STUK-YTO-TR 168 September 2000

EXPERIENCES FROM THE LNPP-P&DSA REVIEW

Lessons learned from RBMK safety studies

T. Mankamo
Avaplan Oy
J. Marttila, H. Reponen
STUK

STUK • SÄTEILYTURVAKESKUS • STRÅLSÄKERHETSCENTRALEN
RADIATION AND NUCLEAR SAFETY AUTHORITY

The conclusions presented in the STUK report series are those of the authors and do not necessarily represent the official position of STUK.

ISBN 951-712-412-0
ISSN 0785-9325

Oy Edita Ab, Helsinki 2000

MANKAMO Tuomas (Avaplan Oy), MARTTILA Jouko, REPONEN Heikki. Experiences from the LNPP-P&DSA review. Lessons learned from RBMK safety studies. STUK-YTO-TR 168. Helsinki 2000. 43 pp.

ISBN 951-712-412-0
ISSN 0785-9325

Keywords: Keywords: Leningrad nuclear power plant, LNPP, LAES, Sosnovy Bor, RBMK, probabilistic safety assessment, PSA, peer review

ABSTRACT

RBMK is the Russian acronym for “Channelized Large Power Reactor”. The Soviet-designed RBMK plants deviate substantially from typical Western BWR or PWR plants. The safety of the RBMK plants has raised severe concerns since the major accident at Chernobyl Unit 4 in 1986. In addition, a fire destroyed the turbine hall of Chernobyl Unit 2 in 1991 resulting in a near-accident: the rector cooling could only be maintained through improvised measures. Another well-known fire event is the control cable room fire at Ignalina Unit 2 in 1989, which led to a partial loss of the main control room functions.

After the collapse of Soviet Union several multilateral safety programs were started to evaluate and improve the safety of the RBMK plants. A Probabilistic and Deterministic Safety Assessment (P&DSA) of the Leningrad Nuclear Power Plant (LNPP) Unit 2 was started in 1996. Phase 2 of the project was completed in January 1999. A Peer Review was performed by Russian and Western experts.

This report describes the insights from the RBMK risk studies, especially from the LNPP P&DSA with emphasis on the deeper understanding of the risk-important design factors and identification of possible ways to increase safety. LNPP P&DSA has meant a significant progress in this respect. Despite of its certain limitations P&DSA Phase 2 could point out short-term measures, which substantially reduced the risk of identified weaknesses, mostly related to the reliability of the emergency feedwater function and its support systems.

The findings of LNPP P&DSA and the review recommendations emphasize the extensions needed to the analysis scope. The spreading and other influences of fires and floods between connected spaces should be analyzed because of incomplete separation and protection in these regards in the 1st generation RBMK plants. High priority should be given to the analysis of external hazards, which were found important at the Loviisa NPP on the Northern side of the Finnish Gulf, e.g. seismic events, mass emerge of algae, frazil ice, high wind and snow storm. An in-depth analysis is needed to evaluate the reliability of the control and protection systems to improve the simplified approach of P&DSA Phase 2. The reliability of the primary circuit piping should be evaluated based on the results of the in-service inspections, which recently have revealed many severe defects at the RBMK plants.

The review recommendations have been taken into account in planning the LNPP In-depth Safety Assessment (LISA), which includes PSA Phase 3. The work thus far adds to the expertise of the PSA earlier started for Ignalina NPP. It is highly recommended that the PSA activity is also launched at the other RBMK plants to support the identification and prioritization of cost-effective safety improvements and to facilitate tackling the generic safety weaknesses of this type of reactor and plant.

PREFACE

As many other countries and international groups, Finland has been running a nuclear safety assistance program to the ex-Soviet reactors, their operators, and national regulators since the early 1990's. The main focus of the Finnish program has been on the Leningrad Nuclear Power plant with its four RBMK units. The international Probabilistic and Deterministic Safety Assessment (P&DSA) of LNPP Unit 2, and its peer review run in 1997–99 by participants from several countries offered an opportunity to utilize the Finnish knowledge of the Soviet-designed reactors. Based on the LNPP unit 2 specific study, this report gives a short overview featuring the risks of RBMK reactors in general, and the LNPP Unit 2 in detail. The improvements to the next phase PSA studies are proposed in order to identify and solve still existing safety problems.

CONTENTS

1 INTRODUCTION

This chapter describes the purpose of the report and provides general background.

1.1 General background

Since the accident at Chernobyl unit 4 on 26th April 1986, the safety of RBMK-type reactors has internationally been considered as a great concern. In many countries this concern has also affected the common opinion on the acceptability of nuclear power in general. After the accident many safety studies and programs were carried out to gain better information and understanding of the risks related to RBMK plants. Efforts to eliminate major risks were also initiated in Soviet Union, operating these reactors.

The fire in the turbine hall of Chernobyl unit 2 on 11th October 1991, was another serious hazard at a RBMK plant, which led to severe disturbances in the main process of reactor cooling. Only some very extraordinary measures to remove residual heat saved the plant unit, with a small margin, from severe reactor accident.

After the collapse of Soviet Union, Western countries launched several multi- and bilateral programs in cooperation with Russia (and Ukraine and Lithuania) to analyze and improve the safety of RBMK plants in different fields. A generic difficulty in these projects has been the lack of general and comprehensive perspective on the design and operational safety of RBMK plants among the Western partners. This is partly due to the large differences in design features in comparison to the Western boiling and pressurized water reactors (BWR, PWR). Consequently many projects have not been very effective from the nuclear safety point of view, even if a number of improvements have been achieved in the scope of activities.

In Western countries, probabilistic safety analysis (PSA) studies were started after the Tree Mile Island reactor accident, which took place in 1979. Nowadays PSA technique provides a valuable tool to give insights into the risk associated with a nuclear power plant in operation as well as new plants in the design phase. E.g. in Finland large programs to develop PSAs for Loviisa and Olkiluoto NPPs were started in early 1980s. Quality, coverage and depth of PSAs have been systematically improved in the course of years. A lot of safety improvements, both in hardware and software, have been implemented on the basis on PSA results and findings. These improvements have largely reduced the initially estimated risk of the plants.

At present, PSA is a practical tool which is widely used in many countries for improving and balancing the overall plant safety and design modifications, as well as in-service inspections, maintenance and operational aspects. The full utilization of the PSA technique necessitates creation of (so called) Living PSA activity and adequate in-house capabilities and resources.

It is an internationally accepted goal to carry out PSA studies also for all Soviet-designed reactors. A Probabilistic and Deterministic Safety Analysis (P&DSA) of the Leningrad Nuclear Power Plant (LNPP), Unit 2, was completed in January 1999, and the Peer Review in September 1999. The P&DSA project utilized the experience from many parallel safety studies, especially the PSA of Ignalina Unit 2 (called also as Barselina project). Barselina and LNPP P&DSA have to be seen as pilot studies and starting points for further development. There are still significant limitations in the scope and quality of the RBMK PSA models but a number of conclusions can be drawn to support the planning of effective safety improvements and to direct continued analysis efforts to right targets. Further progress requires comprehensive deterministic and probabilistic safety studies of high quality. This work will need extensive efforts in the coming years.

Table I. Safety studies of RBMKs.

Plant	Generation	Title	Year	Type
Leningrad 1 Ignalina 2 Smolensk 3	1 2 3	RBMK Safety Review TG9, Pilot Risk Studies	1994	Mini PSA
Ignalina 2	2	BARSELINA Phase 4	1996	PSA Level 1
Leningrad 2	1	LNPP-P&DSA Phase 2	1999	PSA Level 1

1.2 Objectives of the report

This report will partially repeat the general insights from the P&DSA and Peer Review as presented in the Review Main Report [RMR]. However, the focus is different: here the emphasis is on deeper understanding of the RBMK safety problems and issues—from risk point of view—in general and for LNPP Unit 1 and 2 in particular.

In this report the risk studies of RBMKs thus far, Table I, are retrospectively compared. The improvement needs for the next phase of LNPP-P&DSA will be indicated on the way towards the highly recommended development and application of a Living PSA, i.e. to promote a similar development process as found very useful in many countries, e.g. Finland.

2 GENERAL DESCRIPTION OF RBMK

This chapter gives an overview of the RBMK plants and their principal safety features.

2.1 RBMK population

Acronym "RBMK" stands for Russian initials of "Channelized Large Power Reactor". RBMK is a graphite moderated, pressure tube, boiling water reactor. This type of reactor has only been constructed in the ex-Soviet Union. Graphite reactors were originally designed for plutonium production, but later on the design was adapted to electricity production.

Currently, 14 RBMK units are in commercial operation and three units (Chernobyl 1, 2 and 4) are permanently shut down, Table II. Six units are considered to be of 1st generation and ten of 2nd generation. Ignalina 2 contains safety features that are beyond those of other second-generation units. Smolensk 3 is the only third-generation unit in operation. The only RBMK-reactor under construction is Kursk 5. A summary of the general features, and modifications done since the Chernobyl accident in 1986, are presented in [PSA-SUDR, Section 5.2].

The Leningrad Nuclear Power Plant (LNPP) has two stages: twin Unit 1 and 2, and another twin Unit 3 and 4. The main differences between the stages are in the emergency cooling systems and in the reactor confinement systems, which have limited capability in Unit 1 and 2 but have been improved in Unit 3 and 4.

2.2 Main safety features

The peculiar feature of the RBMK reactors is the construction of the reactor core and the primary circuit. The massive graphite neutron moderator core is penetrated by over 2000 vertical channels. In fuel channels (1661 at LNPP 2), the fuel elements are mounted inside Pressure Tubes (PTs). In addition to the fuel channels there are special channels for the control rods and in-core power monitoring detectors. Refuelling takes place daily during full power operation.

The coolant flows inside PTs, which form a part of the pressure boundary in Primary Coolant System (PCS). The reactor is composed of two halves, which are cooled by two separate coolant circuits. The cooling water boils when rising in the PTs. In this sense RBMK is similar to a Boiling Water Reactor (BWR). However, PCS is much more complex in RBMK, because steam separation occurs in disjoint big vessels, Steam Drums (SDs), two on each half of PCS. The coolant is circulated via downcomer pipes, main coolant pumps, suction and pressure collectors, and group distribution headers into the fuel channels. More details of PCS will be discussed in connection with LOCA categories, Section 5.6.

The large size of the reactor core and large number of fuel channels mean that the definition of core damage state is more complicated than in the PSA for a BWR or PWR. Without going into details, three principal core damage states are defined, Table III.

The accident at Chernobyl 4 was related to the reactor core reactivity problems. The core design and fast reactor shutdown function have been improved since then. More recently, the reliability of the PCS piping has been found to be a major safety problem. Another serious weakness in the RBMKs is the plant lay-out and placement of the safety related components with incomplete physical separation between the redundant systems and subsystems. The building structures are not capable to withstand extensive fire or flood. The potential of common mode failures is high. The application of diversity and redundancy principles is insufficient in general, especially in the 1st generation of RBMK plants.

Table II. *RBMK units.*

Plant	Units	Generation	Power level, MWe	Start of operation	Country
Chernobyl	1*–2*	1	1000	1977, 1979	Ukraine
	3–4*	2	1000	1981, 1984	
Ignalina	1–2	2	1500	1983, 1987	Lithuania
Kursk	1–2	1	1000	1976, 1978	Russia
	3–4	2	1000	1983, 1985	
Leningrad (Sosnovy Bor)	1–2	1	1000	1973, 1975	
	3–4	2	1000	1979, 1981	
Smolensk	1–2	2	1000	1982, 1985	
	3	3	1000	1990	

*) Chernobyl Unit 1, 2 and 4 are permanently shut down.

Table III. *Principal core damage states (Hazard States) defined in LNPP-P&DSA.*

Hazard State	Description	Definition
V	Violation state	Damage in one fuel element or rupture of one PT
D	Damage (partial core damage)	Damage in at most 80 fuel elements or rupture of 2-9 PTs
A	Accident (gross damage of the core, severe accident)	Damage in more than 80 fuel elements or rupture of more than 9 PTs

3 OVERVIEW OF THE RBMK RISK STUDIES

This chapter presents an overview of the risk assessments for RBMKs regarding the objectives, scope, organization, uses of the results and limitations.

3.1 RBMK Safety Review TG9, Pilot Risk Studies

Topic Group 9 of the CEC Tacis Programme project "Safety Review of RBMK Reactors" conducted a scoping risk assessment of three units of different design generations [RBMK/TG9/FR], see Table I. The objective has been to review the safety status of RBMKs, to express that in terms of risk level and assess potential safety improvements.

The topic group used a screening method called Pilot Risk Study (PRS) to produce risk estimates. A key idea in PRS is to associate the failure probability of 10^{-3} to a standard safety system with two redundant trains. Specific features were taken into account by influence factors, e.g. related to the following aspects:

- extra redundancy or lack of separation
- high or low test frequency
- complexity of required operator actions

The PRS applications benefited from the Barselina Phase 2, which was completed at that time, and also from the parallel Phase 3. For example, a part of the IE frequencies were obtained from the data gathered for Barselina, while the rest had to be based on generic Western experience.

A part of the qualitative findings from the PRS applications are confirmed by the later PSAs (Barselina 4 and LNPP-P&DSA Phase 2). But another part of the statements based on quantitative PRS results are not substantiated, as will be discussed in more details in Chapter 6. As expected, PRS method could not identify design weaknesses, which are in contradiction with the design rules of Western NPPs. Typically such weaknesses are likely to be detected and removed with the help of the system and safety analyses, which are a part of standard Western FSAR process (compare to LISA in 3.3.1).

3.2 Barselina 4

The Barselina project was initiated in 1991 as a multilateral co-operation between Lithuania, Russia and Sweden. The Swedish Barsebäck plant was used as a reference plant and Lithuanian RBMK Ignalina Unit 2 as application plant, which is the background to name "Barse-lina". Phase 3 was completed in 1994 representing a Level 1 PSA of internal IEs, i.e. covering plant transients, Loss of Off-site Power (LOOP) and LOCAs.

In Phase 4 the scope was extended to cover fires, floods and missiles, i.e. so called Area Events (AEs), by using a simple index method. Also the modeling of control, protection and power supply systems were improved. The scope is similar to LNPP P&DSA Phase 2, which will be discussed in detail in Section 3.3.2. The scope limitations will be commented in Section 5.8. Barselina 4 was completed in 1996 [BR417].

The overall result for the risk frequency (Hazard States A and D) was $3 \cdot 10^{-5}$ /a, which divided up into main contributors as shown in Fig. 1**.** The leading IE is LOOP with dominant contributors from CCF of DGs or multiple failure of MSRVs to reclose. The plant transients together also make a substantial contribution with dominating failures

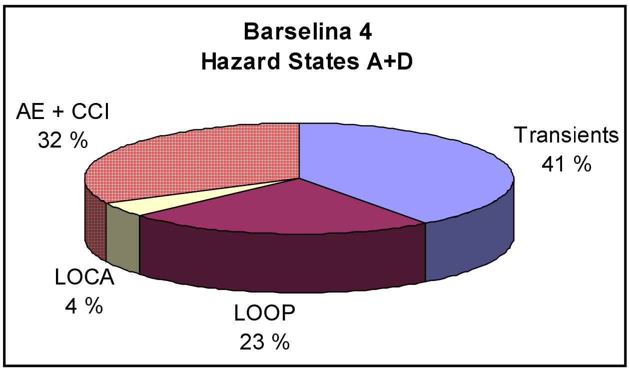

Figure 1. *Risk contributions (Hazard States A and D) for Barselina 4 by IE category.*

in the intermediate cooling circuits. The results including the relatively small contribution of LOCAs will be discussed in more details in connection with the comparisons in Chapter 6.

Phase 4 of the PSA was followed by an extensive project to prepare a Safety Analysis Report (SAR) for Ignalina NPP. This project was accompanied by an independent review [Riskaudit-55]. One of the central issues was the reliability of the control and protection systems, which at the RBMK plants consist of two interrelated systems: reactor control and protection system CPS and process parameter control system AZRT (see more details in Section 5.2). It was acknowledged that Phase 4 of the PSA used a simplified model, which did not take adequately into account dependencies between CPS and AZRT nor between actuation of fast and normal scram. A specific problem is that the control and protection systems of the RBMK plant serve dual purpose to provide both process control during normal power operation and actuation of safety systems in transient and accident conditions. In the Western NPPs the process control and actuation of safety systems are strictly isolated functions.

Ignalina SAR contained Single Failure Analysis (SFA) and Engineering Assessment of the CPS and AZRT. According to the review comments it seems that these tasks could not completely be executed but the above mentioned dependency problems were found evident. The principal outcome was the recommendation to install a diverse shutdown system (DAZ) to generate a redundant reactor scram signal. It is also of interest to notice that the updated reliability analysis of CPS and AZRT gave a result of about 10^{-4} /demand for the failure probability of reactor scram actuation in the current state [BR5-CPS]. STUK´s YVL Guide 2.8 for PSA gives failure probability $\leq 10^{-5}$/demand for reactor scram function as a numerical design objective.

An external review of limited extent was conducted for Phase 3 of Ignalina PSA [PNL-10378], but none for Phase 4 (system analysis issues were later covered in the independent review for Ignalina SAR). This is the background for several weaknesses, which were transplanted from Barselina 4 into LNPP-P&DSA, as will be discussed in more detail in Chapter 5.

3.3 LNPP-P&DSA Phase 2

3.3.1 Organization

The P&DSA of LNPP Unit 2 was started in 1996 and conducted by experts from Russia, Sweden, United Kingdom and United States. It included in-depth system descriptions and deterministic analyses to support PSA modeling. These extended tasks were necessary due to the lack of FSAR, which normally provides the basic information for the PSA from the shelf. The substantial role of deterministic analyses is the background to the use of label “P&DSA”.

Phase 1 of P&DSA served as an initiating phase. Phase 2 was completed in January 1999 and is similar in scope and level with Barselina 4. The supporting organizations were mainly the same as were the general approach and methodology. Thus LNPP-P&DSA can effectively be considered as a successor of the Barselina project. The P&DSA study is being extended to a Leningrad In-depth Safety Assessment (LISA) in compliance with the requirements for granting a long term license by the national regulator. The LISA project will include a further phase of PSA (numbered as PSA Phase 3).

3.3.2 Objectives

The primary objectives were to assess the level of plant safety and to identify the dominant risk contributors and most effective areas for safety improvement as well as to prepare a team of experts capable to carry out continued in-house analyses using P&DSA project results and experience.

3.3.3 Scope

The base case was defined as the fully reconstructed plant (FRP). Other configurations were considered as sensitivity analysis cases. This fundamental scope issue will be discussed in the next subsection. In the analysis and modeling details the scope was defined in the following way [LPR150, Table 1]:

1) Hazards states to be considered are partial core damage (D) and total core accident (A)

Table IV. *Primary safety functions and support functions with the corresponding frontline safety systems and support systems—excluding reactor confinement function, which is not covered in Level 1 PSA. The new systems belonging to the long-term reconstruction program FRP are presented in italics. The systems, which are planned to be modernized in a substantial degree are indicated by asterix *.*

Safety function	Front-line safety system	Building
Reactor shutdown and actuation of safety systems	Control and Protection System CPS	401/B
	Process Parameter Control System AZRT*	401/B
Pressure control of the primary circuit	Main Safety/Relief Valves MSRVs*	401/D
	Steam dump to bubbler BRU-B	401/D
Emergency feedwater	Emergency Feedwater System APEN/EFWS	401/D
	Auxiliary Feedwater System MPEN/AFWS*	401/G
	Main Feedwater System PEN/MFWS	401/G
ECC—short term (2 min)	MCP rundown (inertia) and PEN/MFWS	401/B, G
	ECC tanks	*402/B*
ECC—intermediate term (1 hr)	*Emergency Core Cooling System SAOR/ECCS*	*402/B*
	Emergency Feedwater System APEN/EFWS	401/D
	Auxiliary Feedwater System MPEN/AFWS*	401/G
	Main Feedwater System PEN/MFWS	401/G
ECC—long term (8 hr)	*Emergency Core Cooling System SAOR/ECCS*	*402/B*
	Emergency Feedwater System APEN/EFWS	401/D
Support function	**Support system**	**Building**
Power supply	Electric Power Supply Systems SNES/EPSS	401/D, 475
	Electric Power Supply Systems SNES/EPSS	402/B
Service water	Normal Service Water System NA/NSWS	410
	Reliable Service Water System SNTV/RSWS	*480*

2) Full power state (i.e. 50%...100% nominal) is only considered
3) Initiating events (IEs) to be covered:
   - Internal IEs (transients, LOCAs and CCIs)
   - Area Events (AEs) limited to internal fires, flooding and missiles
4) Time window of 24 hours after the IE is considered

The Large LOCAs (in the pipes of diameter above 300 mm) were excluded. These specific scope issues will be addressed further in Chapter 4 and 5. The review comments on the scope limitations will be summarized in Section 5.8.

3.3.4 Reference configuration of Unit 2, reconstruction issue

The base case model in P&DSA Phase 2 is the plant after the implementation of the full reconstruction program (FRP), which is described in [LPR150, LPR016]. Most essential aspects are highlighted in Table IV, which shows primary safety and support functions and corresponding systems. The new systems comprise first of all new ECCS and new diesel-backed electric power supply system (EPSS) to be located in the new safety building (402/B) as well as new Reliable Service Water System (RSWS) to be placed in the new sea water pumping station (480). Furthermore, new Accident Localization System SOVA/ALS is under design and construction to enhance the reactor confinement function. The realization of FRP goes into the remote future, especially regarding ECCS and ALS.

Also the construction of Emergency Control Room (ECR) and a second independent reactor shutdown system has to be emphasized. They are implicitly taken into account in FRP, e.g. by neglecting AEs, which can affect Main Control Room (MCR), control cabinet rooms and related cable rooms.

Upgrading of many plant systems is an ongoing process. The most significant upgrades to the existing systems are the following:

- MSRVs will be equipped with pilots of new design
- MPEN pumps will be relocated in a separate compartment (currently on the main level in the turbine hall); third pump will be installed (currently two)
- The intermediate cooling circuits will be modernized
- Partial modernization of the Process Parameter Control System AZRT/PPCS

In order to evaluate the safety of the existing state (mid 1998) a dedicated sensitivity analysis model—labeled as SNTV-3—was constructed by the use of model switches (conditional basic events) to remove the planned new safety systems and other safety upgrades credited in FRP. The problems related to switching off the not existing safety upgrades and the general drawbacks of the approach using FRP as the base case model of PSA will be discussed in Section 4.3. At this point it has to be underlined that the SNTV-3 case results contain large uncertainties and have thus to be utilized with great care.

3.3.5 Analysis results

The results for Hazard State A (Accident) are presented for SNTV-3 and FRP by IE category in Fig. 2 and 3, respectively. The most striking aspect is the dominance of AEs, which is mainly due to fires and floods affecting the existing service water system NA/NSWS. This is dominant both for SNTV-3 and FRP condition. Because of the limited capacity for emergency core cooling in the current state

Table V. *Unit configurations analyzed in P&DSA Phase 2.*

Configuration	Description
SNTV-3	Sensitivity case, which approximates Mid 98 condition
PRM-1	Partially Reconstructed Model, which incorporates near term improvements (approximates Mid 99 condition)
PRM-2	Incorporates intermediate term improvements, especially the new Reliable Service Water System SNTV/RSWS
FRP	Fully Reconstructed Plant (base case)
FRP Improved	Improved design of FRP

the small contribution of LOCAs in SNTV-3 is an unexpected result. The explanation can be an underestimation of the LOCA frequencies, see Section 5.6. Also the small contribution of LOOP, especially in SNTV-3, is somewhat unexpected and can be related to optimistic assessment of the LOOP frequency, see Section 5.3.

It must be emphasized that the presented results are conditional with respect to the scope limitations of P&DSA Phase 2. Review insights in this regard will be discussed in Section 4.5.

3.3.6 Recommended safety improvements

The risk levels for the various unit configurations between SNTV-3 and FRP were also evaluated, see Fig. 4 and Table V for the configuration definitions. Furthermore, potential improvements to FRP design were considered in an additional sensitivity case. The results from these sensitivity cases were used to evaluate the benefit and priori-

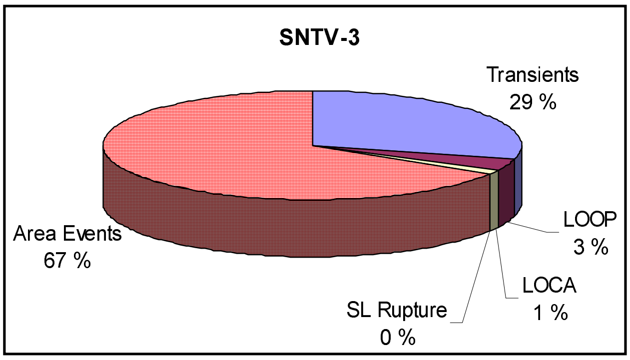

Figure 2. *Risk contributions (Hazard State A) for SNTV-3 by IE category.*

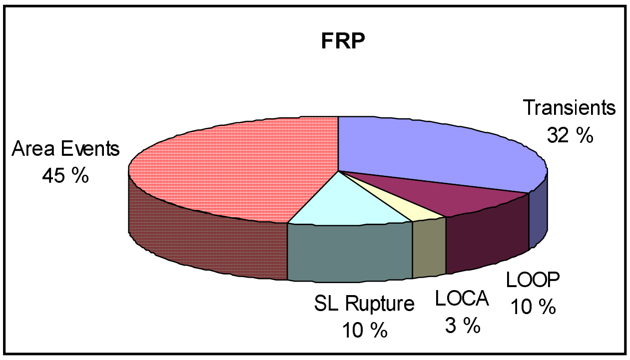

Figure 3. *Risk contributions (Hazard State A) for FRP by IE category.*

Table VI. *Near-term safety measures decided by LNPP (December 1998) for LNPP Unit 1 and Unit 2.*

No.	Description of the safety measure
1	Develop operator instruction to control and monitor the operation of APEN pumps if there is no service water supply for cooling of the motors
2	Develop operator instruction to provide make up to the deaerators (emergency steam condensation system) and APEN tank (using main condense system or unsalted water system in order of turn) in long-term emergency cooling condition
3	Add periodic test for the connection of sea water injection to the APEN suction header
4	Add monthly test for the check valves in the injection lines from APEN to DSs
5	Develop operator instruction to provide sufficient cooling to the diesels on both units simultaneously following loss of offsite power with subsequent failures of Unit 2 service water to restart and establishment of a link to the Unit 1 service water supply
6	Supplement the Study Program of the Unit Control Room operators to provide continuous practice in managing the emergency cases found important in PSA; the emergency cases to be implemented in the analytical simulator
7a	Provide air cooling of the motor of one APEN pump (unconnected cooling pattern)
7b	Provide heat removal from room N°. 049 at operation of APEN (motor cooled by air)
8	Test to demonstrate the operability of APEN pumps in long-term without bearing cooling

ty of the reconstruction items.

The recommendations of the PSA Phase 2 resulted in the improvements, which were decided in December 1998 to be implemented during the first half of 1999 or in the summer outage of 1999 [LNPP-M98]. The safety benefit of these measures is evaluated in [LPR164] and summarized in [LPR150, Section 3.4.1], see Table VI. The measures are implemented both at Unit 1 and 2; they can be regarded as twin units (No.4 has been rejected due to disturbance risk of the proposed periodic test; alternative improvements are under consideration).

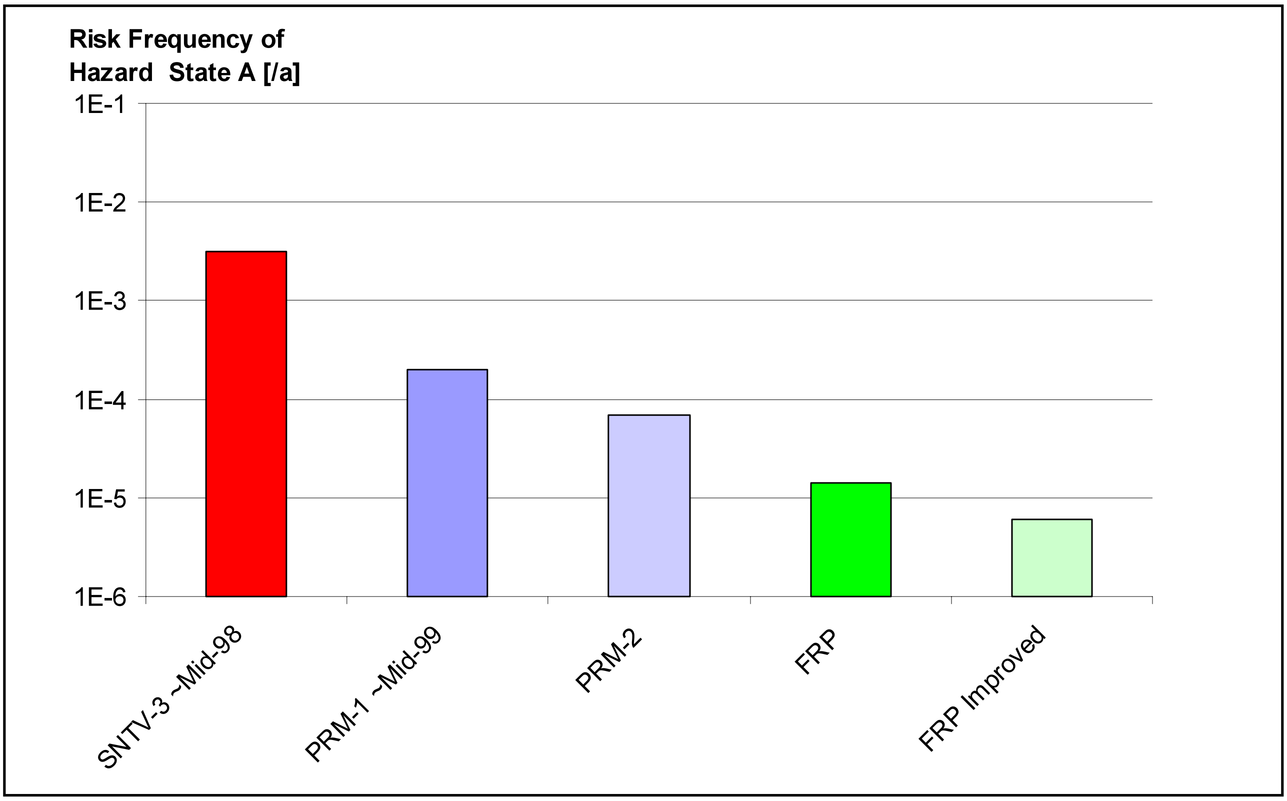

Figure 4. *Risk levels for various configurations (Hazard State A).*

4 EXPERIENCES FROM THE PEER REVIEW OF LNPP-P&DSA

This chapter summarizes the general insight and experiences from the LNPP P&DSA Peer Review. The methodological issues will be discussed in the next chapter.

4.1 Objectives and scope of the review

The main objectives of the review were the following:

1. During the course of the project, to interactively follow the key project tasks, provide comments and suggestions in order to support achieving high quality of the analysis and meeting the defined objectives of the project
2. At the completion of the project, to independently evaluate the quality of the analyses, confidence in the results and usability of the product with regard to intended purposes, especially as a tool for prioritizing safety improvements and developing operational, surveillance and maintenance practices
3. An additional main aspect was the potential to develop the end product into a Living PSA framework at LNPP Unit 2 and capability to transfer and implement it at the other RBMK units.

The conducted expert review is not to be considered as a regulatory review. However, the expert review aimed to serve, among others, as a basis for the Russian regulator to extend the review to the regulatory purposes.

4.2 Organization of the review

The independent review was performed by the Scientific and Engineering Center (SEC NRS) and the local inspectorate (GAN LAES) of the Russian regulatory authority GAN in cooperation with the Finnish and German technical safety organizations STUK and GRS, both funded by their national bilateral programs. A Lithuanian PSA expert from the Ignalina nuclear power plant also contributed to the review.

Generally, the review followed the well-established procedures, e.g. as described in the guides developed by IAEA and U.S. NRC [IAEA-TECDOC-543, NUREG/CR-3485]. In comparison to a usual review work special emphasis was placed on the following tasks:

1. Several plant walk-downs were done, e.g. in order to explore the coverage of area events and other system interactions; the walk-downs provided a useful opportunity to discuss with the plant staff the details of system design, operation, testing and operational experience
2. Key methodological references and data sources were investigated with regard to their relevance and applicability

Details of the organization of the review are presented in [RMR, Chapter 1]. The review documentation contains firstly a main report and then several technical reports and review notes on specific issues as well as the notes from the review meetings. The collected documentation is available on CD from STUK.

The formalities to organize the interface with the Russian supporting institutes proved to be a lengthy process. As a consequence, the time frame for an effective interactive review was severely reduced for PSA portion, and totally disabled for DSA portion. A lot of review work concentrated on the completing phase, in contrast to the initial aim to place weight on the on-line review phase.

The experiences show that organization of an external on-line review for a multilateral P&DSA project is a demanding task. An early management decision is needed to integrate the review and production processes. Dividing up the production process into consecutive phases will facilitate the conduction of the external review as well as the consideration and implementation of the review input during the production time. Such sequencing did not work properly in case of LNPP P&DSA Phases 1 and 2. However, the experiences were very positive from the use of electronic documentation, information distribution via Internet and storage of the information at the P&DSA project Web-site for an easy retrieval.

4.3 Comments on the P&DSA objectives and scope

The project objectives as summarized in Section 3.3.2 are in accordance with the usual objectives for the starting phase of a PSA, and can be considered appropriate and feasible against that background.

The principal aim of the PSA work – to identify dominant risk contributors and point out efficient improvements – is generally met. The developed in-house skills of the local PSA team constitute a good basis for further utilization of PSA at the LNPP, e.g. build up a Living PSA.

It is also positive that the PSA results were used to identify near term measures to directly improve the safety of Units 1 and 2. The failed objectives are connected to the backward approach to the reconstruction issue to be discussed in the next subsection.

The defined scope of P&DSA Phase 2 (see Section 3.3.3) can also be regarded generally appropriate for a starting stage. The scope limitations are, however, not sufficiently emphasized in connection with the results. The scope issues will be discussed further in the coming sections.

The deterministic analyses covered some early selected cases and need to be extended in the continuation to more comprehensively support the success criteria and sequence analysis assumptions. The review findings of deterministic analyses are presented in [RMR, Chapter 5].

4.4 Comments on the reconstruction issue, analyzed plant configurations

The plan of the P&DSA production initially defined that the plant will be analyzed corresponding to the state of Unit 2 after the decided, ongoing reconstruction works.

However, at the very beginning it was envisaged that only a small part of the upgrades will be implemented up to the completion of the PSA Phase 2. Especially, the construction of the new safety systems and service water system to be placed into new buildings 402/B and 480 were realized to go far beyond year 2000. The Steering Committee decided during the project that the base case model will nevertheless be made for the so-called Fully Reconstructed Plant (FRP)—an exceptional base case, which can factually be called a virtual plant model. Additional sensitivity analyses were made by switching off the new, not yet existing safety systems one at a time or in combination. By this way the relative benefit of the reconstruction items could be studied, including the identification and prioritization of near term improvements for the current plant state.

The backward approach to manage the reconstruction issue was heavily criticized by the Peer Review Group, see e.g. [RWW014, RWW020]. During the completion stage of the PSA Phase 2 the production team put increasing effort to analyze the relative benefits of the reconstruction items to support prioritization of the near term safety measures. The management of the LNPP decided [LNPP-M98] to implement in the first half of 1999 the proposed safety measures at Unit 1 and 2, as discussed in Section 3.3.6. These can be regarded as a significant gain from the P&DSA Phase 2 including its review.

Several modeling assumptions and simplifications were made relative to FRP, which means inaccuracy or added uncertainty in the sensitivity case models with new systems switched off. Many crucial modeling details could not at all be treated by “switches”. The importance to consider the existing state and short term safety improvements grew in importance due to the delay in the major part of the reconstruction program.

Because it will take years to complete the full reconstruction program for Unit 2, and even longer at the twin Unit 1, sufficient emphasis should be paid to develop the PSA model to enhance its applicability to consider short-term improvements of the partially reconstructed plant. Of course, it is also important that the design details of the full reconstruction are analyzed and improved by using PSA at early stage to facilitate cost-effective implementations. In this regard, the selective more detailed analyses of area events and external hazards are of high priority as will be pointed out in later sections. In conclusion, two distinct plant models are needed: one for the existing plant condition (to analyze short term improvements) and other for FRP (to optimize the full reconstructed design, to improve cost-effective implementation). A substantial part of those models are common.

The reference condition for LISA and PSA Phase 3 will be the current state of Unit 2. This change fulfills the most strongly urged recommendation by the Peer Review team. Further development of FRP model is postponed for the time being.

4.5 Discussion of the main results and findings

Some principal comments on the presented results regarding the dominant risk contributors were already given in Section 3.3.5. The presented results are conditional with respect to the scope limitations and also to the limitations in the level of analysis/modeling depth. Insights in this regard will be discussed in Chapter 5 and summarized in Section 5.8.

The scope limitations in conjunction with shortcomings in the system descriptions and supporting deterministic analyses mean that the uses of the existing PSA model are poor in the longer term, i.e. to consider prioritization of the next stage improvements during year 2000 and also optimization of FRP. Especially, a further progress in supporting short term improvements is pending for the completion of PSA Phase 3 model.

5 METHODOLOGICAL AND DATA ISSUES

This chapter continues the discussion of the insights from the LNPP P&DSA Peer Review concerning the methodological and data issues, that are characteristic to a PSA of RBMK. Emphasis is on such issues, which demand further analyses and development. Many of these issues were similarly recognized by the production team and placed on the list of items for further studies.

5.1 System descriptions and analyses

The preparation of the system descriptions progressed slowly throughout the project. In Phase 2 documentation the descriptions of several systems were still incomplete (in the very late stage some supplements and updates were published). Especially, the simplified P&I diagrams were missing for many systems until very final report versions.

The vague approach to solve the reconstruction issue also hampered the preparation of the qualified system descriptions, which are fundamental to the PSA modeling (notice the lack of “FSAR”). The system descriptions were prepared for the FRP condition with following shortcomings:

- Incomplete design stage and documentation made it difficult to describe new systems
- Many existing systems were described only superficially; presumably, their importance was underestimated
- Functional dependencies between systems are difficult to track; the descriptions were prepared on a system-by system basis; a needed overall description of the plant design is of poor quality

Furthermore, the interface of the new and existing system parts should be well described. For the impact of fires it is crucial to know cable routing of the new equipment in relation to existing functionally redundant equipment. The lack of those details made it difficult to review the sensitivity case models for the reconstruction items

Because the design of new systems or upgrades can still “live”, it had been advisable to distinctively indicate the system parts

- which are existing and remain as are described in design documents
- which are existing and will be replaced by upgraded new design, and
- which are additional new equipment.

The initial plan for the system descriptions contained also preparation of Failure Mode and Effects Analyses (called also as Single Failure Analyses). This objective was abandoned during P&DSA Phase 2, which can be considered as a significant shortcoming for the modeling, especially regarding control and protection systems and electric power supply systems.

The completion of the system descriptions and Failure Mode and Effects Analyses shall be given a high priority in the continuation (LISA).

5.2 Safety systems

The essential safety systems at LNPP Unit 2 include control and protection systems, primary circuit overpressure protection system and standby feedwater systems, compare to Table IV. Crucial reliability aspects of these systems will be discussed in the following subsections.

5.2.1 Control and protection systems

The control and protection systems constitute of two interrelated systems as shown in the simplified block diagram, Fig.5:

- Reactor Control and Protection System SKUZ/ CPS, which includes the control rods; this system monitors neutron flux parameters and provides initiation signals for fast scram (BAZ) and normal scram (AZ-1) based on various criteria
- Process Parameter Control System AZRT/ PPCS; this system monitors many physical parameters of the main process. It provides initiation signals for normal scram and for other safety functions depending on the transient and accident conditions

The control and protection systems serve dual purpose as they serve process control during normal power operation. This is a specific feature of RBMKs. In the Western NPPs the process control during normal operation and actuation of safety systems in transient and accident conditions are strictly separated functions.

As discussed already in Section 3.2 in connection with Barselina project, the reliability problems of the control and protection systems constitute one central safety issue for RBMKs. Also P&DSA Phase 2 and the Peer Review underlined these insights, especially the following problems [RWR018]:

- Possibility of subtle dependencies due to the lack of isolation or inefficient isolation between the control (operational) and protection (safety) functions
- Insufficient separation between diversified or redundant subsystems or channels in the current AZRT, which is of old design and technology in LNPP Unit 2. CPS was modernized in 1994 and is in these regards in a much better design. The three redundant trains of CPS are placed in separate rooms

The system analyses and modeling of AZRT and CPS showed up rather superficial and incomplete in many crucial aspects.

Several variants were presented in P&DSA Phase 2 for the reactor shutdown criteria, i.e. for the critical number of failing control rods. Besides, the method used to calculate the failure probability of the control rods and the highly redundant parts of CPS is disputable as will be discussed in Section 5.4. The presented results were incredibly low and thus abandoned by the production team. A value of 10^{-6}, being based on engineering judge-

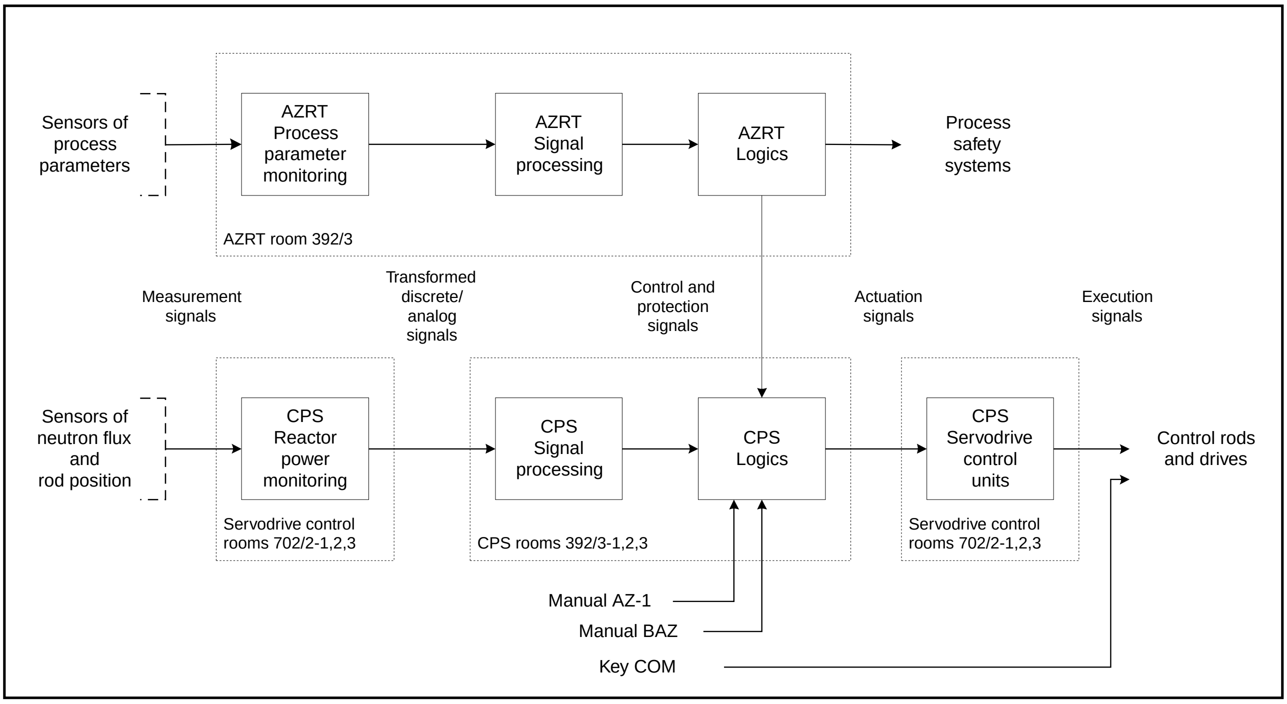

Figure 5. *Schematic diagram showing main parts of AZRT and CPS.*

ment, was used for the failure probability of the reactor shutdown. It was handled as a so called undeveloped fault tree in P&DSA Phase 2 model.

In the continuation an improved approach is needed to address the above mentioned shortcomings.

5.2.2 Overpressure protection system

There are three systems, which serve overpressure protection by dumping steam from the primary circuit in the following order of actuation with increasing pressure:

- Four steam dump valves to turbine condensers (BRUK/SDVC); they are placed on the secondary side of the steam line isolation valves
- One steam dump valve to bubbler-condenser (BRUB/SDVB) of capacity 200 kg/s
- Eight Main Steam Relief Valves (GPK/MSRVs), each of capacity 100 kg/s

At the reactor shutdown sufficient steam dump requires either the operation of the BRUB or two MSRVs. The role of BRUK is that, if the vacuum in the turbine condensers can be retained and main steam lines are not shortly isolated, steam can be relieved first by BRUK and then by BRUB without demand on the MSRVs.

The reliability parameters of MSRVs and BRUB were estimated from the LNPP and Ignalina experience, which provided a reasonable statistical basis. MSRVs are equipped with a dual-actuator pilot valve. The electromagnetic actuator is controlled by remote signal. As a back-up the pilot valve is opened with further pressure increase by the steam pressure acting against its spring, and closed when the steam pressure is decreased. It is unclear, whether the diversified actuating functions have been credited. The simple Beta-Factor Method was used in PSA Phase 2 to model CCFs also for the MSRVs, which is a highly redundant system. The different cases of varying success criteria could not be consistently handled by this approach.

Inadvertent opening of MSRVs and/or BRUB was not considered as initiating event in PSA Phase 2. BRUK and BRUB are controlled also by a separate pressure regulating system, which can be a source of CCFs.

5.2.3 Standby feedwater systems

Following a plant transient, e.g. loss of main feedwater, water to the steam drums will be supplied by the emergency feedwater system APEN/EFWS. As a backup the auxiliary feedwater system MPEN/AFWS can be used. Steam is dumped in the first stage to turbine condensers and then by BRUB to bubbler-condenser as discussed in the preceding section. Cooling of the fuel channels is based on natural circulation in the primary circuit. The reactor can be cooled down to cold shutdown state by BRUB and in the longer term by removing reactor decay heat by SPiR system.

If one main feedwater pump remains intact it can be used in so called pulse mode as a last resort to supply water into steam drums after plant trip. Using main feedwater pump in this mode requires careful manual control of the water level in the steam drums.

In the current state of Unit 2, the standby feedwater systems serve also emergency core cooling in the LOCA situations, see Table IV. The design features in this regard will be discussed in connection with the LOCA issues in Section 5.6.

The results of PSA Phase 2 showed the following weak points in the standby feedwater systems:

- Critical check valves in the injection lines to steam drums
- Dependence on the service water and intermediate cooling circuits for component cooling, see Section 5.3.2
- Need of makeup water in long term cooling to APEN tank or deaerators for MPEN, see Section 5.3.3

There are two critical check valves, one on each reactor half. Feedwater is required to the steam drums on both reactor halves. Therefore, the failure of either check valve violates single failure criterion. The check valves cannot be tested during power operation because of disturbance risk. Thus the estimated probability of check valve to be stuck closed on demand is relatively high. Possible measures to solve this problem are under consideration. Improvements concerning the other two weak points have been implemented as part of the short-term measures based on PSA Phase 2 results (see more details in Sections 5.3.2 and 5.3.3).

5.2.4 Other safety systems

The CPS instrumentation channels are cooled by a special system KoSUZ. A rapid loss of water inventory in this cooling circuit is a potentially important initiating event as it will mean reactivity insertion to the reactor.

The safety systems include also reactor tank overpressure protection system and reactor confinement system; these systems are not discussed here, because they are not part of Level 1 PSA.

5.3 Support systems

The essential support systems at LNPP Unit 2 include Electric Power Supply Systems and Service Water System as well as the make-up systems, which add water to feedwater tanks for long term cooling.

5.3.1 Electric Power Supply Systems

The Electric Power Supply Systems (EPSS) contribute relatively little to the presented results. An indicator is the contribution of LOOP, which is 3% for SNTV-3 and 10% for the FRP condition, see Figs. 2–3. The estimated low result is understandable for the FRP condition, because the new safety systems will be supported by a new, so called Reliable EPSS, which includes three new dedicated DGs, to be located in the new safety building (402/B). For the SNTV-3 condition the result may be underestimated partly due to the relatively low frequency of LOOP, which will be discussed below. Another explanation can be the fact that the power supply connections in the current state could not be adequately managed by the switch-off approach, which was used to reduce SNTV-3 model from FRP model, compare to the earlier discussion in Section 4.4. Especially, modeling of the uninterruptable power supply to vital instrumentation and breakers may need to be improved.

The frequency of LOOP, which is denoted by IE acronym TE, is based on one occurred event at Unit 2 during 1987–97, which yields to the point estimate f_{TE} = 0.091 /year. This estimate is comparable with the generic data, e.g. with the recent evaluation in [NUREG/CR-5496]. But LNPP PSA credits the connection from Narva HPS (hydro power station) as an additional off-site power supply path. According to the system description the connection from Narva HPS is over two 110 kV lines, see Fig. 6. The automatic load transfer circuit of 110 kV starts up Narva HPS, which is specifically picked out for that purpose, clears the 110 kV mains and supplies voltage to the plant's 110 kV lines in an emergency situation.

The unavailability of the back-up supply from Narva HPS is assessed to be 0.01 in SNTV-3 (engineering judgement). The supply from Narva HPS is through the 110 kV switchyard and start-up transformer, i.e. the same route as the supply from 330 kV grid, which supplies through the autotransformer 330 kV/110 kV the 110 kV switchyard, see Fig. 6. Thus there exist potential CCFs, which can affect all off-site power supply paths, e.g. extensive fire in the 110 kV switchyard or transformer area, or adverse weather conditions. For SNTV-3 the effective frequency of total LOOP is about 10^{-3} /year, which is incomparably low. It should be justified by a more detailed analysis of the potential failure mechanisms.

It should be noticed that it is a rather usual situation that the NPP site is connected both to high voltage grid and to a district grid, e.g. 110 kV grid and that a nearby power station—often a hydro power station or gas turbine generator station—can supply reserve power to the NPP in an emergency condition. The data for LOOP normally means total loss of supply through all separate off-site connections, ranging from 0.1/year to 0.01/year. Giving a substantial separate credit to the NARVA HPS connection should be defended by clear arguments. It is of interest to notice that in Olkiluoto PSA f_{TE} = 0.071 /year and it includes the reserve connection from close Harjavalta HPS, which is similar to Narva HPS back-up to LNPP [TVO-PSA].

On the other hand, the off-site power supply is conservatively handled in P&DSA Phase 2, because the recovery possibility is not taken into account, except the reserve connection from the NARVA HPS. In a station black-out the depletion of water from steam drums is critical (steam is blown via safety valves out): it is estimated that the failure to recover feed into steam drums in 1 hr 45 min will lead to core damage (Hazard State D) and in 2 hr 15 min to core accident (Hazard State A). According to the generic data for the US NPPs about 30% of LOOP events lasted over 1 hr 45 min and about 20% over 2 hr 15 min [US_LOSPD].

In the current state the frequency of LOOP is not a very critical issue. However, after near term improvements in the reliability of the emergency feedwater function but before the full completion of the new safety systems and related new SNES/EPSS, it becomes more important, relatively. Thus in the continuation (PSA Phase 3) a more careful evaluation is needed for LOOP frequency and recovery possibilities.

5.3.2 Service Water System

The service water function proved to be very important for the safety according to the results of P&DSA Phase 2, first of all due to the risk of fire and flood, which can affect the existing service water system. Compare to additional discussion in Section 5.5.

LNPP Unit 1 and Unit 2 share a sea water pumping station (Bldg.410). It houses the Main Sea Water System STV/MSWS, which provides condenser cooling, as well as dedicated sea water (service water) circuits, which provide component cooling and residual heat removal function for the safety related systems. The service water systems NA/NSWSs for Unit 1 and Unit 2 are placed at the opposite ends of the pumping station, respectively, Fig. 7.

There exists cross-connecting option between Unit 1 and Unit 2 NA/NSWS through NA headers. In addition, the intermediate circuits for pump cooling and sealing functions can be cross-connected between Unit 1 and Unit 2 (these details are not covered in Fig. 7). The cross-connection is routinely used in repair situations when the unit is in shutdown state and now there exist instructions for the manual operations also for power operating condition.

The plant reconstruction program contains a new (reliable) service water system SNTV/RSWS for emergency situations, to be placed in the new sea water pumping station, Bldg.480. It is under

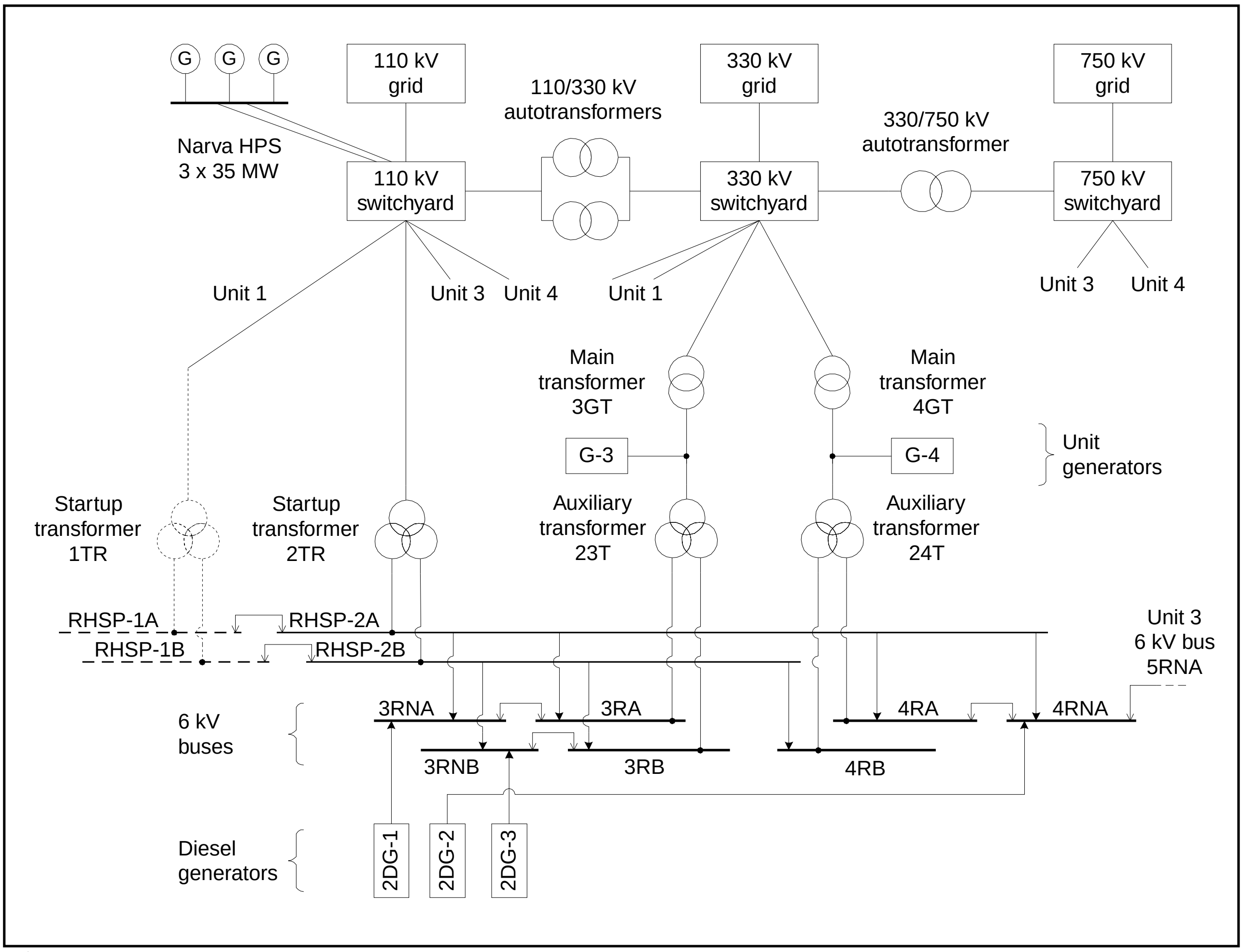

Figure 6. *Off-site power supply paths of LNPP Unit 2.*

construction.

The service water supply is a vital support function, which provides e.g.

- heat sink path for the CPS channel cooling system KoSUZ/ChCS and other reactor auxiliary systems
- cooling of the Main Coolant Pumps (MCPs)
- component cooling of the pumps in the front-line safety systems, especially APEN pumps
- cooling of the existing diesel generators (Bldg.475)
- heat sink path for the decay heat removal, i.e. normal shutdown cooling system SPiR/BCS

According to P&DSA Phase 2 results the most important function requiring service water is cooling of APEN pumps: especially cooling of the electric motor and pump bearings. The presented recommendations included the change of motor into air-cooled type. It was also proposed that the criticality of bearing cooling should be tested: the outcome was that the warm-up of the bearings would be rather slow if service water is lost, allowing time to the operators to control the situation, e.g. by feed and bleed of the bearing cooling circuit.

Another particular feature adding to the risk-importance of service water is the fact that NA pumps (three operating, one in standby) will stop at LOOP and have to be restarted after the DGs are first started into operation.

Modeling of ICCs and many cross-connection options between the ICCs of Unit 2 and 1 have not been reviewed. This topic should be addressed in the continuation.

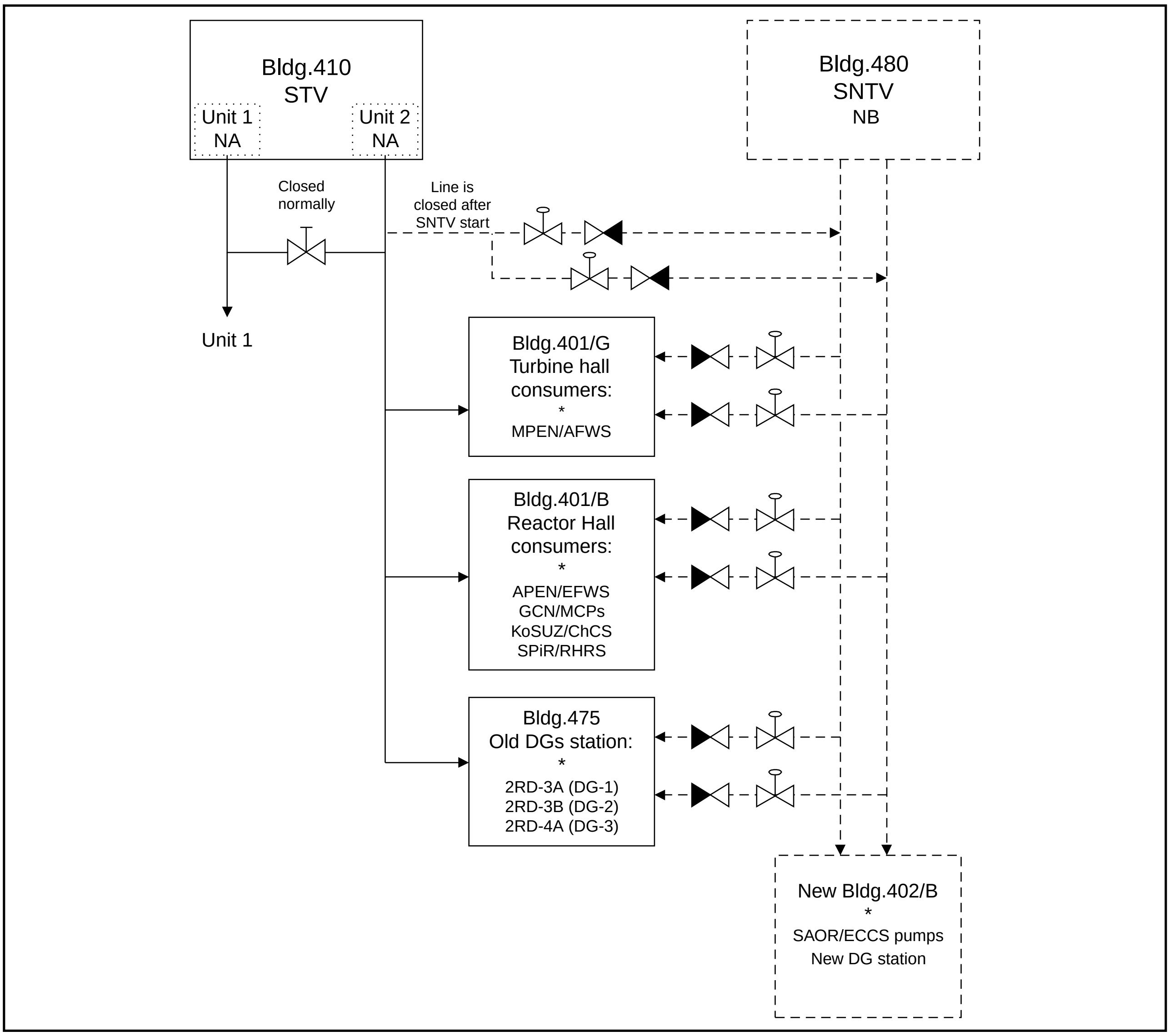

Figure 7. *Schematic picture of service water connections. The parts, which are drawn by dashed lines belong to the reconstruction program, i.e. do no yet exist.*

Table VII. Dependence categories and treatment in LNPP P&DSA Phase 2.

Dependence category	Cover in P&DSA Phase 2	Remarks
Common Cause Initiators	Not covered	Part of CCIs is overruled by Area Events
Internal and external hazards	Area Events analyzed by simple index analysis method	Limited to internal fires, floods and missiles; spreading or influences to adjacent rooms not analyzed
	External flooding of the existing service water pumps	Simple adhoc treatment at the very end of Phase 2
	Many potentially important internal and external hazards not covered	
Functional dependencies	Component information tables used to present the control signals, power supply and other support system connections	No detailed dependency matrices were used; completeness is difficult to track
System Interactions	Not covered	
Dynamic effects	Assessed crudely to a limited extent in a sensitivity analysis	
Common Cause Failures	CCCGs defined only within a single system	Simple Beta-Factor method was used with a global Beta of 0.1
Operator action dependencies	Not covered	

5.3.3 Feedwater make-up systems

There are several systems, which can be used to add water to the deaerators (4×120 m^3, serving MPEN and PEN), and to the emergency feedwater tank (500 m^3, serving APEN). This water makeup is needed in the long-term cooling mission, also in a LOCA situation in the current configuration when the feedwater systems are used for emergency core cooling.

The analyses showed that the make-up arrangements rely on manual operations; the flow arrangements needed in transient conditions are tested infrequently and emergency operating instructions are incomplete or lacking. The short term safety measures proposed by the P&DSA Phase 2 included several improvements in these regards.

5.3.4 Other support systems

Other support systems include potentially important ventilation systems, which serve room cooling/heating function, especially in the intermediate building (401/D) where the main control room (MRC) and safety related I&C-cabinet rooms are located. The ventilation systems were not described in P&DSA Phase 2. According to the information presented in [STUK-YTO-TR 44] the MCR and adjacent electric rooms are equipped with air-cooled ventilation system, i.e. outdoor air is used as heat sink. This system is now connected to the DG backed power system. In the other compartments there are circulation air cooling devices. It is not known whether those components are connected to the DG backed power system.

In Loviisa the loss of room cooling/heating was found to be as a substantial risk. This potential problem will be analyzed for the LNPP Unit 2 in PSA Phase 3.

The importance of ICCs was pointed out in connection to the service water system. The further support systems, e.g. residual heat removal systems of the reactor core and reactor tank are not discussed in this context.

5.4 Dependencies

The various dependence categories are presented in Table VII with brief notes about the cover and treatment method in P&DSA Phase 2. The details will be commented for each dependence category in the following subsections. Compare also to the recent guideline for the analysis of dependencies [K2PG-9]. The treatment of dependencies has been considered in the review reports [RWR011, RWR013, RWW007].

5.4.1 Common Cause Initiators

Common Cause Initiator (CCI) is defined as an event or a combination of events, which both constitutes an IE and at the same time reduces the availability of the safety systems to response on that IE. The category of CCIs is here restricted to the (intrinsic) component failures, which occur inside the plant systems such as failures in the control and protections systems, electric power supply systems, service water system or other support systems. Internal and external hazards (so called extrinsic events), e.g. fires, flooding and missiles can also be of general type of CCI but will be treated as a separate dependence category for practical reasons.

P&DSA 2 lacks the analysis of CCIs, which is a step backward as compared to Barselina 4. It has been defended by the argument that AEs will overrule CCIs, which is however not generally assured.

In the continuation a systematic approach to identify and screen important CCIs is needed. Emphasis should be on the electric power supply systems and support systems. It should be noticed that CCFs of the isolation valves and MSRVs can result in special types of LOCAs. Also the risk from the loss of room cooling/heating should be considered e.g. in the instrument cabinet rooms.

5.4.2 Internal and external hazards

There is a large number of internal and external hazard types, which can be risk-important depending on the site characteristics and plant design. P&DSA Phase 2 considered only internal fires, floods and missiles; i.e. so called Area Events (AEs), which will be discussed in more detail in Section 5.5.

Further types of hazards should be selectively covered in the next phase. LISA will contain comprehensive tasks for the fire safety assessment and external event analysis, and help to improve PSA model cover in the future. The following internal hazards in addition to AEs are expected to be important:

- Damage to underground piping
- Damage to outdoor cable bridges
- Hydrogen explosion (storage and generator cooling circuit)

Compare also to the needed scope extensions of the AEs themselves, to be discussed in Section 5.5. Similarly, the following external hazards are expected to be important:

- Coastal flooding (considered in a very limited way in connection to AEs affecting service water pumps in the old sea water pumping station, see Section 5.3)
- Sea water phenomena, e.g. mass emergence of algae or frazil ice
- Blizzard
- High wind
- Combination of the above hazards, e.g. in a heavy storm

These proposals are part of the scope extension needs that are summarized in Section 5.8.

5.4.3 Functional dependencies

Functional dependencies are documented in the component information tables (part of system descriptions), which show the control signals, power supply and other support system connections. No detailed dependency matrices are prepared, which makes it very difficult to track the system connections. Also the simplified system flow diagrams should be improved in this regards. In some cases block diagrams could be used to show the principal connections, e.g. in the way presented in Fig. 7.

5.4.4 System Interactions

System interactions cover dependencies, which are not ordinary functional dependencies but are specific to actual demand conditions, when the plant systems are actuated and operated under transient or accident conditions. Typically, system interactions are not detected in normal operation or by surveillance tests. The interaction between systems or subsystems can be transmitted by the process medium, via support system route or indirectly via operating environment, e.g. temperature, humidity, pressure waves or vibration. The system interactions are often called as "subtle dependencies" or "subtle interactions".

No attempt was done in P&DSA Phase 2 to cover this dependence category. A survey is recommended to evaluate and screen system interactions. The survey should cover the operating experiences of all RBMKs and also consider the applicability of special events from the other NPPs.

5.4.5 Dynamic effects

Dynamic effects of a pipe break can cause failures of the safety related equipment, which are needed in the mitigation of the IE, or failures, which can otherwise worsen the event sequences starting from the IE.

The analysis of dynamic effects was not in the defined scope of the P&DSA. However, at the end of Phase 2 a sensitivity analysis was made to evaluate some cases regarding the possible risk level. The results showed potential contribution in the range of 10^{-4} to 10^{-5} /a to the accident risk frequency. It is of particular importance that the break of a downcomer pipe (∅ = 295) can cause by jet impact or pipe whip the rupture of adjacent downcomer pipes, escalating into a Large LOCA case, which is a Beyond Design Event at LNPP Unit 2.

Further consideration of dynamic effects is needed requiring appropriate physical analyses. One important category to be studied is constituted by the breaks of feedwater or steam lines, which are routed above the MCR area.

5.4.6 Common Cause Failures

Common Cause Failure (CCF) is defined as the dependent failure of identical (or closely similar) components. The dependence can arise from a shared cause like design error, inadequate testing, maintenance or environmental abnormality or a combination of such common causes. The group of components vulnerable to CCFs is called Common Cause Component Group (CCCG).

In P&DSA Phase 2 the definition of CCCGs was simplified so that only groups of identical components within one system were considered. In the continuation also other component groups should be considered, e.g. isolation valves in different systems or high voltage breakers in different power supply paths.

Alfa-Factor Method was named in the project plan as the main parametric CCF model to be used, and its implementation and data base were already elaborated to a certain degree in PSA Phase 1. During the course of the completion of Phase 2, a drastic simplification was decided—to use Beta Factor model with global Beta = 0.1. This decision can be strongly criticized as it reduces the uses of the Phase 2 results.

There are a large number of highly redundant systems and component configurations at the RBMK. The current combination of over-simplified use of Beta Factor model and/or engineering judgement means large uncertainty.

A specialized form of the Distributed Failure Probability (DFP) method was used to quantify the reliability of control rods and drives similarly as in Barselina 4. The main observations from the evaluation of DFP method are the following [RWW007]:

- The used probability entities are not properly defined and the handling of failure event combinations is not explained. Seemingly, there are mistakes in the combinatorial analysis parts, which explain part of the underestimation as compared to the reference calculations
- Statement: "DFP method is ... the most suitable choice for the assessment of highly redundant systems with sparse data" is right in the meaning that this method **can mechanically** be applied even in the case of data containing one or a few single failures but no observation of CCFs. However, the results for higher order failure probability are then determined by the strong inherent assumptions of the model and the estimation method (prior distribution). The results can thus be arbitrary and in any case very uncertain. The approach will usually overestimate failure probabilities of low multiplicity but underestimate failure probabilities of intermediate and high multiplicity. The underestimation may be very substantial in highly redundant systems.

The result for the control rods and drives obtained by DFP method was, however, disregarded and a value based on engineering judgement was used instead. De facto, this shows that even the authors do not trust on the method. It is recommended that in the continuation the possible approaches are carefully compared before the choice, covering the Common Load Model, which has been used in the Nordic PSA studies for highly redundant systems. Attention has to be paid also on collecting the needed input data for the applications. It has to be noticed also that the functional failure criteria are complicated in highly redundant systems, especially for the control rods, and should be properly determined before any meaningful quantification is possible.

5.4.7 Operator action dependencies

Operator action dependencies cover situations, in which errors can be made in successive operations, affecting the reliability of otherwise independent components or systems or the reliability of successive operator actions in transient and accident sequences after initiators.

This dependence category was not considered properly in P&DSA Phase 2. Especially the treatment of successive recovery actions should be made consistent in the next phase.

5.4.8 Overall strategy to handle various types of dependencies

One of the principal early review comments concerned the lack of the description for the overall strategy to handle various types of dependencies [RWR011]. In the continuation a better planned and balanced approach is needed. Because the analysis of dependencies is resource-consuming, careful planning is recommended with attention to the experiences from the other PSA studies in this subject area.

5.5 Analysis of Area Events

This topic will be discussed comprehensively as it was subject to an in-depth review [RWR014]. AEs proved also to be important risk contributors to LNPP Unit 2.

5.5.1 Index method

The AE analysis uses a simple index analysis method to derive the frequency of the AE initiators (internal fires, floods and missiles). It is a close variant of so called Berry's method and was already used as in Barselina 4. The principal simplification is to assume that in an AE all equipment in the room are rendered unavailable but influences are limited to one room, i.e. no spreading is taken into account. The limitations of the method will be discussed further in Section 5.5.3.

The AE analysis was restricted in Phase 2 to existing rooms that were initially judged as safety-important for FRP condition. The assessed room indices are used to distribute the generic frequency of 0.1 /year for internal fires, 0.01 /year for internal floods and 0.01 /year for missiles over the analyzed rooms.

5.5.2 AE(NA)

The conducted AE analysis produced a significant result as it pointed out the flood and fire risk affecting the existing service water system NA/SWS, denoted as AE(NA). Even though this finding can be considered obvious from the known qualitative safety aspects of Unit 2, the PSA result gave a needed push to undertake near term measures to reduce that risk.

The principal structure of the service water system was already discussed in Section 5.3.2, see Fig. 7. The nominal sea water level is at –6.40 m with respect to zero level of Bldg.401. The NA pumps are at level –10 m, i.e. more than three meters below the sea level. Besides internal flooding, there is a substantial risk to external flooding due to high sea water level. The NA pumps are of horizontal design and there is no separation between the four redundant pumps. This exceptional design makes the NA pump group highly vulnerable to flooding. It should be noticed that usually these kinds of pumps at a nuclear power plant are of vertical design: the motors are high up above the level of possible flooding heights. At Unit 3 and 4 the service water pumps are of vertical design, similarly to the pumps to be used in the new SNTV/RSWS.

AE(NA) is by far the most important AE and is dominating in the risk profile for both SNTV-3 and FRP, see Figs. 2–3. The frequency of fire in NA compartment is estimated as 5.6E–3 /a, flooding as 2.4E–3 /a and missiles as 5.1E–4 /a, which makes 8.5E–3 /a in total (all pumps are assumed to be lost).

Initially the AE(NA) was effectively handled as a common cause event for both Unit 1 and Unit 2 without credit to the cross-tie possibility. This assumption was defended on the basis of the risk of external flood. In principle that is a relevant argument even though inconsistent with the scope of P&DSA Phase 2. The prominent cause to external flood is high sea water level, which however is likely not to be a sudden event but can be foreseen by some time window. This allows preventive measures e.g. shutting down the plant in advance to increase possibility to manage residual heat removal in case the sea water pumping station will be lost.

Triggered by the presented review comments the frequency of AE(NA) was changed at the very end of the P&DSA Phase 2 into 1E–3 /a based on the design base flood (high level of sea water) once in 100 years and credit of 1/10 for the preventive measures. The fire risk was neglected, which is not substantiated.

The principal causal sequences to AE(NA) are outlined in Fig. 8, based on the information deduced from P&DSA Phase 2 (it covers the last minute addition of explicitly considered external flood as described above and the internal fire, flood and missiles with a credit of 9/10 to successfully use Unit 1 cross-tie). In practice, there are much more complex event scenarios, which can lead to total loss of service water for Unit 2. Due to its high importance, the internal and external hazards to NA should be analyzed separately from the index analysis method, which can be used to cover the bulk of the plant rooms. For a consistent treatment the initiating events should be divided into:

1) Foreseen and sudden events
2) Events affecting NA/NSWS of
   a. Unit 1 but not of Unit 2
   b. Unit 2 but not of Unit 1
   c. Unit 1 and Unit 2

The different subcategories should then be modeled accordingly. In addition to the analysis of evidently important coastal flooding risk also other sea water and weather hazards should be considered. Regarding the internal hazards the possibility of loosing both NA/NSWSs in an extensive fire or internal flooding should be considered. Especially, the fire affecting the power and signal cables should be analyzed.

The PSA studies contain examples how the IEs affecting two reactor units with crosstie possibilities of safety systems are logically factored by Boolean expressions into a suitable form to be then modeled by functional events in the PSA model [RWR014, Annex 2].

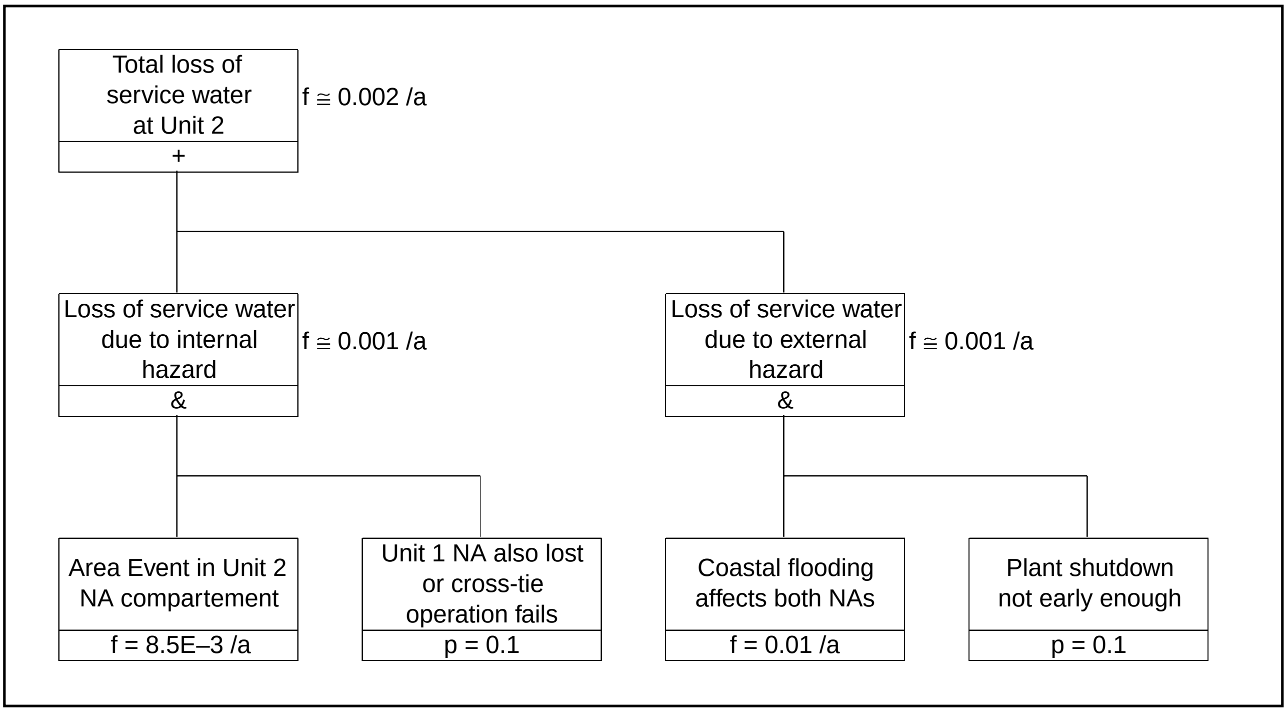

Figure 8. *Principal causal sequences leading to total loss of service water at LNPP Unit 2 in the current state (SNTV-3 model).*

5.5.3 Problems and limitations

The used index analysis method is limited to a crude analysis, although it is certainly a useful screening tool. The benefit of the approach was the reasonable amount of work needed, so it was possible to carry out the AE analysis in P&DSA Phase 2. The AE analysis done thus far provides a good starting point for a further work.

It is peculiar to notice the relatively small contribution of AEs in the other rooms and spaces than NA compartment: namely AE(NA) represents about 99% of calculated AE risk mass in SNTV-3 and about 90% in FRP. The small contribution of the other rooms and spaces is unexpected and presumably indicates the limitations of the approach used in P&DSA Phase 2, e.g. omitting probability of fire or flood to spread into or otherwise influence adjacent rooms. Besides, when starting PSA Phase 3 it was realized that the indexing procedure is not adequate for special types of rooms, e.g. the fire frequency in the switchgear rooms showed up to be substantially underestimated in comparison to experience-based data.

It has to be emphasized that the AE analysis is done for the FRP condition. Many existing rooms (systems) are left out, including several especially important ones before reaching FRP condition, e.g. SUZ and AZRT cabinet rooms, unit battery room and the room containing converters (DC to AC). The AEs are of high importance before the completion of the planned reconstruction. Thus, the cover of the AE analysis with respect to the current condition shall be improved to support the prioritization of the near term safety improvements.

The rooms, which are part of FRP but do no yet exist, are not covered in the AE analysis thus far. This shortcoming has to be removed when developinfg further the FRP model with special emphasis on the interfacing or adjacent parts between the new and existing systems, including routing of the cables. This extension should be done at an early stage in order to benefit from the results before the final design and construction.

Regarding the methodology, the spreading and influences of the AEs to adjacent rooms or spaces should be taken into account, e.g. by the use of scenario models. The scenario technique can also be used to consider realistically different extents of the influence from an AE within a space, i.e. to remove the simplification that all equipment in the space are rendered inoperable with a given AE frequency. It is also highly recommended that the experiences and insights from the severe fire incidents at the NPPs are utilized to enhance the realism of the analysis; see e.g. the scenario description of the fire incident at Chernobyl 2 in 1991 [FE-TECDOC]. The interaction with the ongoing FHA project should be improved. That can help a lot, e.g. in the laborious tracking of cable routes, identification of spreading possibilities and evaluation of fire scenarios.

5.6 LOCA categories and frequency estimation

This topic will be discussed comprehensively, because it was one of the special areas for in-depth review [RWR012]. In the background is the concern raised by the recent findings of severe material defects in the in-service inspections of RBMKs. LOCAs are potentially important risk contributors to LNPP Unit 2, especially in the current state because of the limited mitigation capabilities.

5.6.1 Design features for LOCA

In the current state the Emergency Feedwater System APEN/EFWS fulfills the function of emergency core cooling. The MPEN pumps can be used as a reserve. For the injection into the Primary Coolant System (PCS) there is so called SOPV line, which connects the feedwater header to the emergency core cooling header, see Fig. 9. At the begin of LOCA the fast acting valves in SOPV line will open and main feedwater pumps (PEN) will provide emergency core cooling until the standby feedwater pumps (APEN, MPEN) are started and take over. The feedwater tanks have limited capacity necessitating makeup in long-term cooling, as was discussed in Section 5.3.3.

The reconstruction program contains a new Emergency Core Cooling System SAOR/ECCS. It will have its own support systems, e.g. a dedicated diesel-backed power supply system and new service water system, see Table IV.

Table VIII. *The main elements and components of PCS in LNPP Unit 2. The number of components is factored according to k×l×m, where k is the number of rector halves and l is the number of SD per reactor half, if applicable.*

Component type	Nominal size (inner diameter in mm)	Number of components
Downcomer pipe	295	2×2×12
Suction collector	896	2×1
Main Coolant Pump (MCP)	752	2×4
Pressure collector	896	2×1
Group Distribution Header (GDH)	295	2×22
Pressure tube (PT)	50/80/68	1661
Steam/water riser pipe	68	1661
Steam Drum (SD)	2090	2×2
Steam header	378	2×2×15
Main Safety/Relief Valve (MSRV)		8
Pressure relief valve to bubbler (BRU-B)		1

Both in the current state and after reconstruction the design basis for LOCA is a Double-Ended Guillotine Break (DEGB) of 300 mm pipe. Larger breaks are Beyond Design Events (BDEs), which can lead directly to building structure collapse and the most severe accident consequences. Even more generally, the dynamic effects of the pipe ruptures are of concern, compare to Section 5.4.5.

5.6.2 LOCA zones and size classes

The treatment of LOCAs for a RBMK plant is a demanding and complicated task because of the large amount of piping and other pressure retaining components of the PCS as well as of the connected steam system. Especially, the reactor cooling circuit is a complex structure due to the large number of fuel cooling channels (FCC) and associated piping components. The main elements and components of PCS are listed in Table VIII. A general description of the structures is presented in [STUK-YTO-TR 44].

PCS is divided into zones according to specific consequences of a pipe break, see Table IX and Fig. 9.

Size classes of Large, Medium, Small and Very Small LOCA (LLOCA, MLOCA, SLOCA and VS-LOCA) are defined with respect to the diameter of the effective flow area as presented in Fig. 10. In LNPP PSA (similarly as in Barselina) the LOCA sizes are shifted towards larger size in comparison to the standard definition for PWRs and BWRS, see Fig. 10. In particular, SLOCA range of LNPP-PSA belongs normally to MLOCA range.

SLOCA range is relatively narrow. The boundary between SLOCA and VSLOCA is not orderly explained in LPR010. Substantiation by termohydraulic analyses does not show up. VSLOCA is handled as TM (manual shutdown), which is neither clearly substantiated. It should be noticed that a break of diameter of 50 mm can lead to an outflow of 70 kg/s (250 m^3/h), which corresponds to the capacity of one APEN or MPEN pump. In comparison, the capacity of one small make-up (hydro sealing) pump NGU is 30 kg/s (100 m^3/h): thus all three NGU pumps would be needed to compensate maximal VSLOCA.

The pressure tubes and other sections of FCCs are classified in SLOCA (Zone 2, 3 and 4) as the inner diameters are in the range from 50 to 80 mm. Each channel comprises six pipe sections, including the inlet control valve. Using the generic pipe rupture rate of 5E–10 /h [EPRI TR-100380] results in the following estimate (assuming 7000 hours of operation in pressure state in a reactor year):

$$f_{FCC} = 6 \cdot 1661 \cdot 5E{-}10\ /h \cdot 7000\ h/a = 3.5E{-}2\ /a$$

This estimate is reasonably compatible with the knowledge that there has been several FCC ruptures within the cumulated about 200 RBMK yea-

Table IX. *LOCA Zone Categorization [LPR150, Table 2-4]. A more detailed definition of the components belonging to each zone is presented in [LPR010].*

ZONE ID	Location
Zone 1	Inside the primary circuit confinement from the downcomers (at a point of their entrance to the confinement) to the GDH check valves (upstream of those). • Zone 1T: Pipe sections above the top of the reactor core • Zone 1B: Pipe sections below the top of the reactor core
Zone 2	Inside the primary circuit confinement after (downstream of) the GDH check valve. Plus Zone 1 events with failure of one or more GDH check valves
Zone 3	Inside the reactor cavity.
Zone 4	Outside the primary circuit confinement, on the primary circuit side of isolation check valves.
Zone 5	Outside the primary circuit confinement, on the secondary side or interfacing system side of isolation check valves.

rs. One of those incidents occurred at LNPP (Unit 3, 24 March 1992), when the spindle of the inlet control valve broke off. However, the rupture rate for FCCs as estimated in P&DSA Phase 2 is 1.8E–3 /a, i.e. more than one order of magnitude lower than the above generic estimate (also the other comparisons show similarly possible underestimation of the LOCA frequencies in P&DSA Phase 2 as will be discussed later). It should be noticed that the pressure tube rupture leads to Hazard State V (Violation), compare to Table III.

5.6.3 Insights from the in-service inspections, Leak Before Break concept

Nondestructive tests have been carried out at LNPP by the Finnish experts since 1992, see [RWR012, Annex 1]. Significant defects have been detected in five locations of PCS. The most significant are intergranular stress corrosion cracks (IGSCCs), which are detected in the downcomers. Also IGSCCs of the domed end welds in GDHs are

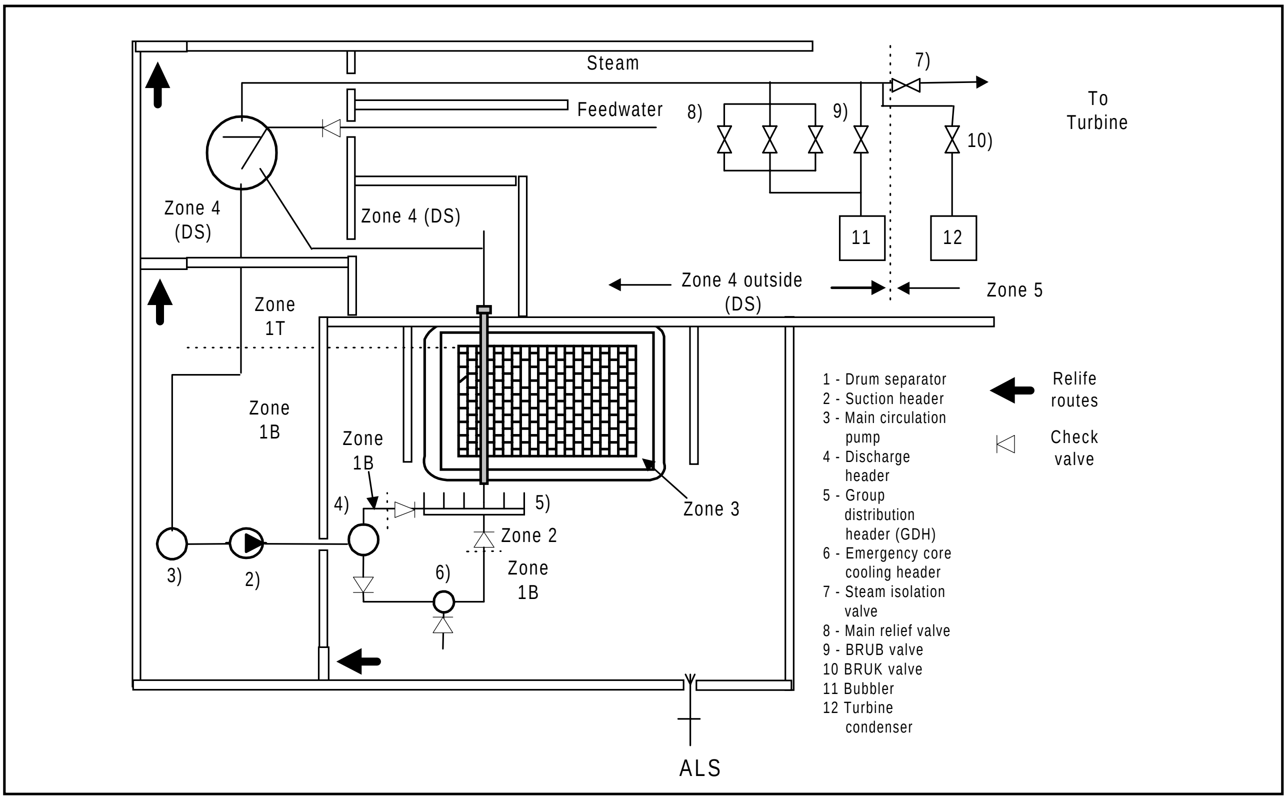

Figure 9. *LOCA Zones for LNPP Unit 2 [LPR150, Fig.2.3]. It shall be noticed that the identification numbers for (2) suction header and (3) main circulation pump are mixed in the diagram.*

of high significance. Similar types of defects have later on been observed also at the other RBMK plants. IGSCC in the heat-affected zone of piping made of unstabilized or stabilized high carbon content austenitic stainless steel is a generic issue in boiling water type reactors (BWR, RBMK).

The application of the Leak Before Break (LBB) concept to the LNPP PCS piping is discussed in [RWR012, Annex 2]. The LBB concept is based on an assumption that a crack-like defect in the piping component will be detected via leakage long before the crack size would challenge the fracture resistance capacity of the pipe material under any design condition. This assumption has a high impact on the leak and break frequencies.

Several activities have been going on for LBB concept application to RBMK plants. The findings from these studies, in conjunction with the recent experiences of IGSCC at RBMKs, show that the LBB criteria cannot be demonstrated for the time being due to uncertainties and incomplete knowledge about key factors of structural integrity, e.g. material properties, loading conditions, stress patterns, efficiency and coverage of leak detection and in-service inspections. A comparison of the available information on each factor indicates that

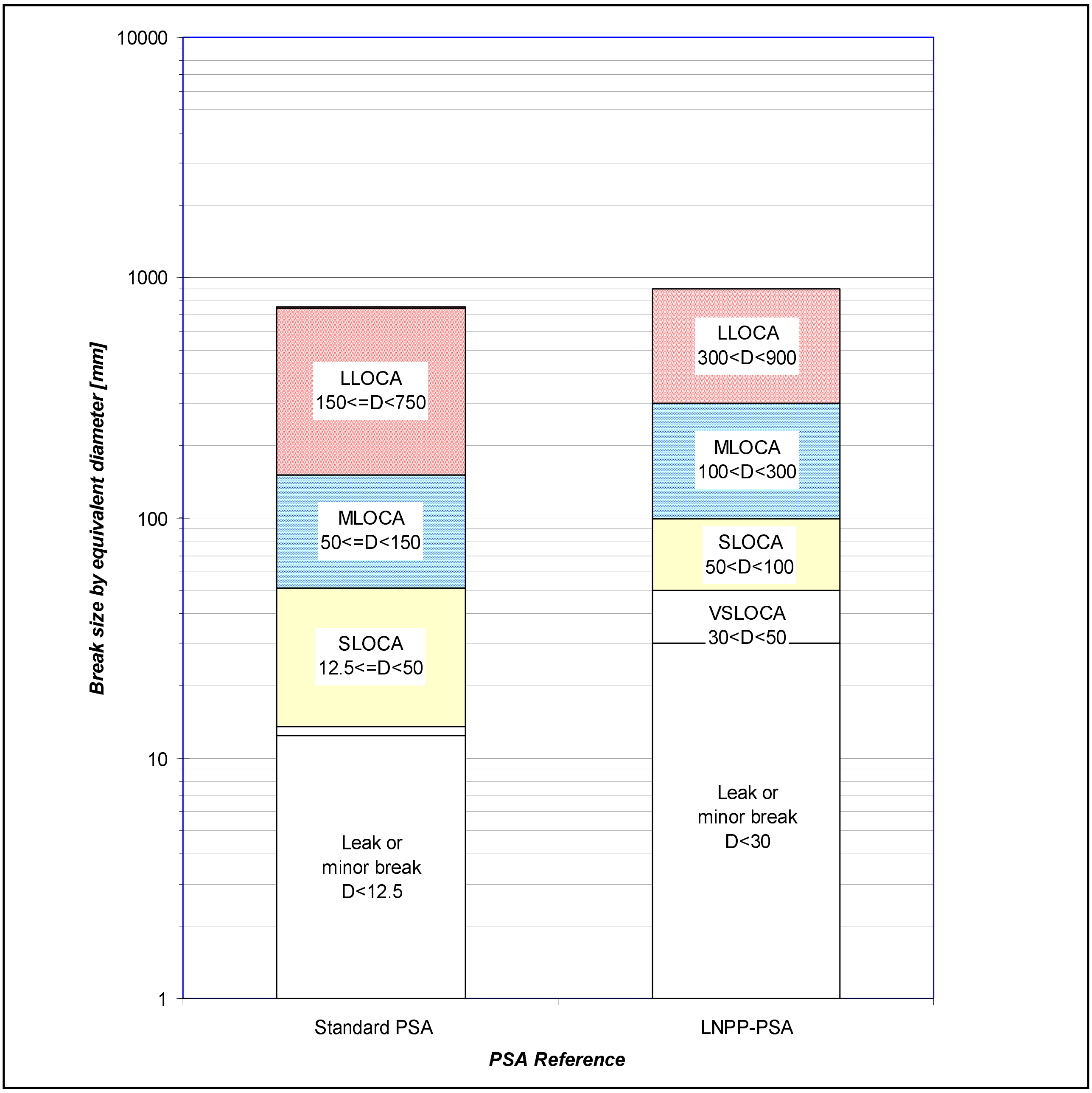

Figure 10. *LOCA size classes in LNPP-PSA compared to the standard definition of BWRs and PWRs. D is inner diameter of pipe [mm].*

for the LNPP, substantially higher break frequency may result than obtained e.g. in the recent studies for BWRs. In conclusion, these findings suggest that the most conservative generic estimates for the break frequency should be used under current circumstances.

It is of interest to notice that [EPRI TR-100380] gives following information. So called Break Before Leak ratio is about 10% according to US experience, i.e. among the total number of ruptures and leaks about 10% has developed directly into a rupture without a prior leaking condition. Applicability of this insight to LNPP Unit 1 and 2 is uncertain.

5.6.4 Frequency estimation

The current estimates for LOCA frequencies as presented in [LPR094] are based on so called zero event estimate for 50% confidence level (hereafter shortly called as zero event estimate), and none non-compensated breaks (LOCAs of any size) having occurred at the RBMK plants over 1973–97, within about 185 reactor years. This results in the estimate of 3.75E–3 /a for the sum of LOCA frequencies.

Generally, zero event estimate can be accepted as a crude estimate for an item with negligible risk-importance, when it is not reasonable to put effort for a more specific estimation. Widespread use of this approach should be avoided because it can severely distort the relative results and reduce the usability of PSA in many applications. Besides, the zero event estimate is a *median* estimate (for 50% confidence level): it is generally recommended that the risk analysis shall use *mean* estimates; in case of large uncertainty (weak direct evidence) the mean can be substantially higher than median.

It has to be emphasized also that the past experience of RBMKs without any larger pipe breaks cannot be directly extrapolated to the remaining lifetime without supporting qualified, well-documented evidence. The world-wide experience shows that especially the rupture mechanisms related to IGSCC do not follow a constant failure rate assumption (i.e. time/age independent model).

The frequencies for each LOCA zone and size class are derived by firstly treating VSLOCA separately, with an assumed frequency of 1.50E–3 /a. The derivation of this value is nowhere explained. The remaining frequency is 3.75E–3 /a – 1.50E–3 / a = 2.25E–3 /a, which is distributed over LLOCA, MLOCA and SLOCA, and zones according to the number of piping components in these size classes and zones. Material and other properties of the different piping subsystems are not taken into account. Downcomers, GDHs and FCCs are rather specific components. Generic ratios for break frequency between piping elements may not be applicable. Besides, there are longitudinal welds in the MCP suction and pressure lines (inner diameter 830 mm); the total length of the longitudinal welds is 900 m (twice the length of these pipelines). The frequency estimation process has been commented systematically in RWR012.

5.6.5 Needed improvements

To summarize, the recent experience of IGSCC at RBMKs in conjunction with the concerns and uncertainties connected to the contributing factors—e.g. material properties, efficiency of leak detection and coverage/efficiency of inservice inspections—leads to the conclusion that break frequency values lower than the generic Western estimates cannot be substantiated for LNPP Units 1 and 2. The used estimates for the break frequency (per piping section) are in PSA Phase 2 by a factor of about 4 lower than the generic estimates in size categories small, medium and large; and by a factor of about 100 lower than the generic estimates in size categories of very small (inner diameter less than 50 mm in LNPP PSA Phase 2). The latter ratio is totally unrealistic. According to all evidence the break frequency of small size piping is higher or same in comparison to the break frequency of large piping.

A concise effort is needed in the continuation to obtain more specific estimates and to reduce the uncertainty in the LOCA frequencies. The operating experience and findings from the material inspections at RBMKs should be analyzed comprehensively, and that information should be related to the LBB concept application at least in a comparative manner, e.g. relating the facts with the recent similar studies for BWRs.

Many questions and comments about the details were raised during the review. These should be considered in the next phase of the PSA. Furthermore, following shortcomings were identified regarding the coverage of special types of LOCAs including:

- Inadvertent opening of safety/relief valves
- Main Coolant Pump seal leak or break
- Interfacing system LOCAs

These issues are discussed in more detail in connection to the data review [RWR019].

5.7 Reliability data

Plant specific reliability data were collected at Unit 2 for period 1987–97. The collected data cover a large part of the needed single failure data, which is very positive, and also the most frequent transient categories. Regarding the component reliability data the main critical comments from the in-depth review and comparison with other data sources are following [RWR019]:

- Spurious opening of the safety relief valves is not adequately handled and the frequency estimation is not explained
- An incomparably low failure rate is used for the diesel generators during the mission time, i.e. regarding failure to run. Ignalina-2 data entry is used, because no events of this failure mode were identified for the diesel generators of Unit 2. A probable explanation is that the cooling circuits were omitted

The operational experience for all units should be analyzed in the continuation to obtain more accurate LNPP specific data. The collection of RBMK generic data, which was started in Barselina, should be continued and extended. The continued data collection at LNPP, and in the longer term at other RBMK plants should cover also identification and analysis of CCFs, because this can be effectively combined with the collection of single failure data.

5.8 Scope issues

The defined scope of the PSA Phase 2 was presented in Section 3.3.3. The various limitations have already been discussed in the preceding sections. To summarize, the most significant scope limitations are following:

- The present analysis is limited to full power operation. An extension to low power and shutdown states is not of high priority. Now it is most important to complete the full power PSA of Level 1.
- The consideration of internal/external hazards is limited to internal fires, flooding and missiles (designated as AEs). The cover should be extended to other hazard categories, e.g.
  - fires in the outdoor equipment such as transformers and switchyards
  - explosion in the hydrogen system
  - loss of room cooling or heating
  - damage of underground piping
  - coastal flooding
  - abnormal weather conditions such as strong wind, heavy snowing and blizzard
  - sea water phenomena such as mass emergence of algae and frazil ice
  - earthquakes.

External hazards can occur also as a severe combination, e.g. in a heavy storm. The simple index analysis method used for AE analysis revealed substantial shortcomings. In many special cases the estimation of fire and flood frequency should be based directly on the relevant operating experience data; all cases cannot be adequately covered by a general indexing procedure. Furthermore, the spreading possibilities of fire and flood between the rooms have to be analyzed

- Operator actions and recovery are analyzed in more detail only in limited extent. In many cases simple engineering judgement has been used. This part should be selectively improved.
- Functional criteria are substantiated by deterministic analyses only to a limited degree.

In addition to the above principal scope limitations PSA Phase 2 made significant modeling simplifications, e.g.

- Large LOCAs, dynamic impacts and other Beyond Design Events were excluded, except that a crude sensitivity analysis was made showing that their contribution is potentially high.
- Modeling of control and protection systems was very simplified.

- Many other parts of the modeling were significantly affected by the incomplete system descriptions. Systematic FMEAs were lacking—they are especially vital for qualified modeling of the control and protection systems, and electric power supply systems.

The influences of the scope limitations and modeling simplifications to the results will be discussed in Chapter 6. The general conclusion is that the results should be used with great care and proper understanding that they are conditional with respect to the limitations. Substantial improvements are needed in PSA Phase 3. However, it has to be emphasized that the near-term improvements [LNPP-M98] were well-founded irrespective of the limitations of P&DSA Phase 2, because they eliminated evident weaknesses, which constituted substantial risk in the mid 98 condition.

6 RETROSPECTIVE COMPARISON

This chapter presents a comparison of the main results of the Pilot Risk Studies for LNPP Unit 1 and Ignalina Unit 2, which were performed in 1993, with the recent P&DSA of LNPP Unit 2 and Barselina 4 (PSA of Ignalina Unit 2, Phase 4). Explanations to the qualitative and quantitative differences are discussed.

6.1 Comparison of Pilot Risk Study results with plant-specific PSAs

The methodology of Pilot Risk Study (PRS) was briefly described in Section 3.1.

Fig. 11 compares PRS results of LNPP Unit 1 (1993) with SNTV-3 for LNPP Unit 2 (Mid 1998 condition). There are specific differences between LNPP Unit 1 and 2. Also the time difference of the studies (1993 and 1998) has certain implications, because some reconstruction works, but not identical in all respects, have advanced at the units. For the crude comparison discussed here those differences have a negligible influence. The main differences between the results of PRS and SNTV-3 are following:

- AEs make a large contribution according to SNTV-3, which is primarily due to fire and flood risk of the service water pump compartment. The recent insights indicate that the fire and flood risks are substantial also in other locations of Unit 2. The internal and external hazards were not considered in PRS, which must be regarded as a major limitation
- Relative underestimation of transients and LOOP by PRS is somewhat surprising, because PRS should be expected to be on conservative side in this area. The evident explanations are design weaknesses in the emergency and auxiliary feedwater systems including first of all the following items (it is understandable that these kinds of details could not be covered by the crude PRS method but require plant-specific PSA):
    - Check valves in the injection lines to steam drums, which violate single failure criterion, see Section 5.2.3
    - Dependence on the relatively unreliable service water system and intermediate cooling circuits, see Section 5.3.2
    - Makeup of feedwater tanks requires manual operations, see Section 5.3.3
- In contrast to the above IE categories PRS estimated LOCA risk higher than SNTV-3. This can be mainly explained by the fact that PRS covers large and unprotected LOCAs, while they are omitted in SNTV-3 (scope limitation of the P&DSA Phase 2). An additional explanation is the relatively low LOCA frequencies of P&DSA Phase 2, which may have been underestimated as discussed in Section 5.7.

The PRS results of LNPP Unit 1 can be regarded misleading as they diverted emphasis on the LOCA issue, i.e. core cooling capacity by the front-line safety systems, while the actual problems (especially in 1993 condition) were according to later insights mainly related to the risk of internal and external hazards in combination with weaknesses in the support systems.

Fig. 12 analogously compares PRS results with Barselina 4—both for Ignalina Unit 2 but in 1993 and 1997 condition, respectively. The comparison raises following comments:

- AEs and CCIs were not considered in PRS. As said, this is a principal limitation of the PRS applications, which were conducted as part of the RBMK Safety Review [RBMK/TG9/FR]
- Overestimation of transients and LOOP by PRS is expected, but still the difference of one order of magnitude is big
- Strong overestimation of LOCA risk by PRS is mainly due to the pessimistic assumption that the recirculation of the cooling water would be critical in the partial break of one fuel cooling

channel (in the size category of Very Small LOCA). An additional explanation is the difference in the LOCA frequencies. Barselina 4 used the same estimation approach, which was then adopted in LNPP P&DSA, and may have similarly underestimated the LOCA frequencies

The above comparisons provide in general quite a controversial picture. The early PRS study gave quite high risks for some event classes. However, in general the PRS method is not necessarily on the conservative side. One unknown element behind the compared results is the lack of an in-depth peer review for Barselina 4. Therefore, little

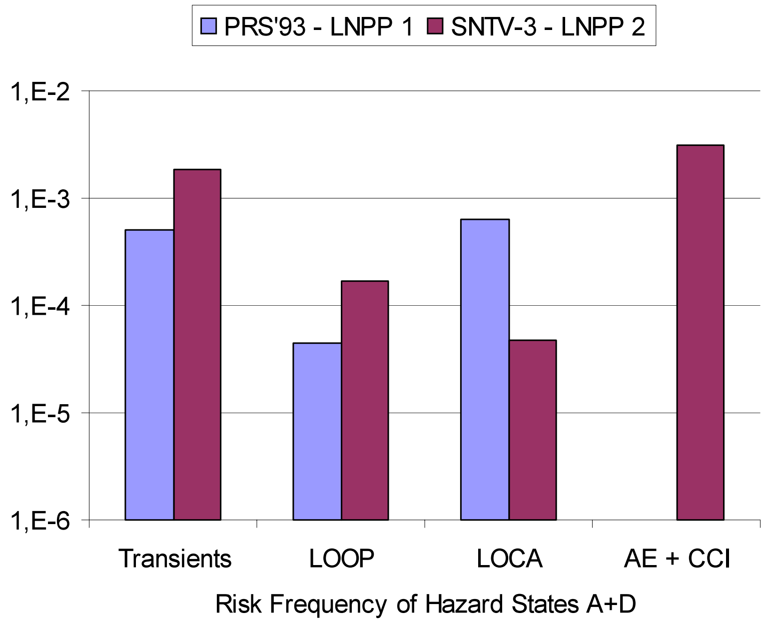

Figure 11. *Summary of the results for Pilot Risk Study for LNPP Unit 1 (1993) and SNTV-3 for LNPP Unit 2 (Mid 1998 condition). Loss of off-site Power (LOOP) is considered separately from 'Transients'.*

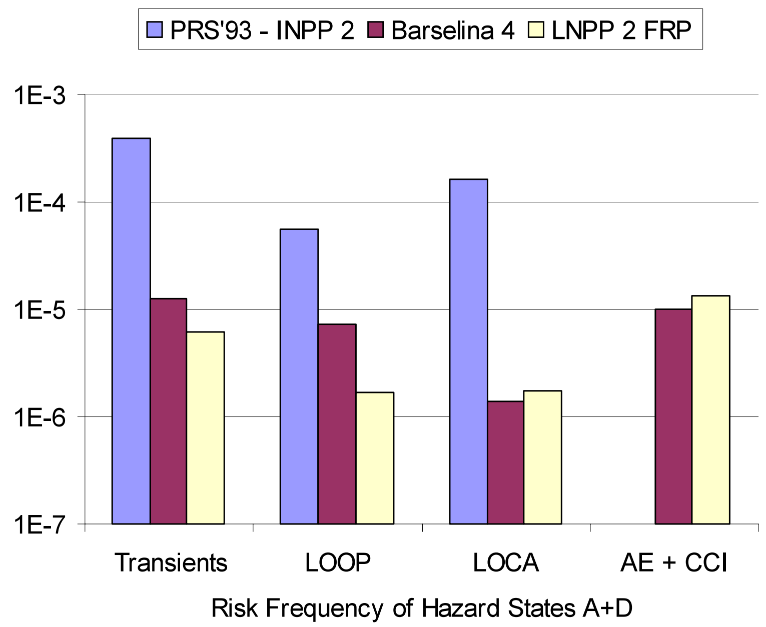

Figure 12. *Summary of the results for Pilot Risk Study and Barselina 4 for Ignalina Unit 2, and for FRP condition of LNPP Unit 2. Loss of off-site Power (LOOP) is considered separately from 'Transients'.*

information is available about the significance and influence of the scope limitations and main assumptions to its results.

6.2 Comparison of LNPP-P&DSA results for FRP with Barselina 4

Fig. 12 shows reasonable compatibility in the results of LNPP-P&DSA for FRP in comparison to Barselina 4. This is certainly expected, because the analysis and modeling procedures are the same, a lot of same generic data are used and also a part of the production teams is same. Besides, it is expected that LNPP Unit 2 (representing 1st generation of RBMK) can be brought by a complete reconstruction to the same safety level as Ignalina Unit 2 (2nd generation of RBMK with specific design enhancements).

6.3 Lessons to be learned, insights from the safety levels

An evident conclusion from the presented comparisons is the need of plant-specific PSA. A simplified approach such as PRS can be useful as a first learning step but the produced risk profile is very uncertain and can be even misleading for the purpose of identifying and prioritizing needs for safety improvements.

Because the design principles of the older plant generations do not provide adequate protection to internal and external hazards such as fires and floods, their exclusion from the analysis scope is a very substantial limitation.

The picture of the RBMK safety level is obscured by the uncertainties in the presented results. Even in the current phase of the plant-specific PSAs for Ignalina Unit 2 and LNPP Unit 2 the uncertainties are substantial due to the limitations in the scope, modeling depth and relevant input data. Especially, the results shown in Fig. 4 for the upgraded configurations of LNPP Unit 2 do not provide full picture of the risks. The following areas are of primary importance when evaluating more accurately the existing and achievable safety level of LNPP Unit 2:

- Extension to consider fire spreading and the use of more specific fire frequency data can result in finding that the actual fire risk may exceed 10^{-3} /a (core accident frequency). A high priority should be placed on the fire safety analysis, which is being started within LISA, and on the improved treatment of the fires in PSA Phase 3
- Extension to consider Large LOCAs as well as dynamic effects of pipe breaks can increase the current LOCA originated risk substantially above 10^{-4} /a (core accident frequency). One influencing factor is that the pipe break frequencies may have been underestimated in PSA Phase 2. Construction of the needed enhanced emergency core cooling capacity seems to be possible only in the long term. Thus any measures to increase and monitor the reliability of primary circuit piping are of high priority in the near term. Improvements in the coverage and efficiency of the in-service inspections and integrated analyses of the inspection results are needed. Joint efforts covering all RBMK plants should be undertaken to reach the aim.

The retrospective comparison reinforces once more the value of in-depth peer review in increased understanding of the analysis limitations and simplifications, i.e. the conditions for the credibility of the produced results.

7 CONCLUDING REMARKS

The progress made in LNPP P&DSA means significant advancement in understanding the dominant risk contributors and most effective ways to improve safety. The results of P&DSA Phase 2 brought up weaknesses and helped to prioritize short-term improvements at the LNPP Unit 1 and 2, which substantially reduced the acknowledged high risk peaks. The created in-house skills of the local PSA team provide a good basis for the started Living PSA development and continued applications.

LNPP P&DSA adds to the expertise of the PSA of Ignalina NPP and RBMK safety review programme. It is sincerely recommended that solid PSA activity is started also at the other RBMK plants.

The Peer Review of P&DSA Phase 2 pointed out shortcomings and development areas with emphasis on the needs for scope extensions. Many of the limitations were similarly recognized by the production team. The review recommendations have been taken into account when planning the LNPP In-depth Safety Assessment (LISA), which includes PSA Phase 3.

Especially, a more detailed analysis of fires and floods is needed taking into account spreading and other influences between connected locations, because the design of 1st generation RBMK does not provide adequate protection in these respects. External hazards were found important at the Loviisa NPP on the Northern side of the Finnish Gulf, e.g. seismic events, mass emergence of algae, frazil ice, high wind and snow storm. These should be evaluated also for the LNPP, starting with a screening analysis. The analysis of the control and protections systems were simplified in P&DSA Phase 2: an in-depth reliability analysis is needed. The condition of the primary circuit piping should be evaluated based on the results of the in-service inspections, which have recently brought up many severe defects in critical pipe sections of RBMKs.

Many of the problem issues are generic for the RBMKs. Joint efforts are thus much desired including the collection and evaluation of the operating experiences.

The reference condition for LISA and PSA Phase 3 will be the current state of Unit 2, in contrast to the fully reconstructed condition, which was the reference condition of Phase 2. This change fulfills the most strongly urged recommendation by the Peer Review team. Because of the predicted slow progress in the full reconstruction, the new strategy will facilitate using the limited resources most effectively to improve the safety in the short and intermediate term both at LNPP Unit 2 and also at the twin Unit 1 with some additional consideration of the slight design differences.

The RBMK plants form an important part of the electricity production capacity in Russia and, without doubts, will still be operated for many years. The safety of the reactor type requires continuing improvement. Contribution to the efforts by qualified Western experts is seen necessary also in the future.

REFERENCES

LNPP P&DSA peer review reports

RMR
Review Main report, Issue 3, 28 February 2000.

RWR011
Handling of Common Cause Failures and Needed Parametric Data. Review report by T.Mankamo, 07 September 1999.

RWR012
Estimating LOCA Frequencies. Review report by T.Mankamo, R. Keskinen, J. Marttila and H. Saari, 12 September 1999.

RWR013
Methodology Selection and Procedures Establishment. Review report by T.Mankamo, 07 September 1999.

RWR014
Review of the Area Event Analysis. Review report, prepared by T.Mankamo, H.Aulamo and J.Marttila, 07 September 1999.

RWR018
System Analysis for the Reactor Monitoring, Control and Protection System. Review report by Andrius Bagdonas and Hermann Scaefer, Issue 1, 10 December 1999.

RWR019
Data for Initiating Events and Component Reliability. Review report, prepared by T.Mankamo, 07 September 1999

RWW007
Benchmarking and Reference Calculations on the DFP Method and Its Use in the Reliability Analysis of RCPS. Work notes, by T.Mankamo, 25 January 1998.

RWW014
Concerns about the External Review of LNPP-P&DSA. Position paper, prepared by H.Aulamo, J.Marttila, H.Reponen and T.Mankamo, 2 October 1998.

RWW020
Current State of LNPP Units 1 and 2, Urgent Needs to Safety Improvement. Position paper, prepared by H.Aulamo, J.Marttila, H.Reponen, H.Schaefer, E.Shubeiko and T.Mankamo, 31 December 1998.

LNPP P&DSA production reports

LNPP-M98
Measures to Improve LNPP Unit 2 Safety (Resulting from PSA). LNPP, December 1998.

LPR010
Leningad PSA—Initiating event analysis. Anders Agner and Gunnar Johansson, Rev.2, 1998-11-27

LPR016
Brief Description of LNPP Unit 2 Reconstruction for P&DSA Project. Sergey Kukhar, Rev.1., 1998-10-26.

LPR094
LOCA Frequency Assessment. Eugene Shiversky and Gunnar Johansson., Rev.0, 1998-06-15.

LPR150
Leningrad P&DSA—Phase 2 Summary Report. Per Hellström et.al. Rev.0, 1999-01-26.

LPR164
Prioritization of reconstruction measures (SNTV case). S. Koukhar, N. Stebenev, M. Dillistone, Final Draft, 26.11.98

Other references

BR417
The Barselina Project Phase 4 Summary Report. Prepared by Gunnar Johansson, Per Helström, Gennady Zheltobriuch and Andrius Bagdonas, December 1996.

BR5-CPS
Reactor Control and Protection System. Andrius Bagdonas and Gennady Loskutov, Barselina Project Report BR5-5, 1999-11-08.

EPRI TR-100380
Pipe Failures in U.S. Commercial NPPs. Prepared by K.Jamali, Halliburton NUS, July 1992.

FE-TECDOC
Root Cause Analysis for Fire Events at Nuclear Power Plants. Draft TECDOC, IAEA, 5 January 1999.

IAEA-TECDOC-543
Procedures for Conducting Independent Peer Reviews of PSAs, Guidelines for the IPERS Programme, Vienna 1990.

K2PG-9
Analysis of Dependencies, PSA Task Guide, Kola NPP Unit 2. Prepared by T. Mankamo, K. Jänkälä, M. Kattainen, A. Angner, G. Johansson and A. Lioubarski, Final Draft, 03 March 2000.

NUREG/CR-3485
PRA Review Manual. Prepared by A. El-Bassioni, et.al., BNL 1985 for the USNRC.

NUREG/CR-5486
Evaluation of Loss of Offsite Power Events at NPPs: 1980–96. Prepared by C.L. Atwood, D.L. Kelly, F.M. Marshall, D.A. Prawdzik and J.W. Stetkar for USNRC, Idaho National Laboratory, November 1998.

PNL-10378
Peer review of the Barselina Level 1 PSA of the Ignalina NPP, Unit 2. Prepared by Sam L. McKay and G.A. Coles, Pacific Northwest Laboratory, January 1995.

PSA-SUDR
Current Status of Probabilistic Safety Assessments for Soviet Designed Reactors. Final Report EUR 17567 EN.

RBMK/TG9/FR
RBMK Safety Review, Final Report of Topical Group 9: PSA. Vols. 1–2, March 1994.

Riskaudit-55
Review of the Ignalina NPP Safety Analysis Report, Summary, Riskaudit Report No 55, January 1997

STUK-YTO-TR 44
The Leningrad Nuclear Power Plant, A General Description. Timo Eurasto, Jorma Sandberg and Jouko Marttila. Finnish Centre for Radiation and Nuclear Safety (STUK), Helsinki, January 1993.

TVO-PSA
Probabilistic Safety Assessment of Olkiluoto 1 and 2.

US_LOSPD
LOSP Data for US NPPs. Work report prepared by Tuomas Mankamo, 15 January 1993.

ACRONYMS

First list contains general abbreviations, while the second one collect LNPP Unit 2 specific system abbreviations. For convenience, both Russian-based and English-based abbreviations are presented.

General abbreviations

Acronym	Description
A	Core Accident State
D	Core Damage State
V	Violation State
IE	Initiating Event
AE	Area Event
BDE	Beyond Design Event
LOCA	Loss of Coolant Accident
LLOCA	Large LOCA
MLOCA	Medium LOCA
SLOCA	Small LOCA
VSLOCA	Very Small LOCA
LOOP	Loss of Offsite Power
TM	Manual shutdown (IE category)
CCCG	Common Cause Component Group
CCF	Common Cause Failure
CCI	Common Cause Initiators
CPS	Control and Protection System
DG	Diesel generator
DSA	Deterministic Safety Assessment
FCC	Fuel Cooling Channel
FMEA	Failure Mode and Effects Analysis
FRP	Fully Reconstructed Plant
FSAR	Final Safety Analysis Report
HPS	Hydro Power Station
IGSCC	Intergranular Stress Corrosion Cracking
LBB	Leak Before Break
LISA	LNPP – In-depth Safety Analysis
LNPP	Leningrad Nuclear Power Plant
LNPP-P&DSA	LNPP – Probabilistic and Deterministic Safety Assessment
MCP	Main Coolant Pump
NPP	Nuclear Power Plant
P&I	Process and Instrumentation
PRS	Pilot Risk Study
PSA	Probabilistic Safety Assessment
PT	Pressure Tube
RBMK	Russian acronym for “Channelized Large Power Reactor”
SAR	Safety Analysis Report
SFA	Single Failure Analysis
SNTV-3	Sensitivity case to approximate mid 1998 condition of LNPP Unit 2

LNPP Unit 2 systems

Russian	English	Description
APEN	EFWS	Emergency Feedwater System
AZRT	PPCS	Process Parameter Control System
BRUB	—	Steam dump to bubbler
BRUK	—	Steam dump to condenser
GPK	MSRV	Main Steam Relief Valve
KoSUZ	ChCS	CPS Channel Cooling System
MPEN	AFWS	Auxiliary Feed Water System
NA	NSWS	Normal Service Water System (existing)
PEN	MFWS	Main Feed Water System
RGK	GDH	Group Distribution Header
SAOR	ECCS	Emergency Core Cooling System (planned)
SKUZ	RCPS	Reactor Control and Protection System
SNES	EPSS	Electric Power Supply Systems
SNTV	RSWS	Reliable Service Water System (planned)
SOVA	ALS	Accident Localization System
SPIR	BCS	Blowdown and Cooling System
—	DS	Drum separator
—	ECR	Emergency Control Room (planned)
—	ICC	Intermediate Cooling Circuit
—	MCP	Main Coolant Pump
—	MCR	Main Control Room
—	PCS	Primary Coolant System