. S. Nuclear Regulatory Commission; 1985.

2. W. E. Vesely; evaluations of allowed outage times (AOTs) from a risk and reliability standpoint, NUREG/CR-5425, U. S. Nuclear Regulatory Commission; 1989.

3. I. S. Kim, S. Martorell, W. E. Vesely, P. K. Samanta; quantitative evaluation of surveillance test instervals including test-caused risk; NUREG/CR-5775, U. S. Nuclear Regulatory Commission; 1992.

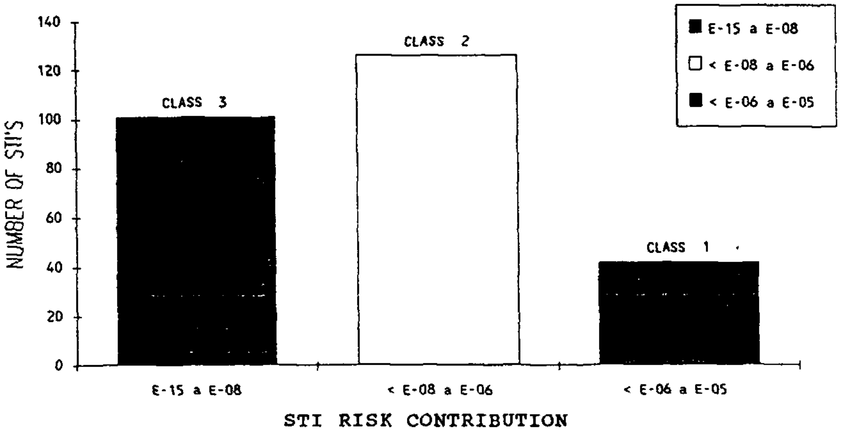


FIG. 2. Present STI risk for Laguna Verde

204 PROBABILISTIC ANALYSIS OF THE INTERACTION BETWEEN ALLOWED OUTAGE TIME AND SURVEILLANCE TEST INTERVAL REQUIREMENTS

S. MARTORELL, V. SERRADELL, G. VERDU
Departamento de Ingeniería Química y Nuclear,
Universidad Politécnica de Valencia,
Valencia, Spain

P. SAMANTA
Risk and Reliability Analysis Group,
Brookhaven National Laboratory,
Upton, New York,
United States of America

Abstract

Technical Specifications (TS) define the limits and conditions for safe plant operation. In Spain they are divided into five categories, and two of them, Limiting Conditions for Operations (LCO) and Surveillance Requirements (SR), have been selected as the main items to be evaluated using probabilistic methods. The LCO will assure that the safety systems are either ready for use on demand. The action statements require the plant to be brought into a safer operational state if faulty equipment cannot be restored within its Allowed Outage Time (AOT). The SR prescribe periodic tests for detection of faults and verification of operability of safety equipment. The time interval between two consecutive tests is called the Surveillance Test Interval (STI).

At this time a significant operating and design experience has been accumulated and a number of problems appeared which require modifications in some TS rules. The goal of the modifications is to further improve the nuclear safety and also to enhance the effectiveness and flexibility of plant operation, maintenance and testing.

Developments in PSA have made possible the evaluation of effects due to AOT and STI modifications from a risk point of view. Thus, some changes have already been adopted in some cases, but AOT or STI modifications have been independently analyzed so far and the acceptance criteria have been based on the constraint that there was no significant reduction in plant safety when the proposed changes were incorporated. The lack of a methodology for evaluating and optimizing the combined effect of several AOT and STI changes, i.e. through their *interaction*, has limited the benefits of the changes and has not allowed to analyze several problems.

This paper presents the main results of the study on AOT and STI interactions which led to one of the authors to conclude his PhD Thesis. The presentation encompass with the following parts:

- definition of AOT and STI interactions and their main reasons,
- quantification of interaction in terms of risk using PSA methods as a tool,
- approach for evaluating simultaneous AOT and STI modifications through their effects on the risk level,
- sensitivity analysis involving the main parameters, and
- assessment of strategies for giving flexibility to the plant operation through simultaneous changes on AOT and STI, using the trade-off based risk criteria.

1. INTRODUCTION.

1.1 Background.

Introduction to Technical Specifications.

Technical Specifications (TS) define the limits and conditions for safe plant operation. Therefore, TS can be seen as a set of operational safety rules and criteria, which defines the allowed operational range for the nuclear power plant from the safety point of view. The ultimate goal of the TS is to prevent radiological accidents in the plant, and thereby to protect the health and safety of the public and plant personnel. These rules were originally formulated with margins on the safe side, mainly on the basis of:

1. deterministic analysis prepared for the FSAR of the plant, and
2. engineering judgement.

In Spain the TS depend on the plant origin, and because the most of them come from the USA, they are divided - the same as in this country - into five categories. The Limiting Conditions for Operations (LCO) and Surveillance Requirements (SR), both given in the TS, have been selected from the beginning as the main two items to be evaluated using probabilistic methods.

The LCO will assure that the safety systems are either ready for use on demand. The action statements require the plant to be brought into a safer operational state if faulty equipment cannot be restored within its Allowed Outage Time (AOT). The SR prescribe periodic tests for detection of faults and verification of operability of safety equipment. The time interval between two consecutive tests is called the Surveillance Test Interval (STI).

Risk and reliability methodology.

Technical Specifications are safety concerned and thereby they are related to systems reliability and plant risk. Both of them can be assessed using the probabilistic methodology, then several topics in TS can be evaluated using this methodology. For instance, it is only needed an approach to model AOT and STI requirements from a risk point of view. In this way AOT and STI modifications can be evaluated in terms of their effect on risk level.

With that sense the Probabilistic Safety Analysis (PSA) models are an important tool to be used for evaluating AOT and STI requirements. In Spain every plant have to complete its own PSA, and the next development stage of the PSA studies would be to use it within a living PSA concept for TS evaluation, in particular AOT and STI requirements. The overall task of evaluating TS with probabilistic methods circles around two main issues:

1. the baseline risk of the plant, and
2. temporary risk increases.

The first one is the risk level during power operation assuming no failures are detected and no subsystems are intentionally isolated for test or maintenance. Obviously, systems unavailability and thereby plant risk would continuously increase as a function of the time, at least that some measures were taken, for example surveillance tests and scheduled maintenance.

The second one is concerned to component outages in standby safety systems which will temporarily increase the total plant risk above the baseline level. These increases may be involuntary - repairs - or voluntary - tests (every STI given in the TS), preventive maintenance, etc -, with the AOT, also given in the TS, as the maximum length of involuntary component outages during which the power operation is allowed. Temporary risk increases may also be due to planned, or not, plant shutdowns.

The total risk as calculated in PSA is the average risk over the baseline and temporary risk increases states, and it is known as an unconditional risk. The risk associated to each component outage is known either as a conditional risk. In order to control AOT and STI modifications it is only necessary to control both the unconditional and conditional risks.

Definition of the problem.

At this time a significant operating and design experience has been accumulated and a number of problems have appeared which require modifications in some TS rules. Thus, it is well known that operating plants have had several problems in the implementation of AOT and STI requirements. These problems are related to forced outages within surveillance testing with forced plant shutdowns in some cases due to system exceeding its allowed downtime. In addition, human errors due to inadequate time to complete equipment repairs or due to inadequate test intervals, too much large or short, have been identified. In several cases, plant availability and plant safety margin have been reduced. So, it is not sure that AOT and STI are optimized from a risk point of view and the desirability of several changes on them is recognized.

The goal of the modifications is to further improve the nuclear safety and also to enhance the effectiveness and flexibility of plant operation, maintenance and testing.

Developments in PSA have made the evaluation of effects due to AOT and STI modifications from a risk point of view possible. Thus, some changes have already been adopted in some cases, but AOT or STI modifications have been independently analyzed and the acceptance criteria used in their analysis have been based on the constraint that there was no significant reduction in plant safety when the proposed changes were incorporated. In this way, several changes with large effect on the risk level could not be accepted. Furthermore, lack of a method to evaluate and optimize the combined effect of several AOT and STI changes, for example through their *interaction*, has limited the benefits of the changes and has not allowed to analyze several problems that result of their interaction when only one of them is modified.

Among the benefits, we can improve plant safety and give flexibility to plant operation, maintenance and test. Among the problems that it is necessary to address when one change is required we can find the common cause failures and the test after failure problems and their relation with AOT and STI requirements.

1.2 Objective of this paper.

The main results from the developed study concerning the AOT and STI requirements interaction problem, which finally led to one of the authors to conclude his PhD Thesis[1], are briefly presented in this paper.

Firstly, the AOT and STI interaction is defined, and the main reasons are pointed up together with advantages of considering such an interaction. Then the interaction is quantified in terms of risk using the risk and reliability methodology taking into account the PSA methods as a tool. Thus, an approach to model AOT and STI modifications and their effects on the risk level, which considers their interaction, is derived.

Then using above model several sensitivity studies involving the main parameters are conducted, and finally several strategies to control the risk which allow us to give flexibility to the plant operation and optimize the risk level are assessed.

This new approach has been divided into several steps. It ranges from the component unavailability to the core melt frequency assessment. Here only the component level will be treated in depth.

2. AOT AND STI INTERACTION.

2.1 Sources of interaction.

With a general sense, the AOT and STI requirements interaction can be seen in terms of their common effect on the risk level and it becomes from two main sources:

1. TS requirements definitions, and
2. safety related components and systems disposition or function in the plant.

Firstly, both requirements have been established in order to intent to control the plant risk, both the risk due to detected component downtimes (concerned to AOT) and the risk due to undetected ones -failures- (concerned to STI). In this way, TS relate AOT and STI requirements for a component or a set of them (system, function, etc), and therefore the interaction becomes from the intent to control both risks.

Secondly, due to the safety criteria that have been adopted in designing nuclear power plants, there is a lot of redundancies among the components into a safety system or function, and among safety systems to prevent different accidental sequences following an initiating event. For instance, there are several Support systems which are shared by different Front-line ones, and in some cases more than one system or component is necessary to carry out a safety function or instead one system or component can be required to carry out different functions. That means it exists an interaction among several components and systems to preserve plant safety, and in this way the interaction becomes among their AOT and STI requirements, firstly preserving components availability, then system or function reliability and as the final goal preserving the plant safety. The common cause failures and test strategies play an important role in the interaction in this source.

2.2 Advantages of considering interaction.

As we have already said the AOT and STI interaction approach provides us with a method to evaluate and optimize the combined effect of several AOT and STI modifications from a risk point of view, where the risk contributions due to both detected and undetected component outages can be trade off - by means of AOT and STI trading off - in order to control and in some cases .to minimize the risk level, and this for a component, system, function, and so on.

At the same time using the different effects of AOT or STI modifications on the unconditional risk - normally both have opposite effects - it is possible to give flexibility to the plant operation by means of allowing AOT and STI to have a tolerance which can be controlled within a small variation in terms of their effect on risk level, using the AOT and STI interaction approach as a tool.

It is also worth noting that both AOT and STI modifications affect, because their interaction, both unconditional and conditional risk, and thereby the average and instantaneous plant vulnerability is affected in the same way. Other items which also have significant effect on the plant vulnerability concern the test strategies and common cause failures and test after failure problems. Using the AOT and STI interaction approach it is possible to manage successfully both problems, improving in this way the plant vulnerability.

3. COMPONENT LEVEL ANALYSIS OF INTERACTION.

The component level is important because: 1) most of the AOT and STI requirements directly affect to safety components of the plant, and 2) since we use the PSA methods as a tool, the component unavailability approach forms the basis of the risk approach at higher levels, such as system, function, sequence, and so on.

At the same time when studying the component approach it is possible to focus on the most important parameters into the model to be taken into account to establish the criteria for controlling the risk at component level and similarly at higher ones.

3.1 Risk evaluation model.

As we have previously pointed up the total risk is the average risk over the baseline and temporary risk increases states, which at component level becomes the average component unavailability. For a component periodically tested this unconditional risk between two consecutive tests can be distributed in several contributions, either related to one period in the average test cycle, which length is given by:

$$L = T + C + D \qquad (1)$$

where C is the test duration, D is the maximum length allowed for a repair following a failure detected by the test - also called AOT - and T is the period not included within both other ones which is usually called STI.

According to expression (1) the component average unavailability can be evaluated through the following contributions:

$$q_m = q_T + q_C + q_D \qquad (2)$$

In obtaining above expression for every contribution it must be addressed subjects related to component standby or on demand failures, human errors, test-caused failures or degradations, test override capability, test inefficiencies, test duration, corrective and/or preventive maintenance and their average duration, AOT and STI.

3.2 Definition of interaction.

At component level only the first source is possible when analyzing the AOT and STI interaction. Both requirements have been established to control both the risk due to detected component downtimes -represented by q_D- and the risk due to undetected ones -represented by q_T-. The term q_C represents the risk introduced by the test which has the benefit of detecting component failures to be repaired.

Studying above expression it can be found out that T mainly affects q_T contribution in the sense that increasing T means this contribution also increases, but has a smaller opposite effect on q_D. On the other hand, D only affects q_D contribution. When D increases also q_D contribution increases. The term q_C only depends on T in a similar manner as q_D. Thus, expression (2) model the AOT and STI interaction.

This simple relationship have to be well known because other effects, such as T or D initial values, component characteristics, test and repair conditions, can change the importance of every contribution to q_m and thereby the sense of such an interaction. At the same time a well knowledge of (2) and above mentioned influences could reduce the complexity of next studies by adopting several approaches without losing the validity of the method.

3.3 Dominant component characteristics.

Using above expression (2) sensitivity studies have been developed to account for different influence of each parameter in the AOT and STI interaction. As a final result from this step it has finally been concluded that the test contribution and thereby their associated parameters - test degradation, inefficiency, duration, and so on - have no important effect on interaction, and the other contributions can be evaluated using the following simplified expressions:

$$q_T = \rho + \frac{1}{2}\lambda T \tag{3}$$

$$q_D = (\rho + \lambda T)\,\frac{D}{T} \tag{4}$$

where λ is the failure rate associated to standby failures and ρ is the on demand related failure.

Expressions (3) and (4) have to be carefully used because both have important constraints. Thus, when T is too small the q_C contribution becomes as important as other ones and it has to be taken into account. On the other hand, the constraint $\lambda T < 0{,}1$ has to be satisfied when T becomes larger. Furthermore, in obtaining expression (4) the average repair time has been bounded by the AOT.

3.4 Approach to incorporate AOT and STI interaction.

In developing the methodology several approaches was assessed using the previous expressions as a tool to incorporate AOT and STI interaction. These approaches depend on the risk criteria adopted to control the risk. Finally, one of them was selected, where the risk criterium was that the component average unavailability should keep constant when an AOT or STI modification is required. That means for a given risk level q_m (related to TS requirements), T and D are tied in the sense that if a D or T modification is studied, it is required to trade-off their contributions to keep the same risk level. Thus, increasing D, that increases q_D contribution, must be balanced by decreasing T to an appropriate q_T level.

From a mathematical point of view above relation can be expressed in terms of the D and T relation for a given q_m, which is obtained by substituting (3) and (4) into (2) and then rearranging terms, to yield:

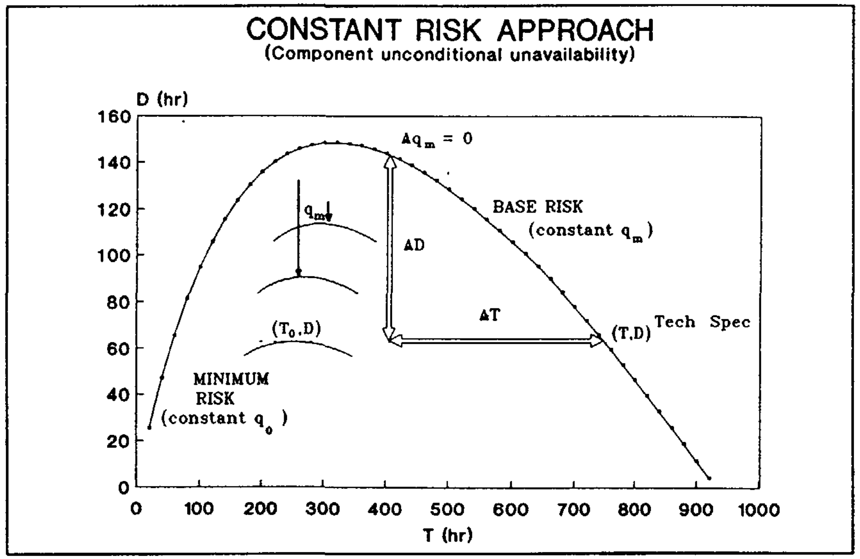
$$D = \frac{q_m - (\rho + \frac{1}{2}\lambda T)}{\rho + \lambda T}\, T \tag{5}$$

Expression (5) is known as the interaction function at component level and it depends on the risk level q_m and component characteristics (ρ,λ). The general expression for AOT and STI interaction, or D and T relation, is:

$$D = D(q_m, T, \rho, \lambda) \tag{6}$$

At component level it exists more dependencies than these observed in expression (6), which have been studied through our work, but above dependencies are the most important ones.

Expression (6) is represented for a safety component in Ilustr. 1 for a constant risk level (q_m value), where above relation, dependencies and constraints are shown.



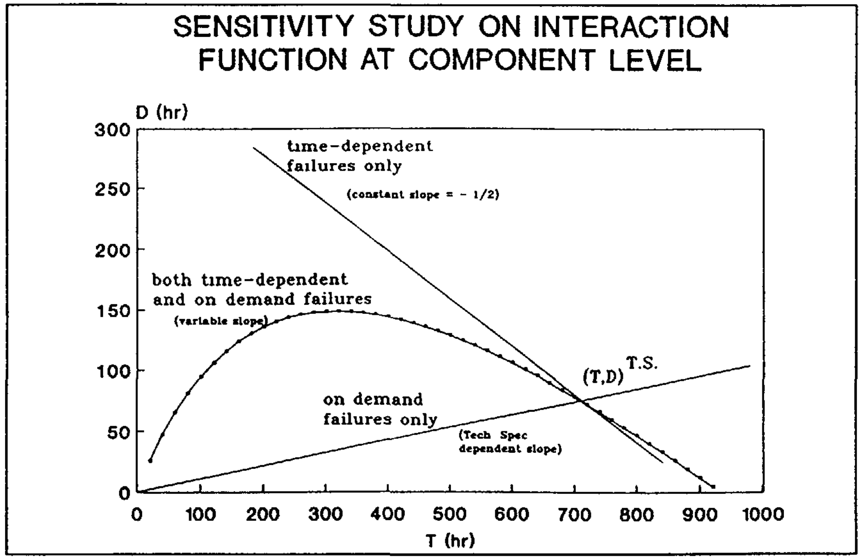
Ilustr. 1: Interaction function at component level.

In Ilustr. 2 sensitivity studies of the interaction function on λ and ρ are plotted, where the importance of both parameters becomes significant.

3.5 Implementation choices in defining AOT and STI considering interaction.

Above expression (6) as shown in Ilustr. 1 can be used to find pairs (T,D) on the trade-off criteria, which satisfy that the risk is kept constant when one requirement in a couple (T,D) - set up by Technical Specifications - is intended to be modified.

In addition, expression (6) can be used to optimize AOT and STI requirements, given by TS, at least in the component level. For instance, $(T,D)^{TS}$ is not a optimized couple from a risk point of view. Here, optimization means to change the STI requirement in order to minimize the risk level for an AOT given.



Ilustr. 2: Sensitivity studies on component characteristics.

Thus, the top of the curve represents a couple (T_0, D) which minimize the risk for a D value given. To find T_0 value using expression (2) it has to satisfy the following restriction:

$$\frac{dq_m}{dT} = 0 \quad \textit{(constant D value)} \tag{7}$$

where, using expressions (3) and (4) yield:

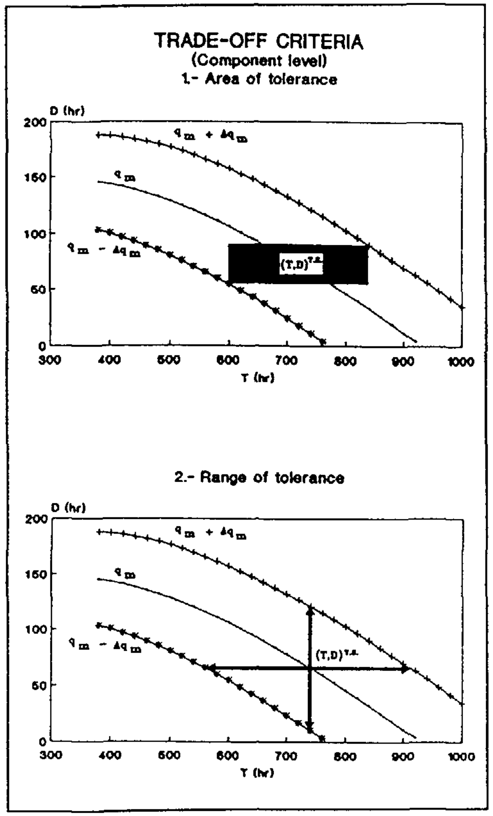
$$T_0 = \sqrt{\frac{2\rho D}{\lambda}} \tag{8}$$

The couple $(T,D)^{TS}$ satisfies the Base Risk curve while the couple (T_0,D) satisfies the Minimum Risk curve, which represents expression (5) when q_m becomes the minimum risk q_0, which is given by expression (2) using the pair T_0 and D.

Furthermore, an important application of the interaction function approach is to give flexibility to plant operation by means of giving some flexibility to AOT and STI requirements. In this way AOT and STI could be implemented into Technical Specifications taking into account the component importance and their impact on risk. Two possibilities was analyzed which have been represented in Ilustr. 3:

Area of tolerance:
AOT and STI should be set up with a tolerance (permanent), in such a sense that the risk level should always keep within an acceptable risk tolerance around a base risk. This possibility suppose that both AOT and STI will be able to take this tolerance simultaneously and permanently.

Range of tolerance:
AOT and STI should be set up without a tolerance, but a variation in only one of them could be eventually accepted as long as the risk level kept within and acceptable risk range or margin around a base risk. This possibility suppose that only one of them will be able to take a variation or tolerance where the risk level keeps into an admissible tolerance.



Ilustr. 3: Strategies to give flexibility to the plant through AOT and STI requirements.

Both strategies are adequate to propose AOT and STI modifications on the unconditional risk point of view. However, time-dependent risk and conditional risks due to component unavailabilities can not be controlled using this approach. It is possible to handle both problems at system or higher levels where tolerances on risk at component level must satisfy those set up at higher ones.

4. INTERACTION-BASED APPROACH EXTENSION TO SYSTEM AND HIGHER LEVELS.

Despite being worth the component approach and its analysis, it became necessary that the methodology presented herein was able to handle simultaneously several components and requirements because the following reasons:

1. to consider several items, i.e. to include test strategies and common cause failures effects on risk, which could not be addressed at component level,

2. there are more AOT and STI requirements to be modified and thereby it exists a larger range of possibilities for giving flexibility to the plant, and

3. the risk assessment have to be placed at system or higher levels very often.

The system level is important because the risk-based approach which incorporates AOT and STI interactions is similar to those derived at higher levels, i.e. function, sequence and core melt. These approach are founded on the component approach and on the relation among several components, that is modelled through the minimal cut sets (MCS) obtained for the system, function, sequence, and so on, using the PSA study for the plant.

4.1 Definition of interaction.

At these levels the second source of interaction have to be taken into account in addition to the first one. Thus, the relation among several components together with their characteristics and requirements have to be considered. This relation becomes from the component disposition in the plant, test strategies, common cause failures and strategies for test after failure. It can be modelled through fault or even trees logic structures obtained from the PSA study, or in terms of MCS.

4.2 Approach to incorporate AOT and STI interactions.

Two identical components MCS.

Now, the risk evaluation model will represent the average MCS unavailability. Using this model under the trade-off criteria a relation between D and T can be derived in a similar way as it was obtained at component level, which yield:

$$D = D(Q_m, T, \rho, \lambda, \beta, S) \qquad (9)$$

known as the interaction function at MCS level, where Q_m is the average MCS unavailability, and ρ and λ are well known from previous study.

In expression (9) can be see how D and T relation has others dependencies than those seen at component level (see expression (6)). These concern to test strategies (represented by S) and common cause failure probability (represented by β). Unfortunately expression (9) can not be obtained analytically -as expression (5)- and it has to be solve numerically. It will be always the same at levels higher than component.

Now expression (9) can be used to analyze test strategies and common cause failures effects in the light of AOT and STI interaction, or instead to study implementation choices in defining AOT and STI considering above dependencies, as it was done in the whole work[1].

System level.

The interaction-based approach extension to system and higher levels can be easily understood taking into account that the component approach forms the basis of the approach at higher levels. Extension consists in defining all existent sort of relations among components which will be modelled through the MCS that lead to the Top event on each situation.

Now, the risk evaluation model will represent the system unconditional unavailability and it will be given by a set of equations. This set will consist of:

1. a subset of expressions representing each a component unconditional unavailability or the component approach when it is possible,

2. a subset of expressions representing each an average MCS unavailability, which represents a relation among several component failures that leads together and without exceptions to the top event, and

3. a final expression which represents the unconditional unavailability for the top event, that is associated to the whole combination of component failures or MCS.

4.3 Additional constraints on changes on AOT and STI requirements.

Above set of equations models AOT and STI interactions at system or higher levels and it can be used to study changes on these requirements in the light of the unconditional risk.

However, there are other restrictions or limits on such changes which have to be taken into account. They are concerned to: AOT and STI modifications for a component or several of them in a group (i.e. when they are tested in the same test strategy), maximum tolerance on average component unavailability, etc.

On the other hand, as we have already said in this paper (see section 1.1), in order to control effects on risk due to AOT and STI modifications it is necessary to focus both the unconditional and conditional risks. When considering the last ones it can be obtained a set of equations - similar to the unconditional risk - which introduces constraints on the conditional risks.

4.4 Procedure for studying changes on AOT and STI requirements.

The next step after defining above restrictions to changes on AOT and STI requirements for a system, function and so on, is to study solutions to the global set of equations. In this set AOT and STI requirements for a subset of components together with their unavailabilities will be considered variables. Solutions will be those combinations of changes on above requirements which satisfy above set of equations or restrictions.

The existence, or not, of solutions for this set depends on its degrees of freedom, it is the number of variables in relation to the number of equations in the set. When for a given subset of components there is not solution it is possible to increase above subset of components to increase in this way the variables. If there are not enough variables at the actual level of evaluation because the limited number of components, it should extend the study of changes to higher level where there are more components.

In contrast, when existing more than one solution it is necessary to define an adequate strategy to find pairs (T,D), which will differ from their initial values. In our case the trade-off based risk criteria for both unconditional and conditional risks have been used.

Above set of equations constitute a non-lineal algebraic system which can not be solved analytically, so it is necessary to find pairs (T,D) using numerical methods. To help to do it, a mathematic algorithm was developed and implemented into a computer program called ASIA[1].

5. CONCLUSIONS.

A significant operation and design experience has been accumulated and a number of problems have appeared which require modifications in some TS rules, specially in some AOT and STI requirements. The goal of the modifications is to further improve the nuclear safety and to enhance flexibility of plant operation.

Using probabilistic methods, some changes have been adopted in some cases but above goal has not fully achieved because two main reasons: 1) AOT and STI modifications have been independently analyzed, and 2) the acceptance criteria have been based on the constraint that there was no significant reduction in plant safety.

The above goal can be entirely achieved using the methodology presented herein. Thus, using the interaction based approach the analyst can study several changes on AOT and STI requirements which aim to optimize components and systems reliability and thereby the plant operation and safety from a risk point of view. At the same time when adopting the trade-off based risk criteria it is possible to give flexibility to the plant operation through several strategies which have been presented herein.

In this document the bases of such a methodology have been introduced, ranging since the component level to system and higher ones. Further studies were conducted in the whole work[1] where this methodology was successfully used to study several changes on AOT and STI requirements for the AFWS in a PWR plant. To help to do it, a mathematic algorithm was developed and implemented into a computer program (ASIA).

REFERENCE

[1] **Sebastián Martorell,** "Análisis de la Interacción entre los Requisitos de Tiempo Máximo Permitido de Inoperabilidad (AOT) e Intervalo entre Pruebas de Vigilancia (STI) de Componentes de Sistemas de Seguridad de Centrales Nucleares", PhD Thesis presented in the Chemical and Nuclear Engineering Department of the Polytechnic University of Valencia, Spain, May 1991.

APPLICATION OF PSA TECHNIQUES FOR EVALUATION OF PROPOSED CHANGES TO DG MAINTENANCE AT KOZLODUY-3 NPP

I.G. KOLEV
Risk Engineering Limited,
Sofia, Bulgaria

Abstract

This presentation is a brief overview of a study done by *Risk Engineering Ltd* for EP-2 Directorate of the *Kozloduy NPP Branch* of the *National Electric Company* of Bulgaria. The complete report is contained in REL document NRI/D-06, May 1992 (in Bulgarian).

The PSA techniques has been applied for evaluation of the impact on CDF of the additional maintenance of DG electrical systems and components, proposed by the personnel of the Electrical Dept. of Kozloduy-3 NPP. The proposal included a request to the regulatory body to allow the proposed maintenance to be performed once per month on each DG train without starting-up of other trains, which should normally be done for all on-line maintenance of the safety systems according to an action statement in the plant Technical Specifications. The study had to be done without an existing PSA.

The study includes discussion on the applicable accident sequences and analysis of the relevant safety functions, including restoration for the existing as well as for the proposed maintenance practices on an yearly-averaged basis. The comparative character of the study allows the use of generic data, but the available plant statistics has also been used, and sensitivity calculations has been done for the key modelling parameters.

1. Introduction

The Kozloduy-3 NPP is a double-unit plant (units 5 and 6 at the Kozloduy site) with VVER-1000 reactors. Unit 5 started official operation in 1989, and unit 6 is being operated on different power levels since 1990 and the licence for full-power operation is expected later this year. The overall operational experience is about 5 reactor-years including the initial lower-level operation.

The main features of each unit include 3 independent trains of all safety systems, including diesel generators (DG) for back-up of essential power supply system. The plant Technical Specifications (TS) does not allow any scheduled maintenance of the safety systems, while the unit is in power operation.

The un-scheduled maintenance is mainly connected with the on-line surveillance tests of safety systems that are being done once per month on a staggered scheme, i.e. one train each 10 days and include testing of all safety system's functions and all major components, including control and instrumentation systems and electrical systems. If a failure state or malfunction of component or system is detected, the action statements require the restoration to be done in one-shift (8 hours) period, and the other two trains of safety systems are to be started on recirculation during the restoration period. All repairs or restoration activities are to be followed by a full-scope test prior to the declaration of normal-operation conditions.

During the several operational years, the personnel of the Electrical Dept. of the plant observed number of small (as described by the staff) faults in electrical equipment of the DGs, that are usually revealed during the surveillance tests and the corresponding components are usually restored in a very short time (in 10-20 minutes, up to one hour in rare cases). However, the stringent requirements of the TS had to be followed, thus imposing additional load to both personnel and safety equipment.

In connection with the on-going activities for upgrading of plant Technical Specifications, the Electrical Dept. staff proposed changes to be introduced, that would allow for an on-line maintenance activity to be done on each DG's electrical equipment prior to each surveillance test (the overall time for this maintenance has been assessed to about 5 hours). In the same time it was proposed that the other two trains will not be started during this maintenance, on the ground of bigger wear-out of the equipment and bigger load on the staff as well as on the ground that the corresponding DG will be disconnected from the Emergency Safety Feature Automatics (ESFA), but will still be in hot-standby condition.

Before submittance of this proposal to the Regulatory body, the plant Management required a risk impact study to be performed, and Risk Engineering Ltd has been commissioned for the analysis. The tasks has been defined as evaluation of the impact of proposed changes to plant safety by a comparative study. The study had to be done in a very short time to fit with the time-schedule of TS upgrading activities and had to be done in the absence of any PSA-related analyses for this plant.

2. Probabilistic Models

2.1. General Approach

The general approach to the analysis has been defined according to the task and the unavailability of basic PSA study. The core damage frequency (CDF) has been used as measure of the risk and yearly-averaged time-independent models and quantification has been used for assessment of CDF.

The main steps of the analysis are as follows:

- qualitative determination of the applicable Initiating Events (IE) and accident sequences with major impact on plant safety in connection with the performance of systems and components challenged by the proposed change; developing of the master CDF equation;
- development of probabilistic equations for the unavailability of the safety functions in the master CDF equation for the existing situation and for the situation after the implementation of the proposed changes;
- analysis of system unavailabilities by the Fault Tree (FT) method, quantification of other modelling parameters (maximum use of the available plant data has been requested);
- final quantification of both configurations, incl. parametric analysis with respect to the uncertain modelling parameters.

The sections below present this items in more detail.

2.2. Accident Sequence

The proposed changes to DG maintenance would only affect the performance of DG back-up of the Essential Power Supply Systems (EPSS). This is a stand-by safety function, that only comes into operation in case of loss of the two other power sources of the EPSS, namely (1) preferred power supply from the 400 kV grid through the main and house-load transformers (the main generator is equipped with generator breakers to allow for the preferred power source to be used in case of Turbine Generator (TG) trip) and (2) reserve power supply from 220 kV grid through the auxiliary (start-up) transformers. This layout allows us to consider that the importance of DG is bounded by the accidents with total Loss of Off-Site Power (LOSP), thus outruling for the purposes of this study any other Initiating Events (IE).

The safety functions that are challenged in case of LOSP, are as follows:

(1) **reactor and TG trip**: multiple independent signals are foreseen for both reactor and TG trip in case of LOSP;

(2) **secondary side integrity**: the loss of main condensers vacuum in case of LOSP require opening of the Steam Dump Facilities with atmosphere discharge (SDFA), that are available on each Steam Generator's (SG) steam line, these are backed-up by 2 SG safety valve per SG. For the case of stack-open situations, the steam lines are provided with fast-acting isolation valves as well as with passive check valves, that would isolate the corresponding SG form the rest of the steam lines system. In addition, the SG safety valves can be manually re-closed without degrading of their primary function;

(3) **emergency power supply** is provided by Accumulator Batteries (AB) for the Uninterraptable Power Supply System (UPSS) and by DG for EPSS; the UPSS is realigned to DG after their start-up;

(4) **decay heat removal** is provided initially by the run-down of Reactor Coolant Pumps (RCP) leading to natural circulation conditions in the primary loops and by secondary heat removal via steam discharge form SGs; when the DGs provide power for safety systems, the Auxiliary Feed Water System (AFWS) comes into operation to keep the SG water level and steam discharge is continued by SDFA in SG-pressure maintenance mode. The reactor is to be kept in hot-shutdown in LOSP environment for 1 hour, then, if LOSP situation is not removed, operators have to initiate a cool-down procedure by opening of Reactor Emergency Gases Removal (REGR) valves (or opening and reclosing of Pressuriser Safety Valves), aligning the High Pressure Injection Systems (HPIS) (all safety systems are started on recirculation by DG Gradual Loading Automatics (DG-GLA) to maintain reactor pressure and coolant level and to increase the coolant boron concentration while decreasing the coolant temperature by secondary side heat-removal. When the necessary cold-shutdown boron concentration is provided, the Core Flooding System (CFS) function is blocked, reactor pressure is decreased and Residual Heat Removal (RHR) configuration of the Low Pressure Injection System (LPIS) is operated for long-term maintaining of cold-shutdown state of the reactor.

For the reasons explained above, the functions (1) and (2) where considered to be lower-margin contributors to the probability of CDF in case of LOSP and were discarded from further analysis. Thus only functions (3) and (4) were considered.

With the assumptions explained above, the core damage in case of LOSP would be a result of the following accident progression sequences:

(1) failure of the secondary decay heat removal (loss of all feed-water supply), followed by a failure to use feed-and-bleed for primary decay heat removal as well as failure to restore preferred or auxiliary power supply in time to prevent core damage;

(2) failure of the emergency power supply (unit blackout) followed by failure to restore power supply in time to prevent core damage.

The (1) above includes multiple failures of safety functions either by hardware or human faults. All systems, as well as operator actions, that provide those functions depend on the power supply for their operation or for providing of indications for correct diagnosis of the accident progression. The non-power-related faults necessary to degrade those functions are multiple and independent. It was considered appropriate for the purposes of this quick study to make the conclusion that the CDF will be dominated by the blackout sequence (2). The CDF for that sequence will be expressed by:

$$CDF = I \cdot Q_{DG} \cdot P_{OP} \tag{1}$$

where:

I = frequency of the Initiating Event (LOSP)

Q_{DG} = unavailability of the power supply from DGs

P_{OP} = probability of nonrestoration of off-site power within the available time

Because of the comparative nature of this study, the fact that the proposed changes do not interfere with the performance of EPSS beyond the DG electrical equipment, the EPS function has been substituted with the DG unavailability, which is considered to be a dominant contributor for the unavailability of EPS. The Eq. (1) is the master CDF expression used in the study.

The available time for restoration of the power supply in case of blackout has been defined rather conservatively by the following arguments:

(1) the turbine-driven FWPs are not designed to work in power supply failures, thus the only source of FW to the SGs remain the AFWS with motor-driven pumps that depend on EPSS;

(2) the horizontal SG's large water inventory allows for the boil-off cooling of the reactor for at least 3-4 hours, presuming that the motor-driven SDFA (so called BRU-A) will correctly function in pressure-maintenance mode, but

(3) the capacity of ABs, that would supply SDFA in blackout, according to the design is only 30 min (it is not verified, whether AB can really supply SDFA, that is a quite large consumer, for 30 min);

(4) the loss of Component Cooling System (CCS) in case of blackout will eventually lead to leaks from RCP seals; leaks may be significant in about 1 hour since loss of CCS;

(5) rapid reactor cool-down requires additional boron injection, provided by power-dependent HPIS.

In this circumstances, the conservative assumption has been made that the AB capacity is the limiting factor, leading to 30 min being defined as the allowable time for power restoration in case of blackout. After 30 min, the operator will no longer control the unit due to loss of Control and Instrumentation (C&I), SDFA will be fixed in unknown position, with increasing leaks form RCP's seals. No procedures are available for plant personnel actions in such situation, and some core damage may be possible. The 30 min bound has been used independently of the time, when the blackout occur (immediately following LOSP or after some time due to DG run failures) because the operator is not supposed to cool-down the reactor until 1 hour into the accident, and after that the partial probability of non-restoration of off-site power is only a small fraction of the total and corresponding accident progression is not expected to significantly change the results.

The frequency of IE has been conservatively evaluated to be 0.2 per reactor year. This figure have to be treated as an upper bound, because it reflects the experience with power failures in older units on the site and is independent from the power failure periods; it also do not reflect the more reliable preferred power scheme of the new units.

2.3. Power Restoration

The probability of non-restoration of the off-site power in the defined available time, has been evaluated by the approach, based on the assumption for exponential distribution of restoration times. Generally, the probability of non-restoration in time t' if the failure has occurred in $t=0$, will be

$$P = 1 - \int_0^{t'} r \cdot \exp(-r\,t)\,dt = \exp(-r\,t') \tag{2}$$

where

r = restoration rate: $r = 1/\tau$, (τ = mean time to restoration).

The probability of non-restoration in time t' if the accident started at $t = 0$ and the blackout condition has occurred at any time moment ($t : 0 < t < t''$), where t'' is the mission time, will be

$$P = \int_0^{t'} \exp[-r(t+t')]dt \;=\; \frac{1}{r}\exp(-r\,t')\,[1-\exp(-r\,t'')] = \\ = \tau\,\exp(-\frac{t'}{\tau})\,[1-\exp(-\frac{t''}{\tau})] \tag{3}$$

The Eq. (3) has been used for estimation of the probability for non-restoration of the off-site power. The mean time to restoration has been evaluated by expert opinion (experts from both NPP and Grid Control Centre participated in the evaluation) to be in the interval 15-45 min depending on the actual reason for LOSP accident. This time is bounded by the possibility to provide temporary power line from other units. The probability of catastrophic external events, that may cause long-term power failures, is quite low in comparison with other causes for LOSP, so their weight in mean restoration time is also low. Parametric calculations has been done to reflect the uncertainties of the off-site power restoration time.

During the DG unavailability analysis, explained below, it was considered to include the probabilities for non-restoration of DG in the specified time to prevent core damage. The quantification of this probability has been done by Eq. (2) above, and the mean restoration time has been evaluated from plant records and has been found to be about 3 hours. This figure has been considered too optimistic with respect to generic figures based on more statistical data, so a parametric calculation has also been done for bigger times to restore power supply from DGs. The mean time to restore the DG that is in the proposed additional maintenance reflects the fact that it has to be kept in hot stand-by.

2.4. Unavailability of DGs

The unavailability of DGs that is included in Eq. (1) had to be evaluated separately for the two cases: (0) the existing situation and (1) the situation after the eventual introduction of the additional on-line maintenance.

Three different configurations of DGs were found to be relevant for this study, namely:

(n) the normal on-line configuration of three trains in hot stand-by: the total unavailability have to account for failures to start or run of three DG trains as well as for the probability of non-restoration of a failed DG in the specified time;

(m) configuration in unplanned on-line repair of one train according to existing practice to start-up the other two trains: the total unavailability have to account for failures to run of two DG trains and non-restoration probability (the train that would be in maintenance was not accounted for in the model);

(a) configuration during the proposed additional maintenance with 2 trains in hot stand-by: the total unavailability accounts for failures to start and run of the two DG trains, the probability of non-restoration of a failed train as well as the probability of non-restoration of the train in maintenance (that is to be kept in hot standby).

Thus the DG unavailability formulas will be as follows:

$$Q_0 = (1-k_m)Q_n\,P_n^3 + k_m\,Q_m\,P_n^2 \tag{4}$$

$$Q_1 = (1-k_m-k_a)Q_n\,P_n^3 + k_m\,Q_m\,P_n^2 + k_a\,Q_a\,P_n^2\,P_a \tag{5}$$

where

k = fractions of time when the corresponding configuration exists

P = probability of non-recovery of a failed DG or DG in planned maintenance

and the indices are as denoted in the explanation above.

The time fraction of the unplanned on-line maintenance has been evaluated from plant records, and the time fraction for the planned additional maintenance - from the proposed maintenance programme.

The unavailabilities of DG in Eqs. (4) and (5) above have been modelled with 3 different FTs and quantified with generic data. Common cause failures for DGs have been included in the models and quantified by the Multiple Greek Letters (MGL) method using also generic data.

3. Overview of Results

The main results of the study are presented below. The Table 1 presents the results of quantification of the FTs developed for 3 different configurations:

Table 1. Quantification of DG unavailability FTs

Configuration	Unavailability
Three trains start and run	1.8 E-03
Two trains run	2.6 E-03
Two trains start and run	6.7 E-03

Table 2 lists the average unavailability of DGs according to the existing and to the proposed procedures for DG maintenance which also includes the restoration (according to Eqs. (4) and (5)).

Table 2. Unavailability of DGs with respect to existing and proposed maintenance procedures

Maintenance procedure	Unavailability
Existing	1.10 E-03
Proposed	1.17 E-03

As stated earlier, several modelling parameters have been used for a parametric calculations in order to assess the sencitivity of results to this parameters; only one of this calculations is presented here. *Table 3 below presents the results of the study in terms of CDF due to blackout for 3 different values* of the mean time to restore off-site power. The table incudes results for the existing and proposed procedures and the percentage of CDF increase.

Table 3. Expected CDF due to blackout with respect to existing and proposed maintenance procedures

MTTR for Off-Site Power	CDF for Existing Procedures	CDF for Proposed Procedures	CDF Increase, %
15 min	9.52 E-06	1.01 E-05	6.1
30 min	5.15 E-05	5.45 E-05	5.8
45 min	1.08 E-04	1.14 E-04	5.5

The results of other parametric calculations, including different combinations of the parameters, were also inside the 5.5 - 6.4 % increase of CDF for all cases considered. The results reflect the additional DG unavailability imposed by the additional proposed maintenance in the framework of a plant that is, generally speaking, not designed to withstand a blackout situation and with quite a big impact of DG performance on plant safety because of small capacity of AB and dependencies of most safety systems on power supply. The results also reflect the relatively small unavailability of DG due to unplanned maintenance

Following the study, the proposed changes has been outruled by plant management. The Electrical Department personnel has been requested to prepare a new preventive maintenance programme that would solve the existing problems but would not significantly increase DG unavailability.

RISK-BASED EVALUATION OF ALLOWED OUTAGE TIMES (AOTs): CONSIDERING RISK OF SHUTDOWN*

T. MANKAMO
Avaplan Oy,
Espoo, Finland

I.S. KIM, P.K. SAMANTA
Brookhaven National Laboratory,
Upton, New York,
United States of America

Abstract

In failure situations of safety systems during power operation, the Technical Specifications (TS) usually limit the repair within Allowed Outage Time (AOT). If the repair is not possible within AOT, or if no AOT is allowed, plant is required to be shut down for the repair. However, if the capability of removing decay heat is degraded, shutting down the plant with a need to start up and operate the affected decay heat removal systems, may impose a substantial risk as compared to the continued power operation over a usual repair time.

Defining a proper AOT should thus basically be considered as a risk comparison between the repair in full power state with temporarily increased risk level, and the alternative of shutting down the plant for the repair in zero power state with a specific associated risk. Obviously, if both of these alternatives impose a small risk, then a flexible AOT for repairs in full power state can be accepted without a closer evaluation.

The methodology of the risk comparison approach, with a due consideration of the shutdown risk, has been further developed and applied to the AOT considerations of residual heat removal and standby service water systems of a boiling water reactor plant . Based on the completed work at this stage, a number of improvements to the TS requirements for the systems studied can be suggested.

1 INTRODUCTION

1.1 Problem formulation

Defining the Allowed Outage Time (AOT) will be considered here as a risk comparison between:

CO: Continued operation alternative: repairs undertaken while at an increased risk level, in the full power operation state

* Work performed under the auspices of the US Nuclear Regulatory Commission (USNRC). The views expressed are those by the authors and do not necessarily reflect any position or policy of the USNRC.

SD: Decided shutdown alternative: a controlled shutdown undertaken in order to make repairs in a zero power state (usually cold shutdown state)

SD alternative includes a specific risk constituted by the disturbance transients possible during power reduction and cooldown. Furthermore, if the initial failures affect the residual heat removal (RHR) function, the need to start up and operate the degraded RHR systems in SD alternative, may impose a substantial risk. These risks cannot be readily determined but require a closer evaluation. The operational decision alternatives, and relevant operational flow branches for an AOT case, are illustrated in Fig.1. This will be discussed in more detail in Section 2, along with highlighting the specialities of the approach as compared with more conventional, risk-based AOT considerations.

The uses of this kind of analysis are to

- identify noncoherent requirements in the TS that may result in increased risk as opposed to alternative, safer options
- alert plant personnel about situations where quick diagnosis and resolution of the encountered problem is important
- provide basis for risk-effective, practicable action statements and to minimise risk-impact of operational events

1.2 Background and scope

The methodology builds on the recent work and application for the residual heat removal (RHR) and standby service water (SSW) systems of a BWR plant in the USA [1], and on the earlier work for a BWR plant in Finland [2-3]. The basic development and criteria for risk-based AOTs are more completely presented in Refs.[4-5].

This paper will describe key features of the risk comparison approach, supplementing earlier publications. Especially, the risk addition from a preset AOT on the long term risk will be handled. The interpretation and uses of the risk comparison results will be discussed.

The completed work and practical applications this far have resulted in a number of suggestions for the improvements in the TS action statements. These insights will also be covered.

2 RISK COMPARISON APPROACH

The methods and approach will here be illustrated by the use of example results from the recent pilot application, for failure situations of three redundant SSW trains [1]. These SSW trains constitute a part of normal RHR path, but serve also vital component cooling function of most front-line safety systems, and jacket cooling of diesel generators.

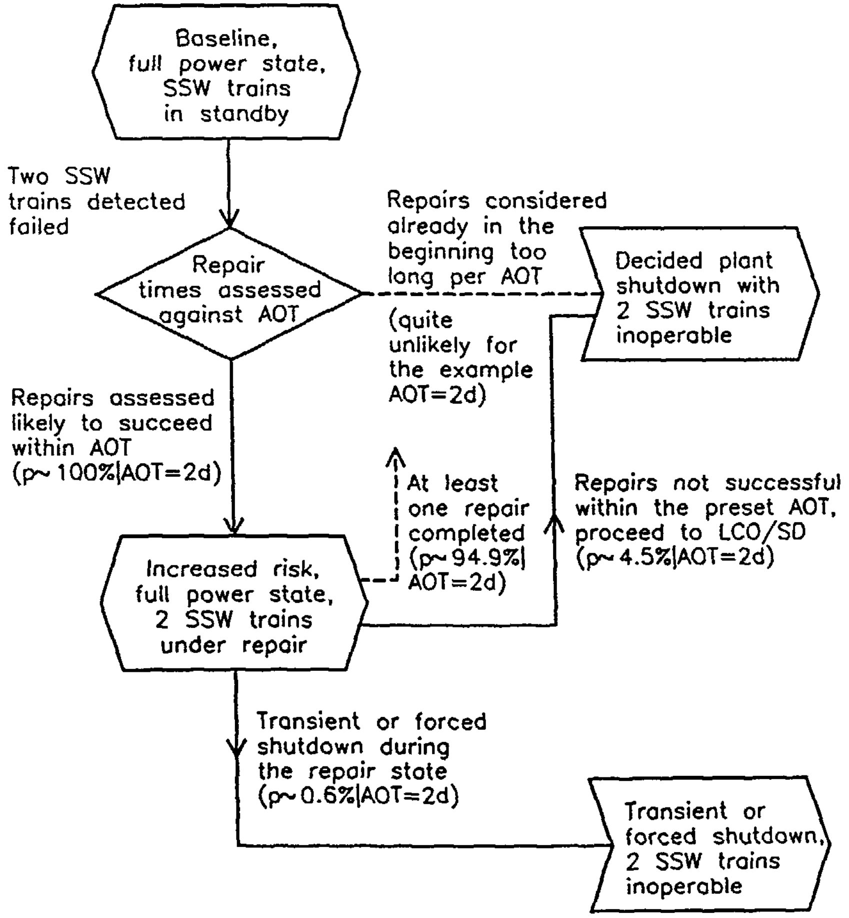

Baseline, full power state, SSW trains in standby
Two SSW trains detected failed
Repair times assessed against AOT
Repairs considered already in the beginning too long per AOT
(quite unlikely for the example AOT=2d)
Decided plant shutdown with 2 SSW trains inoperable
Repairs assessed likely to succeed within AOT (p~100%|AOT=2d)
At least one repair completed (p~94.9%| AOT=2d)
Repairs not successful within the preset AOT, proceed to LCO/SD (p~4.5%|AOT=2d)
Increased risk, full power state, 2 SSW trains under repair
Transient or forced shutdown during the repair state (p~0.6%|AOT=2d)
Transient or forced shutdown, 2 SSW trains inoperable

Figure 1. ESD for the operational states and flow paths in a failure situation of a standby safety system. Likelihood of the branches are here illustrated by the use of data relevant for SSW train failures in a BWR plant [1].

2.1 Basic operational alternatives

Let us consider a failure situation covered by an AOT, and the relevant operational states and flow branches as presented in Fig.1. At the instance of failure detection, the increased risk, full power state is first entered. There are three principal exits:

coA Repairs or some other type of restoration is *successful* within the AOT. In multiple failure cases, already the completion of one repair usually reduces significantly the situation specific risk, and means transfer to another, safer state (not shown explicit in Fig.1)

coB A random transient or some critical cause forces the plant shutdown during the full power repair state

sd A controlled plant shutdown is undertaken because the repairs *are not successful within* the AOT

The likelihood of exit path *coB* is usually small, because the probability of the transients and forced shutdown needs is low over the normal mean repair time.

The likelihood of exit path *sd* is determined by the repair time distribution against the AOT.

If no AOT is given, then the operators will promptly proceed from the failure detection to a controlled plant shutdown. In this case, the expected risk is constituted merely by *sd* branch, neglecting the short duration risk while still in the increased risk, full power state. This is the principal SD alternative defined in Section 1.1.

If an AOT is given, the expected risk per failure situation is constituted of the net contribution from all the three possible branches above, weighted according to their likelihood. Assuming infinite AOT, or in practice, a long AOT as compared with the mean repair time, this corresponds with the principal CO alternative defined in Section 1.1. (The influence of AOT in the region of the mean repair time will be discussed later.)

In a "conventional" AOT consideration, plant shutdown risk is assumed negligible in comparison with the temporarily increased risk level, and cumulated risk over a repair time, in the failure situation concerned. This may be a reasonable assumption for the failure cases of some specific systems, but not necessarily for the RHR systems especially needed in the plant shutdown states, as shown by the results from the recent studies.

2.2 Risk measures for comparing operational alternatives

In the SD/CO risk comparison approach, the primary risk variables to be considered in setting AOTs, are the instantaneous risk frequency in the failure situation, and the cumulating risk over a predicted repair time (also a situation specific risk). These are illustrated in Fig.2 by using SSW case data [1]. In addition, the incremental influence by a preset AOT in the long term risk average is of interest, and will be discussed later.

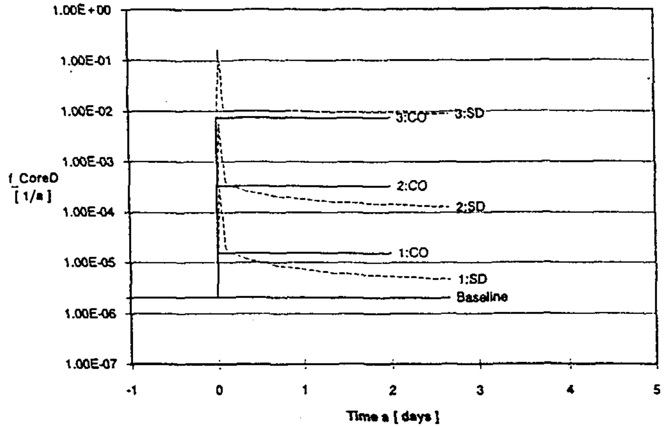


Figure 2a. Instantaneous risk frequency for the continued operation (CO) and plant shutdown (SD) alternatives in failure situations of SSW trains. For example, 2:CO denotes the continued operation alternative in the failure situation of two SSW trains being inoperable.

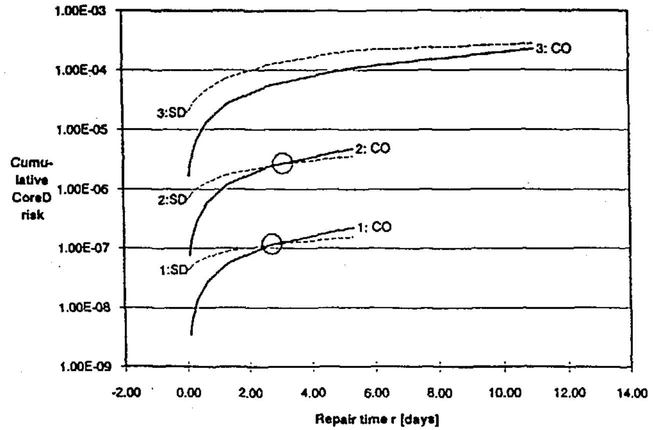


Figure 2b. Cumulative risk over predicted repair time in failure situations of the SSW/trains. For example, 2:CO denotes the continued operation alternative in the failure situation of two SSW trains being inoperable.

2 2 1 Instantaneous rısk frequency

The ınstantaneous rısk frequency, ı.e. the probabılıty of undesıred end event per unıt of tıme (here core damage frequency as defıned ın so called PSA Level 1 analysıs) ıs shown ın Fıg 2a both for CO and SD alternatıves, over dıfferent multıplıcıty of faılure sıtuatıons of three redundant SSW traıns [1] The maın ınterest focuses on whether a lower rısk level wıll be reached after plant shutdown, because thıs ıs a precondıtıon of SD alternatıve beıng vıable at all from the rısk poınt of vıew. There may exıst such extreme cases, where the rısk frequency would be hıgher ın zero power state as opposed full power state, for example, ın a total faılure of the standby RHR systems of a BWR plant, where the normal power conversıon system/turbıne condenser ıs unstable to be used at low steam rates

2 2 2 Cumulatıng rısk over predıcted repaır tıme

The cumulatıng rısk over predıcted repaır tıme, ı.e. the ıntegral of rısk frequency over a gıven repaır tıme, ıs shown ın Fıg.2b, also both for CO and SD alternatıves, over dıfferent multıplıcıty of faılure sıtuatıons of three redundant SSW traıns [1]. The maın ınterest ın these curves ıs, at what repaır tıme do the SD/CO alternatıves cross? SD alternatıve ıs motıvated for longer repaırs than the threshold value. Therefore, thıs rısk varıable should be consıdered most essentıal ın the determınatıon of a proper AOT ın the SD/CO comparıson approach.

Generally, the AOT should be comparable wıth the crossıng poınt of the cumulatıng rısk over predıcted repaır tıme. In practıce often, the SD/CO curves are close to each other, and hence the crossıng poınt should not be followed too strıctly, specıally when takıng ınto account the uncertaıntıes of the rısk calculatıons (to be dıscussed later, compare wıth Fıg 5). Practıcal/operatıonal reasons may motıvate to utılıse only lımıted, dıscrete values for AOTs such as 1, 3, 7, 14, 30 days.

2.2.3 On the concept of "baselıne" state and rısk

The baselıne rısk (compare to Fıg.2a) wıll be used here to refer to the rısk level ın case the safety systems are ın theır nomınal state For most safety systems thıs means standby state wıthout any components known to be ınoperable The latent faılures of these components are only detected by surveıllance tests, or at demand sıtuatıons. Theır lıkelıhood ıs the prıme ıngredıent of the baselıne rısk. For some safety systems, or components, the nomınal state may also be operatıng state Consequently, faılures of those components are usually dırectly revealed by ınstrumentatıon or process symptoms If an ınıtıatıng event occurs durıng the baselıne state, the ınstantaneous unavaılabılıty ıs ınıtıally zero for these systems, but they may faıl durıng the mıssıon perıod, and contrıbute ın that way also to the baselıne rısk.

Dısconnectıon for testıng or maıntenance, and detectıon of crıtıcal faults ın surveıllance testıng of standby components, or faılure to run of operatıng components etc , are devıatıons from the baselıne state

When consıderıng AOT sıtuatıons for a safety system, ıt ıs ımportant to carefully exclude from the baselıne state all unavaılabılıty states of safety system components, whıch would ınterfere wıth the LCO rules for the consıdered systems Such ınterferıng combınatıon cases should be consıdered explıcıt as dıstınct AOT sıtuatıons, not ıncluded "ımplıcıtly" as ın PRA studıes ıs normally done for repaır and maıntenance downtımes.

The long term rısk ıs composed of the average baselıne rısk plus the expected value of the ıncrements due to all kınds of devıatıons from the baselıne In practıce, thıs ıs a too tedıous way of obtaınıng the total average rısk level. Instead, the standard PRA approach ıs motıvated to be used for that purpose The baselıne rısk level ıs a dedıcated concept to be used ın connectıon to AOT consıderatıons.

2.3 Contrıbutors to the shutdown rısk

The rısk peak ın SD curve of the ınstantaneous rısk frequency, Fıg.2.a, or equıvalently the nonzero startıng value of cumulatıng rısk for SD alternatıve, Fıg.2.b, represents the rısk assocıated wıth the state change of the plant ın a controlled shutdown. Fırst of all, ıt ıncludes the rısk of dısturbance transıents. In the example SSW faılure cases, the maın contrıbutors are

- loss of normal power conversıon system (PCS) durıng power reductıon or reactor cooldown
- loss of off-sıte power (LOSP) caused by a shutdown transıent.

Besıdes, the rısk peak may ınclude also the rısk of remaınıng RHR systems faılıng to start. In the example SSW faılure cases, thıs contrıbutıon lacks, because PCS ıs operatıng through a smoothly proceedıng controlled shutdown, and ıts use can be extended, ıf the standby RHR systems faıl to start.

In SD alternatıve, the rısk frequency decreases after power reductıon, due to dımınıshıng decay heat level, whıch allows more tıme to recovery, ıf a crıtıcal faılure combınatıon occurs later durıng the shutdown coolıng mıssıon Nevertheless, the rısk frequency may stay at a substantıal level after plant shutdown. In the example SSW faılure cases, the maın contrıbutors durıng the shutdown coolıng mıssıon are

- loss of ınstrument aır supply, whıch accordıng to operatıng experıences has a rather hıgh faılure rate ın the zero power state
- LOSP, whıch ıs especıally crıtıcal because SSW traıns serve also jacket coolıng of the dıesel generators therefore, dıesel generators are functıonally unavaılable ın those subs where SSW traıns are ınıtıally detected faıled

In comparison, the risk frequency of the full power operation state is in the example SSW failure cases strongly dominated by LOSP. Thus the risk profile is rather different from that of a controlled shutdown (SD alternative). It should be emphasised, that the risk frequency of the full power operation state (CO alternative) is composed of initiating event frequencies and the expected risk of the various kind of transient and forced shutdowns associated with the initiating events. These risk decomposition and modelling details are further discussed in Refs.[1,3].

2.4 Influence of AOT onto expected risk addition

The instantaneous risk frequency and cumulative risk over predicted repair time, considered in Section 2.2, are concerned with situation specific risk. They lack control for the frequency of repair downtime occurrences. For this purpose it is motivated to consider in parallel also the long term risk addition from the AOT situations. This expected risk addition is named here as delta risk *dfav*, and expressed most conveniently as an increment to the annual average risk, i.e. in units [1/year]. It is related through

$$\mathrm{dfav}_X(\mathrm{AOT}) = \lambda_X \cdot \mathrm{rrs}_X(\mathrm{AOT}) \qquad (1)$$

with

λ_X = Rate of failure situations X

$\mathrm{rrs}_X(\mathrm{AOT})$ = Expected risk per failure situation X, with a given AOT

In principle, the existence of AOT influences the delta risk as shown in Fig.3, through the following two contributions (this decomposition will be discussed in more detail in Section 3):

dfav_co The expected risk contribution of repair time while in power state. If AOT is longer than the mean repair time, so a large part of faults will be repaired within AOT. Therefore this contribution saturates to a level corresponding to the risk over mean repair time.

dfav_sd The expected risk contribution of LCO shutdowns and repair time in plant shutdown state. If AOT is short, the expected number of LCO shutdowns increases and also the associated expected risk contribution *dfav_sd*.

Summing up these contributions produces the delta risk - AOT correlation curve, Fig.3. It may have different detailed forms depending on the plant specific features. In many cases, the minimum in the delta risk - AOT correlation curve proves not very pronounced. The essential conclusion then is that if AOT is reasonable in comparison with a normal repair possibility, longer than about three times the mean repair time, the delta risk becomes insensitive for AOT. This is based on the assumption, that no significant relaxation in the repair process does not happen for long AOTs. It need to be emphasised, that the plant staff should have a strong motivation to carry out repairs without unnecessary delays, even with long AOTs, because this reduces the occurrence possibility of complex cross combinations of failures.

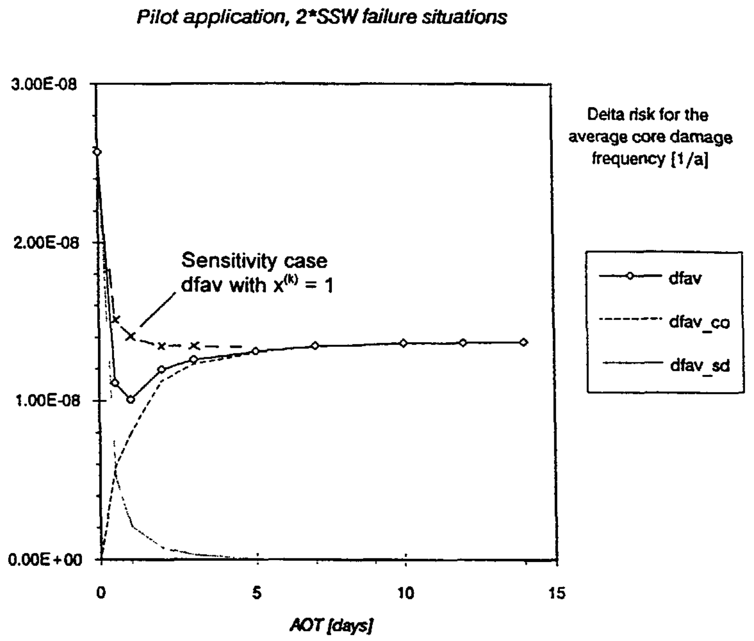


Figure 3. Delta risk - AOT correlation for the double failure case of SSW trains [1].

Usually, delta risk is small for a group of components, mostly about one percent or less in comparison with the total risk. However, the delta risk sum over all components covered by AOTs, may become significant, and need to be especially considered against acceptability criteria.

The delta risk - AOT correlation is rather sensitive in regard to calculation uncertainties, as will be discussed in more detail in Section 3. Futhermore, there may exist also indirect influences, which are harder to evaluate. For example, it could be expected that an AOT shorter than normally needed to complete the repair, may result in negative side effects, if faults are attempted to be repaired hastily in order to avoid plant shutdown.

3 KEY ISSUES OF THE METHODOLOGY

Main features of the developed methodology are summarised below. As a complement to earlier presentations, we will concentrate here on particular details of the delta risk - AOT correlation. A more complete methodology presentation is included in Refs.[1,3].

3.1 State modelling approach

The most essential methodological development is concerned with the use of Extended Event Sequence Diagram (EESD) for the description of event sequences, as a substitute for the traditional event tree/fault tree approach. EESD incorporates intermediate and stable process states as embedded. This enhances timedependent modelling of operational scenarios and recovery paths. The latter is viable for a realistic quantification of the decreasing risk (frequency) level while in zero power, due to diminishing decay heat production (prime motivation for a LCO shutdown). Fig.1 is a simple example of EESD, showing some flavours of the approach, especially the use of an embedded state (compare with the state block "Increased risk, full power state, 2 SSW trains under repair").

Connected with modelling process states and recovery paths, parallel modelling of process behaviour is necessitated such as the temperature behaviour of the suppression pool in a BWR plant, as this is an essential heat buffer allowing substantial time to recovery in case of RHR function is lost. Besides, developments have also been required in order to more consistently handle repair and recovery time distributions, specially in multiple failure situations where alternative recovery paths are available.

Existing PRA models are, however, of great support for an EESD based approach, both concerning the construction of event scenarios, and in modelling of system details.

3.2 Data requirements

Data input needed is to an large extent similar as in a PRA study. Additional, special data are required for the likelihood of disturbance transients during a controlled shutdown, and for the repair and recovery time distributions.

3.3 Influence of a preset AOT

A preset AOT evidently has an influence on the repair time distribution, especially when AOT is near to the mean repair time, because the operators are then certainly looking for possibilities to speed up repair arrangements in order to avoid plant shutdown. These possibilities include shortening the time spent to administrative tasks as well as giving a high priority to the critical repair while postponing possible other, less urgent works.

3.3.1 Influence onto repair time distribution

Influences observed in the early Finnish-Swedish DG study [4], are reproduced here as Fig.4. Based on these insights, the following influence model is developed [6]:

- quite soon after failure detection, the operators are able to determine the severity class of the repair
- severity class is described by an exponential repair time distribution, which to a certain extent covers the variability and uncertainty of repair time prediction
- under AOT constraint, the operators/maintenance staff are able to shorten the repair time to a specific fraction x, from the beginning if AOT is less than the mean time for the repair severity class, otherwise from the time point when the remaining AOT equals to the mean repair time

Nominally, fraction x = 0.5 has been used in sensitivity analyses.

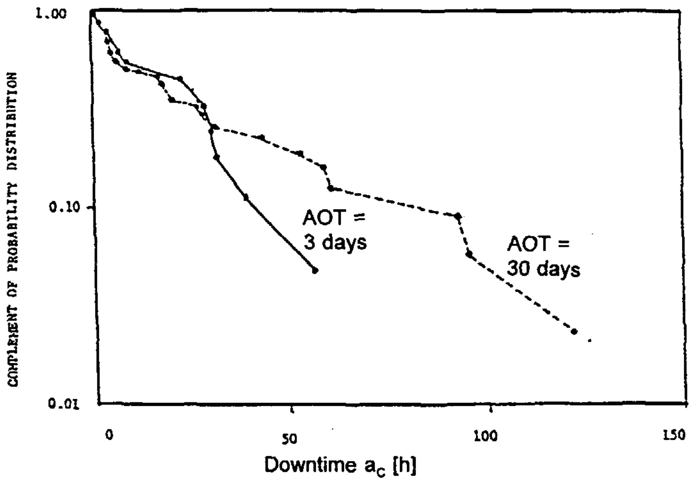


Figure 4. Effect of AOT on the down-time distributions for critical faults of diesel generators [7].

3.3.2 Delta risk - AOT correlation

The delta risk contribution *dfav*, for specific failure situations *X*, can be derived by the use of the following breakdown (compare with Figs.1 and 3)

$$dfav_X(AOT) = dfav\_co_X(AOT) + dfav\_sd_X(AOT) \qquad (2)$$

with

$$dfav\_co_X(AOT) = \lambda_X . [1 - pnr_X(AOT)] . rco_X(AOT)$$

$$dfav\_sd_X(AOT) = \lambda_X . pnr_X(AOT) . rsd_X(AOT)$$

$$rco_X(AOT) = P\{CoreD| \text{Initiating event occurs during full power repair state}\}$$

$$= \frac{\int_0^{AOT} da.fco_X(a).pnr_X(a)}{1 - pnr_X(AOT)} \qquad (3)$$

and

$rsd_X(AOT)$ = P{CoreD| Initiating event occurs during a controlled LCO shutdown or while in the cold shutdown repair state}

$$= \frac{\int_{AOT}^{\infty} da\ fsd_X(a)\ pnr_X(a)}{pnr_X(AOT)} \qquad (4)$$

where

λ_X = Rate of failure situations X

$fco_X(a)$ = Instantaneous risk frequency during full power repair state

$fsd_X(a)$ = Instantaneous risk frequency during a controlled LCO shutdown and while in the cold shutdown repair state

$pnr_X(a)$ = Complementary repair time distribution, i e probability of nonsuccessful repair up to time a

The risk is associated here to the core damage event CoreD, as usual in the PRA Level 1 considerations. An example of the calculated delta risk - AOT correlation is presented in Fig.3. Beside of the nominal repair reduction fraction x = 0.5, also the case of x = 1, i.e. no credit for repair speed-up, is shown.

It should be noted, that in some other applications, there is unrealistically assumed that given any AOT, it all will be used in every repair. This results in erroneous correlation between the delta risk and AOT. The stated assumption together with omitting shutdown risks, means that the delta risk would increase linearly as the function of AOT. A more detailed comparison is included in Ref.[6].

The consideration of AOT influence in this way was earlier presented by Kani, et.al.[8]. In our approach, the shutdown risk and repair time distribution of the initial failure state are more precisely quantified.

3.4 Sensitivities with regard to uncertainties

The uncertainties in the AOT considerations, and in the risk comparison approach described here especially, are similar to PRA studies and other risk-based applications. Additional difficulties may be connected to the specific modelling features and data requirements discussed in Sections 3.1-2: i.e. in obtaining probability estimates for disturbance transients, and repair or recovery time distributions.

Fortunately, in the AOT considerations using risk comparison approach, the relative results matter, and they are often to a large part not very sensitive in regard to uncertainties. For the part of important uncertainties, systematic sensitivity analysis can then be used in order to verify conclusions. An example of a typical sensitivity analysis is shown in Fig.5. In the upper bound alternative, the likelihood of disturbance trips in increased by a factor of 2, and in the lower bound alternative decreased by a factor of 3 This affects directly SD alternative, but CO alternative is insensitive (the three curves overlap in Fig.5). The crossing point moves, with a sensitivity range from about 3 days through 5 days, in this example case.

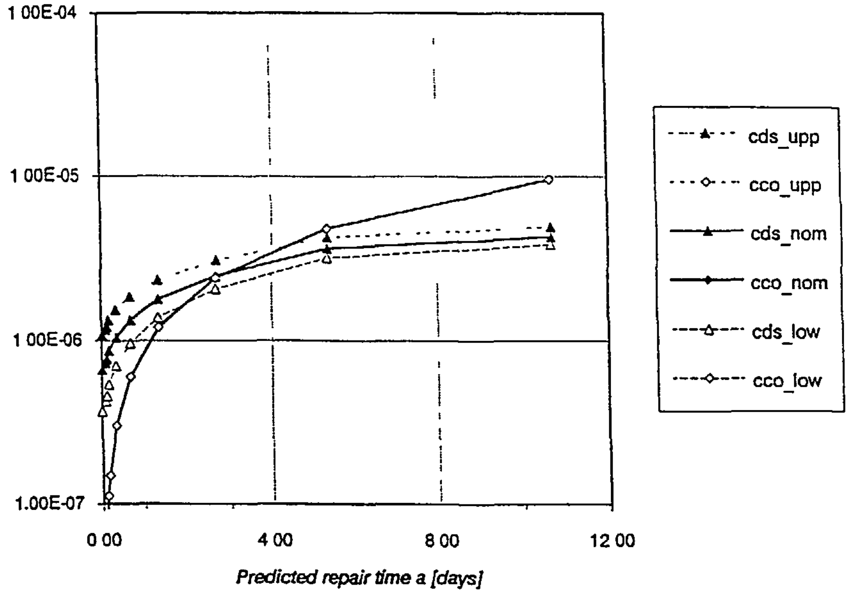


Figure 5. Sensitivity for the likelihood of disturbance transients in a controlled SD. Cumulative risk over predicted repair time in the double failure case of SSW trains is shown [1].

4 SUMMARIZING CONCLUSIONS

This kind of approach and methodology is needed in order to properly infer, how the predicted risk of the plant shutdown alternative compares with making repairs in full power operation state. It proves especially important when determining AOTs for the systems related to RHR function, because the plant shutdown with degraded RHR capability proves to be a substantial risk, based on the results from practical case studies this far.

Insights obtained lead also to suggestions about operational details of TS action statements. In many failure situations, the additional condition check or prior test of the redundant operation paths is recommendable for proper operational decisions. Also the timing and desired end state of the LCO shutdown (i.e., the state where to undertake the bulk work of repairs) may be better optimised.

Experiences show that the results of risk-based AOT considerations depend on many plant specific features, such as vulnerability to disturbance transients during a controlled shutdown, and the operational reliability of the systems to be used while in zero power state. It need hence to be emphasised, that the example results from the pilot study, shown here in order to illustrate the approach and methodology, should not be regarded generally applicable.

REFERENCES

1. Risk-based improvement of Technical Specification action statements requiring shutdown: Pilot application to the RHR/SSW systems of a BWR. Prepared for U.S. Nuclear Regulatory Commission by T. Mankamo, I.S. Kim and P.K. Samanta, to be published in 1993.
2. Mankamo, T. and Kosonen, M, Operational decision alternatives in failure situations of standby safety systems. IAEA Technical Committee Meeting on The Use of PSA to Evaluate NPP's Technical specifications, Vienna, 18-22 June 1990.
3. Mankamo, T. & Kosonen, M., Continued plant operation versus shutdown in failure situations of standby safety systems, application of risk analysis methods for the evaluation and balancing of AOTs for the RHR systems at TVO I/II plant. IAEA/TechSpec Pilot Study Programme, NKS/SIK-1(91)4, August 1991.
4. Vesely W. & Samantha P.K., Risk Criteria Considerations in Evaluating Risks from Technical Specification Modifications. Technical Report, BNL & SAIC, Draft, January 1989.
5. Optimization of technical specifications by use of probabilistic methods - a Nordic perspective. Final report of the NKA project RAS-450. Ed. K.Laakso. Prepared by a team consisting of K.Laakso, M. Knochenhauer, T. Mankamo & K.Pörn. Nord Series 1990:33, May 1990.
6. Work notes: Delta risk - AOT correlation. T. Mankamo, 25 June 1991.
7. Pulkkinen, U., Huovinen, T., Mankamo, T., Norros, L. & Vanhala, J., Reliability of diesel generators in the Finnish and Swedish nuclear power plants. Technical Research Centre of Finland, Report SÄH 7/82, June 1982. (Enhanced version published as VTT Research Notes 1070, 1989)
8. Hioki, K. & Kani, Y.,Risk based evaluation of technical specifications for a decay heat removal system of an LMFBR plant. IAEA Technical Committee Meeting on The Use of PSA to Evaluate NPP's Technical specifications, Vienna, 18-22 June 1990.

IMPACT OF SHUTDOWN RISK ON RISK-BASED ASSESSMENT OF TECHNICAL SPECIFICATIONS

S. DERIOT
Direction des études et recherches,
Electricité de France,
Clamart, France

Abstract

This paper describes the current work performed by the Research and Development Division of EDF concerning risk-based assessment of Operating Technical Specifications (OTS).

One of the objectives of the OTS is to determine what actions have to be taken when a component or set of components is unavailable. In France, many Allowed Outage Times (AOTs) have been evaluated a few years ago based on a probabilistic criterion used in agreement with French Safety Authorities: "the additional occurrence probability of a serious accident (leading to core melt) while the nuclear plant is operating at full power during the authorized time period, given the partial unavailability of the safety system, must not exceed 10^{-7} ".

In addition, EDF conducted the project PSA 1300 (level 1 Probabilistic Safety Assessment of the Paluel nuclear power plant). A computerized knowledge base called LESSEPS 1300, which is a set of reliability models, computation methods and computer tools, was developed in the framework of this project.

One of the main lessons of the PSA 1300 is that the shutdown states largely contribute to the core damage risk. As a result, the following question becomes relevant: does the shutdown really lead to minimizing the increase of risk due to the unavailability of a safety-related component ?

In the PSA 1300, the partial or total unavailibilities of safety systems are generally introduced in the form of a "balloon" (all the components rendered inoperable during maintenance) for which outage rate is calculated on the basis of feedback from operating experience on the Paluel power plants. By performing sensitivity studies to the outage rates associated with each balloon, LESSEPS 1300 allows to measure the "new" hourly risk in each reactor state.

A case study is presented. It shows that:

- a hot shutdown could be preferable (from a core melt probability point of view) to an intermediate shutdown with the Residual Heat Removal System valved-out, which is the most frequent safe shutdown condition,
- the increase of risk can be higher than 10^{-7} , whatever the present managements of the operations may be.

Therefore, taking into account shutdown risk suggests that the present OTS should be modified.

By considering different kinds of accidents in different reactor states, the PSA 1300 helps to determine not only the AOT, but also the "real" safe shutdown condition and the method for shutting down. The main outline of this new method for risk-based assessment of OTS is also presented.

1. INTRODUCTION

This paper describes the current work performed by the Research and Development Division of EDF concerning risk-based assessment of Operating Technical Specifications (OTS)

The current risk-based assessment of OTS at EDF is presented Then, the level 1 Probabilistic Safety Assessment of unit 3 of the Paluel nuclear power station (called PSA 1300) is described It is fully computerized and takes into account the risk in shutdown states

A case study is presented It shows that the fact of considering shutdown risk suggests that the current OTS should be modified.

2. CONTEXT

At EDF, one of the objectives of the OTS is to determine what actions have to be taken when a component or set of components is unavailable Many Allowed Outage Times (AOTs) have been evaluated a few years ago based on a probabilistic criterion used in agreement with French Safety Authorities "the additional occurrence probability of a serious accident (leading to core melt) while the nuclear plant is operating at full power during the authorized time period, given the partial unavailability of the safety system, must not exceed 10^{-7} " The AOT is the duration of time that the component or system can remain out of service before the plant has to shut down

Then, the AOT associated with the unavailability of a component or system can be calculated using the following relationship

$$\Delta\, \mathbf{R} \,.\, \mathbf{T} = 10^{-7}$$

where

Δ **R** is the increase in plant's core melt hourly risk as result of the unavailability of a component or system

T is the suggested AOT (in hours), which is afterwards debated between EDF and the safety authorities

Figure 1 describes this relationship

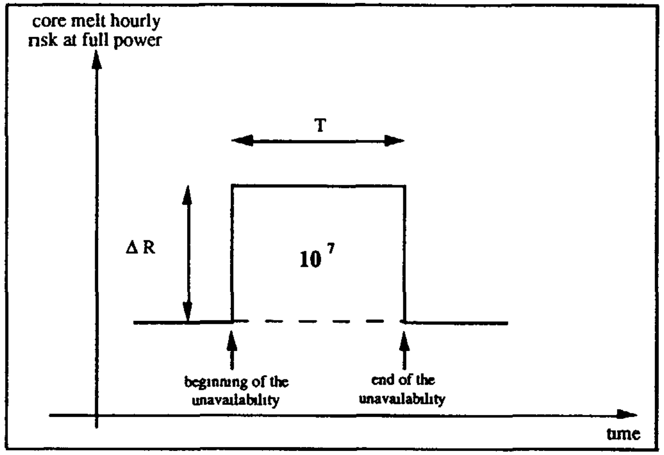


Figure 1

Since we consider the increase of risk as a result of the unavailability of a component or system in a reactor state (in this case, full power), <u>only the accidents relevant to this unavailability and this reactor state require to be studied</u>

3. PRESENTATION OF THE PSA 1300

EDF conducted the project PSA 1300 from 1986 to the end of 1989 (1) (2)

Two aims have been assigned to the PSA 1300 project

- evaluation of the probability of damage to the core of reactor unit 3 in the Paluel nuclear power plant, in all reactor states and with a degree of detail as high as possible,
- provision of a computer program for the performance of this evaluation, the LESSEPS software package, in order to produce a PSA with scope for development (3)

3.1 Operating profile

The analysis of the operational feedback made it possible to establish the average time spent in different unit states The reactor states defined for the PSA and the annual durations associated with them, are as follows

STATE	SUB-STATE	DESCRIPTION	TIME IN DAYS
state a		Operating point (pressure, temperature) above (P11, P12) (139b, 295°C at Paluel) which corresponds to the standard states	
	a1	- reactor in power, set coupled	268
	a2crit	- reactor critical, set not coupled	12
	a2sub	- reactor subcritical	15
state b		Operating point (pressure, temperature) between (P11, P12) and Residual Heat Removal System conditions (30b, 177°C)	2 (38 hours)
state c		Shutdown on RHRS, Reactor Coolant System (RCS) full, closed and vented	11
state d		RCS partially drained or open (conservatively, it is the state in which the level of the RCS is in the low work range of the RHRS and where there is minimum reactor coolant mass)	19
state e		Refuelling cavity full with at least one fuel element in the vessel	9

3.2 LESSEPS 1300

A computerized knowledge base called LESSEPS 1300 was developed in the framework of the project PSA 1300 It is a set of reliability models, computation methods and computer tools It comprises about 200 fault trees, 150 states graphs and 200 event trees (4)

The partial or total unavailabilities of safety systems are generally introduced in the form of a "balloon' (all the components rendered inoperable during maintenance) for which outage rate is calculated on the basis of feedback from operating experience on the Paluel power plant. By performing sensitivity studies on the outage rates associated with each balloon, LESSEPS 1300 allows the evaluation of the "new" annual risk in each reactor state If we divide by the annual durations spent in different reactor states, we could deduce the measure of the "new" mean hourly risk in each reactor state, given the unavailability

3.3 Limitation about the use of the PSA 1300 for OTS

Since the PSA 1300 is a level 1 PSA, only systems that take part in preventing core melt have been modelled This is the reason why the number of single unavailabilities relevant with respect to the use of the PSA 1300 is quite low The PSA 1300 is not useful at all for components that are only involved in containment or in the operability of the plant (e g , Containment Atmosphere Monitoring System, primary coolant pumps)

4. CASE STUDY

One of the main lessons of the PSA 1300 is the significant role played by shutdown states (which account for approximately 55% of risks) Then, the following question becomes important does the shutdown really lead to minimizing the increase of risk due to the unavailability of a safety-related component ?

The study of the long-term unavailability of a Medium-Head Safety Injection (MHSI) pump was carried out

NB. the results presented below do not include the results of the following accident sequence studies the total loss of heat sink and the total loss of emergency power supply, which have been updated recently, but which have not yet received approval

4.1 Description of the study

In the 'reference" calculation of the hourly risk in each reactor state, none of components is assumed to be in maintenance This is the reason why all outages have to be put to zero

However, the impact of outages on the results is almost negligible: for example, the risk at full power with the basic outages of the PSA 1300 is about 5.8E-10 /h, while the same one without any unavailability is about 5.6E-10 /h.

For each event tree, we calculate the hourly risk for all reactor states associated with this event tree.

Particular attention has to be paid to one dilution sequence. For this dilution sequence, the initiating event is the loss of the main electric power supply (leading to the loss of the primary pumps) during dilution related to the criticallity search after a shutdown.

This criticallity search occurs after a refueling shutdown, or after a hot shutdown or after a cold shutdown if it is the beginning of cycle. Its duration depends on the kind of shutdown. Then, the annual risk associated with this sequence depends on both the annual number and the kind of shutdowns. Moreover, the hourly risk due to this sequence is not the division of the annual risk by the annual duration of the state "reactor subcritical".

The hourly result of this sequence is then subtracted from the hourly risk in the state "reactor subcritical" and put aside.

Supposing the unavailability of a MHSI pump, and putting to one the outage rates associated with the balloon of the pump, a sensitivity calculation can be performed. Figure 2 shows the comparison of the results of the "reference" calculation with the results of this sensitivity study.

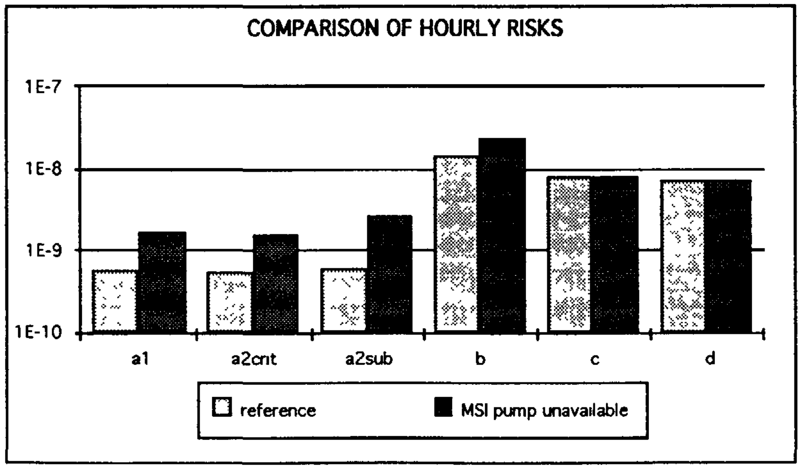


Figure 2

The AOT associated with the unavailability of a MHSI pump can then be calculated using the following relationship:

$$\mathbf{T = 10^{-7} / (R'_{a1} - R_{a1})}$$

where:

T is the suggested AOT

$\mathbf{R'_{a1}}$ is the hourly risk at full power, given the unavailability of a MHSI pump

$\mathbf{R_{a1}}$ is the hourly risk at full power without any unavailability

$$\mathbf{T = 10^{-7} / (1.67E\text{-}9 - 5.6E\text{-}10) = 90\ hours}$$

Thus, the AOT associated with the unavailability of a MHSI pump and calculated with the current method seems to be about 4 days.

Suppose that the failure of the MHSI pump requires 5 days to be repaired. The current safe shutdown condition is the intermediate shutdown with the Residual Heat Removal System (RHRS) valved-out (30b, 177°C). Figure 3 shows the distribution of the hourly risks in different reactor states and the evolution of the primary pressure when the current OTS are enforced. The specific sequence occurring during a phase of dilution is included; here, after a hot shutdown, the duration of this phase of dilution is about 2.5 hours.

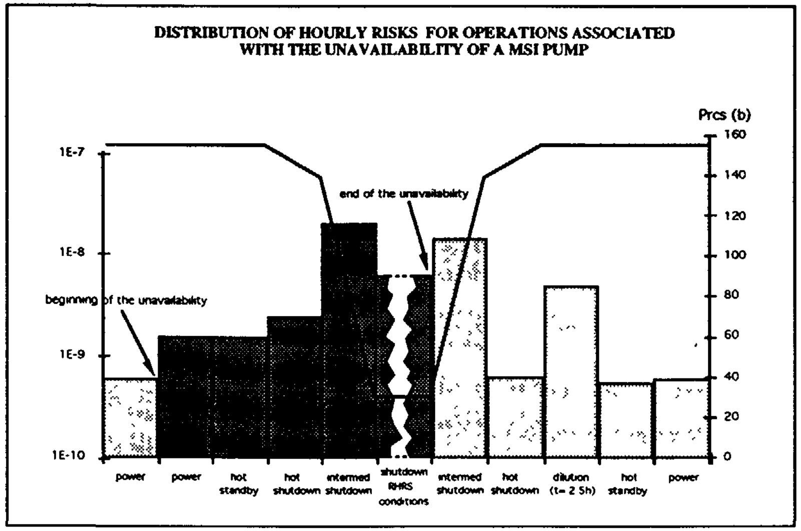


Figure 3

We can easily notice that, whatever the duration of the unavailability of the MHSI pump may be, the increase of risk associated with operating until the "safe" shutdown condition is far higher than that associated with remaining at full power or shutting down until hot standby. As a matter of fact, by operating until the intermediate shutdown:

- one denies oneself the automatic start-up of the Safety Injection System (SIS) for most of LOCAs, even if this system is partially unavailable;
- one increases the frequency of the accident for which the unavailable component is principally designed, because the isolation valves on the relief lines of pressurizer are forced open.

4.2 Discussion about results

The PSA 1300 was conducted in order to evaluate the probability of damage to the core per unit and per year. Thus, some conservative assumptions were kept because they had no impact on the annual probability. Here, for risk-based assessment of OTS, we argue about hourly risks. This is the reason why some of those assumptions have had to be reviewed.

Concerning the case study, the main assumptions are the following ones:

- The rate of primary breaks per hour has been assumed to be equal to that applied at the nominal temperature and pressure. Although this might seem to be a conservative estimate, most breaks are caused by erosion or corrosion, and are more likely to arise under transient conditions than under normal operating conditions. In this respect, there has been no proof that failure rates are substantially lower at low pressure or low temperature than under nominal conditions.

- The success criteria of SIS for a small LOCA are the same during the whole intermediate shutdown; while in the intermediate shutdown state with the RHRS valved-out, one MHSI pump is not absolutely necessary to mitigate a small LOCA: one out of the four safety injection pumps (low-head or medium-head) is adequate to prevent core damage. Therefore, the failure probability of SIS in the safe shutdown condition is lower than in the rest of the intermediate shutdown state.

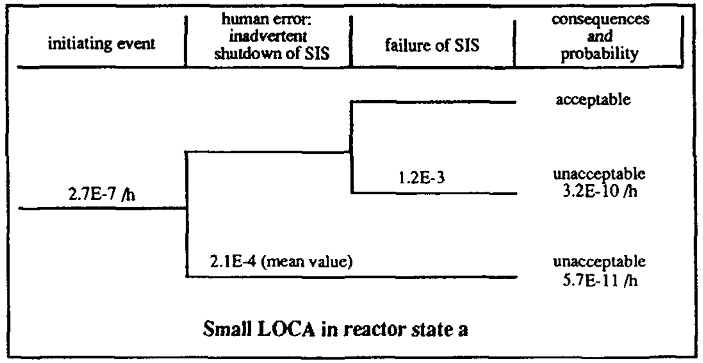
- The time t after which the operators have to start-up the safety injection system in response to a break in a steam line of the pressurizer was assumed to be unique in the whole intermediate shutdown state (i.e., the minimal time corresponding to the upper part of the intermediate shutdown state). Therefore, the probability p of this operator error is lower in the intermediate shutdown state with the RHRS valved-out (30b, 177°C: t=2h and p=1.4E-3) than at the upper part of the intermediate shutdown state (139b, 295°C: t=1h and p=4.2E-3).

The previous distribution of hourly risks takes into account the modifications concerning the last two assumptions, which are related to the construction of reliability models.

4.3 Towards a new management of operations ?

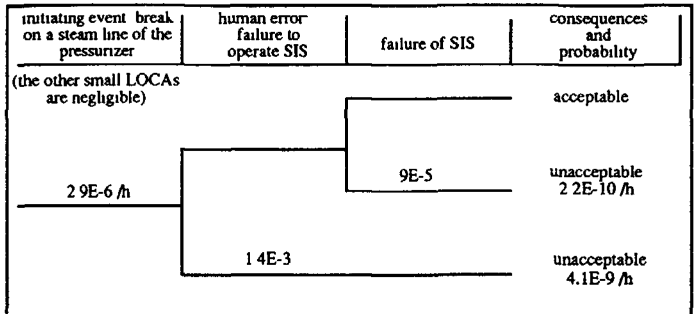
For the long-term unavailability considered (5 days), and whatever the current managements of the operations may be (i.e., remaining at full power or shutting down until 30b), the probabilistic criterion of 10^{-7} cannot be respected. The solution could be a change in the way of shutting down.

Using very simplified event trees, let us compare the accident "small LOCA" in the "safe" shutdown condition and in reactor state a, given the unavailability of a MHSI pump:



Small LOCA in reactor state a

Adding breaks on a steam line of the pressurizer, the overall risk related to a small LOCA in reactor state a is about 4.2E-10 /h.


initiating event break on a steam line of the pressurizer
human error failure to operate SIS
failure of SIS
consequences and probability
(the other small LOCAs are negligible)
acceptable
2.9E-6 /h
9E-5
unacceptable 2.2E-10 /h
1.4E-3
unacceptable 4.1E-9 /h

Small LOCA in the safe shutdown condition (30b, 177°C)

The overall risk related to a small LOCA in the intermediate shutdown state with the RHRS valved-out is about 4.3E-9 /h. It is higher than at full power, although the reliability of SIS is better.

Supposing that a Low-Head Safety Injection (LHSI) pump was manually started-up as soon as the reactor is in state b. The risk in the "safe" shutdown condition due to the accident "small LOCA" would be approximately of the order 10^{-10} /h. This new management of operations would permit.

- to avoid the non-automatic start-up of SIS,
- to profit by the redundancy of the four safety injection pumps.

Thus, the intermediate shutdown state with the RHRS valved-out would be the "real" safe shutdown condition.

4.4 Comparison between the different managements of operations

The duration of the unavailability of the MHSI pump is supposed to be 5 days.

The increase of risk associated with remaining at full power is

$$S_1 = (R'_{a1} - R_{a1}) \, 120$$

where

R'_{a1} is the hourly risk at full power, given the unavailability of a MHSI pump

R_{a1} is the hourly risk at full power, MHSI pump available

120 is the duration of the unavailability in hours

$$S_1 = 1.3E\text{-}7$$

The risk associated with operating until the return to the initial state (and through the current "safe" shutdown condition) is.

$$S_2 = \Sigma_i \, R'_i \, t_i \; + \; \Sigma_j \, R_j \, t_j \; - \; R_{a1} \; (\, 120 + \Sigma_j \, t_j \,)$$

where

i is the reactor state from power until the safe shutdown condition

R'_i is the hourly risk in state i, given the unavailability of the MHSI pump

t_i is the duration of time in state i

j is the state from the safe shutdown condition (not included) to return to power

R_j is the hourly risk in state j, MHSI pump repaired

t_j is the duration of time in state j

The calculation gives $S_2 = 8.5E\text{-}7$

As was planned in figure 3, the current management is not the best one.

Supposing that one LHSI pump was manually started-up as soon as the reactor is in state b. Another calculation gives the increase of risk associated with this arrangement: it is about 1E-7 We can notice that the gain (with regard to remaining at full power) is not very important for this duration of the unavailability of a MHSI pump. This is due to the risk during the transient states. The gain would be higher for a longer duration of the unavailability.

5. CONCLUSION

This paper is aimed at demonstrating that the PSA 1300, which is fully computerized and which takes into account risk in shutdown states, is a powerful tool for risk-based assessment of Operating Technical Specifications (OTS)

The PSA 1300 emphasized the importance of risk in shutdown states The current design of reactor units is, in fact, based on the premise that there will be little risk arising in shutdown states Consequently, the majority of analyses carried out and design considerations adopted for systems and automatic equipment have been based on reactors under operating conditions It is therefore essential to consider the increase of risk associated with operating from the occurrence of the unavailability of a component until the return to initial condition People involved in PSA area become more and more aware of this necessity (5) (6)

The computerized PSA represents an overall view of safety of the plant, and not a "system view" of safety. When we consider the increase of risk at full power, only the accidents at full power impacted by the partial or total unavailability of a safety system require to be studied. But it becomes essential to take into account all the accidents when we consider a change of reactor state. For example, considering the unavailability of a diesel generator and the accidents impacted by this component, i.e., essentially station blackout, the "safe" shutdown condition seems to be the intermediate shutdown. Thus, we "forget" that the unit is, in this reactor state, quite vulnerable towards primary breaks. The computerized PSA does not "forget"...

Thus, it appears that a risk-based assessment of OTS has the potential to better control plant operational risk compared to a deterministic assessment. Nevertheless, it is necessary to remain modest: there are many factors, physical and operating, that a purely probabilistic approach cannot take into account. Moreover, the use of this tool is confined to a limited number of safety components.

In this paper, a new method, developing at Electricité de France, for risk-based assessment of OTS has been presented through a case study. The main outlines of this method are an evaluation of the core melt hourly risk (due to all types of accidents) in different reactor states and an interpretation of results. It can help to determine not only the Allowed Outage Time, but also the "real" safe shutdown condition and in some cases the way of shutting down. However, some improvements in the reliabilistic models in shutdown states have to be made.

REFERENCES

(1) Villemeur, A., Berger, J.P., Dubreuil-Chambardel, A., Moroni, J.M., "Living Probabilistic Safety Assessment of a French 1300 PWR NPP Unit: Methodology, Results and Teachings", 2nd TÜV-Workshop on Living PSA Application, Hamburg, 7th-8th May, 1990.

(2) Berger, J.P., Villemeur, A., De Guio, J.M., "PSA 1300; Results and Future Prospects", International Symposium on the Use of Probabilistic Safety Assessment for Operational Safety, PSA'91, Vienna, Austria (3-7 June 1991).

(3) Ancelin, C., Lucas, J.Y., Magne, L., Bouissou, M., Molinero, J., "LESSEPS or a Computerized Management of Reliability Studies", 7th International Conference Reliability & Maintenability, Brest, France (June 1990).

(4) Ancelin, C., Dubreuil-Chambardel, A., "From LESSEPS 1300 to the Application of Computerized PSAs to Operational Safety", International Symposium on the Use of Probabilistic Safety Assessment for Operational Safety, PSA'91, Vienna, Austria (3-7 June 1991).

(5) Sandstedt, J., Berg, U., "Living-PSA Applications for a Swedish BWR with the Aid of RISK SPECTRUM", 3rd TÜV-Workshop on Living PSA Application, Hamburg, 11th-12th May, 1992.

(6) Nakai, R., "Application of a Living PSA system to LMFBR", 3rd TÜV-Workshop on Living PSA Application, Hamburg, 11th-12th May, 1992.

REFUELLING PSA FOR TVO I/II

J PESONEN, R HIMANEN, H SJOVALL
Teollisuuden Voima Oy,
Olkiluoto

P PYY
Technical Research Centre of Finland,
Espoo

Finland

Abstract

The utility TVO is conducting a comprehensive PSA programme for its two 710 MWe BWRs The programme was initiated by the utility in the year 1984 and the level 1 PSA was taken into living use in 1992 including internal transients LOCAs and fires during power operation
In the year 1990 the utility decided to extend the PSA study by the analysis of refuelling, shut down and start up One reason for the decision was the good operating experience of both units They have continuously exceeded 90 per cent annual capacity factor due to short and effective refuelling outages and suffered only a few unplanned shut downs
The Shut-down event PRA (SePRA) required development and application of new methods because the human factors are the main contributor both to the initiating events and the loss of safety functions The few studies published were used as a starting point for SePRA The SePRA team consists mainly of the utility´s own personnel completed with an external human error specialist

A remarkable effort was put to reveal risks, i e , to the qualitative analysis The regular preventive maintenance tasks in refuelling outages were analyzed and the important tasks were selected for further studies SePRA team´s view is that this is the only way to guarantee adequate comprehensiveness of the results Besides the severe nuclear risks the utility was interested in the economic risks causing significant extension of outages
The plant specific screening of initiators consisted of a study on the incident history and of interviewing the plant personnel on selected tasks The incident statistics mainly from Olkiluoto and quasi similar ABB delivered plants were classified according to a draft initiator list The list was later used in the assessment of initiator frequencies The operating experience from other BWRs received, e g , from NEA/IRS reports was found to be less useful due to different design of the plants

The qualitative analysis produced three types of initiators LUCs Leakages Under Core top LOCs Leakages Over Core top and LRHRs Loss of Residual Heat Removal Apart from these, special studies were carried out for the unwanted local criticality events for the over-pressurisation of the reactor when steam lines filled with water for the heavy load transportation in the reactor hall and for the transients during short periods with not inerted containment The annual core damage risk from the refuelling outage is of the same order of magnitude as the risk from the power operation The dominant risks ranked by SePRA were decreased in several ways For example the preparedness to close the lower personnel access during the main circulation pump overhaul was increased by two specially trained guards The modifications decreased the core damage frequency during refuelling by about 70 per cent It is foreseen that the SePRA will form a basis of the procedure enhancement for the low power states

1 Introduction

Teollisuuden Voima Oy (TVO) operates two 710 MW ABB Atom type BWR units on the west coast of Finland TVO I was connected to the national grid in 1978 and TVO II in 1980
The utility is conducting a comprehensive PSA programme for its two plants /1/ The programme was initiated by the utility in the year 1984, and the level 1 PSA was taken into living use in 1992 /2/ including internal transients, LOCAs and fires during power operation In the year 1990 the utility decided to extend the PSA study by the analysis of refuelling, shut down and start up One reason for the decision was the good operating experience of both units They have continuously exceeded 90 per cent annual capacity factor due to short and effective refuelling outages and suffered only a few unplanned shut downs Conducting the refuelling in almost in minimum time requires tight coordination between parallel activities going on in three shifts During the refuelling period numerous subcontractors, overtime and reduced safety barriers on the plant itself are assumed to be risk increasing factors The Shut down event PRA (SePRA) required development and application of new methods because the human factors are the main contributor both to the initiating events and the loss of safety functions The few studies published were used as a starting point for SePRA, e g , /3, 4/ The SePRA team consists mainly of the utility´s own personnel completed with an external human error specialist
SePRA consists of operating modes lower than 8 % of nominal power These operating modes are

1 Cold shut-down	(reactor unpressurized, T < 100 °C)
2 Hot shut-down	(reactor pressurized or T > 100 °C)
3 Start-up	(reactor pressure < 70 bar)
4 Hot standby	(reactor pressure 70 bar)
7 Refuelling	

The time duration for these modes has been evaluated as average value through years 1986-92, which correspond best at the present state Average refuelling duration is about 400 hours

2. Main tasks

SePRA was made according to the project plan and procedure /5/ written by the utility and accepted by the Finnish regulatory body (STUK) Project was started in May 1990 and it will be completed in autumn 1992 The total work done is about 3 man years The main tasks are in the project are as following

2 1 Background material collection

The background material collection included documents, which are needed in different tasks during refuelling, for example TVO´s operation, test and maintenance procedures, time tables for refuelling etc

2.2 Assessment of operation experience

The plant specific screening of initiators consisted of a study on the incident history and of interviewing the plant personnel on selected tasks. The incident statistics mainly from Olkiluoto and quasi similar ABB delivered plants were classified according to a draft initiator list. The list was later used in the assessment of initiator frequencies. The operating experience from other BWRs received, e.g., from NEA/IRS reports was found to be less useful due to different design of the plants.

2.3 Analysis of operational, test and maintenance procedures

The utility's maintenance specialists skimmed through the regular preventive maintenance tasks in refuelling outages and selected 16 groups of tasks to be further studied by interviewing techniques. A thorough step by step analysis of each task was performed using a structured questioning form called the 'Human Action Deviation Analysis' (HADA). Special attention was paid to potential confusion of certain task steps and of different tasks, to ways to detect the deviations, to consequences and to remarks mainly dealing with difficulties in the coordination and with possible measures to reduce the risks. Another questioning technique called the 'Analysis of Test Influence' (ATI) was developed for the analysis of tests. Apart from the points included in the HADA, the ATI technique emphasises also the overriding of safety device, the restoration process and the completeness dimension of a test. A remarkable effort was put to reveal risks, i.e., to the qualitative analysis. The SePRA team's view is that this is the only way to guarantee adequate comprehensiveness of the results.

2.4 Determining initiating events, event trees, success criteria and modelling

Besides the severe nuclear risks the utility was interested in the economic risks causing significant extension of outages. Therefore six plant damage states were defined:

1) Mechanical fuel damages
2) Local criticality
3) Overheating of concrete constructions
4) Core uncovery
5) Spent fuel uncovery
6) Severe core damage.

The qualitative analysis produced three types of initiators: LUCs Leakages Under Core top, LOCs Leakages Over Core top and LRHRs Loss of Residual Heat Removal. External initiators were not included to the analysis at this stage. The LOCs and LUCs were divided into five classes according to the compensating water pump capacity available, see Table 1. Physical analyses were made for determining the mass flow of water in different type of leakages.

Table 1. Classified leakage diameters (LUC's and LOC's).

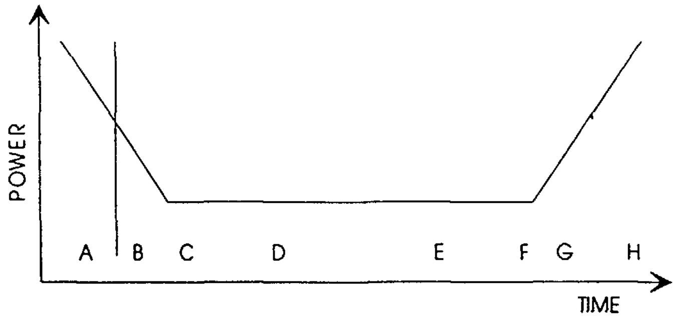
	Leakages under core (LUC)
LUC0	140 mm < D < 198 mm
LUC1	89 mm < D < 140 mm
LUC2	59 mm < D < 89 mm
LUC3	42 mm < D < 59 mm
LUC4	D < 42 mm
	Leakages over core (LOC)
LOC0	234 mm < D < 332 mm
LOC1	149 mm < D < 234 mm
LOC2	100 mm < D < 149 mm
LOC3	70 mm < D < 100 mm
LOC4	D < 70 mm

Available systems for supporting water inventory in the reactor and fuel pools as compensating water are presented in Table 2.

Table 2. Additional water capacity.

System	Total capacity kg/sec	Reservoir capacity without additional water 10^3 kg
323, core spray system	4 x 125	1700
327, auxiliary feed water system	4 x 22,5	900
861, firewater system	100	2500
733, demineralized water system	5 + 60	420 - 570

The LRHRs were classified according to the required compensating decay heat removal capacity. Fig.1. illustrates different stages for residual heat removal during low power operation and refuelling. Shut-down cooling system and pool cooling system are available for residual heat removal. Shut-down cooling system is used in the beginning of refuelling. Pool cooling system has been modified more efficient by adding extra heat exchanger line. This enables taking of pool cooling system earlier in operation, about for days after shut-down and to begin the maintenance of shut-down cooling system .



A = Plant shut-down, power operation PSA
B = Plant shut-down, low power operation, (LRHR0)
C = Refuelling, pool cooling not available, (LRHR1, LRHR1a)
D = Refuelling, decay heat production high, (LRHR2, LUCs and LOCs)
E = Refuelling, decay heat production lower, (LRHR3)
F = Refuelling, pool cooling not available, (LRHR1)
G = Plant start up, low power operation, (LRHR4)
H = Plant start up, power operation PSA

Fig 1 RHR stages dunng low power operation and refuellmg

The decay heat rate, the configuration of the safety systems and the potential to loss the safety systems vary in the course of the refuelling outage Therefore the low power period was divided into sub phases and the safety function success cntena were defined for each of them The low power incidents allow enough time for manual operations and thorough planning of recovery actions with only some exceptions· In case of largest possible LUCs during the Primary Circulation Pump overhaul there is less than one minute time to close the lower containment personnel access

The SePRA initiating event frequencies are low, see Table 3, when compared with transients in power operation mode but the weaker safety barriers cause a less narrow safety marginal, too Initiators for LUC1 and LUC2 were not identified

Apart from these, special studies were carried out for the unwanted local criticality events, for the overpressurisation of the reactor when steam lines filled with water, for the heavy load transportation in the reactor hall and for the transients during short periods with not inerted containment

Event tree technique was used for leakages under and over core and losses of residual heat removal Similarly, the explicit modelling of, e g , the sequences leading to unwanted local criticality required different modelling perspective

Table 3

Leakages under core	Code	Frequency (1/a)
	LUC0	1 8 E-6
	LUC1	
	LUC2	
	LUC3	4 9 E-4
	LUC4	3 3 E-3
Leakages over core	**Code**	**Frequency (1/a)**
(H)	LOC0	2 4 E 4
(H)	LOC1H	5 5 E 3
(L)	LOC1L	2 0 E-3
(H)	LOC2H	3 1 E-2
(L)	LOC2L	4 0 E 3
(H)	LOC3	2 4 E-4
(H)	LOC4	8 7 E-4
Loss of residual heat removal	**Code**	**Frequency (1/a)**
	LRHR0	4 7 E-2
	LRHR1a	2 9 E 2
	LRHR1	1 2 E-2
	LRHR2	3 6 E-2
	LRHR3	6 4 E-2
	LRHR4, includes to LRHR0	

H = leakage over 2 2 m of core grid
L = leakage under 2 2 m of core grid

Task interaction matrix was used to identify coordination errors and to manifest their risk contribution Its is similar to the confusion matrix approach but the thinking is extended to maintenance tasks Barrier model illustrates the differences in the safety barriers during different plant operational modes In the refuelling outage the human initiated safety function is often the only barrier while neither containment nor automated functions do exist
Chronological phase diagram can be used to illustrate explicitly latent error sequences and accelerating event courses /6/ Physical parameters and real time scale can be used at the same image to clarify the situation The diagram was utilised in the analyses of unwanted criticality events, see Fig 2 Method is still under development

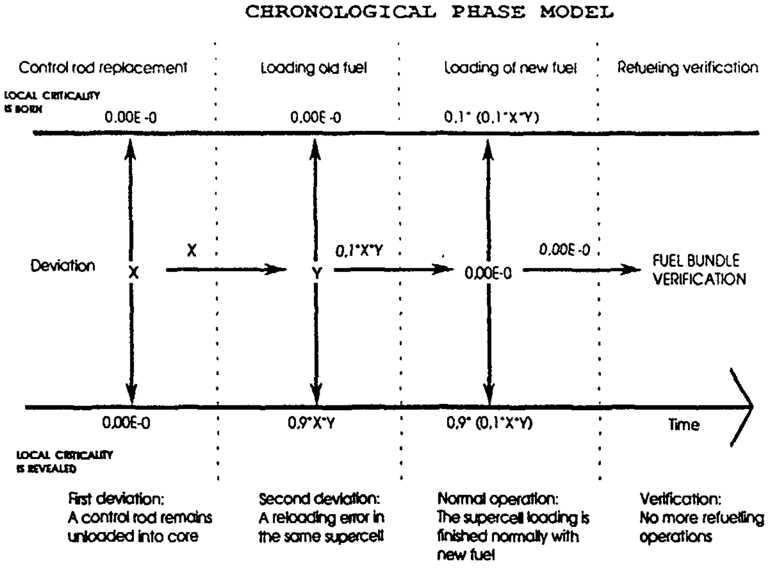

CHRONOLOGICAL PHASE MODEL
Control rod replacement
Loading old fuel
Loading of new fuel
Refueling verification
LOCAL CRITICALITY IS BORN
0.00E -0
0.00E -0
0.1* (0.1*X*Y)
Deviation
X
X
Y
0.1*X*Y
0.00E-0
0.00E -0
FUEL BUNDLE VERIFICATION
0.00E-0
0.9*X*Y
0.9* (0.1*X*Y)
Time
LOCAL CRITICALITY IS REVEALED
First deviation: A control rod remains unloaded into core
Second deviation: A reloading error in the same supercell
Normal operation: The supercell loading is finished normally with new fuel
Verification: No more refuelling operations

Fig. 2. Chronological phase model.

2.5 System analysis and fault tree modelling

The main difficulty encountered in the drafting of event tree models was the lack of written emergency procedures for refuelling period. Fault trees made for power operation were used as starting point for modelling. However extensive modifications were required before linking in low power operation event trees, because their initial conditions and use are different in shut-down state. For example, stand-by systems may be already operating in a RHR state and nearly all the automated functions are overridden. These observations led to an extensive modification of system models. Also the CCF model of 4-train systems with 2 trains prohibited during refuelling requires further investigation.

2.6 Reliability data

Human reliability data was based on operating statistics and engineering judgement. Unfortunately, the plant simulator does not give opportunities for large scale utilisation in a refuelling state and cannot be used to generate human deviation probabilities. Thus, the idea was to use plant specific historical data, when available, and subjective consistent screening values. The principle was followed when assessing human action probabilities for both initiating events and for recovery actions.

For each quantified human act, a verbal description highlighting those performance shaping factors mostly affecting the case is provided. The background of the used estimate can, thus, be in each case checked and argued. This is an important aspect that should be included in every human error analysis.

Equipment failure rates are based mainly on the same source (T-Book) /7/ as power operation. The T-Book contains plant spesific data of TVO NPP.

2.7 Quantitative analysis

Small event tree - large fault tree technique was used to describe and calculate desired sequences. Altogether 15 event trees were made, three for leakages under core l, seven for leakages over core and five for losses of residual heat removal. Sensitivity and uncertainty studies are not yet finished. The SPSA /8/ code on PC (386) is used for calculations.

2.8 Analyzing the results, modifications, reporting

The human deviations dominate all other initiating event classes, except the small LOC. The annual core damage risk from the refuelling outage is of the same order of magnitude as the risk from the power operation. The dominant risks ranked by SePRA were decreased in several ways. The preparedness to close the lower personnel access during the main circulation pump overhaul was increased by two specially trained guards. Mechanical cotter pin was installed at the main circulation pump propeller plugs to prohibit inadvertent lifting of the plug. The use of auxiliary feed water piston pumps for reactor filling is no more recommended to prohibit cold overpressurization. Pool cooling capacity was increased, capping of S/R-valves was given up and the inspection routine of control rods was modified in parallel with the SePRA but initiated earlier. The modifications decreased the core damage frequency during refuelling by about 70 per cent. The final report of refuelling is in preparation and it will be finalised in the end of September 1992.

3. Conclusions

The Shut-down event PRA (SePRA) study has contributed to the reassessment of outage safety level at the TVO NPP. The study demonstrates the position of human actions, which form the largest accident sequence initiator group. Since there are very few automated safety systems for an outage, the human action forms an important part of barriers between an initiator and unwanted consequences. The results of the PRA study have already resulted in actions and they may further lead to procedural changes and completition of the shutdown TechSpecs.

REFERENCES

/1/ Himanen, R Toivola A , PRA Program on NPP TVO PSAM, Los Angeles, February 1991

/2/ Himanen, R , Vaurio, J , Virolainen, R Introduction of Living PSA in Finland - Cooperation between Utilities and Authorities 3rd TuV-Workshop on Living PSA Application, Hamburg, May 1992

/3/ Kiper & al , Seabrook Station Probabilistic Safety Study Shutdown (Modes 4, 5, and 6) New Hampshire Yankee, May 1988

/4/ Brisbois & al , Probabilistic Safety Assessment of French 900 and 1,300 MWe Nuclear Plants Revue Général Nucléaire, International Edition - Vol B - December 1990

/5/ Himanen, R , Project Procedure for SePRA (in Finnish), Teollisuuden Voima Oy, 1990

/6/ Pyy, P , Human Factors in Scheduled Production Outages, 7th Symposium in Loss Prevention and Safety Promotion in the Process Industries, Taormina, Italy, May 1992

/7/ ATV-kansliet, Studsvik AB, Tillförlighetsdata för komponenter i nordiska kraftreaktorer (in Swedish)

/8/ I Niemela, STUK living PSA code (SPSA), International Symposium of Use of Probabilistic Safety Assesment for Operational Safety, PSA'91, Vienna 3-7 June 1991

PSA APPLICATIONS ON A SWEDISH BWR WITH THE AID OF RISK SPECTRUM

J SANDSTEDT
RELCON AB,
Solna, Sweden

Abstract

This paper describes a part of the work conducted within the joint Nordic project "Safety Evaluation, NKS/SIK-1" The project deals with Living PSA (LPSA) and Safety Indicators

An LPSA model has been developed for the Oskarshamn 2 BWR, and the PSA software Risk Spectrum has been used to build the event tree and fault tree models and to perform all calculations This LPSA model has been used in several different applications

- Risk follow-up with the operating year 1987 as an example
- Evaluation of Allowed Outage Times (AOT) and comparison with existing Limiting Conditions of Operation (LCO)
- Evaluation of test intervals and comparison with existing Technical Specifications (TS)

The different applications are described including assumptions, methods and results

The results show that the LPSA methods are useful within the application areas that have been studied

In all types of LPSA applications, the following items have been found to be important

- The completeness and realism of the model and data are very important, much more so than in regular PSAs
  The software is very important for the possibility to perform the calculations involved in various applications It must allow modifications of model and data that reflects the changes in plant configuration and status and it must be sufficiently powerful to allow calculations within a reasonable time frame and without simplifications that could invalidate the results

1 INTRODUCTION

This report describes a part of the work conducted within the joint Nordic project Safety Evaluation NKS/SIK 1" The project deals with Living PSA (LPSA) and Safety Indicators

Under a contract with the Swedish Nuclear Power Inspectorate (SKI) and OKG (the utility), RELCON has developed a plant specific LPSA model for the Oskarshamn 2 BWR using the existing level 1 PSA as a basis This LPSA model has been used in conducting several application studies These applications are

- Risk follow-up
- Evaluation of allowed outage times
- Evaluation of test intervals

The report consists of the following parts

- Description of the LPSA model (section 2)
- Presentation of the different applications (sections 3-5)
- Description of model limitations (section 6)
- Conclusions and recommendations (section 7)

2 MODEL DESCRIPTION

The following description deals only with the modifications and additions that have been made in the LPSA model compared to the normal PSA model

2.1 THE EXTENT OF THE MODEL

The extent of the LPSA model is roughly the same as for the normal PSA model The model is developed with the aid of the PSA software Risk Spectrum PSA /1/

The initiating events considered are LOCAs, transients and inadvertent isolations For each initiating event, an event tree has been developed The function events of the event tree are directly connected to fault trees in the Risk Spectrum model, which allows direct evaluation of sequences by the fault tree linking method

The system level modelling is somewhat more comprehensive than in a regular PSA model The main reason for this is to remove unnecessary conservatism due to model simplifications, and thereby creating a more realistic model also for cases where components are already out of service

Each system is modelled by a single system fault tree These "generic" system fault trees include house events (also called boundary conditions in Risk Spectrum), which can be used to modify the fault tree logic for different situations These house events are, e g , used to activate variations of the system fault tree to be used for different initiating events They are also used to "switch in and "switch out" components or trains in a system to model different system configurations pipe alignments etc The house events and the way thev can be controlled in Risk Spectrum makes it possible to build very flexible fault tree/event tree models where it is easy to "trigger" a particular set of house events to reflect a particular plant configuration a particular initiating event etc

2.2 SPECIFIC MODELLING IN THE LPSA

The models that are used in the regular PSA need to be modified to take into account the possibility to change system configurations The following sections describe the model modifications made on the component, system, and initiating event levels, respectively

2.2.1 Component Level Modelling

The component models in the LPSA should take into account the effect of various types of events and actions such as tests, actual demands, failures and maintenance

<u>Tests</u>

Tests are made to verify the operability of components, sub-systems or systems A test will reveal the failures that have occurred after the last time the component was operated To model the unavailability of periodically tested stand-by components, the following model is used

$$q(t) = q_0 + 1 - \exp(-\lambda_{sb}*(t-t_{lt}))$$

$q(t)$	=	Unavailability for periodically tested component
q_0	=	Time-independent failure probability per demand
λ_{sb}	=	Stand-by failure rate
t_{lt}	=	Last test moment

The unavailability thus has one time-dependent part, and one part which is independent of time The unavailability immediately after a test is equal to the time-independent part, q_0

The failure data used in the study are mainly taken from the "T-Book", the Reliability Data Book for Nordic Nuclear Power Plants /2/ The data in this reference are estimated to fit to a model such as the one described above

A simplification in this model is that the test efficiency is assumed to be 100% (i e all failures are revealed by the test) This is not entirely realistic, but another assumption would make the model more complicated and there is also a lack of data regarding test efficiency

In the Risk Spectrum model the periodically tested components are modelled by "Reliability model 4 (fixed mission time) where the parameter TM (mission time) is used to represent the time since last test It should be noted that this type of modelling is used because it provides a simple way of implementing a parameter that directly represents time since last test Normally in Risk Spectrum there is another special model for periodically tested components

To prepare for a quantification of core damage frequency (CDF) at a particular time point the time since last test has to be specified for all tested components (or rather for the basic events representing those components) This may seem to be an extensive task but the parameter treatment in Risk Spectrum makes it relatively easy to carry out such a change The components (basic events) are grouped if they are always tested at the same time (e g if they are in the same train) All of the basic events in the same "test group" are assigned the same TM parameter To change the time since last test for the group, only one parameter needs to be changed, instead of updating many individual basic event data sets

In a regular PSA, periodically tested components are often modelled with a constant (average) unavailability The advantage with the time-dependent modelling is that effect of tests can be evaluated in any given situation

Actual Demands

An "actual demand" means that the components/systems are activated to fulfil a mission It could be the intermittent, but completely normal, operation of a cooling system or the operation of a safety system after the occurrence of transient in the plant.

The actual demands are credited as tests of systems and components in the LPSA model. This provides for a realistic modelling of intermittently operating systems and for systems where the configuration is changed periodically

The probability of failure during operation after a transient - must also be considered for stand-by components to make the model realistic This probability is calculated according to the following formula

$$q = 1 - \exp(-\lambda_m * TM)$$

q = Probability of failure during operation
λ_m = Failure rate in operation
TM = Mission time

Failures and Maintenance

In LPSA applications there is often a need to model failed components

For components modelled with a time independent probability per demand, the probability is set to 1, in risk follow-up applications for the entire time period the component has been unavailable (or has been assumed to be unavailable) This is normally the time interval from last successful test until completed repair

For components modelled with a time dependent unavailability the unavailability is calculated according to the following formulas in risk follow up applications

$$q(t) - \frac{q_0 + 1 - \exp(-\lambda_{sb} * (t - t_{ll}))}{q_0 + 1 - \exp(-\lambda_{sb} * TI)}$$

q(t) = Probability of an existing failure
q_0 = Probability per demand
λ_{sb} = Stand by failure rate
t_{ll} = Time since last test
TI = Test interval

For risk monitoring/risk control applications failures are modelled by setting the probability to 1 for the time period the failure has been known i e normally from the time the failure is discovered until completed repair

Maintenance activities are modelled by setting the probability to 1 for the "maintenance basic events" during the time interval where there is ongoing maintenance These "maintenance basic events" have a probability of 0 at all other times

In a regular PSA, there are normally no assumed states of components or maintenance activities All of these possible events are modelled by basic events with different types of probabilistic models

One problem with the different types of models described above for LPSA applications is that if the current risk results are plotted in a diagram and the curve is used to calculate "integrated" risk measures, these integrated results will be systematically overestimated The reason for this overestimation is that the failures are "double-counted", both as normal unavailabilities (when the component is not known to be failed) and by setting the unavailability to 1 when the component is known to be failed

2.2.2 System Level Modelling

While the previous section focused on individual component modelling, this section focuses more on system level aspects There are two important modelling features that will be covered CCF modelling and modelling of system configuration changes

CCF Modelling

In the current LPSA applications, a modified version of the MGL method /3/ has been used This modification is called "the minimum-value variation" /4/ and it works in the following way

Each CCF event involves two or more components Of all the components in a particular CCF event, the one with the lowest independent failure probability is used as a basis for calculation of the probability for the CCF event An exception to this rule is the situation where a failure exists, or may have existed (in risk follow-up) among the components involved in the CCF event If this is the case it is the probability of the existing failure that is the basis for the CCF probability For example, if one component is known to be failed (probability = 1) the probability of a second component failure is β until the state of those other components have been verified

One result of this modelling is that when a test is made for one component in a CCF group, the probability for all CCF events involving the component become equal to the time independent CCF probability

System Configuration Changes

In the plant which has been studied there are a number of systems which are included in the PSA model and for which there are different possible configurations E g , there are systems with two redundant trains and normally one train is in operation and one is in stand-by To get a model that accurately reflects the current CDF, there must be a way to "switch" between variations of the model that reflect the various possible configurations

This is accomplished by modelling all possible system configurations in the fault trees, and then using house events that can be switched on or off (TRUE or FALSE) to control which configuration is currently used The implementation of house events and the ways they can be controlled in Risk Spectrum allows this to be made easily

This can be compared with the modelling in a regular PSA, where it is most common to model only a single configuration alternative (the most usual one or the one that leads to the most conservative model.

2.2.3 Initiating Event Modelling

All initiating events are modelled with basic events where the quantitative data is in terms of frequency An exception to this is in risk follow-up studies when a particular initiating event has occurred In such a case, the current core damage probability (CDP) is calculated given the occurrence of that initiating event

In the same way, and for the same reason, as described for component modelling (section 2 2 1) this initiating event modelling leads to an overestimation of integrated risk measures

3 RISK FOLLOW-UP

The purpose of conducting a risk follow-up study is to evaluate the risk significance of events that have occurred in order to improve the experience feed-back

Four different methods to carry out risk follow-up have been identified within the NKS/SIK-1 project These methods are

- Off-line risk monitoring
- Risk follow-up with failure memory only
- Safety margin follow-up
- Accident sequence precursor follow-up

These methods are described in the report "Risk measures in living-PSA applications" /5/

The application presented here is carried out according to the method "Risk follow-up with failure memory only", a method which is quite similar to "Accident sequence precursor follow-up" The risk follow-up study covers an entire operating year (1987)

3.1 DATA SOURCES

To carry out a risk follow-up study over a time-period there is a need to have data about failures, disturbances, tests etc that have an influence on the current risk level The data sources used in this LPSA are described below

3.1.1 Licensee Event Reports (LERs)

The LERs is one of the most important sources of data in risk follow-up studies During 1987, the year that was studied, there were 43 LERs reported for the plant under consideration, and 11 of those affect the core damage sequences included in the LPSA model The year 1987 was selected because it seemed to be an "interesting" year from this point of view with more significant occurrences than a normal year.

3.1.2 Disturbance Records

To get information about plant shut-downs, both planned and caused by transients, the plant disturbance records have been used During 1987, there were 3 planned shut-downs and 3 scrams.

3.1.3 Test Records

The test records is another important data source All tests that are required according to the plant's Technical Specifications are documented in test records Those records contain information about which test was made, at what time-point the test was made and the outcome of the test

3.1.4 Plant Operating Procedures

The plant operating procedures contain information about test procedures, i e which components are activated at each test Instead of going through the plant operating records to find information about the exact time-points for system reconfigurations, the operating procedures were also used to find out how and when such reconfigurations are normally made (sufficient for this example application)

3.2 ASSUMPTIONS

The assumptions made specifically in risk follow-up studies mainly have to do with interpretations of LERs One example of a problem is to conclude whether a certain failure may potentially have been a CCF or not

3.3 METHODS

Since the LPSA is modelled with the PSA software Risk Spectrum this section will mainly discuss how the Risk Spectrum modelling and analysis features were used in carrying out the risk follow up

The description of methods is divided into the two sub sections model modifications and "analysis"

3.3 1 Model Modifications

Step 1 System configuration modelling

The first step is to specify the house events that are to be set to TRUE to "switch in" the model variation that covers the particular plant configuration at a given time point Only the house events that should be TRUE need to be specified, all others are set to FALSE by default

Step 2 Test modelling

The second step is to update the "time since last test" value (the TM parameters) for all periodically tested components The model for those components is according to section 2 2 1 When determining the time since last test, also real demands and other activations of components beside the scheduled tests, are regarded as tests in the sense that they verify the operability of the component

The functions in Risk Spectrum make it easy to update the time since last test for all components affected by a certain test as a group

For components involved in CCF groups, and for which tests of all components in the group are not made at the same time (staggered testing), the TM-value used is the shortest of the TMs for the individual components involved in each CCF event In other words, each successful test of individual components in a CCF group is considered as a successful test against all CCFs involving that component

Step 3 Failure and maintenance modelling

The third step includes modifications due to components that are out of service, either because of failures or because of maintenance

The modification is made by updating the probabilities for all events for which information about failures or maintenance activities is available Some failures can affect probabilities both for individual component failures and for CCFs involving that component If a failure has been discovered at a later time-point this may also affect the estimation of the failure probability for this component at time points before the failure was discovered See sections 2 2 1 and 2 2 2

Ongoing maintenance is modelled by setting the probability to 1 for the basic events that represent maintenance unavailability

3.3.2 Analysis

Two types of analyses are made in the risk follow up study depending on the type of situation that is analyzed One type of analysis is to calculate the CDF in power operation, and the other type is to calculate the CDP given that an initiating event already has occurred

The CDF is calculated by using a top event in Risk Spectrum which analyses all core damage sequences in all event trees The only data required in the top event definition is to specify the consequence" (plant damage state) to be analyzed (here it is "core damage") and a cutoff probability (all cut sets with a probability below this value are truncated)

The CDP given that an initiating event already has occurred is calculated by analyzing all core damage sequences in the event tree for this initiating event The probability for this initiating event is first set to 1 The top event definition is the same as described above, but in this case it is specified that only one particular event tree is to be included in the analysis

3 4 RESULTS

Diagram 1 shows the CDF (f_n = 4 1E 6/year) for the part of 1987 when no component failures occurred Each point in the diagram represents the CDF either directly before or directly after a test or a system re configuration

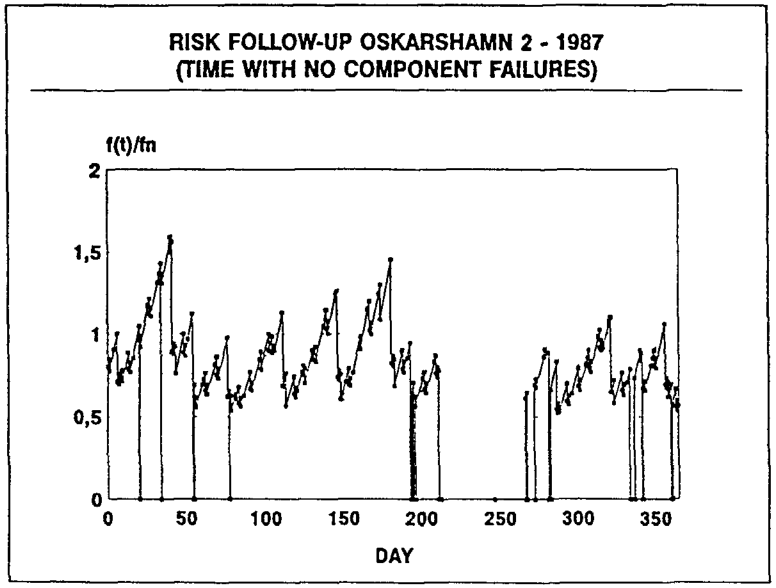


Diagram 1

Diagram 2 shows the CDF for the part of 1987 when component failures did occur

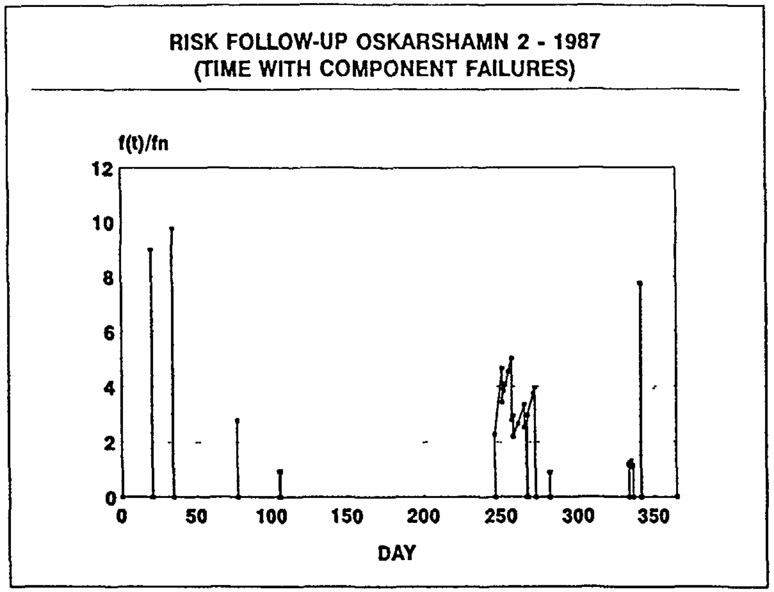


Diagram 2

Table 1

Component failure	Date	CDP
661DG212	870121 (10h)	4.9E-8
661DG212	870204 (3h)	1.6E-8
641SG6	870319 (6h)	9.0E-9
666G222	870714 (16h)	8.1E-9
649G13	870904 - 870924	9.1E-7
649T13	870925 - 870930	2.2E-7
713P1	871009 (8h)	3.9E-9
733P23	871130 - 871203	4 8E-8
661DG212	871208 (16h)	6 7E 8

Table 1 present the CDP for each component failure event that occurred during 1987

Diagram 3 shows the CDF during the time-period September 4-24 1987 The CDF is at an increased level during the entire time-period The reason for this is that a gas turbine failure was discovered in a test September 10 The previous test, which was successful, for this gas turbine was made August 26 The failure thus occurred between August 26 and September 10 The probability that the failure existed at any time-point between those dates is calculated by using the model described in section 2 2 1 (Failures and Maintenance) The failure was repaired on September 10, but the redundant gas turbine was not tested until September 15 Therefore, the failure probability for the second gas turbine was modified during this period to include the probability of CCF given the knowledge that one failure has already occurred The test of the second gas turbine September 15 was successful September 24, the first gas turbine was tested again and failed This time the cause was a failure to correctly restore the gas turbine after the previous repair The nature of this failure was such that it was not judged to be a potential CCF

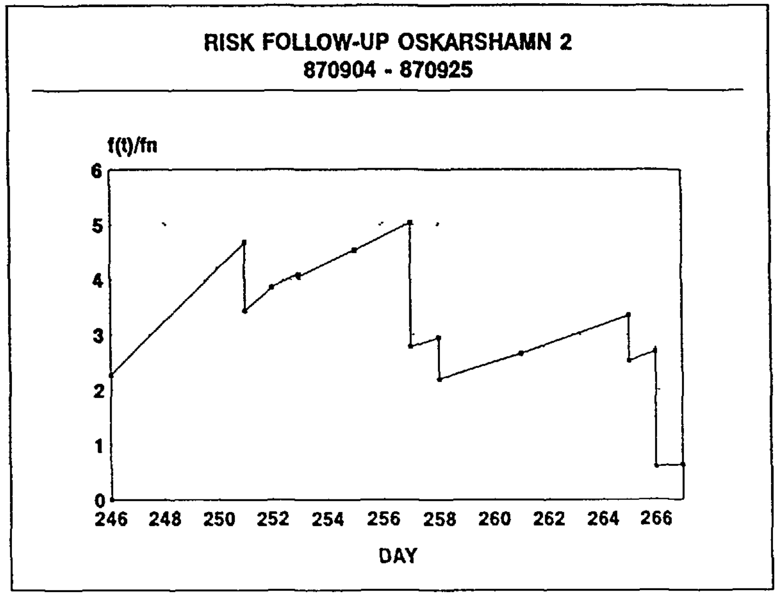


Diagram 3

The CDF due to these two failures is 3 5 times higher than normal for a period of 20 days The experience feedback from the evaluation of this period could be

- Always test the gas turbines after completed maintenance
- Always test the redundant gas turbine directly when a gas turbine has been found to be failed

If these rules had been followed the risk increase would have been only 30% of the increase that actually occurred

Table 2

Initiating event	Date	CDP
TT	870224	1.5E 7
TF	870713	3.2E-6
TP	870715	6.0E-8
TP	870731	7.1E-8
TP	871009	6.8E-8
TP	871227	5.4E-8

Table 2 presents the CDP for each initiating event occurrence during 1987

Table 3

Component failure/ Initiating event	Date	Risk contribution (%)
TF	870713	64
649G13	870904 - 870924	18
649T13	870925 - 870930	4
TT	870224	3
TP	870731	1
TP	871009	1
661DG212	871009 (16h)	1
TP	870715	1
TP	871227	1
733P23	871130 - 871203	1

Table 3 presents the contribution to risk from the different component failure events and initiating events that occurred during 1987

4 EVALUATION OF ALLOWED OUTAGE TIMES

The second LPSA application involves evaluation of allowed outage times (AOTs) according to Limiting Conditions of Operation (LCO) The AOT is the time the component is allowed to be out of service If the component is not restored during this time, the plant must be shut down

When a failure covered by LCO occurs the repair can be made with the plant still in power operation or the repair can be made after shut down of the plant When deciding on the optimum strategy the risk exposure for the two cases should be compared Such calculations can be made for all components covered by LCOs Basically, these calculations are made using the same model and the same type of model modifications that were described for the risk follow up calculations in section 3

4.1 ASSUMPTIONS

The assumptions made in this type of application concerns limits on shut-down risk, acceptable risk in continued operation, and acceptable risk per failure

4.1.1 Shut-Down Risk

The two different situations, and associated risks, that are compared in AOT evaluations are

- Continued operation
- Shut-down

In both cases the component under consideration is unavailable The shut-down risk has three components Risk at shut-down, risk during the shut down period, and risk at power-up It is assumed that the shut-down is similar to a manual shut-down for which an event tree exists in the LPSA model, and only the shut-down itself is considered in the quantification This results in shorter calculated AOTs than if all three phases of a shut-down were to be considered

4.1.2 Acceptable Risk In Power Operation

When the risk in continued operation is compared with the shut down risk one should also consider the risk accepted in normal operation (with no known existing failures and no ongoing maintenance) According to our calculations, the normal CDF varies between 0 51*f_n and 1 7*f_n (f_n = 4 1E-6/year) In this application it is therefore assumed that a CDF of 1 7*f_n is acceptable It should be emphasized that this is purely an assumption made for demonstration purposes during this project, and it does not reflect the official view of any involved party regarding what is "acceptable "

4.2 METHOD

The same model modification steps are carried out when analvzing allowed outage time (AOT) as in the risk follow up application (section 3 3 1) The only difference is that here the calculations are always made for one (assumed) component failure at a time

Note that the results from the AOT calculations depend on the current plant status and configuration If tests are performed or if systems are re-configured the results can be different This also means that there are measures available to actively affect the risk level or, possibly to prolong an AOT in a given situation without having an increased risk

The AOT calculation is based on the formula

$$\int_{t}^{t+AOT} (f(x,t) - f_a)dt \le \int_{t}^{t+t_1} P_{MSD}(x,t)dt + \int_{t+t_1}^{t+t_2} P_{SDP}(x,t)dt + \int_{t+t_2}^{t+t_3} P_{PU}(x,t)dt$$

AOT	=	Allowed outage time
f	=	CDF in continued power operation
f_a	=	Acceptable CDF in power operation (1 7*f_n)
P_{MSD}	=	CDP for manual shut-down
P_{SDP}	=	CDP for shut-down period
P_{PU}	=	CDP for power-up
x	=	Plant configuration

Only the probability of one initiating event shall be considered during the time period AOT when calculating the CDF in continued power operation

The formula is simplified to

$$AOT = \frac{P_{MSD}(x,t)}{f(x,t) - 1\,7 * f_n}$$

4.3 RESULTS

The two first diagrams visualizes the operating time that provides an equilibrium between the CDF that exceeds the acceptable level, 1 7*f_n (f_n = 4 1E 6/year), and the CDP for a manual shut-down

Diagram 4 shows how the CDF increases from 0 62*f_n to 2 25*f_n when a gas turbine fails at day 0 (September 10 1987) The CDF of 2 25*f_n assumes that the redundant gas turbine is successfully tested

A manual shut-down given one failed gas turbine and a second redundant one which has just passed a successful test, results in a CDP of 6 0E-8

The data above yields the following results

$$AOT - \frac{6\,0E\text{-}8}{(2\,25 - 1\,7)*4\,1E\text{-}6} = 2\,7E\text{-}2 \ years = 8\,3 \ days$$

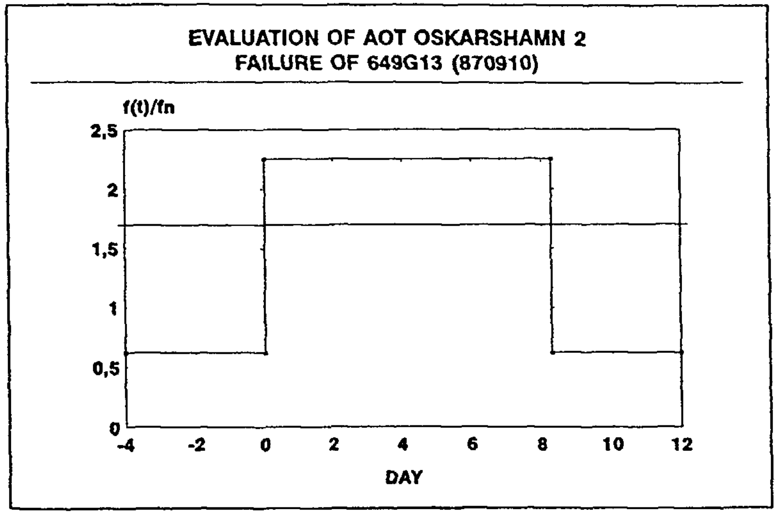


Diagram 4

The area in the diagram bounded by the CDF of 1 7*f_n to 2 25*f_n and by 0 to 8 3 days represents the same total CDP as the manual shut-down

Diagram 5 shows how the CDF increases from 0 77*f_n to 128*f_n when a battery-backed bus-bar fails (at day 0)

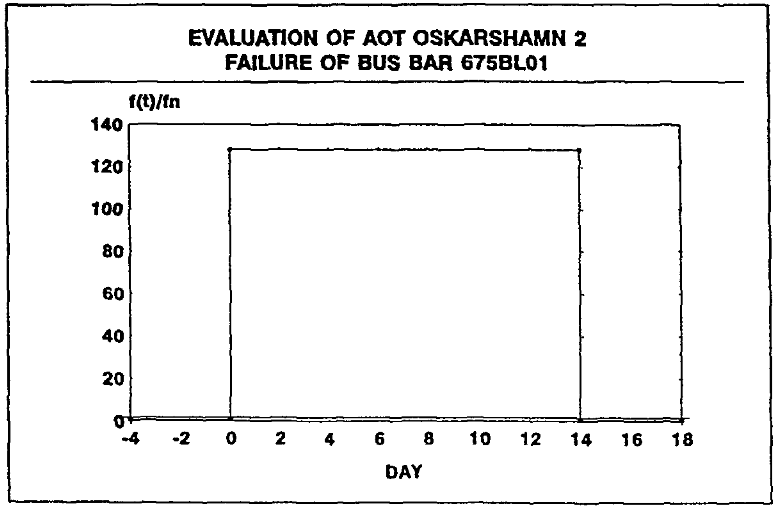


Diagram 5

A manual shut-down, given the same bus-bar failure, results in a CDP of 2 30E-5.

The data presented above yields

$$AOT = \frac{2.30E\text{-}5}{(128\ -\ 1.7)*4.1E\text{-}6} = 4\ 4E\text{-}2\ years = 14\ days$$

The area in the diagram bounded by the CDF of 1 7*f_n to 128*f_n and by 0 to 14 days represents the same total CDP as the manual shut-down

Table 4 presents a comparison between calculated AOT and the AOT according to the present LCOs for four different components

Table 4

Component failure	AOT (days) Living PSA	AOT (days) TS
Core cooling pump 323P1	6	2
Gas turbine 649G23	8.3	30
Diesel generator 661DG212	4	2
Battery-backed bus-bar 675BL01	14	1

The AOTs according to present LCOs are shorter than the calculated AOTs, except for the gas turbine.

For the auxiliary feedwater system, a failure of single pump resulted in a calculated CDF that did not exceed 1.7*f_n. This leads to unlimited calculated AOTs and ARTs. Another analysis was performed where both auxiliary feedwater pumps failed due to CCF. According to LCO, the plant must be shut-down in this case.

Table 5 present the calculated AOT and the mean repair time (MTTR) for these pumps. The calculated AOT is longer than the MTTR. A manual shut-down is therefore questionable in the case of failure of both auxiliary feedwater pumps

Table 5

Component failure	AOT (hours) Living PSA	MTTR (hours)
CCF auxiliary feedwater pumps 327P1/P2	6.1	6

4.4 RISK CONTROL

Of primary concern is the possibility to actively control risk in cases where a failure has occurred, and thereby possibly prolong the AOT. Examples of possible measure that can be taken to control risk are:

- Perform different types of tests
- Take systems into operation
- Change system configurations/pipe alignments
- Complete ongoing maintenance activities

4.4.1 Method

The method used when increasing the AOT, given a particular situation, means that one further step is carried out to identify the most effective risk control measure. The most optimal risk measure is identified by studying the risk reduction worth (RRW) for TM parameters calculated by Risk Spectrum The TM parameters are used to model the time since last test or the time since last re-configuration This means that their RRW values will reflect the possible risk reductions that could be achieved by performing tests or making re-configurations The most optimal action is selected, and when this action has been accomplished and fed into the model a new calculation is made to find the optimal risk reduction measure in this situation

4.4.2 *Results*

Diagram 6 presents an example of prolonging the AOT. This example is based on the gas turbine failure September 10 1987, which has been discussed previously.

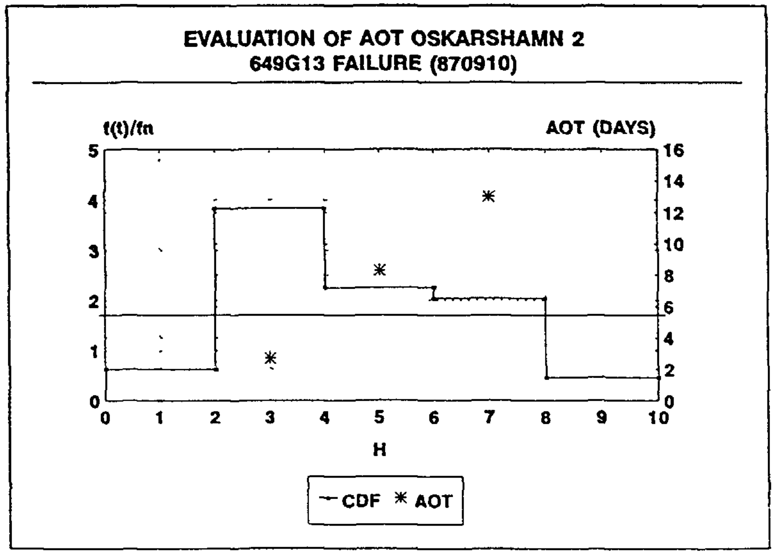


Diagram 6

The CDF increases from 0 62*f_n to 3 83*f_n when the gas turbine failure occurs (at hour 2). Calculated AOT, according to section 4 2, is in this situation 2 7 days, with no particular measures taken to reduce risk

When the redundant gas turbine is tested, the CDF is reduced to 2 25*f_n (shown at hour 4 in the figure). The calculated AOT in this situation is 8 3 days In other words, the time available for repair of the gas turbine increases by about a factor of 3 if the redundant gas turbine is successfully tested

Further selection of the next optimal risk reduction measure results in a test of a diesel generator. If this test is made also, the AOT will be 13 days

Depending on the status of the plant, the optimal risk control measures may be different and the amount of risk reduction possible can also vary E g , if the same gas turbine failure were to occur in the end of an operating year, i e shortly before refuelling rather than shortly after refuelling, the results would be that AOT can be increased from 2.9 days to 7.2 days The reason for this difference is that some components in the plant are tested only at refuelling which leads to a changing risk profile for the plant over the operating year

5 TEST INTERVAL EVALUATIONS

The fourth application conducted during this project was to evaluate the test intervals that are specified in the plant's Technical Specifications and the reconfiguration intervals according to the plant operating procedures The main purpose of such an evaluation was to find a way to decrease the number of tests and reconfigurations without affecting the average risk

First, an upper bound of risk level in normal power operation (with no existing failures and no ongoing maintenance) is decided. This risk level is selected in such a way that the average risk (see below) becomes approximately equal to the average risk when tests are performed according to the present Technical Specifications.

5.1 ASSUMPTIONS

In the studied plant the CDF varies between 0.51*f_n and 1 7*f_n (f_n = 4 1E-6/year) if tests and reconfigurations are performed according to Technical Specifications (see diagram 7). If the upper bound of CDF is set to 1 15*f_n, and the procedure described above is followed, the resulting average risk becomes the same as in the case when tests and reconfigurations are made according to Technical Specifications.

5.2 METHOD

The procedure that was used in this application involve the following steps

1 Starting in the beginning of an operating year (after refuelling), the CDF is calculated each day until it reaches the predetermined upper bound (it increases due to the time-dependent part of the unavailability for stand-by components, see section 2 2 1)

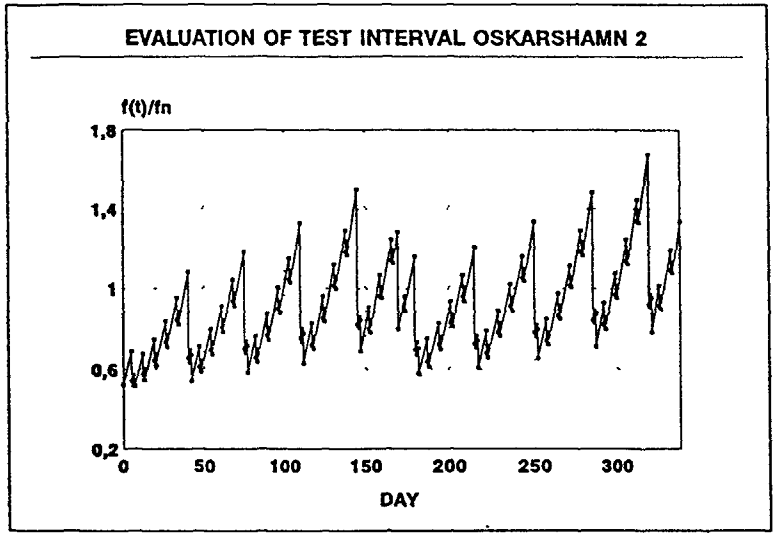


Diagram 7

2. At this time-point, find the test or reconfiguration that has the highest risk reduction worth, and perform this test.

Steps 1 and 2 are repeated through the entire operating year.

It is also possible to change the procedure in different ways, such as.

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

5.3 RESULTS

Diagram 8 shows the fluctuation of the CDF when the procedure described above is used.

When following this procedure, the total number of tests and reconfigurations made during an operating year is 67 This can be compared with the 117 tests and reconfigurations that need to be made according to Technical Specifications The number of tests has thus decreased by 43%, but the average risk is maintained at the same level

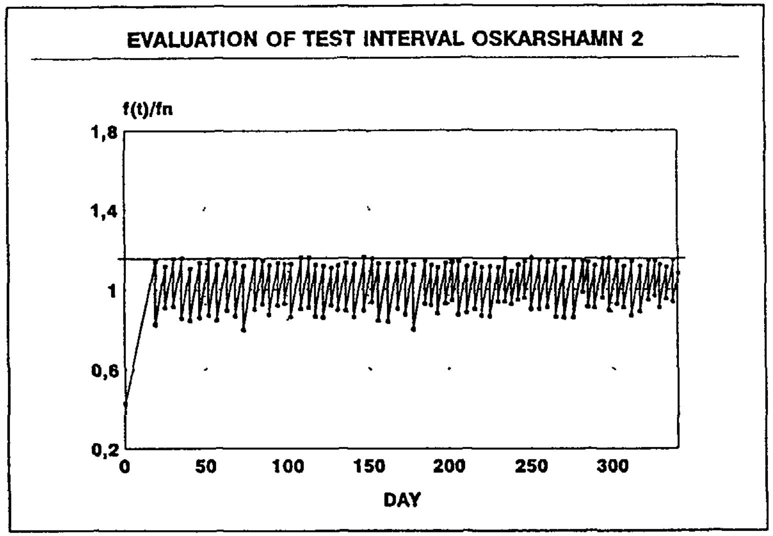


Diagram 8

Table 6 present the number of tests according to the described procedure compared with the number of tests according to Technical Specifications for a number of different components and systems.

Table 6

System	Number of tests Living-PSA	Number of tests TS
Depressurization system 314	2	1
Core cooling system 323	13	10
Auxiliary feedwater system 327	7	10
Gas turbine 649G13	10	24
Gas turbine 649G23	9	24
Diesel generator 661DG211	13	24
Diesel generator 661DG212	13	24
Total	67	117

Table 7 present the variation of test interval lengths over the operating year for the same components. These values are also compared with the test intervals according to Technical Specifications

Table 7

System	Test interval, Max (days) Living-PSA	Test interval, Min (days) Living-PSA	Test interval (days) TS
Depressurization system 314	127	115	170
Core cooling system 323	35	14	35
Auxiliary feedwater system 327	54	39	35
Gas turbine 649G13	38	30	14
Gas turbine 649G23	40	33	14
Diesel generator 661DG211	30	22	14
Diesel generator 661DG212	31	18	14

6 LIMITATIONS

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

6.1 INCOMPLETENESS

The incompleteness problem has to do with missing parts of the model, i e the entire risk is not covered by the model These can be either known, but excluded for one reason or another, or unknown

The incompletenesses identified so far are all such that it is possible to remove the deficiencies in the future

Incompletenesses may not only result in anerroneous absolute risk level, it may also result in wrong relative importance for individual failures This may in turn lead to wrong decisions based on the LPSA application results It is therefore important to remove as much as possible of all incompletenesses

One very important incompleteness in the LPSA model used currently in this project is that it only includes a sub-set of all possible initiating events
Examples of excluded initiating events that may be significant are fires, internal flooding, different types of common cause initiators, initiating events in other operating modes than full power operation

A number of incompleteness issues arise around component failure modes: Some failure modes are missing, possible dependencies are not modelled, the test efficiency is not 100% as assumed, etc.

6.2 CONSERVATISM

In many cases, normal PSA models are made with conservatisms built into the model and data. The reason is usually to simplify the model while at the same time making errors on the conservative side. This is acceptable in situations where the main purpose of the calculations is to verify a certain absolute risk level.

In many LPSA applications, however, the conservatisms may lead to wrong relative importance and wrong decisions, and thereby in the end leading to non-conservative actions.

The success criteria used for the different safety functions in the event trees are in many cases conservative. The conservatisms are of various types. In some cases credit is not taken for safety functions or support functions. Another example is that recoveries are not taken into account properly.

7 CONCLUSIONS AND RECOMMENDATIONS

The results obtained show that LPSA methods are useful in the applications that have been investigated:

- Risk follow-up
- Evaluation of allowed outage time
- Risk monitoring/risk control
- Test interval evaluations

In all types of LPSA applications the following items have been found to be important.

- The completeness and realism of the model and data are very important, much more so than in regular PSAs. This is due to the fact that an LPSA model should cover, and be quantitatively accurate in many different situations (e.g. when failures have occurred), and not only in "average". Also, in some cases conservatism in the model may lead to wrong (and possibly unconservative) decisions.
- The software is very important for the possibility to perform the calculations involved in various applications. It must allow modifications of model and data that reflects the changes in plant configuration and status, and it must be sufficiently powerful to allow recalculations of all core damage sequences within a reasonable time-frame and without simplifications that could invalidate the results. This project has been carried out successfully by using the Risk Spectrum PSA software. In the future, it may be even better to develop a specialized software with functions tailored to allow quick and simple modelling and quantification. Such a software could use Risk Spectrum's models, data bases and calculation "engines", but with a user interface that is tailored to the particular tasks performed in LPSA applications.

REFERENCES

1 Risk Spectrum PSA Users Manual, RELCON Teknik AB, March 1992.

2 T-book, Reliability Data Book for components in Nordic nuclear power plants, Version 3, Prepared by ATV-kansliet and Studsvik AB, 1992.

3 Mosleh, A. et al., Procedures for Treating Common Cause Failures in Safety and Reliability Studies. NUREG/CR-4780, 1988

4 Erhardsson, U-K., Test av några tidsberoende CCF-modeller. Report PK-168/90, Vattenfall, October 1990. (In swedish)

5 Holmberg, J., Johanson, G. and Niemelä, I., Risk measures in living PSA applications. Report NKS/SIK-1 (91)38, Swedish Nuclear Power Inspectorate, 1992.

246

ALMARAZ PROBABILISTIC SAFETY ANALYSIS APPLICATION

M.D. MORALES
CN Almaraz

E. GUTIERREZ
UITESA,
Madrid

I. FUENTE
E. Agrupados

Spain

Abstract

In December 1990, Almaraz Nuclear Power Plant submitted to the Consejo de Seguridad Nuclear (C.S.N., Spanish Regulatory Body), the review 1 of the Level 1 Probabilistic Safety Analysis (PSA), including a fire analysis. This review included all the C.S.N. comments to the review 0 delivered in November 1989, achieving in this way the regulatory body requirements. Some months later, in April 1991, the C.S.N. expressed their final approval to the analysis performed.

In this way, a new working tool is now available at the Almaraz Nuclear Power Plant in the safety field, complementary to the ones which were already being used in a deterministic way. The new tool includes a very detailed and systematic analysis of all the feasible initiating events in the plant that may occur, together with the response of the mitigating systems against those incidents, taking into consideration all kind of potential human mistakes, component failures, unavailability derived from test and maintenance and, dependencies and common cause failures. All this is documented in a systematic and exhaustive way, which allows not only to easily reproduce the whole study, but also to change any aspect and to review its impact into the results of the core frequency damage, towards to improve the safety of the plant.

According to the above, this study has been applied at the Almaraz Nuclear Power Plant on a broad way since the conclusion of the PSA, trying to integrate it to the organizational structure and to make good use of its possibilities as a support tool for decision making in the different aspects concerning to the safety of the plant.

Nevertheless, the spectrum of potential applications for the probabilistic analysis of safety is very broad, therefore the possibility of its future increase in number and type is being considered, as far as it is useful and convenient to the plant.

The most significant applications carried out at the Almaraz Nuclear Power Plant up to now, are developed in the following areas:

- Training seminar.
- Procedure improvements.
- New preventive maintenance procedures.
- Data collection.
- Optimization of Technical Specifications.
- Setting priorities and optimization of test and maintenance.
- Fire analysis.
- Definition of strategies for safety improvement.

Each application is described in detail in the paper.

1.- <u>INTRODUCTION</u>

In December 1990, Almaraz Nuclear Power Plant submitted to the Consejo de Seguridad Nuclear (C.S.N., Spanish Regulatory Body), the review 1 of the Level 1 Probabilistic Safety Analysis (P.S.A.), including a fire analysis. This review included all the C.S.N. comments to the review 0 delivered in November 1989, achieving in this way the regulatory body requirements. Some months later, in April 1991, the C.S.N. expressed their final approval to the analysis performed.

In this way, a new working tool is now available at the Almaraz Nuclear Power Plant in the safety field, complementary to the ones which were already being used in a deterministic way. The new tool includes a very detailed and systematic analysis of all the feasible initiating events in the plant that may occur, together with the response of the mitigating systems against those incidents, taking into consideration all kind of potential human mistakes, component failures, unavailability derived from test and maintenance and, dependencies and common cause failures. All this is documented in a systematic and exhaustive way, which allows not only to easily reproduce the whole study, but also to change any aspect and to review its impact into the results of the core frequency damage, towards to improve the safety of the plant.

According to the above, this study has been applied at the Almaraz Nuclear Power Plant on a broad way since the conclusion of the PSA, trying to integrate it to the organizational structure and to make good use of its possibilities as a support tool for decision making in the different aspects concerning to the safety of the plant.

Nevertheless, the spectrum of potential applications for the probabilistic analysis of safety is very broad, therefore the possibility of its future increase in number and type is being considered, as far as it is useful and convenient to the plant.

The most significant applications carried out at the Almaraz Nuclear Power Plant up to now, are pointed out in the following pages.

2.- APPLICATIONS PERFORMED

The basic areas in which the applications have been performed at the Almaraz Nuclear Power Plant are the following:

- Training Seminar.
- Procedure improvements.
- New preventive maintenance procedures.
- Data collection.
- Optimization of Technical Specifications.
- Setting priorities and optimization of test and maintenance.
- Fire analysis.
- Definition of Strategies for Safety improvement.

Each application is described in detail in the next paragraphs.

2.1.- Training Seminar

A course has been given to personnel with license upon human actions with short available time. The purpose of the course was to draw the operators' attention in relation to the fast performance needed from them in these cases.

Some illustrating examples are, among others, actions taken for changes from injection to recirculation of the charging pumps in small LOCA, feed & bleed in small LOCA and realignment from injection to recirculation of the RH and SP systems in large LOCA.

Additionally, the most important results and conclusions from the fire analysis developed have been included in the seminars to the fire brigades, and there is an intention to take into account those results in future fire simulations.

2.2.- Procedure improvements

During the development of the PSA, a systematic review of the procedures associated to safety related systems and function has been carried out in order to fit the systems and accident sequence models to the plant's actual operation. Likewise, comments have been made to the initial reviews (rev. A and rev. 0) on symptoms based emergency operation procedures (EOP's).

As a result of this systematic review of procedures, some of them have been altered regarding the following reasons:

* To improve the performance of certain periodical tests, widening its objectives (16 cases).

* To guarantee the systems' operability under specific operational circumstances (12 cases).

* To correct mistakes and errors regarding equipment denomination, valve alignment, etc.(22 cases).

2.3.- New preventive maintenance procedures

The convenience of guaranteeing the periodic test of certain components has been observed in the detailed analysis of systems carried out. Therefore, new types of maintenance procedures have been designed (6 cases).

2 4 - Data collection

In the area of data collection and analysis, support has been given to the definition of different criteria for the development of the Spanish data base (DACNE), regarding the number and type of components to be included as much as its physical limits and the failure definition, operation timing and the number of demands over such components

Additionally, some accurate comments have been made to certain criteria established in the SAMO (Operation Aids Computerized System) The system's availability analysis, performed by GE, has been also reviewed

2 5 - Optimization of Technical Specifications

Some applications already carried out as has been the evaluation of the proposal of changes coming from the licensing area and PSA itself, in order to analyze its impact to the core damage frequency, to determine its feasibility from a safety point of view Some of those applications has been evaluated and accepted by the regulatory body (C S N)

Examples

* Decrease to a minimum the time needed to put in service the derivation line of the BIT in case of necessity because of injection failure through the standard path of injection

* Possibility of maintaining out or service an inverter during 72 hours, if the critical bus gets energized within a 2 hour period, or two inverters from a same non operating chain during 24 hours

* Possibility of operating during 72 hours with switchgear room emergency cooling unit, provided that the air temperature in the rooms, measured every 4 hours, does not exceed 40º C

2 6 - Setting priorities and optimization of tests and maintenance

The impact of the unavailability derived from tests and/or maintenance of the different components, to the global core damage frequency can be very important In this way, as consequence of the PSA results, different recommendations have been given to the plant personnel

Among those advices, we should remark the following

To set priorities and to reduce the impact of the motor operated valve tests based on the importance given to the different valves (Generic Letter 89-10)

- To optimize the maintenances of the turbine driven pump of the Auxiliary Feedwater System, reducing as much as possible both its frequency and its required maintenance time

2 7 Fire analysis

Has been performed an analysis supporting the study of fulfilment with the Appendix R of the 10CFR50, which comprised the setting of priorities among the fire zones, according to its importance from the PSA point of view, and reanalysis such zones to combine the deterministic and probabilistic criteria in order to define the fire protection measures that are required to be installed in order to fulfil the regulation and to improve the safety of the plant

The analysis has been divided in three parts

The reanalysis of the most critical fire zones from the PSA point of view, within the ones involved in the deterministic study of fulfilment with Appendix R

The reanalysis of the rest of the fire zones involved at the above mentioned deterministic study, and which do not appear as critical in the probabilistic analysis of fires This analysis justifies the reasons because of which the zones are not considered as significant from a safety point of view

- The reanalysis of the fires zones not considered in the deterministic study for the fulfilment with the Appendix R, and which appear to be important according to the results of the probabilistic analysis of fires

According to the above considerations, several specific proposals for the installation of fire protection measures in different zones have been made, which has been reviewed now by the regulatory body (C S N)

2 8 Definition of strategies for safety improvement

Bearing in mind that the Almaraz Nuclear Power Plant owns two similar units at the same site, the advantage of this situation could be seized Therefore, the project has been started defining the strategies for safety improvement This has come about with the modification of some procedures which allows the use of shared resources between both units or the use of similar equipment between each other, in certain emergency situations

In fact, modifications have been made to the OP1-IF-40 and OP1-IF-41 procedures to allow the recovery of water from essential services and of components cooling water, aligning a pump from one unit to another This consideration has been included into the models developed in the PSA and has been taken into account for core damage frequency cuantification

SUMMARY AND CONCLUSIONS

The probabilistic safety analysis constitute a complete, systematic, detailed and reproducible study of the evolution of transitory events and accidents in the plant, as well as of the behaviour and importance of the mitigating systems in each case, all documented in a precise and consistent way

As explained before, we consider all that to be a very useful tool to bear in mind in the decision making processes, which may affect the safety of the plant for they allow to evaluate the impact of any modification made in the design or in the procedures, in a global and systematic way, thus analyzing its incidence at a component level as much as at system level, its sequence of accident and its potential damage to the core

Under this prospect, the Almaraz Nuclear Power Plant has already developed a number of applications from its Probabilistic Safety Analysis - Level 1-, currently concluded and approved by the C S N These applications are expected to continue in the future and to be of use as a support tool to improve the availability and safety of the plant

Up to now, the most outstanding areas where applications from PSA have been performed are the following

- Training seminar
- Procedure improvements
- New preventive maintenance procedures
- Data collection
- Optimization of technical specifications
- Setting priorities and optimizing of test and maintenance
- Fire analysis
- Definition of strategies for safety improvement

The evaluation of the changes in design has been limited at the moment to the consideration of those modifications that have emerged as a consequence of the PSA results themselves, without discarding the fact that in the future some other modifications proposed by different departments within the plant may be evaluated from the PSA point of view In this way, the probabilistic evaluation of safety will be an additional aspect to be taken into account in the decision making process

LESSONS LEARNED IN APPLYING PSA TECHNOLOGY TO DIVERSE RISK MANAGEMENT APPLICATIONS

K.N. FLEMING
PLG, Inc.,
Newport Beach, California,
United States of America

Abstract

Brief overview of various PSAs performed by PLG, Inc. during the last two decades is given. Selected case studies in PSA applications are presented. Broad number of specific applications are described. Information related to PSA scope and modelling requirements is also given. The use of dynamic decision aids for plant operators is pointed out as one of the most promising new developments.

1. INTRODUCTION

During the past two decades, PLG has been deeply involved in the development and application of probabilistic methods for safety assessment and risk management of nuclear reactor plants. During this time, PLG has been involved with 33 major probabilistic safety assessment (PSA) projects that have provided opportunities to apply PSA methods to solve real problems. These projects involved mostly commercial light water reactor (LWR) nuclear power plants in the United States, but they also included plants in Europe, Japan, and the Republic of China (Taiwan) as well as nonpower reactors at U.S. Department of Energy facilities. The associated plants spanned a spectrum of different designs and a full coverage of commercial LWR reactor types that have been designed in Western countries, as indicated in the table below:

Reactor Type	Number
Pressurized Water Reactor (PWR)	
• Siemens KWU	1
• Westinghouse	14
• Babcock & Wilcox	4
• Combustion Engineering	2
Boiling Water Reactor (BWR)	10
Nonpower Reactors	2
Total	33

Each of these projects presented a set of unique problems and challenges to the PSA project because each plant's detailed design and siting features were unique, and each project was performed for a different purpose. For example, almost half of the PSAs were performed on Westinghouse PWRs with large, dry containments, yet each set of PSA results in this and every other group revealed plant and specific risk controlling factors. The surprisingly high degree of plant-to-plant (and reactor unit-to-reactor unit) variability that we have observed in the results has shaped our approach to performing the PSAs and has taught us the importance of developing an in-depth understanding of the details of the plant design, the way in which it is operated and maintained, and the impact that these factors have on the way in which accident sequences can initiate, progress, and be terminated. As PSA methods and tools have matured, there has been progressively less reliance on generic models and databases, and an increased ability to model the way they were actually built and to define accident sequences the way they would really occur.

The original purposes of performing these PSAs were essentially unique. Most were unilaterally initiated by the plant owners, some were performed to meet a variety of regulatory requirements, but each was required to address a unique set of problems. As a result, the work scopes and levels of completeness that were required varied. Most of the PSAs included a full treatment of internal and external events and the development of a plant-specific database. Nearly all were eventually extended to Level 2 to address containment performance and source terms, and about two-thirds were extended to Level 3 to address offsite consequences of severe accidents. PLG performed the first PSA of accidents initiated at shutdown (Reference 1), the only full-scope Level 3 PSA of shutdown accidents that has been completed to date (Reference 2), and is currently involved with shutdown PSA projects on three other plants.

Although each PSA project has been initiated for a different purpose, the vast majority of them have culminated in a decision by the plant owner to pursue some sort of a "living PSA" program. The original purposes and the ultimate PSA applications of these programs span a very large number of end uses. Virtually any type of decision making that could impact safe operation of the plants can potentially benefit from information obtained from a completed PSA or by exercising, in some way, the PSA models and databases developed for the plant.

Listed in Table 1 are major categories of PSA applications that have been or are being addressed, specific examples of each category, and some of the implications that these applications have on the requirements for the PSA scope and the capabilities of the PSA models. These requirements have shaped PLG's technical approach to performing a PSA as well as the computer software that was developed to help implement this approach. This software is known as RISKMAN®, and is the subject of a companion paper presented at this workshop (Reference 3).

Although many PSA projects were originally performed to address a specific need or decision, a common goal among owners of PSA models is to implement the so-called "living PSA concept." To achieve "living PSA" status, the transition is made from a one-time assessment to address a specific issue at a snapshot in time to a dynamic model of risk that is always current and able to support essentially all decision making during plant lifetime that could impact plant safety. There are some general requirements that a "living PSA" model must meet to be effective. These include:

- Up-to-date configuration management.

- Ease and speed of update.
- Flexibility and adaptability.
- Ability to measure risk significance of decision options.
- Ability to communicate risk information to decision makers.

Table 1. PSA Applications and Requirements for PSA Methods

PSA Application Type	Specific Applications	PSA Scope and Modeling Requirements
PSA Updating	• Plant Experience Update • Design and Procedures Update • Precursor Evaluation	• Ease/Speed of Update • Bayesian Treatment of Data • PSA Configuration Management
Design Evaluation	• Vulnerability Evaluation • Backfit Optimization • Safety Enhancement	• Design Visibility in Models • Modularized PSA Models • Ability To Analyze Risk-Controlling Factors
Maintenance Optimization	• Technical Specification Changes • Maintenance Prioritization • Root Cause Diagnostics • Outage Risk Management	• Explicit Treatment of Test and Maintenance Impact on Risk • Use of Risk Importance Factors • Treatment of Shutdown Events • Expert Diagnostics Systems
Performance Monitoring	• "Risk Meter" Concept • System/Component Trending • Plant Scenario Diagnostics	• Tie-In to Plant Computer • Graphical Interfaces to PSA • Expert Diagnostics Systems
Operations Support	• Emergency Procedure Evaluation • Accident Management • Operator Training	• Adequate Scenario Definition • Explicit Model of Procedures • Extension of PSA to Level 2
Emergency Planning	• Emergency Planning Zone Determination • Emergency Action Level Evaluation • Emergency Plan Evaluation	• Extension of PSA to Level 3 • Explicit Model of Evacuation • Three-Dimensional Dispersion Models
Licensing/ Regulatory	• Seismic Siting Issues • Postaccident Restart Issues • Individual Plant Examinations	• Realistic and Balanced Treatment of Seismic Events • Ability To Identify Weaknesses • Documentation To Support Successful Regulatory Review

With these capabilities in place and in constant use, a greater awareness is achieved of the risk significance of all activities in reactor design, maintenance, and operations. The most important result is an enhanced safety culture among all of those who are involved in the management of the plant.

2. SELECTED CASE STUDIES IN PSA APPLICATIONS

To provide a clearer picture of what has been and can be accomplished through effective use of PSA models and results, we turn our attention to a number of case studies in which PSA has been used to solve real problems. A summary of the plants that provide these examples, some brief information about the respective PSA models, and a listing of actual PSA applications are presented in Table 2. Several of the applications that were made for these plants are discussed more fully in the balance of this paper.

2.1 ZION AND INDIAN POINT PSAS

The purpose of these projects (References 4 and 5) was to provide a basis for the plant owners' response to a petition by the Union of Concerned Scientists to permanently shut down the two reactor units at each plant due to concerns that they were sited too close to the metropolitan areas of Chicago and New York City, respectively. At issue in the Atomic Safety and Licensing Board hearings that were conducted in response to this petition were the following: whether the plant should be permitted to continue operation and whether costly backfits should be installed to reduce the risk of severe accidents. These backfits, which had been proposed from what can now be safely described as a naive perspective of the nature of severe core damage accidents, included:

- A filtered, vented containment backfit.
- A refractory core ladle backfit.
- A hydrogen recombiner backfit.

These PSAs were specifically done to determine the safety adequacy of the as-built design of these plants in light of the claims made in the petition and to quantify the risk reduction benefits of the proposed backfits. Due the large stakes involved, it was necessary to advance the state of the art in PSA of the mid-1970s by incorporating external events and by extending the PSA methods that were developed in the Reactor Safety Study (Reference 6) to address the risk of the industry at large to address plant- and site-specific issues.

The end results of the hearings that followed the completion of these PSAs were quite favorable for the plant owners as well as for the rest of the nuclear industry. First, the PSA results were accepted as a basis to justify continued operation of these plants without the need for backfits. Second, the PSA results showed that these costly backfits would have a negligible impact on risk. In fact, after these PSAs, the lively discussion about the merits of such exotic backfits as "core catchers" was largely silenced in the United States. Finally, the precedent was set in these hearings that PSA results provided a legal basis to resolve regulatory issues. One such issue on decay heat removal was addressed in a subsequent extension of the Zion PSA by performing the first PSA of accidents initiated at shutdown (Reference 1).

2.2 SEABROOK STATION PSA

The Seabrook Station PSA (Reference 7) was originally performed as an independent safety assessment to help resolve a hotly contested licensing issue for this plant, which seemed to be the focus of intervenor efforts to stop nuclear power after the resolution of the Zion and Indian Point hearings. At the late stages of the licensing proceedings, the Governor of Massachusetts effectively blocked the issuance of a license by refusing to participate in the development of emergency plans for this plant. At issue was the ability to safely evacuate a nearby beach population as well as Massachusetts towns within the 10-mile emergency planning zone (EPZ) that was imposed after the Three Mile Island accident. The emergency planning requirements had changed during construction of the plant. Ironically, the owners had invested in a costly double containment concept to avoid the need to plan for a beach evacuation or for the need to involve the state of Massachusetts in the licensing process using the ground rules in effect when the site was selected.

Table 2. PSA Applications at Selected Nuclear Power Plants

Plant Name/Description	PSA Model and Scope (Reference)	PSA Applications Issues Addressed
Zion Unit 1/Indian Point • Westinghouse PWR • Large, Dry Containment	• Level 3 PSA (4,5) • External Events • Multiple Designs Modeled	• Shutdown Petition Denied • Costly Backfits Rejected • PSA Results Accepted in Legal Proceedings
Seabrook Station • Westinghouse PWR • Large, Dry Containment	• Level 3 PSA (7,8,9) • External Events • Extended To Shutdown Modes (3)	• Emergency Planning Risk • Accident Management • Outage Risk Management • Individual Plant Examination (IPE) Requirements • Technical Specification Changes
Beznau • Westinghouse PWR • Large, Dry Containment	• Level 2 PSA (10) • External Events • Multiple Designs Modeled	• Guided Major Backfits • Cost of Meeting Backfits Greatly Reduced
Diablo Canyon • Westinghouse PWR • Large, Dry Containment	• Level 2 PSA (11) • External Events with Extensive Seismic Treatment (IPEEE)	• Resolved Earthquake Siting Issue • IPE Requirements
Beaver Valley • Westinghouse PWR • Subatmospheric Containment	• Level 2 PSA (12) • External Events Planned in Individual Plant Examination for External Events (IPEEE)	• Risk Prioritization of Equipment Maintenance • IPE Requirements • Precursor Evaluation
South Texas Project • Westinghouse PWR • Large, Dry Containment	• Level 2 PSA (13,14) • External Events • Detailed Test and Maintenance Models	• Design Enhancement • Complete Overhaul of Technical Specifications • Graphical Interface for Risk Management
Kuosheng (Taiwan) • General Electric BWR • Mark III Containment	• Level 3 PSA (15,16,17) • External Events • Three-Dimensional Dispersion Model	• Baseline Risk Profile • Determine Emergency Planning Zones for Taiwan Nuclear Power Plants

An early application of the PSA was an emergency planning study (Reference 8) that was performed to quantify the risk reduction benefits of the protective actions covered in the emergency plan such as evacuation and sheltering. As illustrated in Figure 1, this study showed that, due to an exceptionally strong containment determined in the PSA, the risk of offsite consequences at Seabrook with no evacuation was lower than that assessed by the U.S. Nuclear Regulatory Commission (NRC) when it set the EPZ requirement to 10 miles. This application of the PSA was instrumental in resolving concerns regarding emergency planning at Seabrook, and the plant was subsequently licensed.

Because of the focus on the risk of severe accidents that was made in the licensing of this plant, Seabrook was responsible for identifying some of the first accident management procedures that have been identified for U.S. plants. The event sequence diagrams that were originally developed to support the PSA were extended, as illustrated in Figure 2, to identify key accident management strategies to cope with station blackout sequences that progress beyond the point assumed by the existing emergency operating procedures (Reference 9). The strategies included intentional primary system depressurization using the pressurizer power-operated relief valves (PORV), fire water supply to the steam generators, and special DC load shedding procedures. These actions were specifically identified to minimize the risk of early containment failure or bypass due to direct containment heating and induced thermal creep rupture of the steam generator tubes.

2.3 BEZNAU PSA

The Beznau PSA (Reference 10) was a good example of the application of PSA techniques as a design evaluation tool. The purpose of this study was to provide guidance to a major backfit construction project that was required by the safety authorities to bring this relatively older plant up to meet more rigorous safety requirements that were devised after plant construction. The backfit consisted of a new decay heat removal and safety system to augment the safety systems originally provided in the plant. Separate PSAs were performed with and without the safety backfits to help ensure that the backfits had the intended benefit. An unexpected result of the PSA was a justification for saving a large fraction of the backfit construction budget without compromising the safety benefits of the new system. The PSA results showed that the two-train design of the backfit system could be reduced to a single train with about the same impact on risk. These results were accepted, and the cost of the backfits were reduced. The cost savings to the plant owner, in excess of $100 million, were far in excess of the cost of the PSA.

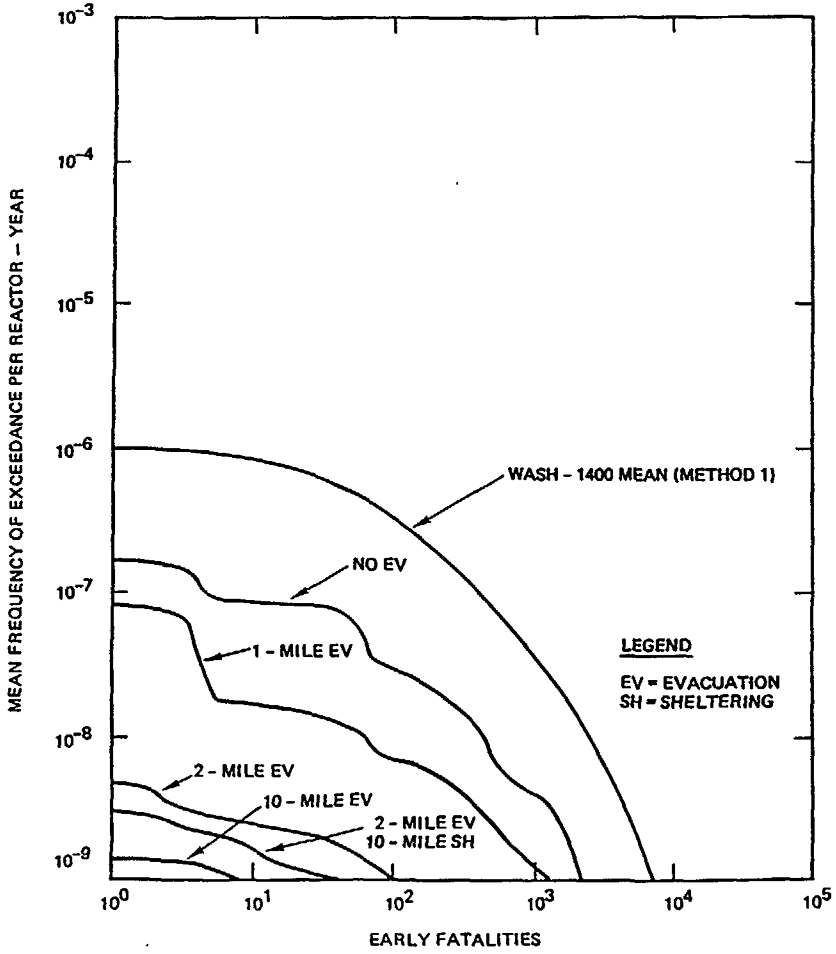


Figure 1. Impact of Different Emergency Planning Options on Risk of Early Fatalities at Seabrook Station

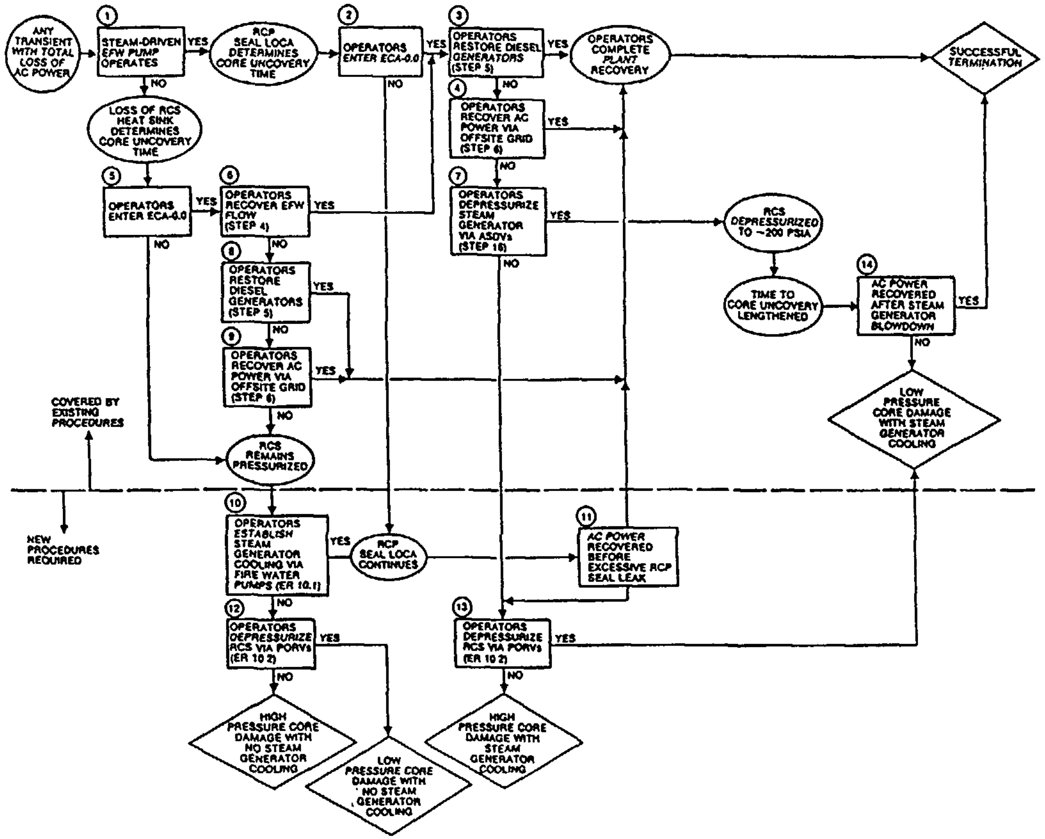

ANY TRANSIENT WITH TOTAL LOSS OF AC POWER
1
STEAM-DRIVEN EFW PUMP OPERATES
YES
NO
RCP SEAL LOCA DETERMINES CORE UNCOVERY TIME
2
OPERATORS ENTER ECA-0.0
YES
NO
3
OPERATORS RESTORE DIESEL GENERATORS (STEP 5)
YES
NO
OPERATORS COMPLETE PLANT RECOVERY
SUCCESSFUL TERMINATION
4
OPERATORS RECOVER AC POWER VIA OFFSITE GRID (STEP 6)
YES
NO
LOSS OF RCS HEAT SINK DETERMINES CORE UNCOVERY TIME
5
OPERATORS ENTER ECA-0.0
YES
NO
6
OPERATORS RECOVER EFW FLOW (STEP 4)
YES
NO
7
OPERATORS DEPRESSURIZE STEAM GENERATOR VIA ASDVs (STEP 16)
YES
NO
RCS DEPRESSURIZED TO ~200 PSIA
TIME TO CORE UNCOVERY LENGTHENED
14
AC POWER RECOVERED AFTER STEAM GENERATOR BLOWDOWN
YES
NO
LOW PRESSURE CORE DAMAGE WITH STEAM GENERATOR COOLING
8
OPERATORS RESTORE DIESEL GENERATORS (STEP 5)
YES
NO
9
OPERATORS RECOVER AC POWER VIA OFFSITE GRID (STEP 6)
YES
NO
COVERED BY EXISTING PROCEDURES
RCS REMAINS PRESSURIZED
NEW PROCEDURES REQUIRED
10
OPERATORS ESTABLISH STEAM GENERATOR COOLING VIA FIRE WATER PUMPS (ER 10.1)
YES
NO
RCP SEAL LOCA CONTINUES
11
AC POWER RECOVERED BEFORE EXCESSIVE RCP SEAL LEAK
12
OPERATORS DEPRESSURIZE RCS VIA PORVs (ER 10 2)
YES
NO
13
OPERATORS DEPRESSURIZE RCS VIA PORVs (ER 10 2)
YES
NO
HIGH PRESSURE CORE DAMAGE WITH NO STEAM GENERATOR COOLING
LOW PRESSURE CORE DAMAGE WITH NO STEAM GENERATOR COOLING
HIGH PRESSURE CORE DAMAGE WITH STEAM GENERATOR COOLING

Figure 2. Operator Action Sequence Diagram — Station Blackout

2.4 DIABLO CANYON PRA

This PRA (Reference 11) provides another example of a regulatory issue that was resolved when the deterministic requirements had resulted in a licensing impasse. This impasse was created when an earthquake fault was discovered in the vicinity of the Diablo Canyon plant during its construction. As a condition to obtain another strongly contested license, the plant owners were required to conduct a seismic research program. This program included the most comprehensive risk analyses of seismic events ever conducted. Significant advances were made to the state of the art of seismic risk analysis in order to obtain a reasonable balance and comparability of results for seismic and nonseismic contributors. Previous seismic PRAs could afford to leave in conservatisms because the seismic risk contributions was still very low. An important part of these advancements was the development of techniques that address the risk of relay chatter caused by the earthquake. Specific procedures were devised in this PRA for operator actions to recover the plant from particular relay chatter events found to be risk significant.

The final results of this PRA for core damage frequency, as illustrated in Figure 3, showed that seismic events made a significant contribution to core damage frequency but not the kind of dominant contribution that some may have expected. On a relative basis, the uncertainties for seismic events were much larger than for other contributors. On the basis of these results and the other elements of the seismic research program, the licensing impasse was resolved, and the plant investment was saved. This was an excellent example of how a specific problem of application addressed in a PRA had a great deal of impact on the way in which the project was conducted and the balance of resources and level of detail allocated to a specific part of the PRA models.

2.5 BEAVER VALLEY PRA

The Beaver Valley PRA (Reference 12) was the first such project completed by PLG that was originally intended to meet the individual plant examination requirements imposed by the NRC. After the project was started, however, a decision was made to perform the study in such a manner that an ongoing risk management program could be supported. This was also the first PSA project completed at PLG that was initially performed using the PC-based RISKMAN workstation software (Reference 3).

In addition to meeting the IPE requirements, there have been two PRA applications that have already been demonstrated using the Beaver Valley models that the authors would like to mention. The first was the use of the risk importance measures provided by the RISKMAN software to set priorities for equipment maintenance and operator actions in the emergency operating procedures. One set of results from this application is presented in Table 3. The risk

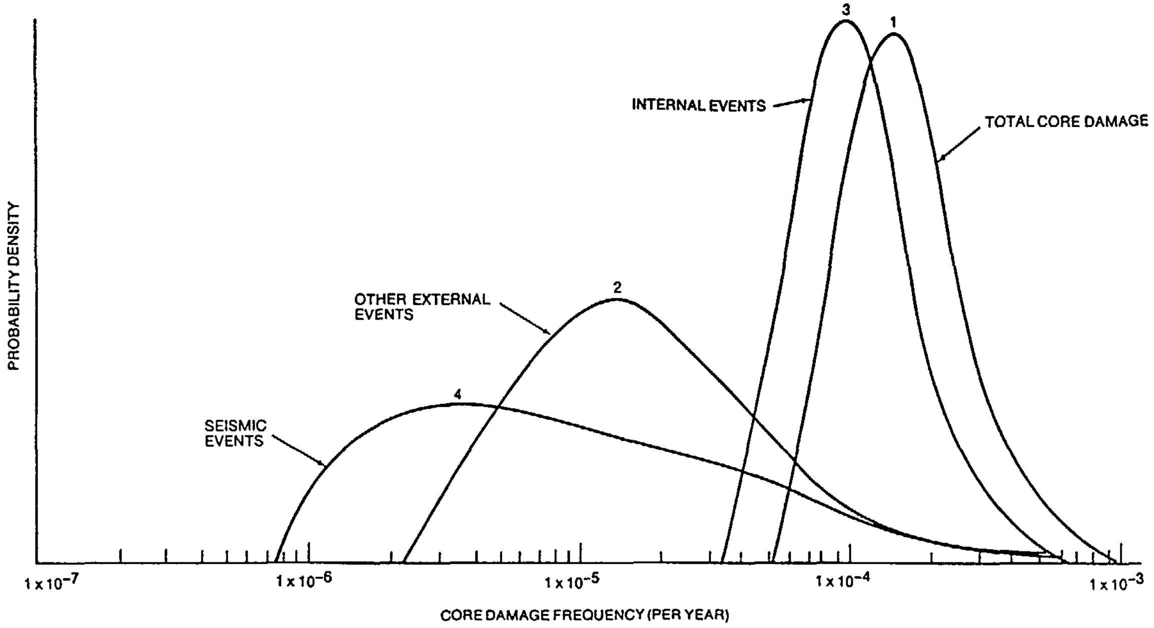


Figure 3. Core Damage Frequency Results of the Diablo Canyon PRA

Table 3. Risk Importance of Major Systems and Equipment

System or Equipment (Initiating Event, Top Event, and Split Fraction Designators in PRA Model)	Risk Importance Factors			Key Components and Failure Modes
	Initiating Event Cause	Response to Initiating Event	Overall Importance Factor	
Emergency Switchgear Rooms HVAC System (BVX)	.406	.083	.489	Dampers Close; Supply and Exhaust Fans Fail
Onsite AC Power System (AOX, BPX)	.059	.315	.374	Diesel Generators Fail To Start and Run
Offsite AC Power System (LOSP, OG)	.223	.028	.251	Loss of Offsite Power
Pressurizer Safety and Relief Valves (SLOCI, PA, PI, PK, PR)	.10	.175	.185	PORVs Failing to Reclose during Transient
Service Water System (WBX, ISFL, VPFL, ABFL, WAX, WXB)	.082	.086	.168	Source of Floods, Pump and Valve Failures
Auxiliary Feedwater System (AF)	--	.136	.136	Turbine-Driven AFW Pump during Blackout
Turbine, Steam, and Feedwater Systems (SGTR, PLMFW, TT, EXFW, TLMFW, LCV, TT, MS, MF)	.077	.001	.078	Transient Initiating Events
High Head Safety Injection System (HH, HC)	--	.061	.061	Operator Prematurely Terminates HHSI after Small LOCA
Refueling Water Storage Tank (SGFL1, SGFL2, RW)	.043	< .001	.043	Source of Floods
RCS Piping and Vessel (SLOCA, MLOCA, LLOCA, ELOCA)	.041	--	.041	Source of a LOCA Initiator
Solid State Protection System (SA, SB)	--	.031	.031	System Failures
Black (ERF) Diesel Generator (BK)	--	.031	.031	Fails To Start or Run
Secondary Component Cooling Water System (CS)	--	.013	.013	Failure of Unit 1 Filtered Water Pump after Loss of Offsite Power

importance factor used here is the fraction of the total core damage frequency associated with sequences in which specific hardware were failed or unavailable. These results reflect a large importance of support systems such as the switchgear room cooling systems, electric power, and service water systems. A high importance was also ascribed to the pressurizer PORVs due to a large contribution from sequences in which these valves lift during transients and fail to reclose. The identification of such sequences requires a detailed definition of event sequences and an explicit treatment of the support systems in this definition process. Conspicuous in their absence and low ranking in Table 3 are frontline safety systems that are normally emphasized in safety analyses. The scenario-based approach employed in RISKMAN always defines equipment importance only in the context of specific scenarios.

The second application demonstrated with the Beaver Valley models was the use of the existing models on RISKMAN to evaluate the safety significance of accident precursors that have occurred at other plants. A flow chart for this process is presented in Figure 4. To evaluate a precursor event using this procedure, the first step is to make use of the current results that, in many cases, can be used to bound the potential risk impacts. Then, if this is not successful, progressive steps are taken to update the current risk models to the extent needed to address the event. Only on rare occasions is a full event tree quantification needed to determine the risk significance of the event. This procedure is currently in use at Beaver Valley to evaluate the relevant precursor events.

2.6 SOUTH TEXAS PROJECT PSA

The PSA project for this plant (Reference 13) was unilaterally initiated by the plant owner to begin a comprehensive living PSA program, which is now in its ninth year of existence and is very active with numerous PSA applications. The first application was the identification of design improvements and procedure enhancements to improve safety. The design improvements that were identified and implemented from the PSA included conversion of motor-operated containment isolation valves in the seal return and purge lines to air-operated valves. This change reduced the likelihood of containment isolation and bypass failure and loss of primary coolant during station blackout sequences. There were also hardware changes to reduce the likelihood of the conditions for reactor coolant pump seal loss of coolant accidents. These

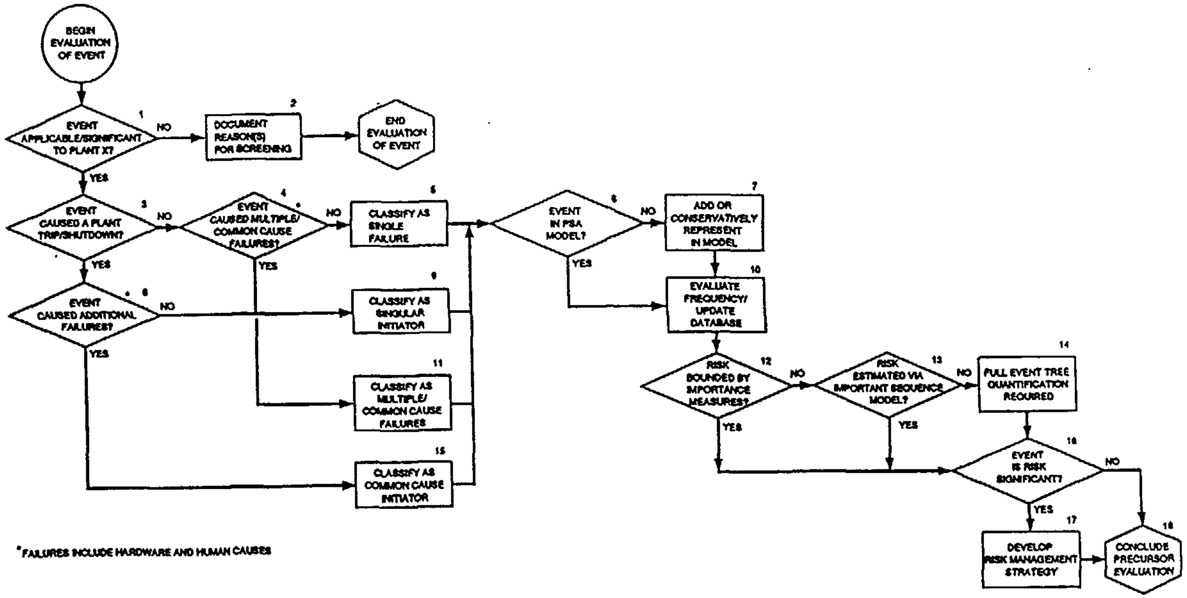

BEGIN EVALUATION OF EVENT
1
EVENT APPLICABLE/SIGNIFICANT TO PLANT X?
NO
2
DOCUMENT REASON(S) FOR SCREENING
END EVALUATION OF EVENT
YES
3
EVENT CAUSED A PLANT TRIP/SHUTDOWN?
NO
4
EVENT CAUSED MULTIPLE/ COMMON CAUSE FAILURES? *
NO
5
CLASSIFY AS SINGLE FAILURE
YES
YES
6
EVENT CAUSED ADDITIONAL FAILURES? *
NO
9
CLASSIFY AS SINGULAR INITIATOR
YES
11
CLASSIFY AS MULTIPLE/ COMMON CAUSE FAILURES
15
CLASSIFY AS COMMON CAUSE INITIATOR
8
EVENT IN PSA MODEL?
NO
7
ADD OR CONSERVATIVELY REPRESENT IN MODEL
YES
10
EVALUATE FREQUENCY/ UPDATE DATABASE
12
RISK BOUNDED BY IMPORTANCE MEASURES?
NO
13
RISK ESTIMATED VIA IMPORTANT SEQUENCE MODEL?
NO
14
FULL EVENT TREE QUANTIFICATION REQUIRED
YES
YES
16
EVENT IS RISK SIGNIFICANT?
NO
YES
17
DEVELOP RISK MANAGEMENT STRATEGY
18
CONCLUDE PRECURSOR EVALUATION
*FAILURES INCLUDE HARDWARE AND HUMAN CAUSES

Figure 4. Flow Chart for Use of RISKMAN PSA Models To Evaluate Precursor Events

changes included the ability to line up the technical support center diesel generator to a positive displacement charging pump that was independent of the electrically driven component cooling water system. In addition, the procedures were enhanced to reduce the likelihood that electrical building room cooling systems problems could result in damage to essential electrical system components. Substantial reductions in the frequency of core damage were obtained from these enhancements, and the effectiveness of the containment was also enhanced.

The next major PSA application at this plant was the use of the PSA to justify a complete overhaul of the plant technical specifications governing the periodic testing frequencies and allowed outage times for component maintenance. To provide a basis for justifying these changes from the PSA, Houston Lighting & Power Company arranged for a detailed review of the PSA with the NRC staff and its contractors that was much more detailed than will be needed for the IPE submittals. The NRC has completed this review and has accepted the results of the PSA to base line the technical specification review (Reference 14). A decision criterion was defined for technical specification changes: individual changes that increase core damage frequency by no more than 5% will be accepted. The plant owners anticipated major changes to the testing intervals and allowed outage times when the review is completed.

A new application that will support a more complete integration of the PSA models into the design and operations support organization at the plant is in progress. The event sequence diagrams that were produced in the PSA as a means of documenting key information necessary to define accident sequences properly are being converted to a computerized, three-dimensional graphical interface, as conceptually illustrated in Figure 5. These diagrams contain all of the sequences modeled in the PSA, explicit representation of key steps in the emergency operating procedures, emergency action levels, and a graphical link between the PSA and the configuration management system at the plant. These graphical "safety sequence diagrams" will become the singular source of information regarding event sequences at the plant. Once this interface is in place, additional applications to support the accident management program and to meet the new "maintenance rule" imposed by the NRC will be developed through the graphical interface.

2.7 REPUBLIC OF CHINA (TAIWAN) EMERGENCY PLANNING STUDY

The final application to be discussed in this paper is an extension of the emergency planning application that was discussed above for the Seabrook plant. Taiwan has two existing nuclear power plant sites on the northern coast of the island within the vicinity of Taipei and very close

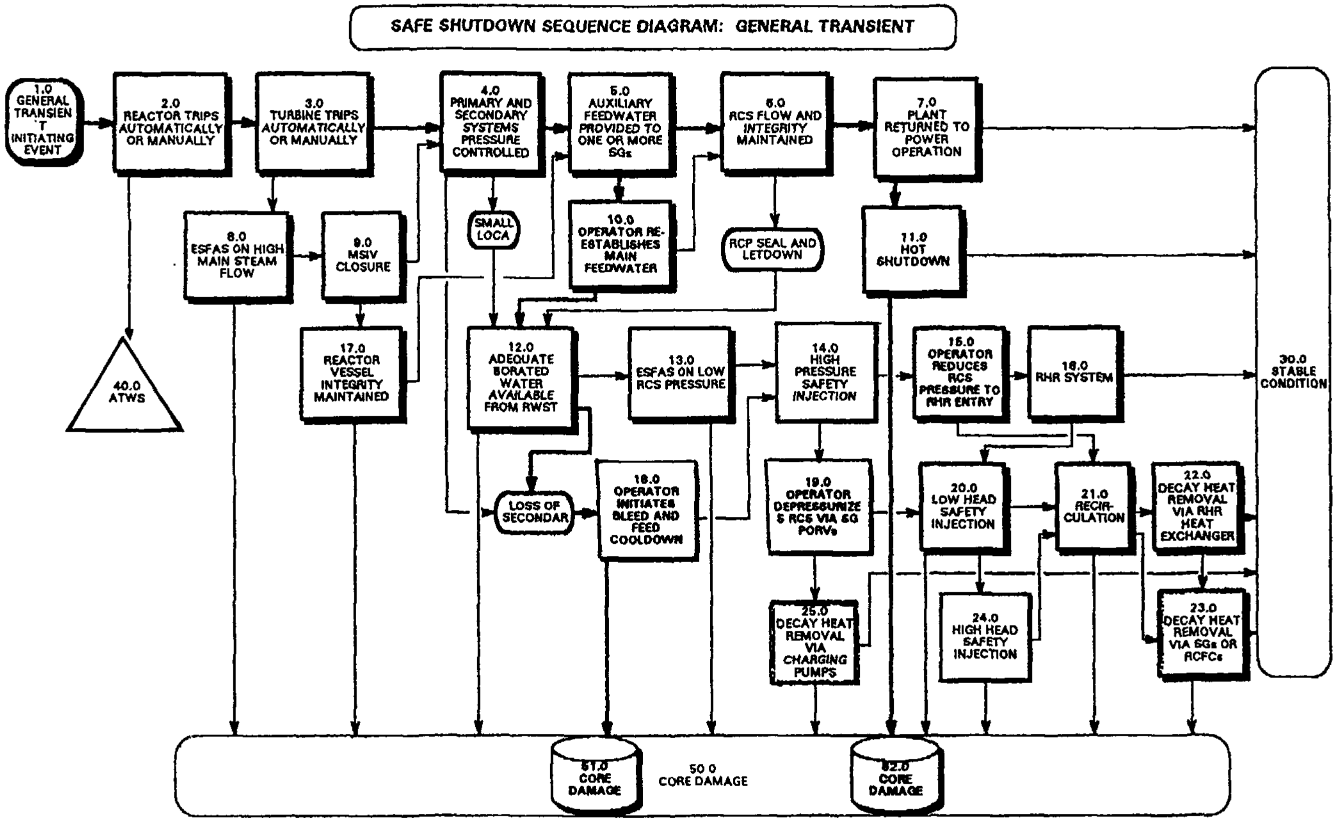
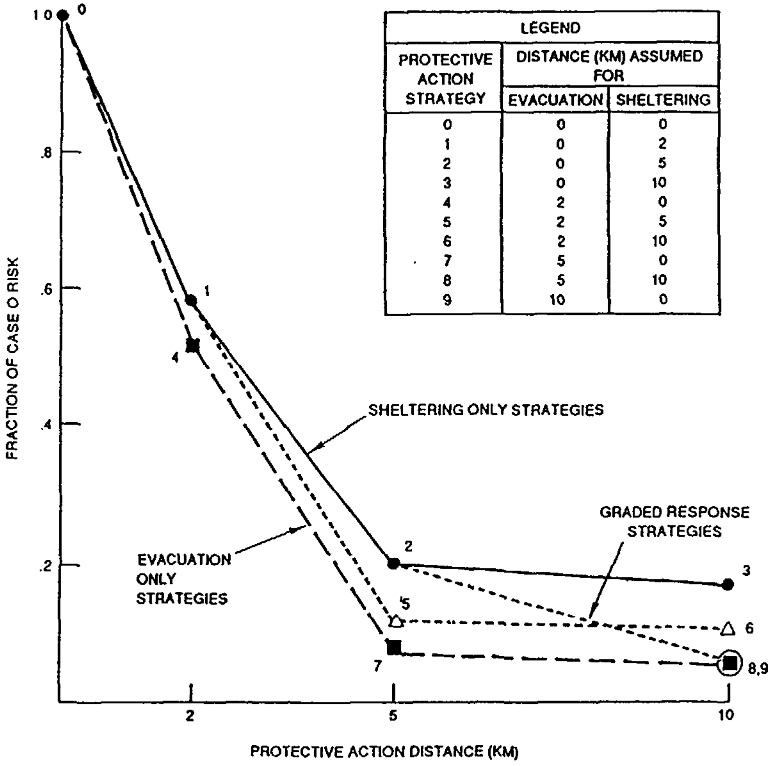

SAFE SHUTDOWN SEQUENCE DIAGRAM: GENERAL TRANSIENT
1.0 GENERAL TRANSIEN T INITIATING EVENT
2.0 REACTOR TRIPS AUTOMATICALLY OR MANUALLY
3.0 TURBINE TRIPS AUTOMATICALLY OR MANUALLY
4.0 PRIMARY AND SECONDARY SYSTEMS PRESSURE CONTROLLED
5.0 AUXILIARY FEEDWATER PROVIDED TO ONE OR MORE SGs
6.0 RCS FLOW AND INTEGRITY MAINTAINED
7.0 PLANT RETURNED TO POWER OPERATION
8.0 ESFAS ON HIGH MAIN STEAM FLOW
9.0 MSIV CLOSURE
SMALL LOCA
10.0 OPERATOR RE-ESTABLISHES MAIN FEEDWATER
RCP SEAL AND LETDOWN
11.0 HOT SHUTDOWN
40.0 ATWS
17.0 REACTOR VESSEL INTEGRITY MAINTAINED
12.0 ADEQUATE BORATED WATER AVAILABLE FROM RWST
13.0 ESFAS ON LOW RCS PRESSURE
14.0 HIGH PRESSURE SAFETY INJECTION
15.0 OPERATOR REDUCES RCS PRESSURE TO RHR ENTRY
16.0 RHR SYSTEM
30.0 STABLE CONDITION
LOSS OF SECONDAR
18.0 OPERATOR INITIATES BLEED AND FEED COOLDOWN
19.0 OPERATOR DEPRESSURIZE S RCS VIA SG PORVs
20.0 LOW HEAD SAFETY INJECTION
21.0 RECIR-CULATION
22.0 DECAY HEAT REMOVAL VIA RHR HEAT EXCHANGER
25.0 DECAY HEAT REMOVAL VIA CHARGING PUMPS
24.0 HIGH HEAD SAFETY INJECTION
23.0 DECAY HEAT REMOVAL VIA SGs OR RCFCs
51.0 CORE DAMAGE
50 0 CORE DAMAGE
52.0 CORE DAMAGE

Figure 5. Graphical Interface for South Texas PSA Scenarios

to a substantial volcanic mountain more than 3,000 meters high. The issue addressed in this study is how to develop a basis for defining emergency planning zones for protective actions of sheltering and prompt evacuation around these plants. Because PSAs had already been performed for the Taiwan nuclear plants, there was a desire to make appropriate use of the PSA information on severe core damage sequences. In this PLG project, decision criteria for selecting the size of the EPZ were developed (References 15 and 16) and applied to one of these plants. The decision criteria addressed the need to control the frequency versus distance over which protective action guideline doses were expected to be exceeded, and the need to obtain an optimum benefit of the emergency plan in terms of the risk averted through protective actions such as evacuation and sheltering. To demonstrate the application of these criteria, an existing Level 2 PSA for Kuosheng was updated to account for a reassessment of severe accident phenomena and source terms, and was extended to Level 3 so that the risk aspects of emergency planning could be addressed.

As illustrated in Figure 6, the risk reduction benefits of evacuation and sheltering were found to be almost fully realized within 5 km of the plant. Extensions to further distances were found to be of marginal benefit. A by-product of this study was the development of a new consequence model called CRACEZ (Reference 17) that models the three-dimensional dispersion effects of terrain that were found to be very important to obtain realistic consequence estimates.



LEGEND		
PROTECTIVE ACTION STRATEGY	DISTANCE (KM) ASSUMED FOR	
	EVACUATION	SHELTERING
0	0	0
1	0	2
2	0	5
3	0	10
4	2	0
5	2	5
6	2	10
7	5	0
8	5	10
9	10	0

Figure 6. Risk Reduction for Alternative Protection Action Strategies

3. CONCLUSIONS

As can be seen in the examples discussed in this paper, there have already been a number of successful applications of PSA in which issues were resolved and better decisions were made. On a number of occasions, the direct benefits of the PSA were immediately realized and were far in excess of the costs associated with performing the studies. Because PSA can be used to address virtually any issue regarding safety, the number and diversity of future applications are expected to grow substantially in the future. One of the most exciting, new developments that we expect to see is the use of dynamic decision aids for plant operators that keep track of the actual configuration impacts on risk and that provide diagnostic aids to deduce the causes of accident sequences and provide guidance to implement the appropriate accident management strategies.

REFERENCES

1. Bley, D. C., et al., "Zion Nuclear Plant Residual Heat Removal PRA," Pickard, Lowe and Garrick, Inc., prepared for Electric Power Research Institute, NSAC-84, July 1985.

2. Moody, J. H., et al., "Seabrook Station Probabilistic Safety Study—Shutdown (Modes 4, 5 and 6)," New Hampshire Yankee, Vols. 1-2, May 1988.

3. Epstein, S. A., "RISKMAN®: A System for PSA," presented at Third Workshop on Living-PSA-Applications, Hamburg, Federal Republic of Germany, May 11-12, 1992.

4. Pickard, Lowe and Garrick, Inc., Westinghouse Electric Corporation, and Fauske & Associates, Inc., "Zion Probabilistic Safety Study," prepared for Commonwealth Edison Company, Vols. 1-10, September 1981.

5. Pickard, Lowe and Garrick, Inc., Westinghouse Electric Corporation, and Fauske & Associates, Inc., "Indian Point Probabilistic Safety Study," prepared for Power Authority of the State of New York and Consolidated Edison Company of New York, Inc., Vols. 1-12, March 1982.

6. U.S. Nuclear Regulatory Commission, "Reactor Safety Study—An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400, NUREG-75/014, October 1975.

7. Pickard, Lowe and Garrick, Inc., "Seabrook Station Probabilistic Safety Assessment," prepared for Public Service Company of New Hampshire and Yankee Atomic Electric Company, PLG-0300, Vols. 1-6, December 1983.

8. Fleming, K. N., et al., "Seabrook Station Risk Management and Emergency Planning Study," Pickard, Lowe and Garrick, Inc., prepared for New Hampshire. Yankee Division, Public Service Company of New Hampshire, PLG-0432, December 1985.

9. Fleming, K. N., et al., "Risk Management Actions To Assure Containment Effectiveness at Seabrook Station," Pickard, Lowe and Garrick, Inc., prepared for New Hampshire Yankee Division, Public Service Company of New Hampshire, PLG-0550, July 1987.

10. PLG, Inc., "Beznau Station Risk Assessment—Plant with NANO," prepared for Nordostschweizerische Kraftwerke AG, PLG-0511, Vols. 1-5, December 1989.

11. PLG, Inc., "Diablo Canyon Probabilistic Risk Assessment," prepared for Pacific Gas and Electric Company, PLG-0637, Vols. 1-9, July 1988.

12. Duquesne Light Company, "Beaver Valley Unit 2 Probabilistic Risk Assessment, Revision (2)," March 1992.

13. Pickard, Lowe and Garrick, Inc., "South Texas Project Probabilistic Safety Assessment," prepared for Houston Lighting & Power Company, PLG-0675, Vols. 1-9, May 1989.

14. Letter from G. F. Dick, U.S. Nuclear Regulatory Commission, to D. P. Hall, Houston Lighting & Power Company, "Safety Evaluation by the Office of Nuclear Regulation related to the Probabilistic Safety Analysis Evaluation, South Texas Project, Units 1 and 2 (Docket Nos. 50-498 and 50-499)," January 21, 1992.

15. Fleming, K. N., et al., "EPZ Determination for Republic of China," PLG, Inc., prepared for Republic of China Atomic Energy Council, PLG-0767, Vols. 1-2, June 1990.

16. Fleming, K. N., and C. Yang, "Risk-Based Approach To Determination of Emergency Planning Zones for the Republic of China," *Proceedings of the International Conference on Probabilistic Safety Assessment and Management (PSAM)*, Beverly Hills, California, pp. 97-102, February 4-7, 1991.

17. Woodard, K., et al., "CRACEZ: A Radiological Consequence Model with Improved Modeling of Dispersion and Evacuation," *Proceedings of the International Conference on Probabilistic Safety Assessment and Management (PSAM)*, Beverly Hills, California, pp. 747-751, February 4-7, 1991.

A COMPUTER TOOL FOR SYSTEMS CONFIGURATION MANAGEMENT BASED ON PSA MODELS AND TECHNIQUES

G. GEORGESCU
Institute for Nuclear Research,
Pitesti, Romania

Abstract

In the frame of the IAEA coordinated research programme for expert systems development, in the Institute for Nuclear Research, a PSA based computer tool for systems configuration management is in progress. The system is designed to be integrated in the future "living PSA" system under development now. The design of the system is mainly based on the PSA model for Cernavoda NPP and the risk-based configuration management methods, taking into account the user requirements.

The system will be developed taking into account the expert systems techniques, specific PSA methods (MCS and path-sets generation, etc.) and friendly user interface features. The work done up to now for the system mainly consist of the users requirements identification, development techniques choosing and top-level system design.

1. Configuration management based on PSA techniques

During the plant operation some of the components can be out of operation due to testing or preventive/ corrective maintenance. If that happened for some critical components in the same time, the global risk can be significantly affected. Even that the outage time is very short the level of risk can be with a few orders of magnitude over the normal yearly level of risk.

The method consist of identification of those components for which the simultaneous outage must be avoided. For this reason the whole PSA model must be requantified considering certain groups of components are down in the same time. To identify all critical components combinations, a systematically approach is necessary:

1. The RAW importances are computed and ranked for all components.

2. The RAW importances are computed and ranked for groups of two components, following the rules:

-Components that are in the same MCS.

-Components that are part of different trains in the same system or from different systems.

3. The same procedure taking combinations of three components. Generally is not necessary to consider groups with more then three components.

The cut-off criteria must be checked to ensure that the combinations are not lost. If yes, the MCS must be regenerated.

The general criteria to define a certain combination of components as critical is the risk increase factor - $1/X^{1/2}$ over the normal risk level X.

It is considered that a certain combination is not critical,but is significant if the increase factor is over $1/X^{1/4}$.

If a combination is critical that must be avoided during operation.

If a combination is significant and that happened it is necessary to compute the risk compensating allowed downtime.

The risk compensating downtime determination take into account the risk relative variations. The method consists of the following steps:

a. Compute the risk increase factor:

If:

F1 - the risk if the combinations of components failures happened.

F0 - the normal level of risk

$F1 = f*F0$, where f - the risk increase factor.

f is the BIRNBAUM or RAW value.

$Rd = dF1 = d*f*F0$ - the risk due to components failures during time d.

d is the downtime express in years equivalent with Rd over 1 year.

b. Compute the allowed downtime to compensate the risk increase.

The risk Rd is expressed using the tolerance factor "n", so that the risk increase is under the normal level.

$$Rd = F0 / n ;$$

$$Rd = d*f*F0 = F0 / n ;$$

$\mathbf{d = 1 / (f * n)}$ - the allowed downtime.

2. System design.

In the present version the system is not designed to be used for the whole plant configuration management, no more than 1000 components being possible to be included in the fault tree model. The system can be used for one plant system configuration management, considering as the normal level of risk the required system unavailability or failures frequency.

The main parts of the system consist of:

- **Fault Trees library** - contains the F/T's model for the plant system of interest;

- **Components Data library** - contains the components and human error data according with the F/T model;

- **Processor module** - contains the main part of the system, designed for risk compensating configuration management and allowed downtime processing. The module is containing three submodules:

  - Fault tree processor - provides the qualitative and quantitative evaluation of F/T, including importances evaluation, according with the Configuration Management Processor requirements.

  - -MCS, RAW, Intermediate results module - library containing the F/T processor results and Configuration Management Processor requirements;

  - -Configuration Management Processor - according with the above described methodology determines the critical component combinations and the allowed downtime for significantly component combinations.

- **Control center module** - smart module providing the F/T library consistency with the Components Data Library, the consistency of the activity inside the Processor Module and the user interaction with the above modules.

- **User Interface Module** - interactive user interface allowing user to modify F/T and Components Data, processing requirements as well as the results presentation.

- **Results Processor** - provide the results presentation according with the user requirements on the screen or/and on the printer.

The ways that the system modules interact are presented in fig. 1.

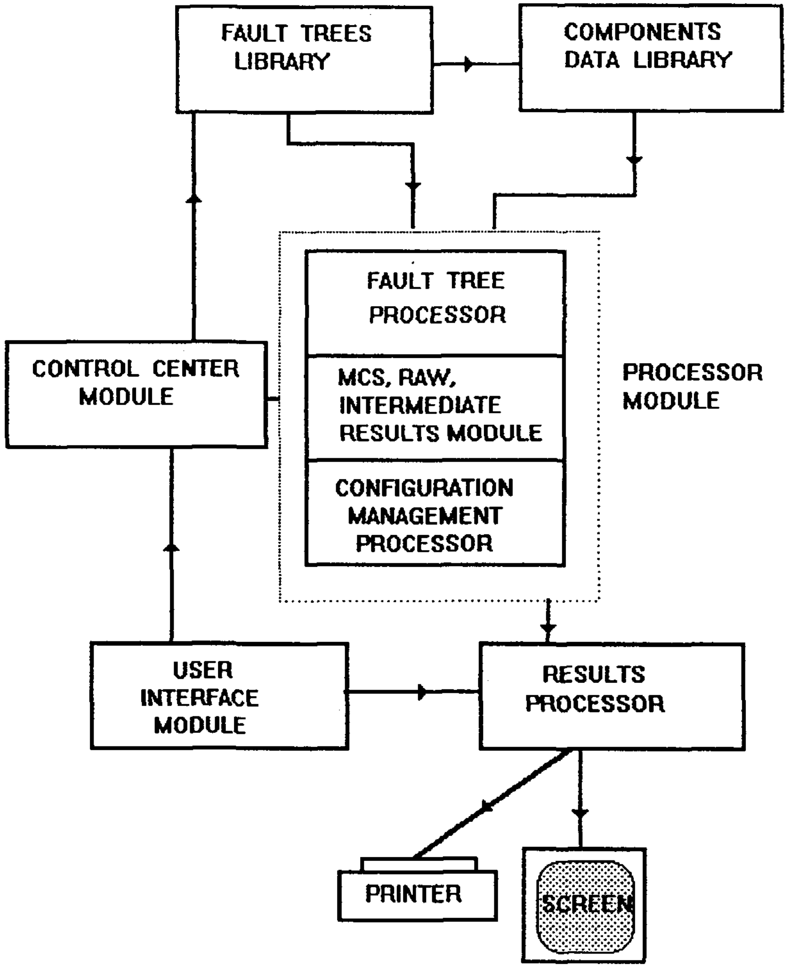


Figure 1

The system is designed to be implemented on a PC and to be used by:

-plant operators for safety systems configuration management;

-plant designer for safety improvements;

-regulatory for normal and emergency operating procedures and technical specifications development;

The top-level design as well as the module detaliated design is almost done.

The methodology was tested using some modules prototypes implemented on PC.

The experience and also some of the models will be included in the "living PSA" system which is under development.

REFERENCES

1. W. Vesely - Workshop on PSA applications, IEAE-INR, Sinaia oct. 1990

2. *** -"Measures of risk importance and their applications", NUREG/CR-3243, 1985

3. *** -"Evaluations and utilizations of risk importance", NUREG/CR - 4377, 1985

4. *** -"Measures of the risk impacts of testing and maintenance activities", NUREG/CR - 3541

LIST OF PARTICIPANTS

BELGIUM

Plys, M G
Fauske and Associates, Inc ,
c/o Westinghouse Energy Systems International,
Rue de Stalle 73, B-1180 Brussels

Wolvaardt, F P
Westinghouse Energy Systems International,
Rue de Stalle, 73, B-1180 Brussels

BRAZIL

Orlando Gibelli, S M
Comissão Nacional de Energia Nuclear (CNEN),
Rua General Severiano, 90 – Sala 412,
22294-900 Rio de Janeiro, RJ

Vieira, A S
Instituto de Pesquisas Energeticas e Nucleares,
Travessa R no 400, Cidade Universitaria - SP,
05422-970 São Paulo

BULGARIA

Kichev, E
Division of Technical Support, Power Production 1,
Kozloduy NPP, BG-Kozloduy 3321

Kolev, I
Risk Engineering Ltd,
ul Srebarna 21, BG-1407 Sofia

CANADA

Ballingall, N M
Atomic Energy Control Board,
280 Slater Street, P O Box 1046, Station ‘B’,
Ottawa K1P 5S9

CROATIA

Valcic, I
Ministry of Energy and Industry,
Av Vukovar 78, 41000 Zagreb

CZECHOSLOVAKIA

Brocko, P
SEP-Atómové Elektrárne, Mochovce, o z ,
CS-935 39 Mochovce

Čillík, I
Nuclear Power Plant Research Institute,
CS-Okruzna 5, 918 64 Trnava

Dusek, J
Nuclear Research Institute,
CS-Řež near Prague 250 68

Ferjencik, M
NPP Temelin, CEZ, a s , JE Temelin,
CS-373 05 Temelin Elektrárna

CZECHOSLOVAKIA (cont)

Hojny, V
Nuclear Research Institute,
CS-Řež near Prague 250 68

Novakova, H
VUPEX,
Bajkalská 27, 827 52 Bratislava

Patrik, M
Nuclear Research Institute,
CS-Řež near Prague 250 68

Rehácek, R
State Office for Nuclear Safety,
NPP Dukovany, CS-67550 Dukovany

Sedlák, J
Škoda Prague, Comp Ltd,
Bezručova 15, CS-316 00 Plzeň

Stanícek, J
Energoprojekt,
Bubenská 1, CS-170 05 Praha

Štván, F
Škoda Prague, Comp Ltd,
Bezručova 15, CS-316 00 Plzeň

Sváb, M
State Office for Nuclear Safety,
Slezská 9, CS-120 29 Prague

Valenta, V
Škoda Concern, Plzeň, Nuclear Machinery Plant,
Research and Development Centre Bolevec,
CS-316 00 Plzeň

FINLAND

Mankamo, T
Avaplan Oy,
Kuunsade 2 DE, SF-02210 Espoo

Pesonen, J M A
Teollisuuden Voima Oy,
SF-27160 Olkiluoto

FRANCE

Deriot, S M F
Direction des etudes et Recherches,
Electricité de France,
1, avenue du Général de Gaulle,
F-92141 Clamart

Reynes, L
Electricité de France, IGSN Direction générale,
32, rue de Monceau, F-75008 Paris

Ringot, C
COGEMA/NUSYS, EURISYS Consultants
14, rue du Printemps, F-750017 Paris

GERMANY

Berg, H-P
Bundesamt für Strahlenschutz,
Postfach 10 01 49, D-3320 Salzgitter 1

Kafka, P
Gesellschaft fur Anlagen-und Reaktorsicherheit (GRS) mbH,
Forschungsgelande, D-8046 Garching

Koban, I
Siemens AG, UB KWU,
Berliner Str 295-303, D-6050 Offenbach/M

Rumpf, J
TUV Norddeutschland e V ,
Große Bahnstr 31, Postfach 540220
D-2000 Hamburg 54

HUNGARY

Bareith, A
Institute for Electrical Power Research (VEIKI),
Zrinyi utca 1, H-1051 Budapest

Czakó, S
Institute for Electrical Power Research (VEIKI),
Zrinyi utca 1, H-1051 Budapest

Dobó, J
Paks Nuclear Power Plant,
P O Box 71, H-7031 Paks

Énekes, B
Paks Nuclear Power Plant,
P O Box 71, H-7031 Paks

Fichtinger, G
National Atomic Energy Commission, Nuclear Safety Inspectorate,
Logodi u 38-40, H-1012 Budapest

Gergely, J
Paks Nuclear Power Plant,
P O Box 71, H-7031 Paks

Holló, E
(Chairman)
Institute for Electrical Power Research (VEIKI),
Zrinyi utca 1, H-1051 Budapest

Karsa, Z
Institute for Electrical Power Research (VEIKI),
Zrinyi utca 1, H-1051 Budapest

Kretschmann, E
Committee for Technological Development (OMFB),
Szervita ter 8, H-1052 Budapest

Levai, F
Technical University of Budapest, Institute of Nuclear Techniques,
Mucgyetem rkp 9, H-1111 Budapest

Macsuga, G
Atomenergia Kutató Intézet,
H-1525 Budapest, Pf 49

Ordogh, M
Power Station and Network Engineering Co ,
Széchenyi rkp 3, H-1054 Budapest

HUNGARY (cont)

Siklossy, P
Institute for Electrical Power Research (VEIKI),
Zrinyi utca 1, H-1051 Budapest

Szabó, A
Power Station and Network Engineering Co ,
Széchenyi rkp 3, H-1054 Budapest

Szikszai, T
Paks Nuclear Power Plant,
P O Box 71, H-7031 Paks

Szonyi, Z
National Atomic Energy Commission, Nuclear Safety Inspectorate,
Logodi u 38-40, H-1012 Budapest

Vöröss, L
Institute for Electrical Power Research (VEIKI),
Zrinyi utca 1, H-1051 Budapest

ISRAEL

Brand, D
Soreq Nuclear Research Center,
Yavne 70600

KOREA, REPUBLIC OF

Kil-Yoo, K
Korea Atomic Energy Research Institute,
P O Box 7, Daeduk-Danji, Taejon 305-606

LITHUANIA

Bagdonas, A
Lithuanian Energy Institute,
Aukstadvario 3, Kaunas 3035

Uspuras, E
Lithuanian Energy Institute,
Aukstadvario 3, Kaunas 3035

MEXICO

Becerra Perez, J A
Comisión Nacional de Seguridad Nuclear y Salvaguardias,
Dr Barragan No 779, Col Narvarte, 03020 Mexico, D F

Nuñez Carrera, A
Comisión Nacional de Seguridad Nuclear y Salvaguardias,
Dr Barragan No 779, Col Narvarte, 03020 Mexico, D F

NETHERLANDS

Preyssl, C
ESA/ESTEC,
Postbus 299, NL-2200 AG Noordwijk

Versteeg, M F
Nuclear Safety Department,
P O Box 90804, NL-2509 LV Den Haag

POLAND

Kulig, M J
National Inspectorate for Radiation and Nuclear Safety
Konwaliowa 7, PL-03 194 Warsaw

ROMANIA

Georgescu, G S
Institute for Nuclear Research,
P O Box 78, RO-Pitesti

Turcu, I
Institute for Nuclear Research,
P O Box 78, RO-Pitesti

RUSSIAN FEDERATION

Frolov, E V
Opitno-Konstrukcioni Biro,
Burnakovsky proezd 15, 603603 Nizhny Novgorod 74, Moscow

Shvyryaev, J V
Atomenergoprojekt,
Bakuninskaya Str 7, Moscow 107815

SLOVENIA

Jordan, R
"Jozef Stefan" Institute,
Jamova 39, 61111 Ljubljana

SPAIN

Gutierrez, E
UITESA,
Juan Bravo 49 Dupl ,
E-28006 Madrid

Martorell, S
Departamento de Ingeniería Nuclear,
Universidad Politécnica de Valencia,
P O Box 22012, E-46071 Valencia

SWEDEN

Sandstedt, K J
RELCON AB,
Box 2057, S-171 02 Solna

Wilson, D G
RELCON AB,
Box 2057, S-171 02 Solna

UKRAINE

Gromov, G
Ukrainian State Committee for Nuclear & Radiation Safety,
St Observatornay 11/1, Kiev 254053

UNITED KINGDOM

Andrews, R M
Nuclear Installations Inspectorate,
St Peters House, Stanley Precinct,
Bootle, Merseyside L20 3LZ

Holloway, N J
UK Atomic Energy Authority, SRD Culham Laboratory,
Culham Abingdon, Oxon OX14 3DB

UNITED KINGDOM (cont.)

Preston, J F
Electrowatt Engineering Services Ltd,
Electrowatt House, North Street, Horsham,
West Sussex, RH12 1RF

Ross, P J
Nuclear Electric,
Booths Hall, Knutsford, Cheshire WA16 8QG

Stewart, J A
BEQE Ltd,
500 Longbarn Boulevard, Birchwood,
Warrington WA2 0XF

Tilstone, A J
British Nuclear Fuels plc,
Risley, Warrington, Cheshire WA3 61A4

UNITED STATES OF AMERICA

El-Bassioni, A A
US Nuclear Regulatory Commission,
Washington, DC 20555

Fleming, K N
PLG, Inc ,
4590 MacArthur Boulevard, Suite 400,
Newport Beach, CA 92660

Joksimovich, V
Accident Prevention Group,
16980 Via Tazon, Suite 110,
San Diego, CA 92127

Singh, B K
US Department of Energy, NE-74,
Washington, DC 20585

Specter, H
New York Power Authority,
123 Main Street, White Plains,
New York 10601

van Erp, J B
Argonne National Laboratory,
Bldg 223, 9700 South Cass Avenue,
Argonne, IL 60439

INTERNATIONAL ATOMIC ENERGY AGENCY

Tomic, B
(Scientific Secretary)
Safety Assessment Section, Division of Nuclear Safety,
International Atomic Energy Agency,
Wagramerstraße 5, P O Box 100,
A-1400 Vienna, Austria