

ORGANISATION FOR ECONOMIC
CO-OPERATION AND DEVELOPMENT

NUCLEAR SAFETY DIVISION

STEERING COMMITTEE ON NUCLEAR SAFETY

RESTRICTED

Paris, drafted: 28-Sept-93
OLIS: 16-Nov-1993
dist.: 18-Nov-1993

NEA/CSNI/R(93)19

Or. Eng.

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

PRINCIPAL WORKING GROUP N° 5

TASK 13

SHUTDOWN AND LOW POWER SAFETY ASSESSMENT - A STATUS REPORT

November 1993

010138

FOR TECHNICAL REASONS, THIS DOCUMENT IS NOT AVAILABLE ON OLIS.



OECD

NEA

TASK 13

**SHUTDOWN AND LOW POWER
SAFETY ASSESSMENT - A STATUS
REPORT**

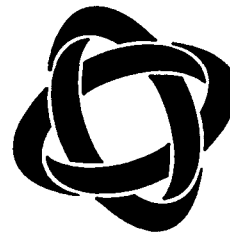
*Prepared by Experts of the Principal Working Group N°5
of the Nuclear Energy Agency of the
Organisation for Economic Cooperation and
Development (OECD)*

Task Force Leader: B. Liwaang (SKI, Sweden)

*Task Force Members: N.J. Holloway (U.K.), J-M. Lanore (France)
B. Liwaang (Sweden), J. Murphy (U.S.), M.P. Versteeg
(The Netherlands), R. Virolainen (Finland),
B. Kaufer (OECD/NEA)*

*Consultants: K. Andersson (Karinta-Konsult) and
P. Karnik (ES-Konsult)*

November 1993



**COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS
OECD NUCLEAR ENERGY AGENCY**

*Le Seine St. Germain - 12, Boulevard des Iles,
F-92130 Issy-les-Moulineaux
Tel: (33-1) 45 24 82 00 Fax: (33-1) 45 24 11 10
Electronic mail: NEA@FRNEAB51*

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The Committee on the Safety of Nuclear Installations (CSNI) of the OECD Nuclear Energy Agency (NEA), is an international committee made up of senior scientists and engineers. It was set up in 1973 to develop and coordinate the activities of the Nuclear Energy Agency concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations. The Committee's purpose is to foster international cooperation in nuclear safety among the OECD Member countries.

The CSNI constitutes a forum for the exchange of technical information and for collaboration between organizations which can contribute, from their respective backgrounds in research, development, engineering or regulation, to these activities and to the definition of its programme of work. It also reviews the state of knowledge on selected topics of nuclear safety technology and safety assessment, including operating experience. It initiates and conducts programmes identified by these reviews and assessments in order to overcome discrepancies, develop improvements and reach international consensus on technical issues of common interest. It promotes the coordination of work in different Member Countries including the establishment of cooperative research projects and results to participating organizations. Full use is also made of traditional methods of cooperation, such as information exchanges, establishment of working groups, and organization of conferences and specialist meetings.

The greater part of the CSNI's current programme of work is concerned with safety technology of water reactors. The principal areas covered are operating experience and the human factor, reactor coolant system behaviour, various aspects of reactor component integrity, the phenomenology of radioactive releases in reactor accidents and their confinement, containment performance, risk assessment, and severe accidents. The Committee also studies the safety of the nuclear fuel cycle, conducts periodic surveys of the reactor safety research programmes and operates an international mechanism for exchanging reports on safety related nuclear power plant accidents.

In implementing its programme, the CSNI establishes cooperative mechanisms with NEA's Committee of Nuclear Regulatory Activities (CNRA), responsible for the activities of the Agency concerning the regulation, licensing and inspection of nuclear installations with regards to safety. It also cooperates with NEA's Committee on Radiation Protection and Public Health and NEA's Radioactive Waste Management Committee on matters of common interest.



CONTENTS

1.	<i>Introduction</i>	1
2.	<i>Use of Shutdown and Low Power Safety Assessment</i>	2
3.	<i>Overview of Assessments</i>	3
4.	<i>Methods and their Implementation</i>	6
	4.1 <i>Methodology</i>	6
	4.2 <i>Implementation</i>	7
5.	<i>Human Interaction</i>	8
6.	<i>Study Results</i>	9
7.	<i>Conclusions and Recommendations</i>	11
	<i>Appendix A: Overview of Assessments</i>	14
	A.1 <i>Power Levels, Outage Types, Plant Operating States</i>	15
	A.2 <i>Initiating Events</i>	21
	A.3 <i>End States</i>	23
	<i>Appendix B: Methods and their Implementation</i>	25
	B.1 <i>General Methodology</i>	25
	B.2 <i>Implementation</i>	27
	<i>Appendix C: Human Interaction</i>	30
	<i>Appendix D: Experiences</i>	32
	<i>Appendix E: Abbreviations</i>	35



1. INTRODUCTION

Traditionally, the focus of safety assessments of nuclear power plants has been on severe accidents caused by initiating events during full-power operation. It has been assumed that the risk originating from events during other modes of operation would be small in comparison with full-power events. This perception has been based on the fact that the potential impact of an accident during low-power and shutdown (LPS) conditions are lower due to decreased decay heat and that more time is available for recovering actions, should adverse situations occur.

During the latest years low-power and shutdown analysis has come more into focus due to a number of reasons. Firstly, full-power analyses have already led to many safety improvements. Furthermore, as a result of maintenance, automatic safety systems are partially unavailable during the other modes of operation. This includes the containment which during periods of shutdown is disabled as a barrier. Another factor is that emergency operating procedures (EOPs) give relatively low attention to emergencies during low-power and shutdown modes.

Furthermore, a number of experiences and events have occurred which have highlighted that LPS modes should be given more attention in the safety work. The Chernobyl accident gave impetus to study possible risks associated with rapid reactivity insertion. Other events, although not resulting in severe consequences, have given concerns about other types of events such as loss of decay heat removal functions, loss of coolant inventory and inadvertent pressurization. For example, the loss-of-power event at Vogtle while the plant was in cold shutdown, has triggered extensive efforts by the U.S. NRC in the area. Indications from new PSA studies, e.g. the French studies on 900 and 1300 MW PWR plants, have also indicated that LPS could give significant contributions to core melt frequency.

Based on these considerations the OECD/NEA Principal Working Group 5 for Risk Assessment decided to form a Task Force (Task 13) to work with this issue. It was decided that the Task Group should compile a report on plans, methods and experiences in the area from the different OECD countries.

The task force leader for this work has been Bo Liwaang at the Swedish Nuclear Power Inspectorate (SKI). For the compilation of the report, Liwaang has been assisted by two consultants: Kjell Andersson (Karinta-Konsult, Sweden) and Peter Karnik (ES-Konsult, Sweden). Contributions to the report have been given by the Task Group members:

Mme Lanore (France)
Mr. Holloway (U.K.)
Mr. Liwaang (Sweden)
Mr. Versteeg (The Netherlands)
Mr. Virolainen (Finland)
Mr. Murphy (U.S.)
Mr. Kaufer (OECD/NEA, Nuclear Safety Division)

In addition to contributions from Task Force participants, information on performed assessments or study plans has on request been acquired from the Nuclear Installations Inspectorate (UK), HSK (Switzerland), Central Service for the Safety of Nuclear Installations (France), GRS (Germany), Vattenfall (Sweden), OKG (Sweden) and Sydkraft (Sweden). Furthermore, the French EPS 900 study and papers presented elsewhere about the U.S. NRC low-power and shutdown studies on PWR and BWR have been very useful information to the Task Group.

The report gives first in Chapter 2 a short description of the use of LPS safety assessment in industry and regulatory organizations. Chapter 3 gives a brief overview of context and scope of some assessments in the area. Chapter 4 deals with study methodologies and their implementation in actual assessments. Problems related to the integration of human interaction in the assessments are separately discussed in Chapter 5. Chapter 6 describes experiences and results from a number of LPS studies. Finally, Chapter 7 is a summary discussion of the "state of the art" of low-power and shutdown safety assessment.

2. USE OF SHUTDOWN AND LOW-POWER SAFETY ASSESSMENT

The main purpose of most LPS safety assessments accomplished so far has been to develop methods and to bring the area up a level where it is possible to put related risks into the context of a total PSA. Some studies have already formed the basis for utilities to introduce safety improvement measures in technical systems, technical specifications and administrative routines.

The licensing authorities have also given the area increased attention. The U.S. NRC has for example stated that their LPS studies (one on PWR and one on BWR) may lead to recommendations regarding possible hardware, procedural, training and staffing changes. In particular, NRC evaluation will form the basis for:

- 1) proposed changes to current technical specifications that govern shutdown operations,
- 2) changes in direction regarding the new standard technical specifications that are being developed by the NRC staff,
- 3) potential requirements to industry regarding abnormal operating procedures,
- 4) modifications to the NRC inspections program.

The NRC staff has developed a working agreement with industry representatives to ensure cooperative efforts in addressing shutdown risk. Topics like evaluation of the technical specifications and emergency procedure guidelines will clearly involve significant interaction between the NRC and the industry.

In Sweden, the Swedish Nuclear Power Inspectorate, SKI, requires that the second round of periodic safety reassessments to be provided by the utilities during the 1990s (ASAR-90) should cover all operating states, including shutdown, equally well. It is also foreseen that SKI will require that more attention must be given to LPS states in Technical Specifications. Accordingly the utilities will continue their development of LPS analysis. The approach by the Vattenfall company is to start with a limited PSA analysis and thereafter complete the shutdown analysis with a "barrier analysis" based on the PSA results. Also the OKG company, operating three BWRs, and Sydkraft, operating two BWRs, have announced that they will use barrier analysis combined with fault trees in their LPS assessments.

A similar situation exists in Switzerland where the regulatory body, HSK, has required that the PSA studies performed by the utilities should be extended to include shutdown, start-up and outage phases. Outlines for the LPS studies have been presented by utilities and the low-power and shutdown PSA studies for all Swiss plants will be completed by 1993/94.

In Finland, the utilities (IVO and TVO) and the regulatory body (STUK) agreed to undertake LPS studies directly after completion of Level 1 PSA involving internal initiators. The

"TVO-SEPRA" LPS analysis resulted in new safety provisions and changes in procedures during the refueling outage in 1993. An LPS analysis of the Lovisa plant (owned by IVO) is in progress.

The French PWR studies included in this report are complete PSAs including LPS conditions. The main objective was to give guidance for the assessment of modifications and procedures and to detect possible weak points. Indeed, actions which have decreased core melt probability, such as improved instrumentation, increased monitoring and increased human redundancy, all improvements relevant to LPS conditions, have already been undertaken.

In the Netherlands major shutdown studies are being carried out for the two nuclear power plants; Borssele (PSA Level 1-2) and Dodewaard (PSA Level 1 and deterministic Level 2 calculations). Major objectives of these studies are to:

- 1) support backfitting and accident management,
- 2) broaden the possible applications of the existing Living PSA,
- 3) complete the safety picture within the framework of a Level 3 PSA.

The Dutch study plans include analysis of fire and flooding events considering that the activities during shutdown could have adverse effects on both protection against initiating events and ability to mitigate the consequences if such events occurred.

In Germany much effort has been given to deterministic analysis of situations with boron dilution and failure of the residual heat removal system during mid-loop operation. Furthermore, a BWR screening analysis has been performed to define plant states with respect to residual heat removal during shutdown. More detailed and systematic analyses of shutdown states are planned for the next years.

3. OVERVIEW OF ASSESSMENTS

This report is based on a number of LPS assessments which been accomplished or, as for the Dutch case, are being planned. These studies are:

Belgium

- Doel 3 and Tihange 2 (PWR)

Finland

- TVO "SEPRA" study (BWR)

France

- EPS 900 (PWR), performed by IPSN
- EPS 1300 (PWR), performed by Electricité de France

(although most references in this report are to EPS 900, it is believed that most characteristics are in common with EPS 1300),

Germany

- GRS-BWR study (BWR-72: Gundremmingen KRB-II-B), performed by GRS

Phase 1: screening analysis (finished 1992)

Phase 2: detailed analysis (until 1996)

- GRS-PWR 1300 study (KWU-PWR), screening analysis, performed by GRS

Netherlands

- Borssele (KWU-type PWR), performed by Siemens/Halliburton NUS

Phase 1: scoping/screening analysis

Phase 2: detailed analysis of relevant POS

Sweden

- Vattenfall - barrier analysis (BWR: Forsmark 2, PWR: Ringhals 4)
- Vattenfall - Ringhals 2 (PWR), limited PSA, performed by Framatome

United Kingdom

- Sizewell B (PWR)

USA

- NRC - Surry (PWR), performed by BNL, focus on mid-loop operation
- NRC - Grand Gulf (BWR), performed by SNL, focus on cold shutdown conditions
- Seabrook
- EPRI studies (BWR and PWR)

The context of the LPS assessment varies between the studies resulting in different approaches to the scoping of plant states. In general, three different levels of scope can be identified:

- 1) the whole operation cycle (power operation, shutdown states and transition states),
- 2) from full-power to cold shutdown throughout the refueling period and start up to power operation,
- 3) only shutdown states for which RHR can be connected.

Typically, the first category are full PSA studies which include LPS. They should thus give an adequate quantification of the contribution to the total core damage frequency from the shutdown and low-power states. The second and third groups (together called LPS studies in Table 1) are studies performed just for LPS conditions in order to complement earlier PSA studies for full-power with LPS contributions.

For the analysis, the low-power and shutdown states must be further divided into a number of plant operating states (POSSs). The selected plant states for the analysis are mainly based on the

Technical Specification modes of operation: start up, hot stand by, hot shutdown, cold shutdown and, specific for the PWR plants, mid-loop operation.

The extent to which transition states between these different POS have been analyzed varies between studies, probably due to the fact that the annual fraction of duration in the transitional modes is relatively low. Transition states have been considered in the NRC reference studies and in studies covering the whole operating cycle. In the French studies the transition state between 139 bars and 30 bars RC-pressure has been analyzed. The results indicate a significant contribution to the core melt frequency from these states.

Table 1 summarizes the context and scope of the studies mostly referred to in this report. The bulk of already presented LPS assessments are Level 1 PSA studies but a number of Level 2 studies are in progress. Fire and flooding has so far been included only in a few LPS-PSA assessments.

Table 1: Context and scope of key PSA studies

STUDY	CONTEXT	PSA	FIRE, FLOOD
Doel 3 and Tihange 2	full PSA	Level 1 + containment response	excl.
TVO-SEBRA	LPS	Level 1	excl.
EPS 900 and EPS 1300	full PSA	Level 1	excl.
GRS-BWR 72	Phase 1: LPS screening Phase 2: full PSA	Level 1 Level 2	excl. incl.
GRS-PWR 1300	LPS screening	Level 1	excl.
Vattenfall - Ringhals 2	LPS	Level 1	excl.
Sizewell B	full PSA	Level 3	incl.
Borssele	LPS (planned)	Level 2	incl.
NRC - Surry	LPS scoping + mid- loop	Level 1 on-going L2	incl. (scoping)
NRC - Grand Gulf	LPS scoping + cold shutdown	Level 1 on-going L2	incl. (scoping)

4. METHODS AND THEIR IMPLEMENTATION

4.1 Methodology

In comparison with full-power, low-power and shutdown conditions have certain special features impacting the accomplishment of safety assessments:

- 1) Plant configuration changes with time which makes the identification of relevant outage types, plant operational states and initiating events to an elaborate task.
- 2) Automatic safety systems are to a large extent unavailable. This implies that more reliance must be given to operator actions to mitigate the effects of potentially serious initiators.
- 3) During shutdown, maintenance actions take place which in general makes the plant more difficult to characterize.
- 4) Technical specifications do not regulate plant conditions as clearly as is the case for full-power.
- 5) In case of serious events, emergency operating procedures are in many cases not available, which makes event trees more difficult to develop.
- 6) Data used in PSA for component reliability during full-power conditions may not always be relevant to LPS conditions.

Still, low-power and shutdown PSA assessments have to meet these problems in the best possible way. Some of the accomplished assessments, such as the French and the Sizewell studies, have been performed within the context of a full PSA, whereas others, such as the NRC studies, have been special efforts for LPS. In some countries other approaches than PSA have been used to assess LPS conditions, such as the barrier analysis performed by Vattenfall in Sweden.

In general, standard PSA methodology with event tree and fault tree techniques have been used in most studies. Due to the changing and relatively weakly defined plant conditions, PSA studies of LPS can be quite elaborate if one strives for as comprehensive assessments as possible. The NRC Grand Gulf example, with about 200 event trees for one plant operational state, illustrates this. An alternative approach is to use merging and bounding analyses to limit the size of effort. Such approaches could make the effort more manageable and more easy to overview. On the other hand, remaining uncertainties would probably be greater.

The problem with the complex LPS environment different from full-power conditions and with much interaction has in the NRC/Surry study been treated by development of event trees in group discussions, involving experts in PWR operations, PSA, human reliability analysis and thermal hydraulics. The same study tackles the problem with changing plant configuration with the "time window approach". Boundaries of the time windows are set to the times when success criteria changes.

As for full-power PSA, event tree development must be supported by thermal hydraulic calculations. In many cases it is sufficient with "back-of-the-envelope" calculations but sometimes this is insufficient. In particular, issues related to boron dilution require sophisticated modelling efforts.

The barrier analysis performed by Vattenfall in Sweden is an instrument for assessing safety margins against selected undesirable events. The result is a qualitative judgement based on the number of barriers and their strength. Although it is not aimed to be a tool for full-scale safety assessments its application has resulted in a number of recommendations for safety improvements.

In summary, low-power and shut-down PSA analyses are more complex than full-power PSA analyses due to a number of reasons, e.g. more complex environment (which also changes with time) and less support from procedures and specifications. The use of traditional PSA with fault tree and event tree methodology is more cumbersome and complementary approaches are being developed.

4.2 Implementation

A quantitative PSA assessment requires data for frequencies of initiating events, system and component reliability and data for human reliability. Plant specific models, analyses and data must be used to capture the essence of shutdown risk. This is due to the fact that refueling outage planning and management practices can vary significantly also between similarly designed plants.

Determination of the applicable initiating events for each considered plant operating state is in many cases based on the set of initiating events from the full-power PSA studies. This approach has been extended with special considerations about LPS conditions such as manual corrective actions and initiating events associated with or resulting from maintenance activities.

Initiating events included in various studies are described in Appendix 1. The procedures and information sources used to identify the initiators are quite similar for the different assessments. For example, the TVO-SEPRA study used the following information sources:

- full-power operation PSA,
- other low-power PSAs published,
- NRC list of initiators,
- systematic interviewing techniques,
- incident reports from ABB plants.

Similarly, the EPS 900 report refers to:

- similar probabilistic assessments,
- French and worldwide experience feedback,
- the safety analysis report (design situations),
- other safety studies (e.g. post-Chernobyl studies).

To determine the frequency of the initiating events during the defined LPS states, the time spent in each of them is one important factor. These time intervals are typically estimated by using the time duration for the different states using average values from plant operating experiences.

In general, specific component reliability data for low-power or shutdown states should be different from full-power data due to e.g. different physical and thermohydraulic conditions. Data being used in published or progressing LPS studies are, however, mostly based on reliability data for full-power operation. For example in the TVO-SEPRA study, data used for hardware reliability are the same as for full-power operation found in the Nordic reliability data book. Also in the French PSA studies, the LOCA frequencies for full-power are used for low-power and shutdown conditions.

In these and other studies it has thus been judged that there is little difference in the equipment failure rates between full-power operation and shutdown. This judgement is sometimes based on a simplistic approach claiming that the reduced loads on systems and components during shutdown states are balanced by increased unreliability due to extensive maintenance activities. Clearly, the component reliability data currently used in LPS studies in many cases are more judgmental than the corresponding data for full-power PSA.

5. HUMAN INTERACTION

Already in full-power PSA is human reliability a difficult problem with respect to completeness in initiating events and accident sequences. The potential dynamical evolution of sequences caused by human behavior can not necessarily be modelled with event trees and fault trees. In LPS analyses these problems are more severe due to factors discussed in the previous chapter.

Some of these factors also emphasize the need for active and correct operator actions, although the time available in accident situations is often, but not always, much longer than for full-power conditions. For example, automatic safety systems are unavailable during periods of time. Many operator responses thus involve more than simply manually initiating normally automatic system responses as is often the case in full-power scenarios. Furthermore, appropriate procedures for emergency operation during accidents at LPS have not been systematically developed.

A natural approach to this problem is to use the traditional methods for quantification of human error such as THERP and SLIM (see Appendix E), with adjustments to LPS conditions. For example, the NRC studies apply existing methods to estimate human error and include measures to take shutdown conditions into account. Still they recognize a very large uncertainty in the human error probabilities. Also the French PWR studies use standardized methods to estimate human error probabilities. It is recognized that the human factor, which is a dominant factor for the results, remains one of the major causes of uncertainty.

Doubts have, however, been raised, e.g. in Belgian studies, about the applicability of human reliability models, developed for full-power states, to LPS conditions. This concerns for example whether the time-dependent reliability curves deduced for operator response to initiating events are applicable to non-power states.

In the TVO-SEPRA study much reliance was given to operating statistics and engineering judgment to arrive at reasonable estimates of human behavior. Much effort was also given to interviews with plant personnel. Also the NRC procedures include interviews with control room operators, outage management personnel and training personnel. Furthermore, the group discussions with different types of experts may create an environment suitable to discuss possible operator errors.

During the past year, the NRC launched a multi-year program to address the developmental needs to improve existing human reliability methodologies in PSAs. In the first report (soon to be published), three major areas were addressed to identify human influence during LPS conditions:

- Identification of factors and characteristics that are unique to the LPS environment in their contribution to human performance and reliability.

- Identification and characterization of the more critical types of human errors that occur during LPS, and their causes. This led to the development and implementation of a human action classification scheme (HACS).
- Development of an interview protocol and conduct of numerous interviews.

Based on these results, four key issues were identified that will be pursued as the research continues:

- Errors of commission must be incorporated into PSA models.
- Dependencies among human actions must be considered.
- More performance-shaping factors (PSFs) were identified and enhancements to the quantification process will be necessary to accommodate the additional PSFs as well as the effects of multiple PSFs on performance.
- Methods need to be developed to address the problems arising from the many multiple concurrent tasks that occur during LPS operations.

6. STUDY RESULTS

Only a few low-power and shutdown studies have been completed.

The results vary with respect to the overall contribution of LPS states to plant undecided events. However, there seems to be a broad consensus that core damage frequency during shutdown or low-power is at least not insignificant when compared to full-power values (see Table 2).

Assessments performed have identified a number of possible initiating events and sequences giving significant contribution to core damage frequency. One type of event which has been given much attention for PWRs, and which is often found to be a dominant risk contributor, is loss of RHR in connection with mid-loop operation. For BWRs, loss of coolant accidents below the core tend to be a significant initiating event contributing to core damage frequency.

All published LPS studies have demonstrated the importance of human actions. Human error could be important both as accident initiator and as a factor in recovery after an initiating event. Since there are few automatic safety systems available during an outage, the human action is a very important barrier between an initiator and serious consequences. The scarcity of technical specifications and procedures applicable to LPS conditions is an important factor in this context.

In spite of all the problems with LPS safety assessments discussed in previous chapters, many safety improving measures have already been taken on the basis of LPS assessments. The improvements cover a wide range of measures including introduction of extra technical barriers for situations with otherwise only administrative barriers in effect, improved instrumentation (e.g. for the monitoring of the primary circuit) and more strict administrative controls. In many cases these safety improving measures seem relatively cheap. It may thus be concluded that PSA for LPS can be a cost-effective tool for safety improvement, maybe even more cost-effective than PSA for full-power.

Table 2: Results from PSA assessments of LPS plant states

STUDY	CONTR. TO CORE DAMAGE FREQUENCY	DOMINANT INITIATORS	COMMENTS
Doel 3 and Tihange 2	Results not yet available	-	-
TVO-SEPRA	> 50 %	1. Leakage below core 2. Loss of RHR	Improvements based on study improved the cdf contribution to about 10 %
EPS 900	32 %	LOCA combined with safety injection not available	Sequences with human error contribute with nearly 70 % to cdf In EPS 1300 the cdf from shutdown represents 70 % of the overall risk
GRS-BWR 72	Results not yet available	-	-
GRS-PWR 1300	No final quantitative results available	1. Deboration during shutdown 2. Loss of RHR at mid-loop oper.	Further studies necessary
Vattenfall Ringhals 2	not applicable (see comment)	Loss of RHR during mid-loop operation	Other (more pessimistic) assumptions compared with "power PSA"
Sizewell B	> 60 %	fires	
Borssele	Studies not completed	-	-
NRC - Surry	11 %	Loss of RHR during mid-loop oper. followed by operator failure	Large uncert. in human error estimates
NRC - Grand Gulf	< 75 %	1. Loss of off-site power during cold shutdown 2. Loss of emergency DC bus during shutdown	Human action is very important

7. CONCLUSIONS AND RECOMMENDATIONS

Significance of LPS accidents

Studies on risks associated with LPS conditions have confirmed that reactor safety is not given by inherent safety in design and processes but that it is the product of systematic and prudent work by reactor operators and regulators. In comparison with full-power PSA some factors, such as lower decay heat and more time available for recovery actions, decrease risks. Other factors, such as unavailability of automatic safety functions, unavailability of barriers (including containment), human interaction in maintenance activities, less operator guidance from technical specifications and emergency operating procedures, tend to increase risk.

The quantitative results already accomplished with PSA studies vary but in general it can be concluded that LPS risks are not negligible in comparison with full-power risks. In some studies LPS contributions dominate core damage frequency. It should be emphasized that the uncertainties in LPS-PSAs are larger than in full-power PSA due to the fact that assessment methodology is in an early stage of development. Furthermore, comprehensive data bases relevant for LPS conditions have not yet been gathered and severe problems arise when human factors are to be taken into account.

Methodologies

The implementation of traditional PSA methods on LPS conditions meets a number of problems. Plant configuration is difficult to characterize due to e.g. maintenance activities and lack of technical specifications. In addition, the plant status changes with time which makes it a large effort to identify relevant operating states and initiating events. In case of serious events the lack of operating procedures makes the PSA effort even more cumbersome.

In principal, standard PSA methods would still be possible to apply given that relevant data could be identified or developed. Indeed extensive traditional PSA efforts have been made in the area. The size of the problem is, however, illustrated by the NRC Grand Gulf study which used about 200 unique event trees, of which some had over 100 outcomes, for one plant operational state. In a small event tree - very detailed fault tree approach, as in the TVO-SEPRA study, the problem size has to be handled at the fault tree level.

In this situation it is natural to try to develop alternative or complementary methodologies. The size of the effort could be limited by various merging or bounding approaches. So far there does not, however, seem to exist any standard technique for this. Another approach is to introduce more qualitative methods such as "barrier analysis" applied by Vattenfall in Sweden. From the PSA analysts perspective such methods may, however, not seem to be enough systematic or comprehensive. Obviously development of overall methodologies, maybe combining existing methods, is needed.

Component data

The data bases for LPS assessments must be also be improved before the area can reach a similar level of confidence as full-power PSA. This concerns both initiating events and possible subsequent failures. So far full-power PSA component data are used in LPS studies to a very large extent although doubts can be raised about their applicability due to different plant conditions (e.g. LOCA probabilities for a depressurized primary system). It may not necessarily be the case that factors increasing risk and factors decreasing risk in comparison to full-power data balance each

other. This introduces extra uncertainties into the assessments. A first step to improve the situation would be to make a more thorough evaluation of the validity of present data bases used in LPS assessments.

Human interaction

The weakest part of LPS safety analyses and the most important factor for uncertainty in the results is deemed to be the treatment of human interaction. The problems existing in full-power PSA are enforced and become more crucial when it comes to low-power and shutdown conditions.

First, the results from most studies show that human error is a very significant, and in some cases dominant, contributor to risk. One reason for this is that unavailability of automatic safety functions makes operator action more crucial. Another reason is that maintenance activities could cause initiating events, or adverse the situation if an event occurs.

Secondly, the operator support in terms of technical specifications and emergency procedures is less developed than for full-power conditions. Also emergencies during LPS conditions is generally relatively little trained in operator education and training programs.

Thirdly, there are doubts that the analytical methods used in full-power PSA for human reliability analysis (HRA) are sufficient for LPS analyses. Already in full-power application they have weaknesses related to completeness of event trees and the dynamic evolution of events, which is difficult to simulate with standard event tree and fault tree techniques. These problems are enforced for PSA conditions. In addition, appropriate data are not available for LPS conditions and the validity of existing simulator data seems very limited.

In conclusion, there are problems with current standardized methodologies to handle human error in the context of PSA for LPS conditions. New promising developments would be welcomed. As for component data a first step could be to clarify more in detail the weaknesses (and merits) of current methods. Their possible role(s) in a systematic and comprehensive safety analysis approach could thereby be illustrated. The needs for new ideas and approaches could thereby also be better defined.

Fire and flooding

Analysis of fire and flooding has so far been included in LPS studies only to a limited extent, but a number of programs, e.g. the NRC and the Dutch programs, have such analyses within their near term plans. The activities during shutdown increase the likelihood of initiating events due to supplies associated with maintenance, increased number of ignition sources, breached fire and flood barriers, changing water levels etc. Furthermore, plant ability to mitigate events can also be adversely impacted due to reduced number of available safety systems, less strict technical specifications and less comprehensive procedures.

Recommendations

Studies have shown that LPS risks are significant and could be dominant in comprehensive safety assessments. It is therefore important to develop appropriate assessment tools and data bases for LPS application.

Much progress is, however, needed before LPS states can be included in safety assessments to the same degree of confidence as full-power. In this work it must be recognized that a standardized framework for LPS safety assessment may be difficult to develop due to relatively

large differences between reactors with respect to routines, especially for maintenance shutdown. Still there is a great potential for progress with cooperation between different utilities, between utilities and regulatory bodies, as well as on an international level. Indeed, work is in progress within IAEA to develop guidelines for shutdown risk assessment.

A program for improving the LPS assessment capabilities should include a systematic evaluation of:

- The potential of standard PSA methods as well as other possible, alternative or complementary, approaches.
- The validity of present data bases used in LPS assessments, especially for component reliability.
- The validity of current HRA methods in LPS environment and the potential of other approaches to human interaction.

Considering that the risks associated with LPS conditions could be about the same as for full-power and considering that the corresponding safety improvements, such as administrative changes and new procedures, usually are relatively cheap, it seems that PSA for LPS conditions could be more cost-effective than for full-power. This should further emphasize the efforts to reduce the uncertainties in the LPS analyses to make the PSA results reliable enough for identification of dominant risk accidents taking full-power and LPS conditions into account at an equal level.

Although still at an early stage of development, LPS assessments have given clear indications on several issues that warrant serious consideration and identified a number of possible areas for improvement, such as outage planning and control, technical specifications, procedures, training and instrumentation. Application of existing methods and data has thus potential for important safety improvements, in spite of existing uncertainties. By performing actual assessments the needs for improvements are also clarified. This should therefore be encouraged.

APPENDIX A: OVERVIEW OF ASSESSMENTS

This appendix gives an overview of the studies which have been included in this review with respect to the considered power levels, outage types, operating states, initiating events and end states. The studies are:

Belgium

- Doel 3 and Tihange 2 (PWR)

Finland

- TVO "SEPPA" study (BWR)

France

- EPS 900 (PWR), performed by IPSN
- EPS 1300 (PWR), performed by Electricité de France

(although most references in this report are to EPS 900, it is believed that most characteristics are in common with EPS 1300)

Germany

- GRS-BWR study (BWR-72: Gundremmingen KRB-II-B), performed by GRS
Phase 1: screening analysis (finished 1992)
Phase 2: detailed analysis (until 1996)
- GRS-PWR 1300 study (KWU-PWR), screening analysis, performed by GRS

Netherlands

- Borssele (KWU-type PWR); performed by Siemens/Halliburton NUS
Phase 1: scoping/screening analysis
Phase 2: detailed analysis of relevant POS

Sweden

- Vattenfall - barrier analysis (BWR: Forsmark 2, PWR: Ringhals 4)
- Vattenfall - Ringhals 2 (PWR), limited PSA, performed by Framatome)

United Kingdom

- Sizewell B (PWR)

USA

- NRC - Surry (PWR), performed by BNL, focus on mid-loop operation
- NRC - Grand Gulf (BWR) performed by SNL, focus on cold shutdown conditions
- Seabrook
- EPRI studies (BWR and PWR)

A.1 Power levels, outage types, plant operating states

Depending on the context of the analysis, the PSA assessments include different ranges of operation from the total operation cycle to just shutdown states for which RHR is connected.

The LPS states are divided into a number of plant states to a varying degree of detail. First the Technical Specification modes of operation can be used: start up, hot stand by, hot shutdown, cold shutdown and, specific for the PWR plants, mid-loop operation. Then the definition of plant operating states can be made more detailed using transition states between these broad modes of operation.

In the following, the context of the assessments in terms of range of power operation as well as the definitions of plant operating states and boundary conditions are described for finalized or still ongoing studies.

Doel 3 and Tihange 2

For the PSA analyses of Doel 3 and Tihange 2, one power state and three shutdown states are considered. They are characterized as follows:

State A: From 100% to hot shutdown.

State B1: Shutdown with RHRS connected: primary pressure between 30 and 23 bar, primary temperature between 120 and 70 °C.

State B2: Shutdown with RHRS connected: primary pressure equal to atmospheric pressure, primary temperature between 70 and 10 °C (since the state has to be reached for interventions on the primary side, it is supposed that during the whole time spent in this state the reactor is in mid-loop operation).

State B3: Reactor open for refueling with RHRS connected, reactor pit filled with water.

State A applies for 90% of the year. Transitional modes of operation are not included, since they only represent 0.7% of time.

TVO-SEPRA

The study consists of operating states lower than 8% of nominal power.

Since the decay heat rate and the possibilities to move it from the core and from the spent fuel pools vary during the course of the refueling outage, the refueling and low-power period was

divided into subphases and the safety function success criteria were defined for each of them. The following phases were used:

- Power reduction and reactor shutdown
- Pool cooling not possible, opening of reactor lid
- Pool cooling available but the amount of decay heat exceeds its capacity
- Pool cooling available and sufficient for RHR function
- Pool cooling not possible, closing of reactor lid
- Startup

EPS 900

The French studies cover the whole operation cycle. On basis of operating experience with reactors in service, six different operating states have been identified:

- State A: This state covers the operating phases from 100% to hot shutdown. The safety injection system, which enables the water inventory in the core to be preserved in an accident situation, is activated by a low primary system pressure signal.
- State B: This state covers the remaining part of intermediate shutdown down to the point where RHRs implementation conditions are reached (temperature between 177 and 280 °C, pressure between 30 and 139 bars absolute).
- State C: This state covers the phases where primary system cooling is provided by the residual heat removal system and the primary system is full.
- State D: This state covers phases in which the primary system is partly drained or open to the point where the primary pipes are half full. A number of specific cases are recognized depending on the location of the opening in the primary system. The RHRs is in operation.
- State E: This state covers cold shutdown for refueling with the reactor cavity full and with at least one fuel element in the reactor vessel.
- State F: This state covers all primary system configurations where all fuel has been unloaded from the reactor vessel.

State A applies for 85% of the year.

GRS-BWR 72 study

The BWR safety analysis consists of a Level-1 analysis for the power state and a screening analysis for different plant operation states (POS) during shutdown. The POSs are defined as follows:

- POS I: Shutdown of the plant via turbine access control valves, RPV isolated.
- POS II: Residual heat removal via the residual heat removal chain, RPV isolated.
- POS III: Residual heat removal via the residual heat removal chain, RPV open, reactor well not flooded.

POS IV: Residual heat removal via the residual heat removal chain, reactor well flooded, suction from dryer and separator storage pool.

Furthermore a screening analysis of reactivity events and core loading accidents was performed.

GRS-PWR 1300 study

In the PWR shutdown analysis all plant operation states during an outage for refueling have been investigated including the heat up period to power operation until criticality has been reached again. The outage time is divided into three phases and every phase is subdivided into five POSs because of different system configurations during the phases. The phases are defined as follows:

- Phase I:** Shutdown. This phase includes the system configurations during shutdown from "subcritical, hot" to cold shutdown with RHR-system connected till a primary temperature of 50 C and a pressure of 2 bar is reached.
- Phase II:** Outage, refuelling. The phase II starts with lowering the RPV lid and includes flooding of setdown pool, refueling, emptying of setdown pool and ends with closing RPV lid.
- Phase III:** Startup. Phase III is running from fill up the RPV-inventory and covers the heat up of the primary system, leak test and the deboration of the primary system.

Borssele

A first step is to identify plant operating types (POTs) differing between forced outages, e.g. requiring only hot or cold standby, and scheduled outages for refueling.

Four different POTs have been defined:

- Hot standby
- Cold shutdown
- Drained maintenance without unloading the core
- Refueling outage type for refueling or repairs for which a longer outage time is expected requiring unloading the core.

For the Borssele study the number of POSs which have been developed are 28 (see list below). For the analysis the frequency of each POT and the duration of each POS in the different POTs is determined. Only the refueling outage requiring unloading the core is covered by all 28 POSs. For the other three POTs, just a number of the defined POSs are applicable.

In addition, the same POS in a certain POT can be reached within different time spans after reactor trip due to different possible timings. This means that there can be different decay heat levels which might cause different accident sequences even if the initiating event occurs in an identical POS. For example, mid-loop operation with reactor pressure vessel closed is reached for planned maintenance in about 35 hours after reactor trip while it takes twice as much time to reach the same POS in refueling outages.

List of POS for Borssele

POS 1: The starting condition for the definition of the POSs was step 2 of the shutdown procedure during normal reactor runback. This first POS consist of the reactor critical

at low power (ca. 20% nominal power), supplying all in-house electrical loads via main transformer. In this POS one condensate pump and one feedwater pump are tripped and turbine bypass valves are in operation.

- POS 2: House load supply is changed to the start-up transformers.
- POS 3: Turbine tripped, heat removal via turbine bypass valves; adjustment of pressurizer level indicators and setting pressurizer heating to about 60% of normal value.
- POS 4: Hot standby, reactor coolant temperature about 290 C, reactor coolant pressure 154 bar, boron concentration greater or equal to CR (Reference boron concentration).
- POS 5: Boron concentration increased to CK (Cooldown boron concentration), cooldown with SG to 120 C and pressure from 154 bar to 29.4 bar. At 34.4 bar isolation valves of ECCS accumulators closed and disabled.
- POS 6: Alignment of ECCS for RHR operation; further cooldown with ECCS in RHR mode to 100 C, pressure maintained at 29.4 bar. High pressure ECCS pumps disabled. Tripping of first reactor coolant pump (RCP) at reaching required boron concentration. At 105 C the SC atmospheric dump valves (ADV) will be opened and the MSIVs will be closed.
- POS 7: Cooldown to below 50 C via RHR. The pumps of the bunkered reserve suppletion system (extra secondary side injection system to allow for decay heat removal via SGs in case normal and emergency feedwater systems are not available) may not be available.
- POS 8: Depressurization to 4.9 bar by switching of pressurizer heating and tripping the second RCP: Primary make-up for regulating boron concentration automatically set to 2200 ppm.
- POS 9: Depressurization to 0 bar by pressure relief from pressurizer to pressurizer relief tank, ECCS sump valves disabled in closed position.
- POS 10: Cold shutdown steady state.
- POS 11: Draining of RCS to mid-loop. Jumper the pressurizer low level signal to avoid low pressure ECCS injection. Triggering of bunkered primary side injection system put in temperature mode in case RCS temperature exceeds 80 C.
- POS 12: Mid-loop operation RPV head closed.
- POS 13: Mid-loop operation, RPV head open (as soon as one bolt is loosened RPV head is considered open). Several sources of unborated water are isolated.
- POS 14: Filling up of the reactor basin with ECCS pumps from inundation tanks and equalizing water level to that in the spent fuel pool. Opening of sluice gate between both pools. Heat removal simultaneously via ECCS - RHR system and fuel pool cooling system.
- POS 15: Preparation of core unloading; removal of RPV intervals.
- POS 16: Core unloading. All fuel assemblies transported to the spent fuel pool.

- POS 17: Core entirely removed from RPC: Sluice gate between pools closed. RHR by fuel pool cooling system. Both doors of personnel lock open. RCS drained.
- POS 18: Core reload after refill of reactor basin. Personnel lock closed. ECCS-RHR put into operation.
- POS 19: Drain RCS below flange of RPV with ECCS pumps.
- POS 20: Mid-loop operation after refueling. RPV head placed, but bolts not yet tightened.
- POS 21: Mid-loop operation after refueling. RPV head closed. RCS connected with off-gas system or containment ventilation system for venting.
- POS 22: Refill of RCS by means of Volume Control System, boron concentration 2200 ppm. Triggering of bunkered primary side injection put in pressure/level mode in case of low level in pressurizer and high pressure in containment in coincidence with RCS pressure less than 117 bar.
- POS 23: Pressurizer heatup to about 230 C, pressurization of the RCS. PORVs are operable and high pressure ECCS is enabled.
- POS 24: RCS heatup with RCPs to 150 C and 28.4 bar.
- POS 25: RCS heatup with RCPs to 270 C and 154 bar, boron concentration 2200 ppm. ECCS accumulators made operable as pressure exceeds 35 bar.
- POS 26: Nuclear heatup and low power operation. Dilution via volume control, heat transfer via turbine bypass, house load via start-up transformers.
- POS 27: Low power operation, turbine running, house loads via start-up transformers.
- POS 28: Synchronizing generator and switch-over main transformers.

Vattenfall - barrier analyses

The considered plant states do not cover the whole refueling outage. The analyses were concentrated to a number of predefined activities/phases during the cold shutdown and refueling states.

Vattenfall - Ringhals 2

The plant states for the analysis are based on the Technical Specification modes of operation: hot stand by, hot shutdown, cold shutdown, mid loop operation, and refueling.

Sizewell B

The study for Sizewell B covers the whole operation cycle. The plant operating states are the basic plant states which will occur as a result of planned operation of the station or may be required following initiating faults. The plant operating states are as follows:

- Power
- Hot stand-by

- Hot shutdown
- Intermediate shutdown
- Cold shutdown
- Refueling
- Steam generator tube and reactor coolant pump inspection
- Post LOCA recirculation

NRC studies

The project is a part of U.S. NRC's research plan in response to the Chernobyl event and will examine all non full-power operational modes at one PWR (Surry) and one BWR (Grand Gulf). These plants were chosen mainly because they were previously analyzed in the NUREG 1150 study. The intention is to compare results of this project with the full-power results from NUREG-1150.

NRC - Surry

There are four different types of outage defined: refueling, drained maintenance, non-drained maintenance with use of the RHR system, and non-drained maintenance without the RHR system. For the refueling outage 15 POSs were identified. For the other outage types, the number of relevant POSs are less.

The 15 POSs defined are:

- Low power operation and RX Shutdown
- Cooldown with SG
- Cooldown with RHR (> 200 °F)
- Cooldown with RHR (< 200 °F)
- Drain RCS to midloop
- Midloop operation
- Fill for refueling
- Refueling
- Drain RCS to midloop after refueling
- Midloop operation
- Refill RCS Completely
- RCS heatup solid and draw bubble
- RCS heatup with RCPs
- RCS heatup with SGs
- RX startup and low power operation

NRC - Grand Gulf

Thirteen POSs were developed:

- Low power operation and RX shutdown
- Cooldown from operating pressure to 500 psig
- Cooldown from 500 psig to initiation of RHR/SDC
- Cooldown with RHR/SDC to 200 F
- Cold shutdown
- Refueling with water level raised to steamlines
- Refueling with water level raised and upper pool connected
- Refueling with water level lowered to steamlines

- Cold shutdown after refueling
- Heatup to point where RHR / SDC no longer available
- Heatup to 500 psig
- Heatup to operating pressure
- Low power operation after refueling

A.2 Initiating events

Determination of the applicable initiating events for each considered plant operating state are in many cases based on the set of initiating events from the full-power PSA studies. This approach has been extended by special considerations about manual corrective actions and, on the other hand, initiating events associated with and resulting from maintenance activities. Examples of initiating events and associated considerations in some planned and progressing assessments are listed below.

Doel 3 and Tihange 2

For establishing the list of initiating events to be covered by the Doel 3 and Tihange 2 PSAs, two main sources of information were used: generic lists of initiating events taken from literature or other PSAs and an analysis of plant specific aspects which could indicate plant specific initiating events. External and internal hazards were excluded.

The two information sources and the limitations mentioned above led to the following list of initiating events to be covered for the shutdown states:

- Loss of coolant accidents
- Transients such as spurious operation of the ECCS, reactivity incidents, loss of cooling systems and loss of RHR
- Loss of electrical power
- Spurious operation of the "bunkered systems"
- ATWS (limited to dilution)

TVO-SEPRA

The study consists of the analyses of leakages and loss of decay heat removal in the planned shutdown conditions. Additionally special studies were performed for cold pressurization, for local criticality events, for heavy load transports and for transients during startup and shutdown.

The qualitative analysis produced three types of initiators:

- Leakage below core top
- Leakage above core top
- Loss of residual heat removal

The first two initiators were divided into five classes according to the need for water to compensate the leakage. The loss of RHR case was classified according to the required compensating decay heat removal capacity.

Loss of external electric power supply and external events such as fires and floods were excluded from the study.

Borssele

The approach used to identify initiating events consists of three steps. These steps attack the problem from three different angles to ensure that a comprehensive set of initiating events is developed.

The steps are:

- Systematic Safety Parameter Review
- Review of other PSA and safety-related documents
- Plant Specific Data Analysis.

The Systematic Safety Parameter Review step is similar in function to a Master Logic Diagram. The Master Logic Diagram that has been used in the Borssele full-power PSA has been used as a starting point for this step. The safety parameters and any noted "potential causes" of initiators have been transferred and evaluated. These parameters and causes have been reviewed, and their applicability during the POSs of this analysis evaluated. Potential causes were extrapolated to fit the various shutdown plant conditions as needed.

For Borssele 46 initiators have been selected for the PSA. In a matrix all the selected initiating events versus POSs were given thereby identifying those specific POSs for which the selected events were applicable. Over 1900 possible combinations were identified in this matrix. In order to have a manageable number of initiating events and plant conditions for the event tree task, grouping was conducted in two steps:

- Grouping of plant operational states
- Grouping of initiators

First the POSs with the same basic plant conditions were grouped. Both steady-state and transition states were included in this grouping. Next, initiating events with similar plant response were grouped together.

Vattenfall - barrier analyses

The barrier analyses were performed with a slightly different approach compared with PSA studies. No actual initiating events were defined, instead the different states during the course of an activity were evaluated with respect to the remaining margins to an undesirable consequence.

Vattenfall - Ringhals 2

Based upon international experience and the results from the earlier performed barrier analyses, the initiating events considered in the study were:

- Loss of RHR
- LOCAs
- Reactivity incidents due to inadvertent dilutions
- Cold pressurization of the RPV
- Cold pressurization of the steam generator
- Refueling incidents

Sizewell B

There are about 160 initiating events identified in the fault schedule as occurring during shutdown conditions. The fault schedule is condensed to a reduced number of faults, which are analyzed in event trees. This leaves faults or initial events which can be categorized as follows:

- Boron dilution
- Cold overpressure
- Auxiliary building leak
- Loss of coolant accidents
- Loss of residual heat removal faults
- Miscellaneous faults

The number of faults and the size of event trees are sufficiently small such that further boundings of faults is not necessary for event tree analysis purposes.

NRC - Surry

Eight major groups of initiating events have been used:

- Loss of RHR
- Transients
- Loss of coolant accidents
- Loss of off-site power
- Low temperature overpressurization
- Reactivity accidents
- Refueling accidents
- Support system failures

Approximately 180 initiating event specific event trees were developed for the different POSs.

NRC - Grand Gulf

Five major groups of initiating events have been used:

- Transient events
- Loss of coolant accidents
- Decay heat removal challenge events
- Special events (e.g. loss of support system events)
- Hazard events (i.e. internal fire, flood events and seismic events)

A number of 41 potential initiating events were identified for all POSs. Of these, 34 survived the screening and were quantified. Approximately 160 initiating event specific event trees were developed for the 7 POSs.

A.3 End states

Consequences considered in the planned or progressing studies in the different countries are listed below.

Doel 3 and Tihange 2

These assessments are PSA Level 1+ (including containment response analysis).

TVO-SEPRA

The study is basically a PSA Level 1 study. However, besides the nuclear risk to the public, TVO was interested in other risks. Six plant damage states were defined: Mechanical fuel damage, local criticality, overheating of concrete constructions (boiling of pool water), core uncover and severe core damage.

Borssele

For Borssele, the Level 2 PSA study for shutdown conditions is in progress.

Vattenfall - barrier analyses

The analyses were not PSA studies, and did not only consider core damage. Less severe consequences were also included like: RCPB leakage, local criticality, deviation from Tech Spec, refueling accidents etc.

Vattenfall - Ringhals 2

This study was a PSA Level 1 including some less severe consequences:

- Severe safety consequences
- Significant safety consequences
- No significant safety impact but public opinion impact

NRC studies

The Level 1 study has been completed. The NRC intends to extend them to PSA Level 3.

APPENDIX B: METHODS AND THEIR IMPLEMENTATION

In Section B.1 general methodologies and approaches to the safety assessment of LPS conditions are overviewed and Section B.2 describes the practical applications of these methodologies, especially with respect to event tree and fault tree development.

B.1 General methodology

Doel 3 and Tihange 2

For the current safety reevaluation of the Belgian reactors Doel 3 and Tihange 2, it has been decided to include LPS states within the PSA analysis. The analysis is a Level 1 PSA with additional analysis of the containment response to accident sequences, excluding external hazards, fires and flooding. The PSA method is based on a small event tree - large fault tree approach.

TVO-SEPRA

To identify potentially important risk initiators, background material including international experiences, TVO analyses and procedures as well as plant incident history was reviewed. The procedure also included a thorough review of maintenance tasks using a structured interviewing technique. Special attention was thereby given to issues like potential confusion of different human tasks and difficulties in task coordination. A special questioning technique was developed for the analysis of tests. The three types of initiators described in section A.2 were thus derived essentially on the basis of a qualitative rather than a quantitative analysis.

EPS 900

The general approach in the EPS 900 study corresponds to standard PSA methodology. The study is a full Level 1 PSA not including external events or internal fires and floods. The main list of initiating events is similar to a conventional PSA. The initiators are grouped into families (e.g. a LOCA-family) and in many cases the families are broken down to subfamilies depending on the functional consequences of the accident. In particular, initiating events relevant to different reactor states (e.g. cold shutdown for refueling) generally constitute separate subgroups. One subgroup within the LOCA family includes breaks in the RHR system.

Systems analysis is made using the conventional event and fault tree method including success or failure of recovery actions. A special effort was given to study post-accident situations of long duration (up to one year), especially for primary system breaks. This effort was made to study problems related to the resistance and utilization strategies of equipment.

GRS-BWR 72 study

Within the BWR safety analysis a screening analysis of low-power states was performed to identify significant initiators and to analyze possible event sequences. A different set of initiators was defined for every POS and an event tree analysis was performed for any initiator. A quantification of the event sequences was not carried out. The screening showed that the analysis might be very complex and extensive due to the specific conditions during outage periods.

More detailed and systematic studies are ongoing.

GRS-PWR 1300-study

The German and worldwide operation experience was evaluated with regard to safety relevant occurrences to identify significant initiators.

With the results of this evaluation and additional considerations on a theoretical basis, a set of initiators for different POSs was defined. A quantification of the analyzed event paths is not yet available. External events, fire and flooding were not analyzed.

Further studies are judged to be necessary especially in the area of human factor.

Vattenfall - barrier analyses

The aim of the barrier analyses performed by Vattenfall has been to develop a method for cold shutdown analysis with the purpose to assess the safety margins for a number of undesirable events. The results are qualitative judgments based on the number of barriers and their respective strength. The analysis was done from the perspective of the control room. Undesirable events were identified on the basis of earlier reports, outage plans and by interviewing plant personnel. The selected sequences were then followed throughout the cold shutdown state and many interviews were made with plant personnel.

The barrier analysis used Barrier-Time diagrams showing physical and administrative barriers against undesirable events as a function of time.

Vattenfall - Ringhals 2

The Ringhals 2 PSA analysis performed for Vattenfall by Framatome used traditional event tree - fault tree methods. The quantification was made starting from the full-power PSA.

NRC studies

The NRC program for LPS analysis involves the investigation of two operating reactors, one PWR (Surry) and one BWR (Grand Gulf). The current plan is a two-phased approach with a screening phase (finalized) leading to a more detailed PSA on LPS conditions at both reactors. Phase 2 has started with one specific plant operational state for each reactor, mid-loop operation for the PWR and cold shutdown for the BWR. The initial Phase 2 effort has been a Level 1 analysis. Level 2 and Level 3 analyses are expected to be completed towards the end of 1993.

During low-power and shutdown modes, plant configuration changes. In the NRC studies, different outage types are thus defined and within each outage type different plant operational states (POSs) are defined. The PSA for a POS in an outage type is similar to a traditional PSA, as e.g. in the NUREG-1150 study. It typically includes identification of initiating events, development of fault trees and event trees and quantification.

The plant configuration changes with time also within each POS as the decay heat changes. In the characterization of this development of plant conditions it was necessary to perform supporting thermal hydraulic analysis.

Initiating events were identified by review of existing studies, search in licensee reports, review of published NRC reports and review of operating procedures. For event tree development, NUREG-1150 event trees were used and if necessary modified. Event trees not similar to full-

power event trees were developed in group discussions, involving experts in PWR operations, PSA, human reliability analysis and thermal hydraulics.

The NRC-PWR study used a **time window approach** to take the dynamics of a situation with decreasing decay heat into account. Boundaries of the time windows are set to the times when success criteria changes. A time window is characterized by the probability that the accident initiator occurs within it, success criteria and timing of the accident scenario. Event trees are then developed for each time window which gives well defined scenarios.

B.2 Implementation

TVO-SEPRA

The TVO analysis used a small event tree - large fault tree technique for the three main types of initiators. However, different modeling approaches were required for sequences leading to local criticality. Task interaction matrix, similar to confusion matrix, was used to identify coordination errors. The fault tree modeling started with full-power fault trees but these had to be extensively modified due to e.g. overridden automatic actuations and already operating stand-by systems. Altogether 15 event trees were constructed for the SEPRA project.

Borssele

The Borssele study uses standard event tree and fault tree techniques for systems analysis using the small event tree -large fault tree approach. Special "procedure event trees" will be used to provide a comprehensive description of operator actions. To reduce the number of events, a grouping is made based on similarity of plant response. This is partly made using engineering judgement to evaluate consequences associated with initiators so that they can be grouped, partly by combining events with identical event trees. Thermal hydraulic calculations will be used to update success criteria and event trees. Reactivity accident scenarios will be evaluated using event tree techniques and special attention will be given to accidents caused by deboration and/or cold water injection.

The fault tree models will address hardware faults as well as human interaction, testing and maintenance unavailabilities. System interactions and dependencies will be accounted for by the linked fault tree technique.

Sizewell B

In the Sizewell B assessment a transient analysis is carried out to demonstrate that the Design Basis Faults (DBFs) identified do not exceed plant safety limits. This analysis is made using a **bounding process** which identifies DBFs. The initial conditions are pessimistic by virtue of assuming the most onerous conditions possible during normal operation on the modes from which the fault could occur. Examples of pessimism are:

- Assuming extreme values for parameters normally automatically controlled (thus assuming maximum expected measurement errors)
- Assuming pessimistic thermal-hydraulic conditions

In a similar way, boundary conditions are also pessimistic concerning e.g. values of fuel related parameters, performance of reactor safety systems and performance of safeguards equipment.

The Sizewell assessment also includes a radiological assessment within design basis considering three levels of risk associated with three dose bands that relate the consequences of release to the frequency of occurrence. Bounding Limiting DBFs relevant to this analysis are:

- Leaks into the auxiliary building at shutdown with the main release pathway via the heating, ventilation and airconditioning system from the auxiliary building room containing the leak
- Reactor building LOCAs at shutdown covering uncontrolled leakages from the primary circuit into the reactor building
- Intact circuit faults
- Refueling route faults including refueling operations and storage in the fuel storage pool
- Radwaste building faults.

For the analysis of releases of radioactivity that could lead to high doses, plant damage states (PDSs) are defined and their frequency of occurrence are calculated. All the possible failure sequences leading to similar types of plant damage are ascribed to one PDS. The PDFs are thus the interface between the plant analysis (Level 1 PSA) and the containment analysis (Level 2 PSA). The PDFs for faults at shutdown are concerned with failure of the RHR system. However, it was found that the accident progression has many phenomenological features in common with faults at full-power and the same containment event trees and probabilities as for full-power are used.

The Sizewell B fault analysis treats shutdown faults alongside power faults throughout; there is no separate treatment.

NRC - Surry

In the NRC-PWR study, typically two fault tree models were developed for each system, one applicable to power operations and one to shutdown conditions. For shutdown conditions, system configuration was identified by review of operating procedures, log books and the system training manual. This led to a number of changes of power fault trees:

- Other failure of valves due to different valve positions during shutdown
- Modification of human error events from backup of automatic actuated systems to manual actuation without automatic backup
- Estimation of maintenance unavailabilities for specific POSs, excluding maintenance events prohibited by check lists (for mid-loop operation)

For the event tree development supporting thermal hydraulic calculations were made. In Phase one this was done on "back of the envelop". For Phase two more detailed calculations are made to determine the timing of feed and bleed operation, the amount of water needed to sustain feed and bleed and the timing of core uncover for different initial conditions.

NRC - Grand Gulf

For the NRC-BWR study, cold shutdown was selected for detailed analysis from the Phase one coarse screening analysis. The analysis included 81 potentially important initial plant configurations with combinations of e.g. state of recirculation, shutdown cooling, main steam isolation valves (MSIV), suppression pool inventory and containment.

Three types of event trees were developed:

- Functional event trees that apply to any transient (non-LOCA)
- Generic system level event trees developed at the mitigating systems level which forms the basis for each specific transient initiating event
- Specific system level event trees developed to model the mitigating system response to each of the 34 initiating events

In total about 200 unique event trees have been developed within the study of which many are complex. Many have over 20 outcomes while some have over 100 outcomes.

APPENDIX C: HUMAN INTERACTION

Human action is very important in reducing the core damage frequency. However, there are problems in modelling operator responses, since they are not always strictly proceduralized and may not be handled explicitly by Emergency Procedures. Furthermore, many operator responses which may be required in LPS emergency situations involve more than simply manually initiating normally automatic system response, as is often the case in full-power scenarios.

Doel 3 and Tihange 2

These PSA analyses use the ASEP methodology by Swain for pre-accident analysis and the French EPS methodology for post-accident human errors (see below).

TVO-SEBRA

Much effort was given in the TVO assessment to achieve reliable human error data. This effort was based on operating statistics and engineering judgment to arrive at subjective but consistent screening values. This approach was followed both for initiating events and recovery actions. An important element in the process was to produce a verbal description of the performance shaping factors that mostly affect each quantification of human action.

EPS 900

Probabilities for human error initiating accident sequences were evaluated using a generic value estimated from experience feedback corrected by a factor for non-recovery, depending on the situation.

Human intervention in an accident was generally identified during preparation of the event trees by analyzing operating procedures and taking actual incidents and simulator observations into account. Quantification of the diagnostic phase was made using curves giving probability of failure as a function of time available for operator action. The curves were prepared on the basis of simulator tests complemented by engineering judgement, taking especially the work of Swain into account. For the operator action phase, a basic value was used corrected by a "context factor" depending on the circumstances for operator action.

Human error was also introduced into the fault trees, thus contributing to the failure of systems.

Four types of human errors were included:

- Incorrect positioning of an actuator prior to the demand of the system
- Omission to open or close a valve at the time of demand of the system
- Omission to make an action or making a spurious action
- Failure to operate a contact or to remedy the unavailability of 48 V power or one of its trends on the demand of a pump in a given period of time

Borssele

It is foreseen that the human interaction modeling in the fault trees will be quite extensive due to many manual actions to perform non-routine tasks during outages. In general, however, recovery probabilities will not be included in the fault tree models. It is judged that non-recovery events are best analyzed at the event tree level. It is also planned to perform recovery analysis following sequence quantification. It is believed that in this way multiple operator actions can be explicitly modeled.

The approach to modelling operator error will be based on previous PSAs. Values for failure rates will be determined in the same ways as in these studies. However, refined methodologies and insights in other studies will be reviewed for applicability and possible incorporation.

Sizewell

Human reliability is modeled in the fault trees, thereby quantifying the failure of post-fault operator actions. Error probabilities are estimated using the human error assessment and reduction technique (HEART) and the THERP method. In modeling the role of the operator in mitigating faults initiated at shutdown, there is no distinction in method to faults initiated at power.

NRC - Surry

In the NRC-PWR study, pre-accident errors are identified partly by using results from earlier full-power studies and partly in the systems analysis task. For post-accident errors the approach is to first qualitatively define the event scenario, required action, factors affecting operator performance and consequences of action failure. Based on the qualitative evaluation, human error probabilities (HEPs) are derived using an adaption of the success likelihood index methodology (SLIM). To quantify the HEPs a rating is performed to relate the relative influence of performance shaping factors (PSFs) on the likelihood of success. The procedure also includes calibration of the numerical model using well-defined actions obtained from other PSAs thus ensuring that the HEPs are realistic and consistent with available data on human behavior.

NRC - Grand Gulf

The NRC-BWR analysis follows a general methodology based on the Accident Sequence Evaluation Program Human Reliability Analysis (ASEP-HRA) Procedure. The procedure allows relatively straightforward adjustments in HEPs as a function of results from interviews with plant personnel, which was judged to be critical where plant procedures are not all encompassing. The procedure includes interviews with control room operators regarding likely responses to various accident scenarios, outage management personnel and training personnel. The results of interviews could be used as a basis for adjusting HEP values in context of LPS conditions and for ruling out unlikely operator actions. With the procedure followed it is possible to take sequence circumstances and LPS environment into account. The HRA analysis has resulted in a total of approximately 100 different human error probabilities.

APPENDIX D: EXPERIENCES

Only a few low-power and shutdown studies have been completed. One major conclusion is that core damage frequency during shutdown or low-power is not insignificant when compared to full-power values. Another common experience is that human action is very important for plant safety. This appendix describes some major results from already accomplished LPS assessments as well as recommendations and safety improvements that they have initiated.

Doel 3 and Tihange 2

Although final results are not yet available, preliminary results indicate the LPS contributions are not negligible compared to full-power PSA. The human factor gives a significant contribution.

TVO-SEPRA

The annual core damage frequency from refueling outage has been calculated to be an order of magnitude lower than for power operation. The measures taken on the basis of the study results have reduced the risk significantly. Without the measures the contribution of the refueling outage would have been over 50% of the annual core damage frequency.

The dominant risks were decreased in several ways. The preparedness to close the lower personnel lock for access to the containment during main circulation pump overhaul was increased by two special trained guards. Mechanical cotter pins were installed in the main circulation pump axis penetration plugs to prohibit inadvertent lifting. In order to prohibit cold overpressurization of the RPV, the use of AFW piston pumps for reactor filling is no longer recommended. Pool cooling capacity was increased and the inspection routine of control rods was modified in parallel with the study.

EPS 900 and EPS 1300

In the EPS 900 study, the shutdown states contribute with 32 % to the total core damage frequency. This figure may result from the fact that there are generally no automatic systems to counter accident situations and human intervention is necessary. Loss of coolant accidents with no safety injection available dominate the LPS contribution to core damage frequency.

In the French study on the 1300 MW reactors, it has been calculated that core damage frequency originating from shutdown represents 70% of the overall risk for all reactor states. The following dominant causes of the calculated risk during shutdown were identified:

- The high number of initiating events
- The inhibition of automatic protective systems and devices
- Diagnostic difficulties
- High rates of maintenance outage times

The results of the French studies have initiated changes in procedures. It was, however, found that this was not sufficient to reach an acceptable level of safety, e.g. for bore dilution and LOCA sequences. Thus additional automatic safety functions were installed.

Vattenfall - barrier analyses

The barrier analyses do not quantify the core damage frequency. Comparisons with full-power operation is thus not possible. However, the barrier analyses have led to a number of recommendations concerning routines for operating orders and introduction of extra technical barriers during specific activities such as top filling of the reactor vessel before dismantling of the cover lid and maintenance of internal recirculation pumps. Examples of findings in the Ringhals 4 barrier analysis are:

- During mid-loop operation with open steam generators and ongoing mounting of the nozzle dams, the equipment hatch of the containment is allowed to be open. If the residual heat removal system gets lost, the estimated time to boiling in the core is about 15-20 minutes. In a similar way as in the French studies, it was recommended to keep the equipment hatch closed in this mode in order to have the containment barrier intact.
- The mounting of nozzle dams must be performed in the right sequence. The last nozzle dam must be mounted on the hot leg. If the order is reversed combined with loss of RHR, a steam bubble can be formed and press the water out of the core. The safety margins have now been improved by making the administrative barrier when mounting the last nozzle dam more strict.

Vattenfall - Ringhals 2

The results from the PSA analysis show relatively high values for severe or significant safety consequences (of the order of 10^{-3} per year) with the main contribution from loss of RHR during mid-loop operation followed by failure of operator action before core uncovering. Other significant contributors to the calculated frequencies are small LOCAs during cold shutdown and spurious SI in hot standby mode. The relatively high frequencies are due to dominant contributions from human error and from the estimated risk of reactor vessel rupture when cold pressurized. The values are deemed to be very conservative and it is judged that better procedures and new calculations for the risk of reactor vessel rupture will lower them considerably.

NRC - Surry

This study found that the predicted core damage frequency during mid-loop operation is comparable to that of full-power operation. The dominant cause of core damage was found to be operator failure to mitigate the accident. However, it is recognized that there are large uncertainties in the human error probabilities.

Very few procedures are currently available for accidents during shutdown. In many cases, the information in the procedures for power operation is helpful, if used for shutdown accidents. However, some procedures written with power operation in mind, can potentially mis-guide the operator if followed during shutdown. For example, the procedure for loss of offsite power states that "When the diesel generators is the only source of power to an emergency bus, the Component Cooling Pump should NOT be in service". During shutdown, component cooling water flow to the RHR heat exchanger is necessary for decay heat removal. To strictly follow this procedure can have an adverse effect on the operator response.

NRC - Grand Gulf

A detailed analysis of potential accidents that could occur in cold shutdown during refueling outages has been carried out. The quantification process has recently been completed and some

generic insights can be concluded. Core damage frequency is not insignificant compared to full-power operation and human action is an important factor.

Seabrook

A Level 3 PSA for the Seabrook station has evaluated the likelihood of severe core damage resulting from events in hot shutdown, cold shutdown and refueling modes. This analysis concluded that the frequency of core damage during shutdown is small, but not negligible in comparison with full-power operation provided relatively low cost modifications and administrative controls. These include instrumentation and alarms to improve operator action at loss of RHR, improved procedures and training.

EPRI studies

EPRI has evaluated events involving loss or significant degradation of the RHR system at both BWR and PWR plants. Major safety implications of these events fall into three categories:

- 1) Loss of reactor coolant inventory via the RHR system
- 2) Inadvertent cold over-pressurization of the RCS
- 3) Loss of long-term decay removal capability via the RHR system.

Follow-on EPRI sponsored PSA studies on one PWR (Zion) and one BWR (Brunswick/Unit 1) have indicated that the core damage frequency due to failure of the RHR system is non-negligible and that risk is highly dependent on human error.

APPENDIX E: ABBREVIATIONS

BWR Boiling water reactor

CDF Core damage frequency

EOP Emergency operating procedure

HACS Human action classification scheme

HEP Human error probability

HRA Human reliability analysis

Methods referred to are:

ASEP : Accident Sequence Evaluation Program

SLIM : Success likelihood index methodology

THERP: Technique for human error rate prediction

HEART: Human error assessment and reduction technique

LOCA Loss of coolant accident

LPS Low-power and shutdown

POS Plant operating state

POT Plant operating type

PSA Probabilistic safety analysis

PSF Performance shaping factor

PWR Pressurized water reactor

RHR Residual heat removal

