IAEA-TECDOC-1042

Safety analysis of nuclear power plants during low power and shutdown conditions

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

The originating Section of this publication in the IAEA was:

Safety Assessment Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

SAFETY ANALYSIS OF NUCLEAR POWER PLANTS
DURING LOW POWER AND SHUTDOWN CONDITIONS
IAEA, VIENNA, 1998
IAEA-TECDOC-1042
ISSN 1011-4289

Printed by the IAEA in Austria
September 1998

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

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

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

FOREWORD

The Technical Committee Meeting on Safety Analysis of Nuclear Power Plants during Low Power and Shutdown Conditions, held in Vienna, Austria, 1–5 December 1997, was organized by the IAEA within the framework of the Technical Co-operation Project RER/9/046.

The 23 participants, representing 14 Member States, reviewed recent developments and discussed directions for future efforts in the area of safety analysis of nuclear power plants during low power and shutdown (LPS) conditions. During the meeting, 18 technical papers were presented, devoted to various aspects of LPS conditions: probabilistic safety assessment studies, description of particular phenomena, calculational analysis of individual events, contents of safety reports, hardware modifications, experience from plant operations, etc.

A number of events at nuclear power plants, as well as results from probabilistic safety assessment (PSA) studies for NPPs, have indicated that events occurring during shutdown modes may contribute significantly to the overall risk associated with NPP operation.

It is recognized that a great deal of work over the past years in the worldwide nuclear power community has focused upon reducing the risk associated with LPS operations by analysing specific phenomena occurring during LPS conditions, improving analysis methodology, implementing additional administrative measures and hardware modifications, and starting incorporation of the LPS conditions to the safety analysis report.

The IAEA expresses its sincere thanks and appreciation to the experts who contributed to this publication. The officer of the IAEA responsible for the TECDOC was C. Lin of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

A number of events at nuclear power plants (NPP), as well as results from probabilistic safety assessment (PSA) studies for NPPs, have indicated that events occurring during shutdown modes may contribute significantly to the overall risk associated with NPP operation.

In spite of the importance of the issue, safety rules and guidelines applicable in most countries do not contain detailed requirements concerning the safety analyses specific for shutdown conditions. Only recently systematic analyses of the accidents during shutdown conditions have been undertaken. The current operating procedures used to cope with shutdown accidents do not provide sufficient details, and are not supported by sufficient analytical results. Since many significant activities are ongoing in all areas related to low power and shutdown (LPS) conditions, exchange of experience among Member States is considered very useful and beneficial.

The IAEA convened a Consultants Meeting on Accidents During Shutdown Conditions for WWER NPPs in November 1995, and a second meeting in October 1996 to develop Procedures for Analysis of Accidents in Shutdown Modes for WWER NPPs (IAEA-EBP-WWER-09). The above two meetings emphasized a deterministic approach. Two other meetings had previously been organized by the IAEA to deal with probabilistic approaches to shutdown safety analysis for all types of reactors. One was a consultants meeting to develop guidelines for shutdown risk assessment in May 1993 and the other was a Technical Committee Meeting on Procedures for Probabilistic Safety Assessment for Shutdown and Low Power Operating Modes in November 1994 in the Netherlands.

1.2. VULNERABILITY OF NPPs AT LOW POWER AND SHUTDOWN CONDITIONS

Events occurring during shutdown operational modes represent a significant contribution to the NPP risk due to the fact that both preventive and mitigative capabilities of the plant can be degraded, e.g. by:

- Failure of automatic startup of some safety systems;
- Equipment in maintenance or in repair;
- Reduced amount of coolant in primary as well as secondary circuit for some modes;
- Instrumentation and measurements switched off or non-functionable;
- Open primary circuit;
- Open containment, etc.

Extensive maintenance work together with a large number of people present due to refueling, preventive and corrective maintenance, modifications, surveillance testing and in-service inspections can increase considerably the likelihood of an inadvertent event. Due to an inherent belief that the unit is in a 'safe shutdown mode' the operating personnel may be unaware of the potential for higher risk during various shutdown conditions.

The number of events occurring during LPS conditions is considerably higher than might be expected compared to the number of events occurring during power operational modes. In many cases higher probability of an LPS event is partially compensated for by the slowly developing nature of the event (i.e., long time to core damage), possibly giving the operators a longer time to respond to the event. In some instances, the operators may even be able to use external equipment not available at the plant to mitigate the accident. However, to properly account for all the various plant conditions and operator actions, an LPS PSA should be performed.

1.3. OBJECTIVE AND SCOPE OF THE MEETING

The main objectives of the meeting were to exchange information on the studies performed and countermeasures taken for coping with accidents during low power and shutdown conditions, and to define the necessity and directions of further activities which may promote safety improvements for NPPs. Participants from east European Member States were requested to present their activities and results on this topic and to participate in the discussions. Experts from selected western countries were requested to summarize the most important results achieved in LPS work in their countries.

The scope of the meeting included:

- Summary of activities in evaluation of LPS conditions (completed, ongoing, or planned);
- Safety analyses of LPS conditions (results, methodology, including deterministic and/or probabilistic, typical examples of analysis, etc.);
- Lessons learned and measures taken for coping with accidents at LPS conditions;
- Status of technical specifications and emergency operating procedures for LPS conditions.

A broad spectrum of approaches and results for various types of reactors operated in the European region (WWER, RBMK, CANDU, Westinghouse PWR, BWR) were covered in the presentations.

1.4. PARTICIPATION AND COURSE OF THE MEETING

Eighteen participants (regulators, operators, engineering institutions) from ten Member States operating NPPs in the eastern European region — namely Armenia, Bulgaria, the Czech Republic, Hungary, Lithuania, Romania, the Russian Federation, Slovakia, Slovenia and Ukraine — and five experts from the USA, Finland, France and Germany attended the meeting. Thus, a total of 14 countries were represented.

Altogether, 18 technical papers were presented, covering various aspects of LPS conditions: PSA studies, description of particular phenomena, calculational analysis of individual events, contents of safety reports, hardware modifications, plant operational experience, etc. Copies of all papers presented at the meeting are available upon request from the Division of Nuclear Installation Safety. In addition to the presentation and discussion of the technical papers, the participants prepared this technical report, which includes information in addition to their presentations. Section 2 of the report summarizes the analysis and measures taken in countries represented at the meeting to reduce risk during LPS conditions. Section 3 explains and discusses selected physical phenomena which are important to LPS conditions: cavitation and depriming vortex during mid-loop operation of NPP, degradation of natural circulation, boron dilution and pressurized thermal shock. In Section 4, selected safety issues relevant to LPS conditions are discussed from the point of view of their significance, their causes, and actions planned or taken to resolve the issues. The experts' opinions were prepared by working groups and were later accepted at the plenary meeting. Conclusions and suggestions, as formulated by the experts present at the meeting, are included in Section 5.

2. SUMMARY OF SITUATION IN MEMBER COUNTRIES

The summary of activities related to safety analysis of shutdown and low power operating modes for countries participating in the meeting is presented in the following sections.

2.1. ARMENIA

At the Armenian plant, under the low power and shutdown conditions, organizational and technical measures have been implemented to meet the following objectives:

- Avoid reduction of boric acid concentration in the reactor coolant system (RCS), makeup and safety injection systems, and systems of organized leakages;
- Ensure essential power supply to safety related equipment;
- Ensure reliable service water supply;
- Ensure natural or forced circulation of the RCS coolant;
- Ensure heat removal from secondary system;
- Avoid formation of air-gas bubbles in different RCS parts;
- Avoid contaminating open RCS components with foreign material;
- Avoid overexposure of personnel;
- Avoid human errors in the course of activating and shutting down equipment;
- Avoid cold overpressure of reactor vessel.

Events which have occurred at the Armenian plant and at other plants worldwide are taken into account in reviewing systems and operations, developing hardware modification, and refining emergency operating procedures. Technical requirements for plant systems and equipment are defined in "Process operational procedures for the Armenian Unit 2". Since there is no technical support organization in Armenia, the engineering support for the Armenian plant is provided by foreign organizations, mainly by VNIIAES, Gidropress and the Kurchatov Institute. The Armenian plant is operated according to Russian standards. However, these standards do not specify requirements for safety analyses during low power and shutdown conditions. This is the reason why such safety analysis have not yet been done. The Armenian plant plans to upgrade these standards to the level corresponding to international practice.

2.2. BULGARIA

Bulgaria has performed Level 1 PSAs for all units of Kozloduy NPP during full power operation.

In the framework of the reconstruction programmes for Units 5 and 6 with WWER-1000 type reactors and for Units 1 to 4 with WWER-440 type reactors, Kozloduy NPP included the task of performing Level 1 PSA analyses for these units during shutdown conditions.

Based on the incident reports for all units, Kozloduy NPP has completed the identification of initiating events which occurred during shutdown conditions for inclusion in the PSA studies. These initiating events are classified into five groups according to the IAEA recommendations. The most important events are:

- Non-condensable gas injection into RCS;
- Loss of power supply;

- Inadvertent blockage of flow through primary circulation loop;
- Loss of cooling of the spent fuel pool.

To date, for Units 1 to 4, Kozloduy NPP has performed thermohydraulic analysis for the following accidents:

- Main steam line rupture inside containment at zero power;
- Main steam collector rupture at zero power;
- Inadvertent startup of high pressure injection pumps (HPIP) during cold shutdown state;
- Boron dilution at hot zero power;
- Interruption of natural circulation;
- Loss of coolant accidents (LOCAs) as initiators of pressurized thermal shock (PTS).

Thermohydraulic analysis of the effects of interruption of forced circulation was also performed for Units 5 and 6.

In the previous stage of the reconstruction programme for Units 1 to 4, several technical measures to improve nuclear safety during low power and shutdown conditions were implemented; for example, installation of a cold overpressurization device in all units, development of a feed and bleed procedure, and installation of complementary emergency feedwater system located outside the turbine hall were completed.

To improve natural circulation monitoring at Units 1 to 4 the following additional devices were installed:

- A new device for temperature measurement at the hot and cold legs (each loop);
- A new water level measurement device in the reactor vessel;
- Additional venting lines for the reactor vessel and steam generator (SG) collectors,
- Additional signals and alarms to detect fuel assembly outlet temperature above 70°C during cold shutdown condition;
- Boronmeters in the pressurizer surge line, makeup pumps and cleanup systems;
- An automatic signal to start up makeup pumps was removed to prevent boron dilution in case of loss of off-site power. Also, a new operational procedure for the interruption of natural circulation was implemented.

In the implementation of the reconstruction programme for Units 1 to 4, technical and administrative measures are included to improve nuclear safety during shutdown conditions.

2.3. CZECH REPUBLIC

Operational procedures

The plant "Technical Specifications" is an important document for NPP operation. Seven operational modes are defined in this document.

The basic operational procedure "Procedure for the Unit T1" is valid for all the operational modes including shutdown.

Loss of natural circulation is one of the events covered by the procedure P4 "Fault Conditions to Cope with Emergency and Abnormal Incidents Elimination".

Analysis completed

The Operational Safety Report which covers ten years of operation, contains only a limited number of events which could occur during low power and shutdown conditions. The following events are included:

(1) Reactivity accidents
- Uncontrolled withdrawal of group of control rods at zero power and at power level of 2%;
- Control rod ejection at zero power.

(2) Rupture of the main steam header at minimum controllable power level.

(3) Faults during fuel handling
- Drop of fuel assembly during refuelling;
- Drop of container with spent fuel.

(4) Fuel storage pool accidents
- Loss of cooling of the fuel storage pool;
- Loss of coolant from the fuel storage pool.

In 1995, a meeting of an expert group from the Moscow Centre of WANO was held at Dukovany NPP on problems concerning the loss of natural circulation for WWER-440 reactors. The events concerning the loss of the natural circulation were discussed and reviewed in detail, the causes were analysed and the remedies were proposed to prevent the reoccurrence of similar events.

Activities under way

The most extensive current project is the PSA-1 for low power and shutdown conditions (SPSA). This project, being performed by the Nuclear Research Institute (NRI) Řež commenced in 1996 and will be finished in 1998. Ten plant operational states (POS) are considered in this study. The analyses of external events such as fires and floods are included, and consideration of sources of radioactivity other than the core are also part of this project.

At present, the PHARE project 2.09/95 “Low power and shutdown PSA” is under way; the Bohunice NPP (V2) is the main beneficiary and the Dukovany NPP is the co-beneficiary. It is intended that the results of this project will be used to check and verify SPSA project.

In order to support the SPSA project, several thermohydraulic analyses are being performed by NRI Řež.

- Loss of natural circulation (several cases);
- LOCA during the primary circuit pressure test;
- Primary circuit boron dilution.

Another important project is the pressurized thermal shocks (PTS). Different cases of involving a break of main steam header (MSH) and steamlines, both at nominal power and at zero power were analysed.

Planned activities

The activities currently under way will continue for the next few years. The "Shutdown PSA" project will be completed next year. Other initiating events will be analysed under the PTS project.

The PHARE project 2.08/95 "Prevention of inadvertent primary circuit boron dilution" will start. The Paks NPP will be the main beneficiary, the Dukovany NPP as well as Bohunice NPP will also benefit from this work..

In addition, the exchange of operational event information will continue. This exchange of information is carried out for WWER-440 NPPs operators and also within the framework of WANO NPPs operators.

2.4. FINLAND

The major LPS PSA study for the Olkiluoto BWRs (SEPRA) was completed in December 1992. Since that time, improvements have added to SEPRA, including fuel ex-core analysis. Use of the specific analytical techniques "Analysis of Test Influence" (ATI) and "Human Action Deviation Analysis" (HADA) made an important contributions to the completeness of the LPS PSA. A Level 2 study was initiated in 1994 and a more comprehensive fire and loss of off-site power analysis during shutdown conditions was started in 1995/96.

In addition to determining the core damage frequency (CDF), the SEPRA study determined the probabilities for eight other hazards during refuelling from criticality to mechanical damage of fuel. These issues have often not been considered important from the safety perspective, but are very important from utility's point of view, since they can cause significant financial losses. The SEPRA study is a pioneering effort in this area.

The results of the SEPRA study have been used for implementing several improvements and for initiating some actions. The low equipment hatch of the containment must now be closed for a certain time period during the main circulation pump overhaul. In addition, procedures and technical specifications have been modified. Altogether, various modifications have resulted in a decrease in CDF by a factor of 10.

Another Finnish NPP, Loviisa 1-2 (two WWER-440 units), is developing its regulatory-mandatory LPS PSA project. The project was initiated in 1994. Some enhancements of safety during shutdown have been initiated, but these were made on the basis of operational experience, rather than on the results of the LPS PSA. During the course of hazards identification, it was determined that several immediate changes of the operating procedures were possible (primary loop level control procedures, several test procedures, etc.). The preliminary findings of the Loviisa LPS PSA have resulted in improvements in operational and test procedures, and/or in technical specifications.

Safety analysis of shutdown states for the Loviisa reactors has been started with analysis of leaks and transient cases during hot and cold shutdown modes. Earlier safety related studies analysed boron dilution events and pressurized thermal shock at low power conditions.

2.5. FRANCE

The initial design of French NPPs takes into account that a certain number of accidents can possibly occur during shutdown conditions (LOCA with RHRS connected, homogeneous boron dilution accident, etc.). Only a few years after commissioning the first unit of the industrial series of NPPs in France (TRICASTIN 1), the first H1-2 (total loss of the heat sink) and H3-2 (Blackout) procedures specific to RHRS-connected states (post-TMI actions) appeared. The first incidental procedure I-RRA2 (Malfunction of RHRS), which results in the introduction of the standby RHRS was implemented at the same time. The first technical specifications related to cold shutdown modes were subsequently implemented since 1988.

From the beginning of the 1990s, the following facts led Electricité de France (EdF) to become interested in the specific risks during mid-loop cold shutdown operation:

- French and international operational feedback (Generic Letter dated 17 October 1988 from the USNRC);
- probabilistic evaluations which show that one initiator is preponderant for the overall risk of core meltdown: the total loss of RHR through pump suction common mode vortex (short term risk).

EdF's approach to the overall study of risks in shutdown conditions has consequently been as follows:

- Step 1: obtain a short term core meltdown risk level during mid-loop cold shutdown operation which is comparable to the one existing with a water level up to the "vessel mating surface mate";
- Step 2: check that the overall risk of core meltdown, taking into account all the initiators and the long term sequences, is acceptable (relooping).

In fact, the first step has been subdivided in two phases:

- Step 1a (from 1990 to 1994): implement additional requirements and limiting conditions for the technical specifications; this provisional step was necessary to give EdF time to perform design studies, in step 1b;
- Step 1b (from 1994): complete design studies and hardware improvements.

Additional technical specifications requirements (step 1a)

The aims of the additional technical specifications requirements were:

- To protect against the potential risks of total loss of the heat removal function by guaranteeing the operability of effective and redundant makeup and monitoring means;
- To optimize the chances of success of procedures, which limit risks of prolonged uncovering of the core;
- To guarantee containment leaktightness, before core uncovery starts.

To achieve these aims:

- A safety criterion has been defined which has enabled an operating condition to be evaluated as acceptable. This criterion is the "operator has enough time" (≃1 hour) to

safely perform a diagnosis and implement the corrective actions before the core begins to uncover;
- The boundary between normal cold shutdown and maintenance cold shutdown (MCS) has been clarified and two submodes in the maintenance cold shutdown ("slightly open" MCS and "sufficiently open" MCS) have been identified.

Hardware improvements (step 1b)

The aims of the improvements are:

- For prevention, improve the primary circuit information and particularly ultrasonic level measurement (with associated alarm and automatic actions). This increases operator information and control.

- For alarm/incident, improve the RHR vortex detection. This system detects the beginning of an incident.

- For ultimate/safeguard, improve the automatic makeup of the reactor coolant. This allows the return to a safe configuration without operator intervention.

In parallel to these hardware improvements, normal, incidental and accidental procedures have been reviewed as a result of the following:

- New studies and tests results (particularly BETHSY loop tests);
- New operational practices;
- Feedback from BUGEY 5 incident of 29 January 1995:
  - No voluntary stop of the pump during a vortex (except normal criteria bound to operation of the pump itself);
  - No voluntary reduction of the RHRS flowrate as an immediate action in case of a vortex.

Re-evaluation of the overall risks during shutdown modes (step 2)

In this phase, hardware improvements (automatic makeup) have been implemented for initiators other than vortex (particularly LOCAs in shutdown conditions with primary circuit open). No major safety problem has been brought to light by EdF during this second step.

Generally speaking, all these improvements lead to a significant reduction in the overall risk of core meltdown in cold shutdown conditions, and to uniform accident sequences and relatively moderate impact on long term accident phases. Specifically, the design of automatic makeup adequately reduces shutdown mode risks (aim of risk reduction linked to short term sequences achieved), and other preventive hardware improvements have proved to be adequate. However, discussions are currently taking place with the French safety authorities to definitively conclude this issue.

2.6. GERMANY

Guidelines for the probabilistic safety analysis have been issued recently. In the guidelines, the analysis of initiating events in other operational states than full power is recommended if essential contributions to the total core damage frequency are to be expected. Efforts have therefore concentrated on limited shutdown analysis for a typical PWR and BWR. A low power and shutdown analysis for one PWR has been completed, one for a BWR will be finished soon and a third, major PWR analysis has just been started.

After safety-significant findings, particularly in the LPS PSAs in France, investigations in Germany started to analyse the transferability of the results of these studies. The 1300 MWe nuclear power plant Biblis, Unit B, which was the reference plant for the German PWR risk study, was also the reference plant for these LPS investigations. An evaluation of possible initiating events (IEs) and an analysis of some events, which were found to be significant in other PSAs, was performed. This included an estimation of the frequencies of selected damage states. The investigations were finished in 1996. Some minor improvements in procedures and hardware were implemented, but no sequences were found with significant contributions to core damage frequency.

For BWRs, LPS events have also been analysed within the BWR Safety Analysis, Phase 2. The reference plant is Gundremmingen, Unit B, a 1350 MW(e) KWU 72-type plant. The main task of this study is the improvement of the methodology and a representative application for relevant initiating events (IEs). This study will be finished in March 1998. The results of these studies are limited to some extent because the full spectrum of IEs has not been analysed. Preliminary results show no significance of sequences with cold overpressurization because of the procedures and measures to prevent such a sequence. The *loss of RHR during cold shutdown* is a main sequence where the residual heat cannot be removed from the containment, but because of independence of injection and RHR in this particular situation, core cooling is not endangered. Consideration of actual availability of safety systems in the plant leads to a much lower frequency of the sequence. Core damage frequency due to loss of injection is very low also. The results for leaks above and below the core are still under discussion. An important advantage of the study is the quantification of the assessment of operator actions. For rule-based action ASEP-NOMINAL has been used; nevertheless, further development is needed to assess decision making processes.

A full scope LPS PSA has recently started for a modern KONVOI-type 1300 MW(e) PWR. The reference plant is Neckarwestheim, Unit 2 (GKN-2). The purpose of the study is a systematic analysis of internal events in relevant operational states with probabilistic methods. Within the spectrum of IEs, special emphasis is placed on IEs with boron dilution. It has become apparent from the first study that for such IEs additional analyses with advanced tools are needed. The general steps in all studies correspond to the respective IAEA guidelines.

In all studies, a normal refuelling outage has been examined. Shutdowns for maintenance or other purposes have not been considered so far.

2.7. HUNGARY

The research activities on SPSA of Paks NPP (WWER-440/213) were started at VEIKI Institute for Electric Power Research Co. in 1994. So far, accident sequences modelled in SPSA have been quantified. The quantified risk measures related to core damage and boiling of primary coolant are currently being reviewed internally. In general, findings from the SPSA study show that risks from the off-power operational states are comparable to that of full power operation. For the off-power operational states, the open reactor states are the primary contributors to core damage probability. According to the previous full power PSA results, the preliminary quantifications are point estimates for the Unit 2 with its condition after the outage of 1995 as a reference state. Results are available, which include the safety upgrading measures performed from that time till the present.

Based on the current SPSA results and preliminary findings, several upgrading measures and improvements at the plant during outage have been formulated.

Several thermohydraulic calculations and other analyses were carried out to determine success criteria for the event tree modelling, support the event sequence development and assist the initiating event analysis. These analyses were performed by the Paks NPP and by the KFKI Atomic Energy Research Institute supporting the SPSA activity. The thermohydraulic calculations were performed for several LOCA scenarios during cooldown and during natural circulation.

Four specific cases were analysed during the outage period as follows:

- Loss of natural circulation;
- Heavy load drop;
- Pressurized thermal shock;
- Boron dilution.

The effects of these cases were considered as initiating events, contributors to initiating events, or as post-initiator human actions in accident sequences, which were to be modelled in event tree level as a header using the appropriate probability value for the required post-accident human action.

2.8. LITHUANIA

The Ignalina nuclear power plant (INPP) is the only nuclear power plant in Lithuania. The power station consists of two units commissioned in December 1983 and August 1987. A significant programme of safety improvements was established by the plant immediately after commissioning. The process of safety enhancement is on-going and a safety analysis report (SAR) has been prepared by the plant with the aid of western engineering organisations and reactor chief designer RDIPE. The review of the SAR has been carried out by a team of eastern and western technical support organisations. Analysis of reactivity initiated accidents (RIAs) at low power has been carried out as a part of accident analysis. The expert team has recommended that a safety analysis of INPP be performed for the shutdown state. Currently, the safety improvements programme (SIP) is being implemented at the plant. The safety analysis of the shutdown mode needs to be completed for the RBMK reactor in the framework of SIP.

2.9. ROMANIA

The CERNAVODA NPP Unit 1 is a CANDU 600 reactor which uses heavy water as moderator and coolant. The fuel is natural uranium supplied in the form of bundles loaded into, and removed from, the reactor during "on-power" operation.

At CERNAVODA NPP Unit 1, the reactor operation at low power and shutdown conditions is specified by the following documents:

- Operating Policies and Principles (OP&P);
- Operating manuals (OM);
- Abnormal Plant Operating Procedures (APOP);
- Shutdown Heat Sink Technical Manual;
- Safety analyses.

The OP&P manual establishes the safety envelope within which the plant is to be maintained and operated under both normal and abnormal conditions. This manual defines the shutdown states and licensing limits, and specifies the heat sinks and their limits.

The operating manuals describe the operating rules and limits and also address low power and shutdown conditions. The heat sink operating manual at outage provides the overall outage heat sink co-ordination function. The objectives of this manual are to ensure that suitable primary and alternate heat sinks are defined for outage, that the support equipment for each sink is known and available, that parameters are defined such that the effectiveness of the primary heat sink and the availability of the alternate heat sink can be monitored, and that the circumstances for initiating a transfer from primary to alternate heat sink are known.

The Abnormal Plant Operating Procedures used at CERNAVODA NPP are event specific APOPs and Generic APOP Heat Sink. The specific APOPs address the events which affect several systems. If the cause of the event is not recognized or the cause is incorrectly recognised, or combinations of failures or actions have occurred, this indicates that the OMs or event specific APOPs do not include such a case, the shift supervisor requires support and the Generic APOP Heat Sink is used. The Shutdown Heat Sink Technical Manual establishes the heat sinks and the conditions that must be satisfied by the heat sinks. For each postulated accident, a safety design matrix is elaborated. The Final Safety Analyses Report presents the accidents that can occur at low power or during shutdown conditions and how these events are included in the safety analyses. The Romanian CANDU 600 reactor with its on-line refuelling and separated coolant and moderator circuits does not appear to have significant safety problems in shutdown operating modes.

2.10. RUSSIAN FEDERATION

Traditionally, a PSA for NPPs with WWER and RBMK reactors is only performed for full power operation.

Operational events occurring during shutdown operational modes represent a significant contribution to the NPP risk. For this reason, there is a need to perform a PSA study for shutdown conditions.

Russia has a certified computer code "Rainbow" which can be applied to analyses of some transient and accident development processes for shutdown modes of WWER. In the future, the "Rainbow" code may be evaluated by applying it to the WWER shutdown modes. There is also a need for a similar work in evaluating computer codes for analysing RBMK shutdown modes.

2.11. SLOVAKIA

The improvements for LPS operation are divided into the following categories:

(1) Administrative, including limits and conditions;
(2) Operational, including outage management;
(3) Hardware, including features of WWER reactors;
(4) Analytical, including PSAs for shutdown and low power conditions.

Administrative improvements

The limits and conditions address the shutdown operation. Seven types of operating modes are defined. They are determined by the primary circuit parameters. For each of these modes the availability of the safety and safety related systems is given by the limits and conditions. Special checklists for mode transition (down and up) were developed and are used.

Surveillance procedures are widely used for testing of all systems with acceptance criteria for each particular operating mode of the plant. All non-standard operations must be performed according to written and approved procedures.

Operational improvements

The basic operational and emergency procedures are valid for individual operational modes of the plant. One part is dedicated to shutdown conditions. In addition, special procedures for safety during shutdown were developed including measures to prevent intake of pure condensate (unborated water) into the primary circuit, conditions for open primary circuit work, work authorization and safety permits. Bohunice NPP introduced shutdown safety as a topic for special pre-outage training of the staff. The training is conducted for shift workers, daily staff and maintenance staff, including contractors, before the outage.

An important part of safety during shutdown is outage management. Various working groups are established for the control of outage activities. Working groups are headed and supervised by specialists from the Operation Division. The outage co-ordination group co-ordinates all activities daily with a focus on safety during the shutdown and safety system availability. The co-ordination group is headed by a licensed specialist with shift supervisor experience. The management and operator supervision is performed according to QA procedures. From a supervision point of view, it is important that chief of the unit (shift supervisor licensed) has his work site in the reactor hall during the outages.

Hardware improvements

Several modifications were implemented to enhance unit safety in Bohunice NPP as follows:

- Interlocks to prevent pure condensate intake into the reactor;
- Cold overpressure protection;

- Reactor level measurement;
- Dump station on each steam line from SG for two phase flow (feed and bleed);
- Hydro-power plant improved and dedicated to Bohunice electricity supply in the case of blackout;
- Special cables and electricity supply prepared for dedicated shutdown equipment;
- Mobile diesel generator for boric acid injection into primary circuit, etc.

It is planned to continue with additional modifications for Bohunice and Mochovce NPPs in Slovakia.

Analytical improvements

Analytical improvements represent activities performed mainly for the safety analysis reports (SAR), including conservative deterministic analyses and probabilistic best estimate analyses (LPS PSA).

The deterministic approach is mainly used to prove the acceptable level of safety. This approach is represented by the part of the safety analysis report (SAR) dealing with LPS during the plant operation. The probabilistic method is used to demonstrate the overall safety reached during LPS operation and to identify possible plant weaknesses during these operational modes.

Probabilistic analyses

The LPS PSAs are being conducted for Bohunice V-2 NPP and Mochovce NPP. The main goals of both LPS PSAs are as follows:

(1) Evaluate quantitatively the probability of core melt on the basis of selected initiating events and operational experience of plants with similar reactor types;
(2) Identify dominant accident sequences with the dominant contribution to the core melt frequency to identify weak points of the plant design;
(3) Perform sensitivity and uncertainty analysis for different system contributions to the total core melt frequency;
(4) Make recommendations regarding safety improvements for plant operation during all operational modes;
(5) Develop PSA models covering both full power and shutdown modes which can be used/modified in the future for:
    - Maintaining a living PSA;
    - Performing real time risk monitoring;
    - Optimizing technical specifications;
    - Performing a Level 2 PSA;
    - Developing a strategy for optimizing maintenance and tests.

The Level 1 LPS PSA of Mochovce Unit 1 includes as internal events LOCAs, transients and internal hazards, i.e. fires and floods. External events included seismic events, air craft crashes, influences of external industrial facilities, and extreme meteorological conditions. Operational experience and results obtained from PSA for Bohunice V-2 NPP and Dukovany NPP as Mochovce NPP are used as much as possible.

In comparison with Mochovce LPS PSA, Bohunice V-2 LPS PSA has a smaller work scope. It does not consider external hazards. Bohunice V-2 NPP has nearly ten years of operation and therefore plant specific operational experience is used in its LPS PSA. However, it is only used as generic source of information for Mochovce LPS PSA.

It is expected that Bohunice V-2 LPS PSA will be completed by mid-1998 and the Mochovce LPS PSA by the end of 1999.

Within the safety improvement programme of Mochovce NPP (under construction), several safety improvements were analysed in more detail and corresponding measures were taken as follows:

- Boron dilution prevention during reactor startup, including hardware and procedure improvements;
- Pressurized thermal shock analysis for the reactor vessel;
- Secondary and primary feed and bleed procedure analysis, including hardware improvements;
- SG thermal shock analysis of EFWS cold water injection into SG;
- Best estimate thermohydraulic analysis of selected initiating events during low power and shutdown conditions.

Deterministic analyses

The deterministic analyses for LPS conditions included in the SAR are:

- RIA at low and zero power (control rod ejection or withdrawal, connection of a cold loop to reactor);
- LOCAs of different size and different system availability conditions;
- Pressurization of primary circuit at low power and temperature, due to ECCS or pressurizer heaters malfunction;
- Steam line break at low primary temperature.

The codes used in SAR analyses were also applied to low power and shutdown analyses (RELAP5, TRAC, CATHARE, DYN3D, MELCOR, MAAP, ADINA, DYNA, etc.).

At present a project is being carried out to summarize all needs for deterministic analyses in shutdown modes, to evaluate the applicability of existing models and methods to the specified conditions, and to create a basis for systematic evaluation of Bohunice NPP safety in shutdown modes. As a result, an upgraded SAR will be provided, reflecting also results of relevant LPS PSA-PHARE 2.09/95, Boron dilution-PHARE2.08, etc.

2.12. SLOVENIA

The Slovenian Nuclear Safety Administration requires a plant specific probabilistic evaluation of the Krško NPP. The requirement is to address all modes of operation. For evaluation in low power and shutdown conditions, an ORAM approach was used.

As requested by the Administration, the study was reviewed by an independent technical support organization. The review found that the study is, in general, a fair representation of risk level of Krško NPP during an outage.

Based on the results obtained in the study, Krško NPP developed the shutdown safety plan (SSP) to provide guidance for the implementation of all outage safety management actions. Some of the recommendations from the study have been already implemented (e.g., availability of both diesel generators when plant is in reduced inventory configuration).

Fires (or other external events) have not been included in the scope of the study although the IPE PSA Level 1 showed an important contribution of fire to the CDF. The screening of the effects of the external events on the Krško PSA will be performed in the near future. One of the expected benefits of the study performed is a reduction in the duration of outage without compromising safety. This will be important in the forthcoming steam generator replacement.

2.13. UKRAINE

At present, the Safety Assessment Programme is under way in the Ukraine. The objective of the programme is to develop new SARs for units which are in operation. These SARs should be developed according to current Ukrainian Regulations recently approved by the Regulatory body, and they should provide the basis for licensing of NPPs. Primary attention is focused on developing DBA, BDBA and PSA chapters of the SAR taking into account evaluation of shutdown and refuelling modes that have not been addressed or sufficiently investigated previously in the frame of existing TOB. Three pilot studies began analyzing all types of WWERs which exist in the Ukraine i.e., SUNPP-1, ROVNO NPP-1 and ZNPP-5. The deadline for pilot studies is the end of 1999. At the present time, the Level 1 PSA for Rovno NPP Unit 1 is completed and the rest of work is in progress at different stages.

2.14. USA

The major USNRC sponsored studies for the Grand Gulf and Surry NPPs have been completed and their results published in NUREG/CR-6143 and NUREG/CR-6144. Those studies were multimillion dollars R&D efforts aimed at developing the state-of-the-art methods and approaches which could eventually be applied to other NPPs in the USA.

The interest in shutdown safety in the USA started in the mid-eighties and was triggered by operational events during shutdown operation, mainly losses of functions like RHR or power supply. One of the first comprehensive analyses was a RHR reliability study for the Zion NPP in the mid-eighties. The study concluded that while there was some risk during shutdown operation, it is significantly lower than for power operation. Another study with even broader scope was performed for the Seabrook NPP. While these studies are not comparable in their scope with current LPS PSAs, the results clearly indicated that the mid-loop operation is the most critical configuration, and that there is a need for maintaining redundancies even during shutdown. The shutdown risk at the Seabrook plant was found to be even higher than the risk during power operation. Modifications (mostly improvements in procedures and administrative regulations) to reduce the shutdown risk were made, even before the plant was put in commercial operation.

The USNRC does not require utilities to perform plant specific LPS PSA studies. However, in light of operational events which have occurred during shutdown conditions, the USNRC Rule on "Shutdown and Low-Power Operation" was proposed. Its purpose was to strengthen configuration control during outages. The USNRC felt that increased administrative and other control by the licensees would assure that the redundancies needed to cope with operational events during outages would be sufficient for maintaining acceptable safety level during outages. The Rule was originally proposed in 1994; in 1997, the USNRC staff sought authorization from the USNRC Commission to issue a modified proposed rule for comment, but the Commission, in a staff requirements memorandum dated 11 December 1997, did not provide the necessary authorization. Rather, the Commission, in a staff requirements memorandum dated 17 December 1997, approved the staff's recommendation to develop a proposed rulemaking to revise the maintenance rule, 10 CFR 50.65, making clear that the maintenance rule applied to all conditions of plant operation, including normal shutdown operations. However, the USNRC staff may decide to evaluate whether any further action, over and above changes to the maintenance rule, will be cost-beneficial.

The requirements for stricter control of plant configurations in outages helped spur the development and utilization of configuration control tools like ORAM, which is now used by the majority of the USA plants. Although the USNRC does not license the use of ORAM, it recognizes the benefits to utilities using this (as well as other) configuration control tools.

Because Grand Gulf and Surry may not be representative of the entire spectrum of US nuclear power plants, and because the completed studies for Grand Gulf and Surry, published in NUREG/CR-6143 and NUREG/CR-6144, do not treat all plant operational states in detail (the Surry study treated only mid-loop operation in detail, with a coarse screening analysis for the remainder of the plant operational states, and the Grand Gulf study treated only cold shutdown in detail), additional shutdown risk analysis research is planned by the USNRC. The research is scheduled to begin in Fiscal year 1999, which starts in October 1998.

The USNRC is currently performing a demonstration project wherein the ATHEANA (a detailed human reliability) methodology is being used to identify the potential for operator actions (e.g., errors of commission and errors of omission) during full power operation for a limited set of conditions at one nuclear power plant. Current NRC plans call for a demonstration application of the ATHEANA methodology to low power and shutdown conditions.

As part of the USNRC's risk-informed regulatory initiative, low power and shutdown conditions should be considered by a utility when making a risk-informed regulatory submittal request for a change to graded quality assurance, in-service-testing, in-service-inspection, or technical specifications.

3. SELECTED PHENOMENA OCCURRING DURING LOW POWER AND SHUTDOWN CONDITIONS

3.1. HYDRAULIC PHENOMENA

The hydraulic phenomena of concern for LPS conditions include cavitation and depriming vortex.

3.1.1. Cavitation phenomena

Cavitation phenomena can affect the pumps and the control valves.

In a liquid, pockets of steam may appear due to a temperature increase, a pressure decrease, or a combination of these two phenomena. The steam pockets are carried along by the liquid and condense when they reach zones where the pressure is higher. This condensation induces:

- Hammering and erosion of the affected surfaces, which may lead to their perforation (deterioration of the concerned valves and pumps);
- Erosion on the pipes downstream of the affected valves and vibration which may lead to rupture of nozzles of small lines due to vibration-induced fatigue.

The signs of abnormal operation caused by cavitation are: local knocking and a slight instability in pump parameters (current, pressure, flow), which can be detected from the control room. No local noise is generated apart from the noise of the pump motor forcing.

The remedies are to change the operating parameters of the circuit (flowrate, pressure, temperature) after appropriate design studies and tests (if necessary).

3.1.2. Depriming vortex

When the level drops in a pipe or in a tank to be drained, a vortex appears in the pump suction pipe. This corresponds to the formation of a spiral which carries along air bubbles. Suction of air then leads to the formation of air pockets in the pump body. As long as the air is carried along to the discharge of the pump, no problem appears. However, if the air fills the upper part of the pump casing, the pump is deprimed and can no longer operate. In this case, the air needs to be bled off before the pump can resume its operation.

The signs which indicate a depriming vortex are: variation in current, pressure and flows detected from the control room, and no local noise is generated, apart from the noise of the pump motor forcing.

3.2. DEGRADATION OF NATURAL CIRCULATION

Natural circulation is a standard means of decay heat removal from WWER-440 reactors in the cold shutdown mode operation. There is basically no other residual heat removal system required. The reason is the large redundancy in six RCS loops that can be isolated from the reactor by closing the main isolation valves in both hot and cold legs. The standard mode of natural circulation cooling is with two loops in operation and one loop in hot standby, the three remaining loops may be void and undergoing repair. Later on in the refuelling outage, only one loop has to be in operation and one in hot standby. Steam generators in the operating and standby loops are filled with water and heat is removed from them by heat exchangers with cooling towers as the ultimate heat sink.

During normal power operation, the water level in WWER-440 reactors is not monitored. In cold shutdown, a standard reactor level measurement is used based on water differential pressure in the U-tube, with the scale between 180 and 250 cm of narrow-range level. The positive reference leg of the U-tube is connected to a tube used for continual monitoring of boron concentration in reactor coolant. This standard reactor level measurement is activated prior to the depressurization of the main reactor seal flange plane and removal of the head.

In PWRs, natural circulation is not a mode of residual heat removal during shutdown conditions as dedicated RHR systems are used. It is only a transient condition in case of a trip of all RCPs. That is why problems with degradation of natural circulation are not reported frequently for PWRs.

A number of events involving degradation of natural circulation at WWER-440 units in cold shutdown for refueling have occurred. Although boiling occurred several times, fuel element cladding integrity was never challenged. A few initiating mechanisms were identified. Operators sometimes have insufficient information on the degradation of decay heat removal and the identification of such events can take a long time. Detailed computer analyses of thermal-hydraulic processes are necessary and operating instructions for efficiently dealing with degradation of natural circulation should be elaborated.

The events associated with degradation of natural circulation were described in particular papers presented during the meeting.

The main causes of degradation of natural circulation include:

- A leak or drainage from the reactor coolant system;
- A bubble formed in the upper parts of the reactor or SG;
- A loss of cooling on the SG secondary side;
- A high cooling rate on the SG secondary side.

The generic lessons learned from these incidents were as follows:

(1) Improvements in operators' understanding of physical phenomena associated with natural circulation cooling and its degradation are necessary. This lesson is in line with the conclusions of Report AEOD/E413 for US PWRs. Operating personnel should be trained in coping with such events.

(2) The formation of a steam bubble in the upper region of reactor vessel resulting from boiling of hotter coolant during an abnormal rapid depressurization should be avoided by controlling the rate of the cooldown.

(3) A reactor in cold shutdown should be vented periodically during normal conditions and following actions which increase the possibility of formation of a bubble.

(4) Continuous recording of the pressure differential and the hot leg temperatures in the operating loops should be provided during natural circulation since both these parameters are needed to determine the adequacy of core cooling.

(5) Measurements of parameters by diverse instruments should provide consistent values under non-nominal pressure and temperature conditions.

(6) Operating personnel should inform the management of abnormal situations to ensure support from other plant specialists, if required.

(7) Operators should use all available means to obtain and record additional information about the event to help in both their decision-making and subsequent analysis.

(8) Valves on RCS support systems, e.g., on equipment vents, should not be left open even if other valves in series could prevent a loss of coolant through them.

Generic issues to be addressed with regard to degradation of natural circulation are as follows:

- In-depth computer analyses of thermal and hydraulic processes should be performed.
- Sufficient information on degradation of residual heat removal should be provided for operators.
- Operating instruction for dealing efficiently with degradation of natural circulation should be elaborated.

Degradation of natural circulation should be accounted for when estimating the shutdown risks in PSA studies.

3.3. BORON DILUTION

To keep the core of a PWR subcritical during cold shutdown states, a certain boric acid concentration in the coolant is necessary. An inadvertent deviation from the prescribed concentration, with the tendency to loose subcriticality, is called a dilution or deboration event. The possibilities for diluting the coolant are generally classified as homogeneous (slow) or heterogeneous (fast) deboration.

3.3.1. Homogeneous deboration

A homogeneous deboration is characterised by the deviation from the prescribed concentration in a large part or the whole volume of the coolant, i.e., mixing mechanisms are effective. An effective mixing is always present when the MCPs circulate the coolant.

Possible initiators of a homogeneous deboration are:

- During shutdown
  - Failure in the boric acid / non-borated water injection system.
- During refuelling
  - Dilution due to leaks of systems with non-borated water, e.g. valves, SG tubes, heat exchangers, etc.;
  - Inadvertant opening of valves in connected systems which contain non-borated water;
  - Maintenance work with non-borated water which is not drained when the work is completed;
  - Filling of the refuelling cavity with an incorrect boric acid concentration.

- During startup
  - Refill of the RCS with the wrong boron acid concentration;
  - Failure during the deboration phase of the RCS.

For any of the described possibilities for deboration, except during shutdown, examples of incidents the have occurred can be found in the international operational experience. Large amounts of non-borated water must be added to reach criticality. Therefore, in most cases enough time is available to detect the dilution either by boric acid concentration measurement or, at a later stage of the sequence, by an increase in the neutron flux measurement. If a criticality of the core cannot be prevented, the consequences depend on the degree of dilution. Consequences may range from a slight power excursion to an opening of safety valves if the RCS is closed to steaming or ejection of coolant if the RCS is open. The power excursion will be limited by the corresponding reactivity feedback effects.

From this phenomenological description, the tasks of an accident analysis can be derived. The analysis should give answers to the following questions:

- What amount of non-borated water is needed to reach criticality?
- What are the possible sources for non-borated water and what mass flows can be expected?
- What is the available time and are the normal operational practices sufficent to detect the deviation in boron concentration within the time window?
- What are the consequences if the available non-borated water of the system in question is injected into the RCS?

3.3.2. Heterogeneous deboration

A heterogeneous deboration is characterized by the formation of a slug of non-borated water or of water with a low boric acid concentration in the primary cooling system. Formation of such a slug is only possible if no circulation, natural or forced, is present, i.e. heterogeneous deboration is only possible if the MCPs and natural circulation are stopped.

Possible initiators of a heterogeneous deboration are:

- During shutdown
  - Loss of all active RHR-systems and passive cooling of the steam in the available SG will form deborated condensed coolant which will concentrate in the lower parts of the loop as a slug.

- During refuelling
  - Components or systems which have been in maintenance are refilled with water with a lower boric acid concentration;
  - If the circulation in the loops is stopped, demineralised water from leaks can form a slug in lower parts of the loop.

- During startup
  - A slug can be formed in the primary system during the deboration phase of the RCS if all MCPs are stopped and the injection from the demineralised water system is not stopped due to a failure.

A local reactivity increase will be the result if the circulation in the loops re-establishes and the slug of water with low boric acid concentration is transported through the core without mixing with the coolant of higher boric acid concentration. Neutronic analysis has shown that a volume of few cubic meters is enough to cause local criticality and, in the worst case, to result in damage of the fuel cladding. The local power increase leads to a pressure transient in the RCS which can be predicted by a coupled neutron-thermohydraulic analysis. The most important phenomenon influencing this sequence is the mixing of the slug with the coolant. Mixing is, however, very difficult to analyse accurately. A reliable prediction of the mixing is probably only possible with 3D fluid calculations.

A detection of the deboration is only possible in an early stage if the circulation has not been started. If the circulation is started, the available time is too short for countermeasures. Therefore, attention should be focused on to preventing a slug formation and identifying situations when a slug can occur. Preventive measures include the automatic interruption of boron dilution if one or more MCPs are stopped and also a careful measurement of the boric acid concentration in systems which will be connected to the primary circuit after maintenance.

Because the condensation of steam always leads to deborated water, any sequence in which steam is forming should be analysed to determine how much and at which location demineralized water can accumulate. The operator should have procedures available which ensure a sufficient mixing of a slug that may form.

3.4. PRESSURIZED THERMAL SHOCK

The brittle fracture temperature of steel is a temperature below which its ductility has decreased so that brittle fracture of material is possible. Neutron flux irradiation of the reactor core causes damage in reactor pressure vessel (RPV) wall material and its brittle fracture temperature decreases. If the RPV is cooled below brittle fracture temperature, there is a danger of brittle fracture if there is an initial crack in the RPV wall material. The phenomenon is called pressurised thermal shock (PTS) and its worst consequence is a catastrophic failure of the RPV. PTS is more relevant for PWRs than for BWRs because PWRs generally have a narrower water gap between the reactor core and the RPV wall than BWRs.

In cold shutdown mode the temperature of the RPV wall can be below brittle fracture temperature. At this stage the RPV is especially vulnerable to brittle fracture if it is pressurised. Also, PTS is more likely to occur at other zero or low reactor power modes then at full power operation because the cooling of the primary circuit and the RPV in leak and transient situations might be larger than during events with full reactor power as the initial condition.

Possible remedies for PTS events are automatic overpressure protection which disable systems that can pressurize the RPV, administrative measures to isolate high pressure systems from the primary circuit, and dedicated outage safety valves. It is also possible to mitigate PTS by recovering the material properties of the RPV through thermal annealing.

4. SAFETY ISSUES RELATED TO LOW POWER AND SHUTDOWN CONDITIONS

4.1. PSA

The following results and conclusions have been generalized from previously completed LPS PSAs or from preliminary results of ongoing LPS PSAs. The results and conclusions have been generalized in an attempt to provide the most benefit rather than simply to present results from a few selected LPS PSAs.

For plants dependent on boration to maintain subcriticality, careful consideration should be given to modelling heterogeneous (and possibly homogenous) deboration events. A detailed search for events and actions that cause or contributed to deboration should be performed.

For plant designs in which natural circulation is an integral part of the decay heat removal process, loss of natural circulation has sometimes been shown to be an important event. Thus, for those plants which require natural circulation, detailed analyses should be performed to identify how natural circulation can be lost or degraded.

Plant specific practices (e.g., operational requirements for specific systems or components) during shutdown conditions and unique plant features (e.g., additional systems) have the potential to significantly affect the final results.

Closure of an open containment without establishment of containment heat removal may not be sufficient to prevent release of radioactive material if core damage occurs.

The contribution of shutdown operational states to the annual CDF and risk may not be insignificant when compared with full-power results. For example, one study indicated that shutdown CDF for one POS could be as high as 50 per cent of the full power value. Risk measures (i.e., early fatality risk and total latest cancer fatality risk) were estimated to actually be higher for the shutdown POS than for full power, due mainly to fewer mechanisms for scrubbing or containing the released radionuclides. However, if the same scrubbing or containment mechanisms exist in shutdown states as for full-power, risk measures should be lower. Both CDF and risk are affected by the time after shutdown.

The risk from fire events during shutdown may be important if systems that are normally used to provide decay heat removal during shutdown conditions are insufficiently fire tolerant (i.e., they have insufficient physical separation). A careful examination of equipment and cabling susceptibility to fire is necessary to ensure an adequate representation of the threat of fire during shutdown conditions.

While "core damage frequency" may be zero for those utilities that choose to off load fuel from the reactor vessel to the spent fuel pool, the shutdown PSA must account for the new location of the fuel and calculations should be performed to determine the susceptibility of the fuel damage in its new location.

LPS PSA models can be used to determine the impact of changes to the timing of various maintenance and test activities during shutdown. In addition, LPS PSA models can be used to identify operator actions that could benefit from additional training prior to entry into shutdown conditions. Furthermore, LPS PSA models and results can be used to identify enhancements to procedures (either normal procedures used during shutdown or emergency procedures) or hardware modifications.

An accurate representation of the plant during shutdown conditions requires extensive and detailed interaction between the PSA analysis team and all organizations at the plant which are involved in work performed during the shutdown. Thus, sufficient time and resources should be allocated to ensure these interactions can take place.

In order to determine the optimum strategy for performing maintenance, balancing risk against cost, it is necessary to assess the risk of performing scheduled maintenance during power operation as compared to periods of shutdown. The measure of risk increase which is most appropriate is the conditional increase in the risk, given one is in a given POS, from taking one or a few components out for maintenance, times the amount of time per calendar year that one does scheduled maintenance on the component or components. This can be compared at full power, and at various shutdown plant operational states. When computing uncertainties in the risk increases, correlation between the risk with components out for maintenance, and the risk with the components not out for maintenance, must be taken into account.

A situation can occur where the corrective maintenance on a component during power operation will exceed the allowed outage time for performing maintenance on the component. The question then arises as to whether the risk from continued operation with the component out of service is greater or less than the risk from shutting the plant down, performing the maintenance and restarting the plant. An example of a component, where maintenance may be less risky during power operation than shutdown, is an auxiliary feedwater pump in a PWR. The auxiliary feedwater pump is not used during normal operation of the plant, but is required for shutdown. After a period of time during shutdown, the auxiliary feedwater system is no longer needed, but the residual heat removal system can be used. Hence, depending on length of time it takes to fix the auxiliary feedwater system pump, it may be less risky to perform the maintenance at power.

As LPS PSAs become available, comparisons between their results and results from full-power operations will be made. It is recommended that a standardized method for making such comparison be developed. For example, such a method should describe how time-averaged results are presented and compared.

The development of a standard for performing LPS PSA should be considered. This recommendation is based on observations made during presentations of PSA results for plants of the same design and reactor size. For example, different initiating event lists, even to the point of defining different LOCA sizes, different definitions of POS and different dominant accident sequences were presented. The standard should be written to minimize variation among PSAs of reactors of the same design and size, but should ensure that plant-specific operational differences are reflected in the PSAs.

4.2. ACCIDENT ANALYSIS METHODOLOGY

During LPS the pressure and temperature of reactor system is lower than during full power operation. There may be a nitrogen blanket in the pressurizer or the primary circuit may be open to atmospheric pressure. The traditional accident analysis codes (e.g. ATHLET, RELAP, CATHARE, TRAC) were not originally developed to take into account these special physical conditions and there may be difficulties in adapting them for analysis of LPS. There is also lack of validation of these codes and their relevant correlations against experiments and plant data under LPS conditions. Further development of codes or at least validation is needed with particular attention in the modelling to:

- Low pressure conditions;
- Non-condensable gases;
- Natural circulation;
- Modelling of free water levels.

Due to the slow progress of accidents and transients initiated during LPS modes, hand calculations or use of simplified models are often sufficient to evaluate the behaviour of the reactor system during these events. However certain events require more detailed treatment of the reactor system and the physical phenomenon in question. These events include:

- Loss of natural circulation;
- LOCA events;
- Overcooling transients;
- Boron dilution events;
- System pressurization.

In order to get a realistic picture of the nature and safety significance of a LPS event, it is sometimes necessary to do a very detailed and comprehensive analysis. A good example of this is a boron dilution event for which models of mixing and 3D neutron kinetics are needed in combination with modelling of primary circuit thermal hydraulics.

Currently the analysis for LPS has been performed only for a small number of cases. However, because of their safety significance, there is a need to perform these analyses for inclusion in final safety analysis reports, for development of emergency operating procedures, and for further development of technical specifications. Due to their potential impact, LPS analyses need to be carried out with the same care as those for full power conditions.

The analyses for LPS should be performed for two purposes. In a traditional conservative analysis the aim is to show that the results fulfill the acceptance criteria of the analysis with minimum safety systems available and with conservative assumptions of operator actions. The other set of analyses are best estimate analyses where the effect of various assumptions on the results is studied. The latter is especially useful for drawing up EOPs and for PSA purposes. In this way the interrelation with PSA studies can also be taken into account.

For WWER reactors, a methodology for analysis of LPS has been developed as presented in the report IAEA-EBP-WWER-09.

There are plans to perform LPS safety analyses for RBMK reactors, but there is no methodology available for this purpose.

4.3. OPERATIONAL SAFETY ISSUES

4.3.1. Administrative improvements

The safety studies for low power operation and for shutdown have confirmed that human interactions are among the most important contributors to the overall risk. This is caused by two factors: more human interactions during shutdown, and relatively few administrative limitations and requirements compared to power operations. The shutdown state was considered to be the safest operating state of reactors and the Limits and Conditions requirements were considered less important. This led to only a few limitations being implemented to assure the availability of systems.

The recent safety studies also indicate that shutdown safety is to a large extent a configuration control issue.

Among the countries and plants that discussed their activities on the topic at the recent meeting, there are different approaches to administrative limitations during shutdown. These depend both on the reactor type and on the overall safety culture in a given country.

4.3.1.1. Limits and conditions

Most of the plants have considered some review relevant to shutdown operations and/or additions to their limits and conditions. However, this process depends on the present status and completeness of their LPS studies.

The administrative limitations addressing shutdown operations should be focused on assuring the availability of additional redundancies or limitation of the duration of specific critical operating modes. Some specific improvements to the limits and conditions that should be considered are:

(1) Introduction of administrative controls on the primary system boundary valves.

(2) Assure full availability of a RHR system when entering the cooldown mode.

(3) Assure that more power sources are available throughout the shutdown period. Limits and conditions would require the availability of a certain number of emergency diesel generators.

(4) Re-schedule the preventive maintenance of some systems. The comparison of the aggregate risk from a given maintenance activity serves as the basis for risk-informed decisions concerning the operational state (including full power operation) during which scheduled maintenance should be performed.

(5) Prevent boron dilutions by requiring specific boron concentrations during the shutdown operation.

(6) Prevent cold overpressurization by implementing effective pressure - temperature limitations, prohibiting the use of specific high head pumps, or requiring adequate relief capability.

(7) Enhance the availability of the residual heat removal function by requiring alternative cooling methods (i.e. spent fuel pool cooling system).

(8) Assure reliable inventory control by increasing the number of redundant safety injection paths.

(9) Increase the time available if entry into a specific configuration is prohibited before the decay heat is below a certain level.

4.3.1.2. Availability of systems and instrumentation

The following general principles, which are valid for all the operating modes, have to be applied in the particular case of shutdown modes:

- The availability of safety functions which are necessary to prevent degradation of the different barriers between fuel and population, and consequently of the systems and instrumentation necessary to implement normal and emergency procedures applicable in the considered mode;
- The response of an operator in the event of violating the normal operating limits or of random inoperability of required equipment (fallback mode and fallback time).

For the case of random inoperability during shutdown modes, it can happen that no particular fallback mode applicable to safety can be defined. In this case, it is acceptable to only require an adapted maximum reparation time.

The safety functions which are to be considered are:

- Reactivity control;
- Inventory control;
- Residual heat removal;
- Containment;
- Support functions (electrical power supply, and other support functions, post-accident monitoring system, etc.).

Adequate redundancy of the required instrumentation and equipment has to be defined in accordance with its safety importance.

Scheduled maintenance on and periodic tests of equipment have to be strictly limited to those conditions where the considered equipment availability is (1) not required in the operational mode and (2) in a stable thermohydraulic and neutronic reactor state. In cases where the availability of equipment is required in all operating modes, scheduled maintenance and periodic tests have to be done in a mode, justified by a specific analysis, where the equipment is less important and preventive measures could be taken, if necessary.

4.3.1.3. Outage management

The safety of NPPs is ensured by redundant or diversified safety systems. In addition to systems which automatically actuate, operators have extensive instrumentation systems to provide accurate information on the status of processes and equipment during operation. These capabilities are not available in shutdown mode. Some automatic systems are blocked and some systems are out of service for maintenance.

To assure safety during the shutdown mode, outage management including outage preparation, execution and evaluation is essential. Administrative measures were implemented by many utilities to address this problem.

One example of administrative control of safety during outages is the preparation of a shutdown safety plan and operational plan for the outage. An operational plan should contain lists of systems and define when specific systems shall be in operation or in active standby to ensure availability of basic safety functions. The plan includes not only safety systems but also primary loops, RHR systems, SG and associated pipes, and systems which support safety systems.

The shutdown safety plan (SSP) is an extension of an outage operational plan and covers the risk management considerations. The SSP should describe possible recovery actions considering systems and equipment which are or may be available at different periods during an outage. Also use of external resources and non-standard systems for accident mitigation should be described.

Another approach to configuration control in shutdown is the use of risk monitoring tools. Such tools allow a utility to optimize an outage by maintaining a configuration which should guarantee low risk. Moreover such tools allow for modelling changes in the outage schedule and adjustment in configuration to maintain required safety barriers.

For maintaining safety during shutdown, daily work co-ordination of an outage is essential. It is recommended that each plant establish an outage co-ordination team with adequate knowledge of operations, safety systems and safety functions success requirements. This team should co-ordinate daily activities, with a focus on safety requirements and safety systems availability. The team should be headed by an expert with shift supervisor experience and/or license.

4.3.1.4. Administrative measures

The shutdown mode was traditionally considered a safe reactor state. As a result, very little administrative control was implemented for shutdown operations. Moreover, outage scheduling was in most cases centered on maintenance activities with less regard for available redundancies, work authorization, systems testing and housekeeping.

Operations personnel should be cognizant of and have control over the detailed status of the plant systems and equipment during shutdown mode. The shift supervisor must be informed of maintenance activities affecting the status of systems and equipment. All work conducted at the plant has to be planned, analysed and executed in a manner that is consistent with the requirements of the shutdown mode. Effective interface between the operation and maintenance groups (including contractors), is essential.

Work should be authorized by the control room operator or the shift supervisor. All work authorizations should be made in writing on approved forms and reviewed at each shift change. Isolated components should be put in their appropriate position and locked. Warning signs such as "Do not Operate" or "Danger" should be placed on isolated components. After work is completed, operations and maintenance groups must ensure that systems and components affected by the work are tested and returned to the stand-by mode or operational mode.

If the outage schedule is modified to incorporate unanticipated work, the original scheduling logic must be used to evaluate the modifications including assessment of risk. Administrative controls should be rigorous enough to ensure this occurs.

Special administrative measures during the shutdown are required to prevent the following:

- undesirable inflow of unborated water to the primary coolant and spent fuel pool, e.g., timely isolation and periodical checking of the potential sources of unborated water
- loss of decay heat removal, e.g., assuring full availability of the RHR system, including checking and maintaining the RHR path
- LOCAs, e.g., written orders for draining of primary circuit, locked boundary valves, assurance that the order of the primary circuit openings is maintained, taking into consideration specific phenomena (such as siphon effect, or use of nitrogen for draining)
- foreign elements from falling into primary circuit, e.g., locked loose flanges, tools, and equipment used above the open primary circuit.

Finally, plant cleanliness and good housekeeping should be evident during all modes of operation including shutdown mode. A programme of foreign material exclusion should be implemented and monitored.

4.3.2. Procedures and training

4.3.2.1. Operating procedures and emergency operating procedures

Most operating procedures and emergency operating procedures are written for events in which the reactor is at full power. Their applicability for events at LPS conditions varies from case to case. However, there might be a general emergency operating procedure that is applicable in any event, whose main goal is to ensure that all the safety functions will be maintained during the event.

Many plants performed reviews of their operating procedures to identify if any of events during the shutdown would lead to a potentially high risk situation. If so, those procedures would then be modified. Some plants have developed and implemented specific emergency operating procedures for mitigation of accidental situations during shutdown. The evaluation of operating procedures is necessary due to new studies, new operational practices, hardware modifications, etc.

Particular attention should be paid to initiators which lead to common mode failures during shutdown modes, for example:

- Total blackout;
- Total loss of ultimate heat sink;
- Malfunction of the normal RHR.

4.3.2.2. Training

Training of NPP staff and contractors is required to communicate that understanding outage risk is very important to shutdown safety. Training activities can increase the understanding of the plant personnel and contractors of the safety issues related to conduct of outage. Many reported events were caused by staff and contractors who were not well-trained.

Many plants have introduced shutdown safety as a special topic for the pre-outage training of staff. This training should also cover risk during the outage, radiation protection, fire protection, industrial safety emergency planning, radioactive treatment and decontamination.

It is recommended that control room operators and maintenance personnel be provided with adequate training on both the risk significant events, and their prevention and mitigation.

4.3.3. Hardware improvements (HI)

The issue is related to a lack of appropriate hardware. Some of the incidents and accidents that have occurred during shutdown clearly show cases such as inaccurate level measurement in reactors; inadequate temperature monitoring in the core because the instrumentation was outside the core; and instrumentation and controls focused on power operation and not on outages.

The HI for shutdown operations are mostly related to instrumentation and controls. These also include installation of various interlocks and alarms aimed at preventing events (like draining of the reactor). Another area of HI is related to maintenance tools and equipment. Some maintenance equipment is being redesigned to reduce the probability of initiating specific occurrences.

Specific hardware improvements implemented at plants are:

(1) Hardware improvements to reduce the probability of LOCA
Interlocks were designed to prevent opening of specific isolation valves in lines connected to the RCS and the spent fuel pool.

(2) Loss of RHR directly related with the low water level in the RCS
Many plants decided to install water level monitoring systems in response to this problem. A typical choice is the ultrasonic level measurement system. Some HI are focused on providing interlocks to automatically terminate the draining upon a low level signal. Other HI concern detection of vortex phenomena and automatic makeup of the reactor coolant system.

(3) A plant implemented specific HI focusing on avoiding consequences of loss of power. This plant installed specific devices which allow connecting mobile diesel generators to the emergency electrical supply busses in case of total plant blackout.

(4) Some HI were implemented to reduce the likelihood of boron dilution events. Instrumentation with alarms and modification of the charging flow intakes are examples of possible solutions. Another plant installed various interlocks to prevent boron dilution in the RCS.

(5) The RCS has enough capacity to relieve the overpressure, but the setpoints or the availability of relief valves during shutdown is the issue. One plant implemented a diverse pressure relief path and cold overpressure protection device that maintains pressure within safety limits during all shutdown modes.

Lessons from a number of events during low power and cold shutdown show that deficiencies in the implementation process for new HI may lead to inadvertent events. The modifications may add new event initiators during shutdown modes. Plant personnel must pay adequate attention during implementation to integration of hardware improvements into operations. Each modification could change the frequency of initiators already known or create the possibility of a well known transient appearing unexpectedly, not described in the procedures.

Hardware improvement is an important way to avoid some of the main problems related to shutdown operation, but to be effective, hardware improvements have to be combined with administrative, procedural and training improvements.

4.3.4. Feedback of operating experience

The feedback of operating experience provides an important source of information for safety analyses during low power and shutdown conditions.

National systems for reporting and analyzing events from plant operation exist in all Member States. In these systems, the operators collect and store information which enables to identify problems in shutdown and low power modes as well. Safety relevant events are reported by the operators to national regulatory authorities. From these safety relevant events, the national safety authorities report the most safety significant events to the incident reporting system (IRS) run by the IAEA together with the Nuclear Energy Agency (NEA) of the OECD. This IRS system stores a large amount of information in computerized form from all Member States with various types of reactors. This information is distributed from the IAEA through IRS national co-ordinators on CD-ROM, and it is a commitment of each country to make the best use of it to prevent re-occurrences of similar events. The operators also report events to the World Association of Nuclear Operators through WANO centers. The information is compiled for various families of reactors.

The information from these different forms of operating experience feedback can and should be used for safety analyses during low power and shutdown conditions to:

- Identify events which represent precursors of states with potential core damage;
- Perform or check the allocation of initiating events into categories;
- Estimate or check the frequencies of initiating events in various Plant Operating States based on actual events;
- Design or check the event trees starting from those initiating events;
- Carry out computer analyses:
  - conservatively for safety analysis reports and PSA studies, and
  - realistically, (best-estimate) for operator training and development of realistic operating and emergency procedures;
- Derive and check the values for availabilities of safety systems or components derived from reliability databases;
- Check the quantitative results of PSA studies.

The use of information from operating experience for safety analyses during low power and shutdown conditions should be made as efficient as possible.

4.4. SAFETY ANALYSIS REPORTS

Progress has been made recently in the scope and quality of safety analysis reports for NPPs in the region and significant activities related to LPS conditions are ongoing in several NPPs. However, the reports are still neither systematic nor complete regarding LPS conditions. This is inconsistent with the relatively high probability of the corresponding events. The situation does not differ considerably between eastern and western countries.

The quality of reports is strongly dependent on the availability of adequate methodology and computer codes for accident analysis. The reports typically include only those events which are analysed using an approach developed for accidents occurring at power operation.

Examples of such events are reactivity accidents and steamline breaks which are regularly analysed at zero reactor power. The quality of the safety analysis report directly influences the quality of NPP documentation, technical specifications and EOPs in particular.

Systematic analysis of events during LPS conditions should be included into a standard format and context of safety analysis reports subject to approval by regulatory authorities. The effort should cover a list of initiating events and set of acceptance criteria typical for LPS conditions. The IAEA report IAEA-EBP-WWER-09, after its extension to cover all LPS plant operational states, provides a good basis for such work. Unfortunately, an equivalent report has not been developed for other reactor types used in the region, i.e., in particular for RBMK types. It has to be emphasized that list of initiating events may differ considerably for PWR, RBMK, and CANDU type reactors.

Co-ordination of activities in the framework of the IAEA could considerably facilitate and accelerate this work.

5. CONCLUSIONS AND RECOMMENDATIONS

In the field of probabilistic safety assessment:

(1) Since the identification of initiating events is a critical step in the performance of a PSA, specific detailed guidance for shutdown should be developed for identifying initiating events. This guidance should be sufficiently general in nature so that all reactor types can use the methodology, and detailed enough to ensure that all relevant initiating events are identified.

(2) To estimate CDF and risk as realistically as possible and to ensure that differences among plant SPSAs are real and not artificial due to different analysis approaches, shutdown operating conditions must be subdivided into plant operating states that allow for relatively constant conditions (e.g., decay heat should not change significantly during the POS and neither should plant equipment availabilities). To this end, a standardized methodology for defining plant operational states should be adopted. This standard should be developed to minimize differences in results for plants that are similar. However, the method should be flexible enough to allow the identification of plant unique operational differences.

(3) Degradation of natural circulation during shutdown conditions, mainly in WWER reactors, should be accounted for adequately when estimating the shutdown risk in PSA studies. Detailed computer analyses of thermal and hydraulic processes should be carried out to show whether and at what time these processes could lead to core damage.

(4) Additional methodological guidance (or development) should be provided in the area of human action (error) identification and quantification. This identification and quantification guidance should be specifically developed for shutdown conditions where multiple human actions may be ongoing and where the time to respond may range from very short to very long. This methodological guidance should ensure that the following human actions are included in the analysis:

- those occurring before the initiating event;
- those causing or contributing to an initiating event;
- those in response to procedural steps;
- those that recover or repair failed equipment.

The methodology should be computerized to minimize the possibility that important aspects (e.g., dependencies) of the identified human actions/errors are lost. This computerization scheme should ensure that all information necessary for documentation purposes is captured and that documentation of any or all human actions could be performed by simply selecting the appropriate human action and producing a report.

(5) Codes used for determining success criteria and the progression of core damage, vessel failure and the transport of radionuclides may need to be enhanced to account for shutdown specific conditions (e.g., an open reactor vessel, an open containment and fuel location other than the reactor vessel).

In the field of deterministic accident analysis methodology:

(6) The effort should be concentrated on validation of available computer codes (RELAP 5, CATHARE, ATHLET, TRAC, MELCOR, RAINBOW) and applicability of their relevant correlations for thermohydraulic LPS conditions analysis.

(7) More detailed/advanced calculations are needed to understand the uncertainties involved with deboration events. One phenomenon that may be of significant importance is the mixing behaviour at the plug of non-borated water as it moves through the surrounding coolant and through the core region.

(8) For RBMK reactors, guidelines for accident analysis under LPS conditions should be developed immediately.

(9) Accidents occurring during LPS conditions should be incorporated into the standard format and content for safety analysis reports. Lists of initiating events and corresponding criteria should be developed.

In the field of NPP operation:

(10) Limits and Conditions should be further developed for shutdown conditions to adequately assure safety under such conditions.

(11) Administrative control of safety during NPP outages should be developed and implemented individually for every outage including co-ordination focusing on safety requirements, safety systems availability and safety functions success.

(12) Normal and emergency operating procedures should be developed and/or improved to reduce incident initiation and mitigate accidents during shutdown modes.

(13) Training of plant personnel and contractors before outages should lead to better understanding of the safety issues related to conduct of outages.

(14) Hardware modifications resulting from accident analysis, SPSA and operating experience should be implemented as soon as possible together with administrative improvements.

(15) The use of operating experience from both national and international sources for safety analysis during low power and shutdown conditions should be made as efficient as possible.

ABBREVIATIONS

BDBA	beyond design basis accident
BWR	boiling water reactor
CANDU	Canada deuterium–uranium (reactor)
CDF	core damage frequency
DBA	design basis accident
EFWS	emergency feedwater system
EOP	emergency operating procedure
HI	hardware improvement
HPIP	high pressure injection pump
IE	initiating event
IPE	individual plant examination
IRS	incident reporting system
LOCA	loss of coolant accident
LPS	low power and shutdown
MCP	main coolant pump
MCS	maintenance cold shutdown
MSH	main steam header
NEA	Nuclear Energy Agency
NPP	nuclear power plant
OECD	Organisation for Economic Co-operation and Development
ORAM	outage risk assessment and management
POS	plant operating states
PSA	probabilistic safety analysis
PTS	pressurized thermal shock
PWR	pressurized water reactor
RBMK	light water cooled, graphite moderated, channel type reactor (Soviet design)
RCS	reactor coolant system
RHRS	residual heat removal system
RIA	reactivity initiated accident
RPV	reactor pressure vessel
SAR	safety analysis report
SG	steam generator
SPSA	shutdown probabilistic safety analysis
TOB	technical justification report for nuclear safety
QA	quality assurance
USNRC	United States Nuclear Regulatory Commission
WANO	World Association of Nuclear Operators
WWER	water moderated, water cooled energy reactor

CONTRIBUTORS TO DRAFTING AND REVIEW

Buslik, A.	Nuclear Regulatory Commission, USA
Cillik, I.	VUJE,Trnava a.s, Slovakia
Carnino, A.	International Atomic Energy Agency
Cvan, M.	VUJE,Trnava a.s, Slovakia
Czakó, S.	Institute for Electric Power Research Co., Hungary
Dusic, M.	International Atomic Energy Agency
Elter, J.	Paks NPP Ltd, Hungary
Gossiaux, J.M.	EOF/CIG, France
Gromov, G.	Scientific Technical Centre, NRA, Ukraine
Hladky, M.	Dukovany NPP, Czech Republic
Jankowski, M.	International Atomic Energy Agency
Jifcu, P.	Medgidia st. No. 1, Romania
Kaltchev, B.	Energoproekt PLC, Bulgaria
Lin, C.	International Atomic Energy Agency
Lipar, M.	Nuclear Regulatory Authority, Slovakia
Lojkine, S.	RF Gosatomnadzor, Russian Federation
Mišák, J.	Nuclear Regulatory Authority, Slovakia
Movsisyan S.	ANPP Company, Armenia
Mueller-Ecker, D.	Gesellschaft für Reaktorsicherheit (GRS), Germany
Ollikkala, H.	Radiation and Nuclear Safety Authority (STUK), Finland
Panashchenko, M.	Rovno NPP, Ukraine
Samiei, M.	International Atomic Energy Agency
Sarkadi, D.	Hungarian Atomic Energy Authority, Hungary
Suchomel, J.	VUJE Trnava a.s., Slovakia
Tarasov, A	Ignalina NPP, Lithuania
Vergelj, M.	Slovenian Nuclear Safety Administration, Slovenia
Whitehead, D.W.	Sandia National Laboratories, USA
Zonev, A.	Kozloduy NPP, Bulgaria