

**International Conference on the Strengthening of Nuclear Safety in Eastern Europe,
Vienna, 14-18 June 1999**

Status of Ignalina's Safety Analysis Reports

Eugenijus Uspuras

1. INTRODUCTION

The Ignalina Nuclear Power Plant is Lithuania's only nuclear power plant. The plant consists of two units, commissioned in December 1983 and August 1987. Both units are Soviet designed RBMK-1500 reactors and are different from the RBMK-1000 ones operating in Russia and Ukraine, having a larger nominal capacity (design capacity of one unit is 4800 MW thermal) and specific design features.

Operating nuclear power plants require a safety analysis report which confirms the original design basis and describes the behavior of the plant for all potential accidental conditions. In accordance with regulatory requirements, the safety analysis should be based on the current status of the systems, structures and components of the NPP, and should consider all the modifications carried out during upgrading outages including those changes which are committed for implementation. For the Ignalina NPP this information is presented in several reports. Since commissioning of the Ignalina NPP a number of the safety analyses have been conducted. These include the Technical Safety Justification Report (TOB) [1], the Safety Analysis Report (SAR) [2] and its review (RSR) [3], level 1 Probabilistic Safety Assessment (Barselina) [4] and Evaluation of the RBMK-1500 Accident Confinement System [5]. A number of safety analyses and safety cases have been recommended by SAR and RSR teams and have been produced during last two years.

The initial safety studies were performed by the Russian design institute, RDIPE. For the evaluation of plant response for different accidents and transients Russian developed computer codes which were never been widely validated to demonstrate that its are adequately represent a reality have been used. Issues discussed in the TOB [1] are limited by System Description and Accident Analysis. The RDIPE calculations were performed before 1988 and therefore used the design thermal power level of 4800 MW. However, after the Chernobyl accident the maximum permissible thermal power level of Ignalina reactors was reduced up to 4200 MW. Due to these limitations a number of international studies related to the different safety aspects of Ignalina NPP have been initiated after Lithuania restore its independence and Ignalina NPP come to its jurisdiction.

2. PROBABILISTIC SAFETY ASSESSMENT

A probabilistic safety assessment of the Ignalina NPP was performed in conjunction with the Barselina project [4]. The project is a multilateral co-operative study conducted by Lithuanian, Russian and Swedish experts. The Barselina project, four phases of which have been completed, was initiated in the summer of 1991. Its long term objective is to establish common perspectives and unified bases for assessing severe accident risk and establishing requirements for remedial measures for RBMK reactors. In this project the Swedish BWR Barseback is being used as a reference plant and the RBMK-1500 at the Ignalina NPP is being used as the applicant plant.

The Barselina project has been split into four phases. Phase 1 included familiarization with and analysis of a limiting number of safety systems and one single initiating event. It ran from October 1991 to the end of March 1992. Phase 2 included analysis of the principal components for all important safety systems and extension to several initiating events, but excluding external events and with limited treatment of human factors. This phase ran from April 1992 to February 1993. During phase 3, from March, 1993 to June, 1994, a full scope Probabilistic Safety Assessment (PSA) model of the Ignalina unit 2 was developed in order to identify the reduction of risk that can be achieved with possible safety improvements. The probabilistic methodology was applied on a plant specific basis for a channel type reactor of RBMK design. To increase the realism of the risk model a set of deterministic analyses were performed and plant-specific data base were developed and used. A general concept for analyzing this type of reactors was developed. During phase 4, July 1994 to September 1996, the Ignalina PSA model was further developed, taking into account plant changes, improved modeling methods and extended plant information concerning dependencies (area events, dynamic effects, electrical and signal dependencies). The PSA model is also

updated to reflect the “as built” plant. The phase 4 PSA work used insights from the peer review performed by Battelle Pacific Northwest Laboratories on the phase 3 work.

The scope of the PSA study in the Barselina project is as follows. The source of radioactivity is the reactor core. The PSA also is based only on full power operation. Internal initiating events such as transients, LOCAs and Common Cause Initiators as well as internal hazards, such as fire, flooding and missiles are taken into consideration. Final consequence of the accident is core damage, equal to level 1 PSA. During the work, however the core damage states have been defined in such a way, that the results can be used partly as level 2 results - the damage stages represent 4 classes of environmental impact.

The hazard states in the core are evaluated on the basis of the development of accident event sequences resulting in conditions of either “safe conditions”, “violation”, “reactor core damage” and “severe accident”. The plant is considered to have met the “safe condition” requirements when temperature limits are not exceeded or exceeded in no more than 3 fuel channels, but cladding temperature of 800 °C are not exceeded in any channels. Safe operation limits are listed in Technological Specification of Ignalina NPP [6]. If the fuel cladding integrity is breached in more than three channels due to cladding defects and damages or because the cladding temperature limit of 800 °C is exceeded, the state is classified as “violation”. The “violation” category can be regarded as belonging to relatively mild consequences. The reactor core damage category is characterized by severe accidental conditions caused by significant deviation from the design scenario which lead to cladding temperatures above 800 °C in no less than 3 and no more than 90 fuel channels of the reactor. Such accidents do not lead to loss of core structural integrity and this category can be looked upon as resulting in medium severity consequences. The “severe” accident category is characterized by severe accidental conditions caused by significant deviation from the design scenario and accompanied by the rupture at high pressure of more than 3 and less than 9 pressure tubes before the reconstruction of reactor cavity over-pressure protection system and 9 pressure tubes after reconstruction. Such an event can be accompanied by fuel melting or fuel damage in more than 90 fuel channels. This is the most severe consequence.

The accident sequence model for reactor cooling is a phased mission model divided into three time period:

- Short term cooling 0-2 minutes.
- Intermediate term cooling 2 minutes - 1 hour.
- Long term cooling 1 hour - 24 hours.

The phase 4 results indicate that the overall core damage frequency is lower than the phase 3 results. The reason for this is the implementation of plant safety improvement features, and improved analytical procedures which eliminated unnecessary conservatism's. The new results are also balanced by the improvements in the modeling of the Control and Protection System (CPS) and ACS systems. The quantitative results obtained are based partly on plant specific data and partly on generic data. The results are not intended to show absolute risk levels, but to give a risk topography and to serve as a basis for identifying risk dominant features and systems design aspects and hence serve as a basis for safety improvement.

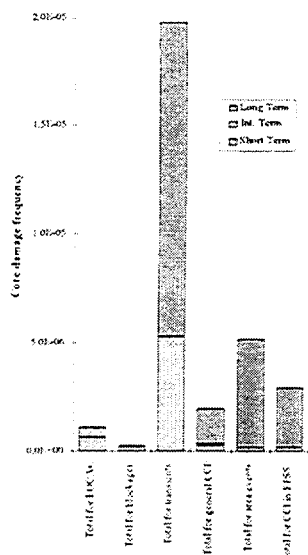


Fig. 1 Damage and accident contributors in different initiating event classes [4]

The general results show a probability of the “violation” end state to be in the order of 10^{-2} per reactor year. This probability is dominated by single channel blockage events. The assessment of probability value is based on operational data. To date 3 such cases have occurred in the RBMK reactors. However, the design of control isolation valves has been changed, which should have a positive impact on the initiating event probability. The “damage” and “accident” end states show probabilities together on the order of 10^{-5} per reactor year, the same range as is expected for “core damage” as defined for Western reactors.

The risk topography is shown schematically in Fig. 1. The characteristic of the risk topography is that for “damage” and “accident” end states transients dominate the risk rather than loss of coolant accidents. Transients contribute more than half of the total frequency. Furthermore it is the long term failure to cool the core that produces the dominating contributions, Fig. 2. The distribution of risk between short term, intermediate term and long term contribution shows that most of the sequences lead to damage or accident only in the long term. Only the core blockage sequences lead to damage in the short term. This demonstrates both the high redundancy of the front line engineered safety systems and the “forgiving” features of the reactor. Low power density and a high heat capacity enables the reactor to survive at least a one hour total loss of electrical power without core damage. In the long term, support functions become more important and their failures become the dominating contributions. The results indicate that a long term lack of coolant leads to severe environmental consequences because the core damage is assumed to occur at high reactor pressure. Human factors also contribute significantly to the core damage frequency. However, the development and introduction of event-based Emergency Operating Procedures is still not accounted for in the phase 4 results.

Since January 1996 a newly formed internal PSA group at Ignalina NPP is responsible for the probabilistic safety assessment. The experience and information from the Barsebäck PSA phases provides valuable information to other projects, e.g., the in In-Depth Safety Assessment of the Ignalina NPP project, for development of the event-based Emergency Operating Procedures and Reliability and Maintenance Management System

3. THERMAL-HYDRAULIC EVALUATION OF THE IGNALINA ACS

The response of the RBMK Accident Confinement System to a large break loss-of-coolant accidents (LOCA), medium break LOCA and small break LOCA is analyzed using the CONTAIN 11AF code. The effect of Condenser Tray Cooling System (CTCS) failure is investigated for the large break LOCA case. The analysis employs a best estimate mass/energy source and considers both short and long-term response of the Accident Confinement System. Parametric studies are performed to evaluate the effects of water deposition on the short-term pressure peak and of by-pass leakage on long-term pressure increases. The study both to summarize the information available regarding the unique ACS which is one of the important safety related sub-systems of the

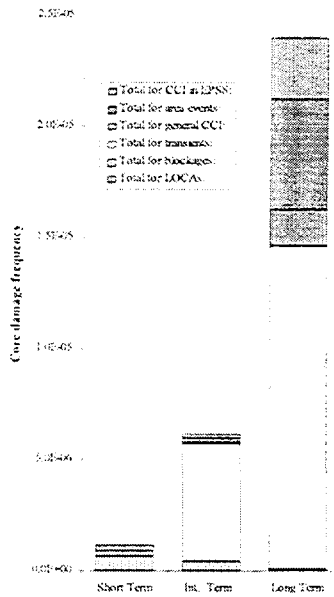


Fig. 2 Damage and accident contributors in short, intermediate and long term cooling [4]

plant and it employs state-of-the-art analysis techniques to verify the response of the ACS to a broad range of LOCA events.

From the containment point of view, the most important boundary condition in the evaluation of a LOCA event, is the mass/energy input that flows from the break. In previous studies the “blow-down” function was taken from the TOB [1], which was prepared by the plant designer. This design basis LOCA source function was obtained as a bounding estimate. It employed simplistic, and in some respects non-physical assumptions. Furthermore, only a single break location and event type was covered. The first requirement for the present study was to determine the break flow using physically justifiable, best estimate methods. The RELAP5/MOD3.2 was employed for this purpose.

The evaluation of the ACS response to a range of LOCA events was performed using CONTAIN 11AF. This version is better suited for RBMK ACS analysis than earlier code releases because it has the capability to represent multiple pressure-suppression vents. Previous studies in this area have been restricted to short-term containment responses, this study considers long-term developments and the computational horizon is extended up to 24 h.

Information regarding the methods and analytical approaches used in the initial design of the RBMK-1500 ACS is very sparse. The earliest available document appears to be an internal report issued by the VNIPIET [7]. The report employs predominantly quasi-steady state computations to evaluate the basic design parameters. No further analytical studies which seek to verify the ACS response are available.

No studies are available which analyze the long-term response of the ACS or which consider the consequences due to malfunction of the active cooling system of the condenser tray water. Furthermore, the available studies do not adequately represent the multi-compartment and multi-suppression pool characteristics of the RBMK-1500 ACS. One of the reasons for this has been the lack of adequate computational tools. The system codes which have been developed for the evaluation of Western type containment turn out to have various limitations when they are applied to the analysis of the considerably more complex RBMK ACS.

An adequate modeling of the Ignalina ACS using western system codes became possible with the release of the C11AF version of the CONTAIN code. This is the first version which incorporates a general flow path model (called an “engineering vent” in CONTAIN terminology). The generalized “engineering vents” can be specified between compartments which during the course of the transient can be exposed either to the atmosphere or can be submerged in water. They can then transmit either atmospheric gases or liquids, or even

both phases at the same time. This is a significant extension of code capabilities, which makes it possible to represent the multiple pressure-suppression vents and multiple condensation pools present in the RBMK confinement system. The main conclusions of report [5] are given below:

1. Best-estimate methods have been employed to evaluate the response of the RBMK-1500 plant to a broad range of LOCA events. The response of the primary system was analyzed using RELAP5/MOD3.2. The mass/energy break flow rates obtained from these calculations were subsequently employed to determine both the short-term and long-term loads imposed on the ACS using CONTAIN (Version C11AF).
2. The LOCA transients analyzed in this study were chosen as to cover the range of conservable break sizes (maximum design basis LOCA to small break) and a variety of break locations.
3. The performed computations show that the pressure loads imposed on the ACS can be divided into two time periods. A "short-term" pressure peak which occurs within several seconds after initiation of the LOCA, and a "long-term" pressure rise which reaches a broad maximum after several hours.
4. The short-term pressure increase is terminated by the rapidly decreasing rate of break flow. This study confirms the conclusions of previous studies that the short-term pressure peak does not exceed design criteria. It is shown that the use of a best estimate source term as compared to the TOB [1] assumption leads to significantly reduced initial pressures.
5. The subsequent "long-term" peak is generated because the temperature of the condenser tray water increases and the rate of energy removal into structures decreases more rapidly than the mass/energy added by the break flow. As the decay energy diminishes, and the stored thermal energy in the graphite block is dissipated (the latter is an important energy source for RBMK plants) the balance between energy source and loss terms is restored and eventually the atmospheric pressure begins to decrease. For most LOCA events, the long-term pressure rise achieves a broad maximum in a 3 to 6 hour time span, the magnitude of the peak in most cases stays well below the pressures imposed during the initial phase of the transient.
6. The heat exchangers of the CTCS constitute one of the principal long-term energy sinks. The assumption of CTCS failure in combination with a LOCA represents a low probability multiple-failure scenario and as such belongs in the "severe accident" spectrum. Two long-term (24 hr) computations were carried out for the design basis LOCA event, one with a fully functioning CTCS, the other for the case where the CTCS is assumed to fail. For the first case the secondary pressure peak is considerably lower than the short-term peak and thus does not pose an additional challenge to the integrity of the ACS.
7. The calculated results for the scenario with failed CTCS, show that even without the assistance of external cooling the pressure rise remains bounded. The energy removed by the very large heat capacities of the RBMK-1500 ACS water pools and concrete structures plus the energy required to heat the subcooled ECCS water to saturation, limits the absolute pressure rise to ~2 bar in the break compartment, and to ~1.9 bar in the compartments beyond the condensing trays. These results are obtained without consideration of by-pass leakage. When estimated by-pass leakage terms are included, the secondary pressure peak stays below design limits.

A summary conclusion of this study is that the analysis of primary system and ACS response of the RBMK-1500 plant to LOCA events employing best-estimate methodology has demonstrated both the complexity and the resilience of these systems. The inherent complexity requires the development of models which push at the limits of currently employed analytical methods. Part of the complexity is produced by the high degree of redundancy and is thus safety related. This becomes especially apparent in the analysis of long-term transients for which the number of alternative options and thus alternative scenarios increases. In most cases a long-term transient analysis will thus not be unique but will depend on the scenario (the main component of variability being operator action) chosen by the analyst. Though, as noted, the methods employed in this study are "best-estimate" an effort was made to choose "conservative" scenarios. In this respect the results also have a conservative slant. It is shown in this study that for the broad range of LOCA events analyzed design loads on the ACS are approached or marginally exceeded only for those cases where multiple failure of safety systems is assumed.

4. IN-DEPTH SAFETY ASSESSMENT OF THE IGNALINA NPP

An in-depth safety assessment of the Ignalina NPP was undertaken and as a result a Safety Analysis Report has been produced [2] and reviewed [3]. The safety assessment of Ignalina NPP is the first attempt to perform Western-type safety analysis for any Soviet-design nuclear power plant. A plant-specific Safety Analysis Report is produced which will form the basis for decisions on future operation of Ignalina NPP. The SAR aims to:

- assess the current level of safety of the plant through an analysis and its review comparable to that

- commonly performed for Western nuclear power plants,
- identify and evaluate any factors which may limit the safe operation of the plant in the foreseeable future,
- assess the Ignalina NPP safety standards and practices,
- recommend any additional improvements which are reasonably practicable and provide estimates of their cost and schedule.

The safety analysis will consider a safety assessment of both units at the Ignalina NPP. The main reference plant for the project is unit 1, but a survey is included which defines the differences between unit 1 and unit 2 and assesses their safety.

The assessment consist of two elements: Safety Analysis Report and an independent Review of Safety Report. The report was Ignalina NPP responsibility, supported by RBMK design institute, RDIPE and Western engineering companies. The review was undertaken by Western and Eastern technical support organizations, including Lithuanian Energy Institute. A Panel of international nuclear safety experts, Ignalina Safety Panel, was established in accordance with the Grant Agreement. The objectives and role of ISP was to monitor and supervise the scope and production of the SAR and its review processes and to make independent recommendations to the Lithuanian Government, Ignalina NPP, VATESI and Donor Countries regarding a decision for continued plant operation and implementation strategies of the SAR and RSR recommendations once the assessment was finalized.

The clear separation of the SAR production and its independent review, performed in parallel and providing interactive feedback has proven very effective in ensuring an objective in-depth assessment. The SAR and RSR teams have identified safety issues and make recommendations on necessary safety improvements in design, operation and safety culture required as sound basis for plant operation.

The overall work program was divided into 10 different sections that encompassed a wide range of topics to produce a broad safety evaluation of the Ignalina NPP. To accomplish these tasks, the following 10 task groups was created for preparation of the SAR and the independent review, respectively:

Task Group 1	Plant Description
Task Group 2	History of Safety and Performance
Task Group 3	Fault Schedule
Task Group 4	System Analysis
Task Group 5	Accident Analysis
Task Group 6	Equipment Qualification
Task Group 7	Management of Aging
Task Group 8	Role of Operator
Task Group 9	Safety Management
Task Group 10	Demonstration of Acceptability

The SAR computations reflect the present operational power level of about 4200 MW. The accident analysis performed in the SAR were undertaken using Western state-of-the-art computer codes. System codes such as RELAP5 and ATHLET were used for thermal-hydraulic analyses and modern Russian codes such as the 3-dimensional codes SADCO and MOUNT which incorporate coupled neutronic-thermal-hydraulic calculations were used for evaluating reactivity initiated accidents. A review of the verification and validation studies which had been performed for each of these codes was undertaken as part of the quality assurance program. The Western codes had been validated extensively for PWR and BWR reactors but had only limited validation for conditions relevant to the RBMK. The Russian codes had undergone varying degrees of verification. In order to compensate for this lack of extensive verification, the codes were used cautiously when any of the critical and unverified regimes were encountered.

A number of accidents sequences which have to be analyzed in accordance with current Lithuanian regulations were not explicitly addressed either in the Ignalina TOB [1] or in the SAR [2]. As noted above, the SAR was initially conceived as a Western-style safety analysis report, but the completion of such a SAR would have consumed several times the resources budgeted for the in-depth safety assessment of Ignalina NPP. The scope, especially the scope of the accident analysis, was therefore defined as including assessment specific essential items [8]. A list of 23 accidents was developed which was intended to cover the “worst case” for each accident category in the sense that these sequences bounded those accidental events which were not included. In order to ensure that no important sequence was omitted an assessment was made by Task Group which undertook the

development of a Fault Schedule. The goal of this task was to prepare a summary of all the accidental conditions which can be identified as having the potential to lead to fuel damage or a release of radioactivity from the plant. However, a thorough comparison of the accidents considered in the Ignalina SAR with initiating events of an extended Fault Schedule showed that they are bounding most of the credible events and no sequences were found which would have required a modification of the essential items list of accidents specified in the Guidelines for production and review of Ignalina SAR [8].

The SAR [2] and its review [3] examined three areas that are equally important to the safe operation of the nuclear power plant: system analysis, accident analysis, and operational issues. First two areas are discussed below, while operational issues are examined in Mr. Negrivoda's paper presented at this Conference.

4.1 SYSTEM ANALYSIS

The SAR defines more than 50 systems which constitute the main operational, safety grade and related support functions of the plant. The scope of analysis of these systems includes Engineering Assessment of the capability of existing systems, assessment of the value of options for removing or reducing non-compliance's and Single Failure Analysis. System analysis is performed primarily to demonstrate compliance with deterministic rules and standards in force in Lithuania and safety practice in the west. Assessment of the value of options forms an important input to the categorization and justification of non-compliance's. Particular emphasis was laid on compliance with the single criterion. An investigation was carried out to determine whether all systems which are claimed as providing protection against faults are able to carry out their functions in the event of any single failure. The procedure to be followed in the work programs required that the vital safety system functions be shown to conform to IAEA Safety Practice [9]. Non-compliance's with requirements for robustness against single failure had to be justified. Additional safety aspects, such as the impact of maintenance, testability, reliability or external events (fire, flooding) on system functions were considered according to Western practice.

The depth of assessment of particular system depends on category of system. The category definitions are as follows:

Category A - These systems are front line safety of mitigation systems, or important process systems. A full Engineering Assessment and Single Failure Analysis was performed for category A system.

Category B - These systems are deemed to be less important than category A systems from a safety perspective, and there assessed in less depth. An Engineering Assessment was performed for each system and includes consideration of single failures.

Category C - These systems are considered less important as category A or B systems, but a separate Engineering Assessment was prepared nevertheless. The depth of the assessment is somewhat less than that for category B systems.

The Engineering Assessment typically comprises the following:

- identification of safety-related and non-safety functional and design requirements based on the review of the system description and relevant Lithuanian regulatory documents,
- identification of relevant regulatory requirements from Lithuanian documents and IAEA guides,
- identification of requirements imposed on system by connected and support systems,
- identification of requirements imposed on the system by other safety-related systems,
- assessment of compliance with the functional and design requirements, with the regulatory requirements, and with requirements imposed by other systems,
- a review of critical installation aspects,
- a review of critical operational issues, including testability, maintainability and system and component reliability,
- a review and assessment of any issues identified at the start of the SAR project,
- an assessment of the differences between unit 1 and 2.

The Single Failure Analysis for a system is performed by identifying in the system, and assessing the impact of, its failure on the safety performance of the system. Recommendations are identified if single failure of a component can impact the ability of the system to meet its safety objective.

The reports of system analysis performed represents significant efforts and form a compilation of issues such as:

- system description, design, operation,
- related functional and regulatory requirements,
- demonstration of capabilities and compliance's with requirements,
- assessment of system and single failure shortcuts,
- consideration of recommendations raised in past studies and missions,
- compilation of non-compliance's and related recommendations.

In order to present a coherent picture of the system analysis performed in the SAR, this Section presents the results integrated according to the following major functions:

- reactor control and protection,
- emergency process protection,
- emergency core cooling,
- accident confinement,
- feedwater and steam supply (normal heat removal),
- support functions.

It is necessary to emphasize that as a general consideration in this work, the international team has performed and reviewed analysis similar to that performed for the Ignalina NPP on nuclear power plants designed to very strict Western standards and criteria. In all cases, issues were identified that required corrective actions. This is not unanticipated. It occurs every time such analysis is performed. In fact, the international reviewers would have been most surprised to have a comprehensive investigation not identify anything that needed to be improved. This is why regulators request NPPs to perform new assessments and investigations - it leads to continuous safety improvement.

4.1.1 Reactor Control and Protection System

The CPS is an integrated system which provides for normal reactor control and power regulation, as well as automatic safety-related reactor shut-down when certain reactor operational limits are exceeded. So, the Control and Protection System serves for dual purpose of reactor power control during normal operation and reactor shutdown under accident conditions. Such a dual purpose system would not be allowably by Western safety authorities. The SAR study of the CPS confirmed the findings from the previous RBMK safety studies that there was inadequate separation of the control and protective functions within the CPS. Specific problems identified includes:

- sharing of common sensors used for both automatic power regulation and initiating emergency reactor shut-down under accident conditions,
- inadequate spatial separation of critical redundant instrumentation and power supply cables,
- physical arrangement of all start-up range instrumentation in one cabinet,
- physical arrangement of all power setpoint devices in one cabinet,
- sharing of common setpoint devices for automatic control and initiation of reactor shut-down,
- inadequate analog signal isolation between circuits used for reactor shut-down and those used for display and monitoring.

The Safety Analysis Report does not make a safety case which justifies the acceptability of the current design of CPS. The design features of the system are only provided in a very limited detail in the system description. This description focuses heavily on the power distribution control and local area regulating systems. Very little description is provided regarding the emergency reactor shut-down provision which effect safety and reliability. The Engineering Assessment was prepared to substantiate the case that the CPS is in compliance with key regulatory requirements. The Engineering Assessment actually produced is based on a very large number of proprietary internal RDIPE technical reports which have not been released for independent assessment. In a number of areas the Engineering Assessment states that regulatory requirements is met. The documentation does not in all cases state how the requirement met. The documentation does not provide an identification of what parts of the regulation there is compliance, specific design features which are not in compliance with regulations, and

the technical justification for allowing continued operation despite the non-compliance's. The Single Failure Analysis is supposed to confirm that no single failures are present that can defeat the functioning of the system. Thus the key documents prepared to demonstrate the safety case fail to identify basic design and operational characteristics, fail to demonstrate how regulatory criteria are complied with, and fail to show that there are not major single failures present in design.

The position taken by SAR was: because the CPS not designed to Western standards, the lack of separation between control and protective function is pervasive, it was proposed that instead of trying to separate the two functions within the existing CPS, a second diverse shutdown system be designed and implemented. This diverse system would provide fast shutdown for all accident sequences and covers all accidents within design basis set for Ignalina NPP. However, such a system requires approximately four years to engineer, install and commission. Ignalina NPP agreed with this proposal.

The RSR evaluated the limited design information contained in the CPS system description, and the SAR Engineering Assessment and Single Failure Analysis. In order to understand the basic design details the RSR conducted two walk-downs of the installed system and met with Ignalina plant personnel involved in operation and maintenance of the CPS. These walk-downs were done without the benefits of any detailed wiring diagrams of the CPS. The Ignalina staff were responsive and they attempted to provide all requested plant documents. The walk-downs, limited as they were due to lack of the wiring diagrams and schematic, confirmed the basic design concerns of the SAR team. The walk-downs and subsequent discussions with plant staff also identified some CPS safety issues not identified by the SAR work. The RSR reject the safety case presented in the SAR submittal on CPS based on the failure to provide the basic design information and supporting information contained in the referenced topical reports which justify compliance with regulatory criteria. The RSR recommended that Ignalina NPP [3]:

- install a trip memory reset button in each of the AZ-1 and FASS trip channels to permit electronically resetting the channels,
- promptly prepare, and submit for VATESI approval, the necessary design and safety information on the CPS which is comparable to that required by any Western nuclear regulatory authority,
- perform and submit for VATESI approval a complete Single Failure Analysis performed from bottom up versus simplified top down approach used in the SAR submittal,
- prepare a safety case justifying continued operation of the existing system based on completion of the above two actions. Such a safety case will identify how the specific design non-compliance's will be dealt with during plant operations, where additional technical specification limitations are warranted, and where other interim measures will be implemented,
- pursue installation of a diverse shutdown system.

The Ignalina Safety Panel holds the view that the most important safety issues in design and operation must be resolved without delay. Among the SAR's recommendations are the installation of second independent shutdown systems at both units, but this would take about 4 years. The Ignalina Safety Panel did not recommend the installation of such system at unit 1 because it is expected to be shut down between 1999 and 2002.

4.1.2 Emergency Process Protection System

The Emergency Process Protection System (ECCS) is an integrated system used to trip or reduce the reactor power for abnormal process parameter conditions. The EPPS is also used to provide for the protection of major equipment. This equipment protection function was not assessed in the SAR because the capability is not credited in the safety analysis. The SAR assessment noted that the major areas of concern are:

- there is a mixture of reactor safety functions and normal reactor operating functions operated by the same circuitry, contrary to Western safety principles,
- there is a lack of physical separation of cabling of the channels which potentially could lead to loss of several trip functions in an area event, such as a fire,
- all circuits in force to trip reactor by AZ-1 use a 40 second latch to seal in a momentary trip condition, which then automatically resets the circuit when the signal is no longer present. This does not allow the operator to investigate spurious or anomalous trips and take corrective action to prevent their recurrence,
- the annunciation system design and operational protocols do not preclude the possibility of a reactor trip function being deliberately disabled without the operator's knowledge.

Very much similar to the case for the CPS, the SAR does not make a safety case which justifies the acceptability of the current design of the EPPS. The design features of the system are only provided in very limited detail in the CPS system description. Very little description is provided regarding the emergency reactor shut-down provision which effect safety and reliability. For the major concerns listed above, the SAR assessment noted the following justification and recommendations for improvement:

- The use of common trip units for protection and control violates Western independence principles. It should be possible to at least segregate into physical trip units, the functions of reactor protection and normal operation. This conditions is particularly noted in the following key process trip functions:
 - * reactor protection for loss of CPS channel cooling,
 - * reactor protection for loss of both turbines,
 - * reactor feeder pipes compartment over-pressure trip,
 - * leak-tight compartment over-pressure trip.

It is recommended that a new diverse and separated trip be installed in Ignalina NPP as a least cost alternative to complete reconfiguring of the existing EPPS.

- The potential loss of several trip functions in an area event such as fire, due to the lack of physical separation of cabling of the channels, is significant. This must be addressed and corrected with high priority.
- The latch with automatic 40 second reset in contrary to Western practice. The SAR team concludes this should be replaced by a permanent latch such as a channeled or parametric trip reset. This would then require the operator to investigate any anomalous channel trips to establish the cause of channel trip and take any corrective actions.
- The annunciation will alert the operator to any deliberate disabling of a detection function even though this loss will not disable the reactor trip function. But, since the alarm system is enabled on the first disabling of a transmitter circuit, means must be developed to detect subsequent disabling of transmitter circuit, so that a reactor trip function cannot be deliberately disabled without operator knowledge.

The RSR underlined that the system analysis of CPS/EPPS were not based on sufficient as built detailed documentation of the system configuration. Reliable Single Failure Analysis were not performed. The recent safety standards of CPS/EPPS raises lots of concerns. Particular weaknesses in system independence (control/protection), lack of segregation, lack of diversity, defects in the operation of the CPS/EPPS (reset procedure, automatic reset function) do not allow RSR to support any statements of conformance to the minimum requested reliability of the shut-down function and actuation of vital safety systems.

The final RSR review of the SAR evaluation of CPS/EPPS resulted in the rejection of the submitted CPS/EPPS safety case based on the failure to provide the basic design information and supporting information. The RSR recommends the Ignalina NPP promptly prepare and submit for VATESI approval, the necessary design and safety information on the EPPS portion of CPS which is comparable to that required by any Western nuclear regulatory authority. This submittal should include a comprehensive safety justification, reliability and single failure assessment, and an integration assessment of the CPS/ECCS. Once the action noted above is complete, the Ignalina NPP should present a safety case to justify continued operation of the current system, which includes additional technical specifications or limitations, where necessary, and any interim measures required to compensate for system design weaknesses during plant operations. This safety case must be submitted for review and approval to VATESI. The RSR also recommends that should the decision be made to install a new diverse shut-down system to complement the existing CPS, Ignalina NPP should perform a comprehensive safety and reliability assessment to document how the EPPS will interface and be impacted by such an installation. This assessment should also include documentation of how the new diverse system may address current EPPS weaknesses. As recommended follow-up actions, the RSR identified the strong need for INPP to:

- perform a complete Single Failure Analysis of the CPS, including provision of all the necessary in-depth supporting documentation to allow VATESI to review the issue. This should include functional block diagrams, circuit schematics, and wiring diagrams,
- perform a detailed assessment of the EPPS reset memory circuits,
- install buttons/circuits to permit resetting of the tripped channels in the CPS,

- perform an engineering assessment, design and testing towards a diverse shutdown system. This includes demonstrating that the diverse system will address identified problems with the existing CPS,
- develop compensatory measures to increase the reliability of the scram function in the short term,
- prepare a safety case justifying limited continuing operation of the existing CPS/EPPS.

4.1.3 Emergency Core Cooling System

The ECCS functions to cool the fuel during LOCAs and some operational transients. The Emergency Core Cooling System works in conjunction with the Main and Auxiliary Feed Water System. The ECCS is supported by several other systems, such as Service Water System, Intermediate Cooling Circuit, Emergency Power System, Accident Confinement System, Parameter Display System, Deaerating and Feedwater Facility, Auxiliary Deaerator Makeup and Demineralized Water System. The adequacy of the ECCS design has been subject of analysis of different SAR teams dealing with system and accident analysis as well as with equipment qualification. The major finding of the SAR was that no single failure of ECCS equipment or equipment in support function would result in failure to meet its safety requirements. In general, the three short-term trains and three long-term trains provide a high degree of redundancy and ensure that there is adequate flow to cool the fuel, although the main and auxiliary feed water pumps may be unavailable as a consequence of the break location or environmental effects. Impairment of the auxiliary feed water pumps can also be caused by a number of different single failures. However, the accident analysis shows that in these cases the accumulators and ECCS pumps provide adequate cooling. Nevertheless, the loss of one short-term train and one long-term train represents a reduction in defense-in-depth.

The SAR considered the overall ECCS design as adequate, provided the agreed upon modifications are implemented. The modifications identified involve mainly initiation logic. The quoted consequential failures have been justified on the basis of the following arguments:

- during all the accident scenarios for which the main and auxiliary feed water weaknesses are expected to emerge, the remaining trains of ECCS pumps or accumulators are considered sufficient,
- more realistic calculations and engineering judgment led to the identification of success criteria for ECCS well below those assumed using calculations performed at the design stage.

The actual ECCS design was found to have more redundancies built in than originally recognized from 3 x 50% to 3 x 100%. This permits reduction or complete elimination of need for supplementary contribution by main or auxiliary feed water, capability to withstand all consequential failures, assumed outages and single failures.

The main recommendations resulting from the assessment of the ECCS and its connected and support systems are as follows:

- Environmental effects may incapacitate the main and feedwater pumps for certain break locations but in these cases the accident analysis shows that adequate cooling after the first 10 minutes can be provided by 4 ECCS pumps. The current Technological Specification [6] permits 1 ECCS and 1 auxiliary feed water pump to be out of service for maintenance, and another pump to be taken out of service for up to 72 hours. If the latter pump is an ECCS pump, and if an additional ECCS pump is assumed to fail due to single failure, there may only be 3 ECCS pumps available. A recommendation has been made to change the Technological Regulation to permit at most 1 ECCS pump being out of service for maintenance.
- There is no automatic ECCS initiation following certain steam line breaks. Fuel failures can occur and activity is released directly to environment. A recommendation has been made to initiate ECCS based on the rate change of drum separator pressure and accident analysis shows that fuel failures are precluded with early ECCS initiation.
- When calculational uncertainties are taken into account in the analysis of partial breaks, fuel failures and possibly fuel channel failures, are predicted because ECCS initiation is not sufficiently prompt to prevent fuel heap-up. A recommendation has been made to initiate ECCS based on low flow in multiple fuel channels. Accident analysis shows that ECCS is initiated promptly on this signal, and predicted cladding and pressure tube wall temperatures are well below the failure criteria. A reactor trip based on this parameter is already being installed, so the recommendation is to extend the signal to initiate ECCS.
- Accident analysis shows that downcomer breaks result in large amount of water accumulating in rooms above the ACS. The drainage capacity is such that large pools of water, which may devolve organic iodides,

exist for long periods of time. In addition, the operator may have difficulty ensuring that the needs of ECCS re-calculation are met because of low drainage rate. A recommendation is made to improve drainage capacity.

- Accident analysis shows that for breaks which affects both loops (e.g., steam line break) oscillation in emergency core cooling flow delivery to the loops can occur. Pressure in a loop increases due to emergency core cooling inflow, so flow is then diverted preferentially to the other loop. Its pressure then builds up, causing flow to go to the other loop. Although adequate flow is maintained, the operator may have difficulty diagnosing phenomena and controlling ECCS flow. A recommendation has been made to provide improved operator training or consider modification that would ensure that emergency core cooling water is delivered to the location where is needed.
- The auxiliary feed water pumps have neither an over-current protection trip in case excessive throughput, nor flow regulation devices to prevent excess flow. Therefore, the response of pumps is indeterminate for certain accidents (feedwater or steam line breaks). In order to ensure adequate defense-in-depth, a recommendation has been made that Ignalina NPP take steps to ensure that the pumps do not burn out due to excessive throughput, by either installing over-current protection or preferably by introducing flow limiters to prevent excessive flow.
- There is a lack of analysis of the dynamic effects on pipework following LOCAs, e.g., waterhammer following check valve closure. A recommendation has been made for Ignalina NPP to request the designer to either provide the calculations or perform new ones to demonstrate the adequacy of the piping system.
- The seismic walk-down of the ECCS identified several areas where improvements are required. Recommendations were made to inspect pump anchors, to replace existing piping anchors with ones connected to structural beams, and to install bumpers to prevent damage due to piping interaction.

All of these recommendations are accepted by Ignalina NPP. The ECCS and AFWS have undergone important modifications during 1996, e.g., the safety injection of water is now directed to the GDHs. The system description and system analysis have not considered these modifications homogeneously. The Single Failure Analysis performed by the SAR have to be characterized as conservative but must be repeated using recent system configuration and actuation.

4.1.4 Accident Confinement System

The ACS consists of a set of structures and equipment, whose main functions are to confine radioactive releases in case accidents and to provide a source of water for emergency water injection to the primary circuit in case of LOCAs. In this last case, part of the steam lost from the break, after condensation, can be used for restoring the water source for ECCS. The geometry of the ACS does not permit a similar reuse of the liquid lost from the break, which is collected in drains and then reused after clean up. As in the other RBMK plants of the most recent generation, the confinement envelopes only parts of the pressure boundary, mostly the parts filled with liquid or located in lower positions. In the design stage, it was decided to envelope only those pipes whose rupture was expected to result in the most significant radiological releases. The main design functions of the ACS are:

- ensure that dose during normal and off-normal plant operation as well as following any design basis accidents do not exceed the dose,
- prevent pressures in leaktight compartments and chambers, in the short-term and long-term, from exceeding specified limits,
- prevent temperatures of concrete structures of leaktight compartments and chambers, in the short-term and long-term, from exceeding specified limits,
- receive and condense steam from the Main Safety Valves in case of over-pressure transients and when MSVs are tested,
- receive and condense steam from SDV-A under normal operation for de-pressurization of the primary circuit and when the valves are tested,
- receive and condense steam released after a break of one fuel channel,
- store a minimum of 1000 m³ of water for use by the ECCS in accident conditions,
- prevent the accumulation of hydrogen to reach explosive concentration level,
- permit periodic sampling of water for analysis of chemistry and quality,
- annunciate alarms in control rooms whenever system alignment or plant parameters are in unsafe positions or outside allowable limits,

- permit periodic testing of functional operability of pumps and valves, the operability of the compressed air system, the leak tightness of reinforced leaktight compartments during periods of preventive maintenance, and absence of clogging of pipes to sprinkler systems.

The primary support and service systems relevant to the ACS that are not mentioned above are:

- Measurement of RBMK-1500 parameters and their display in main control room which is required to provide the operator with information on the status of equipment and conditions in the ACS,
- Electric Power Supply which provides power to pumps and valves in the system,
- Power Supply to Instrumentation and Control Devices which provides power to instrumentation and control devices,
- Auxiliary Deaerator Makeup System which provides a supply of makeup water to the hot condensate chambers of the ACS and can be brought into service manually for long term makeup when there is insufficient inventory in the hot condensate chambers,
- De-mineralized Water System which collects and purifies contaminated water from the hot condensate chambers of the ACS and then returns the water back to the hot condensate chambers and which can be used as an alternative makeup source in the event of failure of the Auxiliary Deaerator Makeup System,
- Service Water System which provides cooling to the ACS heat exchangers when temperature on the shell side exceeds a pre-determined limit and which must provide the ACS with sufficient cooling flow to remove the initial stored energy and residual decay heat,
- Ventilation System which regulates the temperature in ACS rooms containing the ACS pumps and heat exchangers, control cabinets and other equipment needed to perform ACS functions,
- Radiation Monitoring System which monitors radiation level in the ACS and provides a signal to isolate the ACS on high radiation levels,
- Compressed Air System which provides air to the ACS to dilute hydrogen in the event that hydrogen concentration exceeds 0.4 % by volume and compressed air to the siphons for functional tests of the discharge pipe closure and sealing.

A detailed Engineering Assessment and separate Single Failure Analysis were performed for the ACS in the SAR. Separate assessments were performed for connected and support systems. In general, the ACS and its support systems were found to be adequately capable of performing their safety function. Testing of all active components is performed with acceptable test intervals, and is governed by test instructions. Visual inspections both during shutdown periods, when all parts of the ACS and compartments are acceptable, and of critical parts during power operation, are carried out with acceptable scope and frequency. The design of the ACS permits critical parts and components to be maintained as required both during outages and during normal operation. Reliability records shows that the reliability of critical components is consistent with testing performed, and with the test and maintenance intervals.

The main limitation of the ACS in performing the radioactive releases confinement function, as compared to Western compartments, is the limitation of the envelope to part of the primary circuit. This means that ruptures outside of the ACS envelope lead to easy release of radioactive isotopes to the environment. The deficiency in the mitigating capability and in the defense-in-depth concept, is demonstrated to be acceptable for design basis accidents, but does not leave margins for mitigating accidents beyond the design basis, involving possible loss of integrity of pressure boundary outside ACS and multiple failures in ECCS.

Another important limitation is the high leak rate of the ACS, first of all unit 1, mainly attributable to the complex geometries and to the absence of metallic liners on some boundaries. This limitation affects the mitigation capability during design basis accidents and beyond DBAs. Even accidents amongst DBAs might unduly challenge the confinement function due to the leaktightness limitations. Although the limitations outlined restrict its performance, ACS design requirements have to be met in order to avoid exceeding limits to external doses during the loss of coolant accidents inside it.

The significant deficiencies found by assessments are in the area of structural integrity tests and leak rate tests. There have been no structural integrity tests of any of the compartments at pressure equal to either the design pressure or maximum accident pressure. Leak rate tests performed at a pressure of about 2 kPa are too low to permit accurate extrapolation to leak rates at design pressure or maximum accident pressures. It may not be practical to perform structural integrity or leak rate tests at higher pressure, due to leakage from the ACS. Nevertheless, confidence in the ability of the ACS to perform its function under accident conditions needs to be

demonstrated. Additional findings and recommendations have been identified both by the SAR and RSR teams include:

- there is no evidence that adequate analyses have been performed in order to demonstrate the capability of the structures to withstand expected peak pressure during design basis accidents, to verify the strength of the steam distribution pipes and pool structures against expected dynamic loads, or to exclude consequential pipe breaks due dynamic loads induced by LOCAs and subsequent additional loads to ACS,
- there is no evidence that ACS can withstand seismic loads or loads arising from other possible external events (missiles, pressure waves),
- in the Engineering Assessment there are neither reference to analyses nor requirements addressed to the expected simultaneous discharge of steam to the dedicated pool from safety valves (high pressure) and from broken fuel channels (low pressure) in case of loss of coolant accidents in the reactor cavity.

The accident confinement system was not built according the recent regulatory requirements. The need to demonstrate the structural integrity of the ACS to withstand expected peak pressure during design basis accidents still remains. The steam distribution pipes and pools were never verified to withstand dynamic loads.

The above mentioned ACS deficiencies have been recognized as highly safety important and Ignalina Safety Panel recommends to perform safety cases for the ACS before licensing.

4.2 ACCIDENT ANALYSIS

Design basis accidents are events which bound accident categories (e.g. the guillotine break of the largest pipe in a system). The response of the plant to design basis accidents is evaluated using conservative assumptions. The nuclear power plant, its systems, structures and components is then designed to withstand the evaluated loads for such events without releasing harmful amounts of radioactive materials to the outside environment. A set of DBAs is postulated for each type of reactor, covering the consequences of all failure combinations. The following groups of design basis accidents are considered for RBMK-type nuclear power plants [10]:

- Accidents initiated by equipment failures, including loss of flow transients.
- Loss of coolant accidents.
- Reactivity initiated transients.
- Fuel handling accidents.
- Other accidents.

Design basis accidents are classified according to the type of initiating events. A list of initiating events which should be analyzed for each group of DBAs is given in the Subsections which follow.

Depending on the accident sequence, the process used to assess consequences of a particular design basis accident in the Ignalina SAR involves different assessment tasks [2]. If the fuel cladding loses its integrity, a key barrier to a release of fission products is breached, and the coolant in the heat transport system becomes further contaminated by radioactive released from fuel. In turn, the contaminated coolant can be released into the environment by means of normal leakage or by means of accidental discharge either inside or outside of the Accident Confinement System. If the accident does not challenge the fuel cladding and pressure tube integrity, no detailed analysis of other accident issues need to be performed. If there are fuel failures, mass, energy and fission product transport paths must be defined for explicit analysis of radiological consequences. The maintenance of pressure tube integrity is one of the design targets for the design basis accidents. Should a pressure tube fail, it must be shown that the integrity of the reactor cavity is not jeopardized. In addition, for all accidents with mass and energy discharge into the Accident Confinement System, the integrity of this system needs to be verified in order to confirm that the transport path used in analysis of radiological consequences are correctly defined. These steps ensure that, for all accidents addressed in analysis, the compliance with the regulatory dose limits will be demonstrated with adequate confidence.

One of the tasks undertaken in the SAR project was the development of a set of acceptance criteria for each type of accidents [2]. The following acceptance criteria are used in accident analysis:

- fuel cladding integrity criteria,
- pressure tube integrity criteria,

- heat transport circuit integrity criteria,
- reactor cavity integrity criteria,
- ACS integrity criteria,
- permissible doses.

Regulatory document [11] prescribes the acceptable conditions in terms of how many fuel rods can have perforated cladding, and what type of fuel cladding failure is permissible:

- number of fuel rods with perforated cladding is not to exceed 1 % for all the rods in the reactor,
- number of rods that are perforated such that the coolant can come into contact with ceramic fuel is not to exceed 0.1 % of all the fuel in the reactor.

Regulatory document [11] defines also that the peak cladding temperature must not exceed 1200 °C and that the local fuel cladding oxidation must not exceed 18 % of the initial wall thickness. These criteria are pertinent to the maintenance of coolable fuel geometry during an accident and beyond.

Fuel cladding integrity criteria conservatively define the cladding failure thresholds for all fuel cladding failure mechanisms. The following conditions are sufficient to confirm that the fuel cladding integrity is maintained in an accident [2]:

- maximum fuel enthalpy remains below 712 kJ/kg,
- fuel temperature does not reach the UO₂ melting point of about 2800 °C,
- fuel cladding temperature does not exceed 700 °C.

These simplistic criteria are useful for a fast screening of accident analysis results. If these conditions are not exceeded, no further analysis is required to confirm that the accident does not threaten the fuel cladding integrity. If any of these criteria is exceeded, it does not necessarily mean that fuel failures have occurred. It means that supplementary analysis is required. During an accident, fuel cladding can fail due to thermal-mechanical interaction between the fuel and the cladding, or due to thermal deformations of the cladding under positive or negative pressure differentials. The first type of failure is prototypic of rapid and large fuel power excursions where a hot, and possibly molten, UO₂ material may come into contact with the cladding material. The other failure mechanisms are associated with cladding temperature excursion, either when the external pressure is higher than the internal one, or when internal pressure is higher than external one. In first case fuel cladding could fail due to collapses onto the fuel pellet stack and deformation into any gaps between fuel pellets, while in the last case fuel cladding could fail due to ballooning of hot cladding away from the fuel pellet stack. Cladding temperatures at which the failure occurs due to cladding collapse are listed in the Table 1. These failure conditions were quantified for the operating pressure of 7 MPa and the lowest internal pressure within the fuel element as a function of axial gap between the fuel pellets. Cladding temperatures at which the failure occurs due to cladding ballooning are listed in the Table 2.

Pressure tube integrity criteria conservatively define the pressure tube failure thresholds. The following conditions are sufficient to confirm that the pressure tube integrity is maintained in an accident [2]:

- pressure in the pressure tube does not exceed 13.4 MPa,
- pressure tube temperature in any cross-section of its wall does not exceed 650 °C.

If any of these criteria were to be exceeded, the affected pressure tube can potentially fail and supplementary analysis must be performed to establish whether or not the pressure tube integrity is maintained.

The requirement for the integrity of the heat transport circuit is not prescribed by regulations, but has been employed in the Ignalina SAR [2] to avoid complex and costly analyses of accident consequences following pressure boundary failures. The heat transport circuit can withstand three pressure levels. The pressure tubes can withstand at least 13.4 MPa. All fuel channels are hydrostatically tested at this pressure. The piping between the MCP check valve and the pressure header is designed and hydrostatically tested to withstand at least 12.3 MPa. The rest of the of the heat transport circuit piping is designed and tested to withstand at least 10.4 MPa. These test values are applicable to operating temperatures because the ratio of yield stress at the two temperatures is less than 1.4. The lowest of the test pressures is taken to be the acceptance criterion for the accidental pressurization of the heat transport system.

The maintenance of reactor cavity integrity is a derived requirement of acceptable plant response to any accident that involves a discharge of coolant into reactor cavity. Permissible pressure loads on the reactor cavity structures were quantified by the designers of these structures. The permissible loads were evaluated for casing, upper and lower plates. The lower plate can withstand 294 kPa cavity pressure, the casing can withstand 255 kPa cavity pressure. The lowest pressure value corresponds to conservative estimates of pressure needed to lift the upper plate. Cavity pressure exceeding 214 kPa has been described as having possibility to lift the upper plate breaking the reactor seal, the pressure tubes, and affecting the operating of other safety functions. The smallest of these loads is taken as a conservative criterion for maintaining the integrity of the reactor cavity.

The Ignalina NPP is protected against accidental discharges of contaminated coolant by an Accident Confinement System. In accident analysis the maintenance of ACS integrity is a derived acceptance criterion. An acceptance hydrogen concentration in any ACS compartment is taken to be 4 % by volume.

Table 1 Temperatures of failure by cladding collapse at P=7 MPa [2]

δ , mm	2	4	6	8	10	14	20
T, °C envelope	1300	1300	1280	1260	1240	1120	900
T, °C onset	1200	1200	1180	1150	700	700	700

Table 2 Temperature of failure by cladding ballooning [62]

ΔP , MPa	1.0	2.0	4.0	6.0	8.0
T, °C envelope	1000	830	800	790	780
T, °C onset	850	730	700	700	700

The regulatory dose limits are taken to be the key criteria of acceptance. Permissible radiological doses to the population after an accident are defined by [12] as follows:

- whole body dose to a member of the population not to exceed 50 mSv,
- critical organ, i.e. thyroid, dose to member of the population is not to exceed 300 mSv.

For design basis accidents, the doses are to be accumulated for a period of one year after the accident at and beyond the Ignalina NPP exclusive zone, i.e., beyond a 3 km radius from the plant. In analyses of design basis accidents doses are evaluated by conservative analyses that assume:

- fission products escaping from the plant are released as a single “puff” at the elevation appropriate to the postulated accident,
- least favorable meteorological conditions are assumed,
- a critical individual, i.e. child, is assumed to remain at the boundary of the plan exclusion zone indefinitely.

One of the requirements for the accident analysis is to account for the effect of single failure in the accident analysis. The single failure criterion is defined in the IAEA Code of Practice on Design [13]. In order to comply with IAEA practice, analyses would ideally be performed as follows:

- assume that each mitigation system is operating at the start of the accident, with as much equipment out of service as is allowed by the operating procedures,
- perform the accident simulation assuming that all systems operate as described above plus assume that one component of the system has failed,
- repeat the simulations as many times as necessary, each time assuming a different single failure of one component of one system,

- evaluate consequences of all cases and select that which produced the worst consequence.

This ideal approach is difficult to apply in practice and in order to meet the intent of [13] a conservative approach was adopted in the Ignalina SAR project:

- assume that all mitigating systems with equipment credited in the analysis simultaneously experience a single failure of one of its components when the component is called upon to act,
- if the analysis with the plant configuration assumed above produces results which meet the acceptance criteria, no further analysis of this accident sequence is required. However, if the results indicate a non-compliance with acceptance criteria, it is permissible to analyze a less conservative progression of the accident sequence. This less conservative analysis can be achieved by assuming that one or more systems operate in a manner consistent with operating limits, as opposed to having all mitigating system failed simultaneously,
- additional failures of mitigating systems caused as a consequence of initiating event are taken into account.

The analyses evaluate two initial plant states: Design Reference state where all processes and protective systems function as designed, and a plant state where a failure is assumed in each system that is active during the Design Reference accident. This last state is referred to as the Multiple Failures (or Limiting) Plant state.

In addition to the rules for evaluating the effect of single failure for each initiating event, the following deterministic rules are also applied in accident simulations:

- the most effective absorber rod is assumed to be unavailable,
- the second trip parameter is credited in accidents where two parameters are available. Where the second parameter is not available, it must be shown that a sufficient time is available from manual intervention following an unambiguous annunciation of the accident in control room,
- in order to cover any undetected failures in the signals or trip activation logic, where the system has 2 out of n logic, the trip is credited when last signal is reached.

4.2.1 Accidents Initiated by Equipment Failures

All accidents initiated by equipment failure occur in the intact heat transport system. Therefore, the following issues are relevant to this family of accidents:

- an imbalance between the heat generation in the reactor core and the convective heat removal from the core if and when the forced circulation is lost or impaired,
- a pressurization of the heat transport system if and when the turbines are disconnected,
- a long term coolant makeup to the heat transport system if and when the main heat sink is lost.

Some accidents in this group are subject to only one of the above issues, e.g. a pump power seizure concerns only the issue of the power-cooling mismatch in the channels. Other accidents encounter several above issues simultaneously, e.g. a loss of AC power supply encounter a loss of circulation as well as pressurization. The equipment failure accidents addressed in SAR are as follows:

- single MCP trip,
- multiple MCP trips,
- MCP seizure,
- loss of normal AC electrical power supply,
- turbine generator trip,
- loss of main heat sink,
- loss of feedwater,
- grid frequency reduction,
- spurious opening and failure to re-close of the main safety relief valve.

However, in accordance with regulatory requirements [10] the following accidents initiated by equipment failure should be also analyzed:

- break of GDH check valve disk,
- break of disk of MCP check valve or main gate valve,

- reduction or loss of flow in one fuel channel,
- complete station blackout,
- failure of feedwater system.

Consequences of all the accidents initiated by equipment failure are explored by three cases that are simulated explicitly: MCP seizure, loss of AC power and loss of feedwater supply. The remaining accidents are assessed qualitatively. It is explained how these latter cases relate to the simulated cases, or it is shown that adequate provisions are available in the current plant to make the accident benign.

For the pump failure cases the automatic power reduction is the only required mitigation action. Analysis of the most severe conceivable power-cooling mismatch shows that cladding dry-out is avoided. A combination of a timely power trip, a pump costdown, and relatively early ECCS water injection maintains the cladding and pressure tube wall temperatures below their initial values for accidents that involve a global impairment of forced circulation, i.e. a loss of AC power and a loss of feedwater supply. There is no potential for power-cooling mismatch in accidents that maintain forced circulation, e.g. turbine trip and loss of main heat sink. The accidents that lead to an impairment of steam removal from the heat transport system, i.e. loss of AC power, loss of turbines and loss of heat sink, activate the MCC over-pressure protection system. The SAR analysis shows that this system is adequate, if the timely power reduction is given.

The SAR analysis shows that the reactor power is reduced in a timely manner in all accidents initiated by equipment failures. Either power setbacks AZ-3 or AZ-4, or a trip AZ-1 are performed by the CPS on signals by the EPPS. There are at least two EPPS signals issued in close succession, based on diverse process parameters. Hence, reliable signals are available to activate the reactor power reduction.

The short-term ECCS is not activated in any accidents initiated by equipment failures because there is no break in the MCC to produce the necessary conditioning signal of high pressure in one of reinforced leak-tight compartments. However, the long-term emergency core cooling function is activated quite early in accidents that involve an impairment of steam removal or feedwater supply. The long term emergency feed water supply is preferentially provided by the AFWPs drawing hot water from the deaerators. If AFWPs cannot provide this emergency supply, the ECCS pumps, already running in a re-circulation mode, supply “cold” water from the condensate chambers in the ACS. No automatic system is available to regulate the emergency water supply in the long term, and to establish a long-term heat sink for the removal of decay and stored heat. These functions are performed by operators. Analysis shows, that adequate time is available to initiate the manual operator actions.

Thus, results of analysis show, that the class of events included under accidents initiated by equipment failures are unlikely to cause power plant conditions that would result in violation of the design criteria to avoid fuel damage, maintain integrity of pressure boundaries, and not exceeded regulatory dose limits. The existing protective system at the Ignalina NPP are adequate to bring the plant into a safe state following all accidents initiated by equipment failures.

4.2.2 Loss of Coolant Accidents

Pipe breaks in one of the two main circulation loops, the service water system and purification and coolant system as well as steam and feed water line breaks are classified as loss of coolant accidents. The full range of loss of coolant accidents have been assessed. Piping breaks resulting in a loss of coolant from the circuit may occur within the reinforced leak-tight compartments of the ACS or in compartments that are connected to the outside environment. In accordance with regulatory requirements [10] the following loss of coolant accidents should be analyzed for nuclear power plants with RBMK-type reactors:

- break of MCP header or pipeline (e.g., full break of MCP pressure header),
- break of a group distribution header downstream and upstream of check valve,
- break of steam separator downcomer pipe,
- main feedwater line break,
- main steam line break,
- break of water communication line,
- break of steam-water communication line,
- break of pressure tube,
- break of service water pipeline,

- break of purification and cooling system pipeline.

The LOCAs addressed in the SAR include the following accidents:

- full break of the MCP pressure header,
- full break of the GDH downstream of the check valve,
- full break of steam separator downcomer pipe in drum separator compartments,
- partial breaks in a GDH downstream of the check valve which can lead to flow stagnation conditions,
- partial breaks in the pressure header which could potentially lead to stagnation conditions,
- full feedwater line break,
- full steam line break in different compartments.

The SAR concluded that the Ignalina NPP is quite well protected against the breaks that occur in the reinforced leak-tight compartments if they do not result in local flow degradation. A prompt activation of the ECCS occurs for breaks with large discharge rates and for breaks with coincident failures that impair global circulation. However, the emergency core cooling system activation is not fast enough to ensure that dangerous, early temperature excursion do not occur following partial breaks in one GDH. However, note that if local deterioration of channel cooling occurs during this LOCA scenario, the contaminated coolant discharges to the ACS. Analysis also shows that four emergency core coolant pumps, i.e. either the ECCS pumps, or the AFWPs, are sufficient for adequate long term cooling.

In the LOCA scenarios analyzed, the peak fuel temperature did not exceed 1200 °C, and the fuel cladding oxidation did not reach the maximum allowable levels. The fuel cladding failure criterion of 700 °C is exceeded in the following LOCA scenarios: full break of the pressure header accompanied with multiple failures, full break of the GDH, and partial break of the GDH. Analysis shows that, except for the last case, the fuel cladding failure criteria are violated for only a very short period of time during the initial phase of accident. Thus, fuel cladding failure is not expected in the first two cases. In the LOCA scenario with flow stagnation conditions in one GDH, fuel elements could fail in several channels. Design modification to improve the activation of the short-term ECCS was recommended and accepted by the Ignalina NPP. This improvement would be implemented during implementation of the SIP-2.

The SAR analysis shows that for all LOCAs which occur inside the reinforced leak-tight compartments, pressure tube temperatures do not exceeded the failure criterion of 650 °C. Results of analysis also states that for all breaks inside the reinforced leak-tight compartments, the existing prescribed public dose limits would not be exceeded. However, for breaks outside the ACS, especially for main steam line breaks, peak cladding and pressure tube temperatures as well as doses could exceed acceptance criteria. The main reason of this is that breaks outside of the reinforced leak-tight compartments do not trip the reactor nor do they activate the ECCS. Violation of acceptance criteria could also result due to a large number of pre-existing cladding failures permitted during normal operation, and due to a limited drainage capacity in the vented compartments. The SAR analysts propose a number of hardware modifications and changes in regulations and procedures to overcome the design weaknesses and to better protect the surrounding population against radiological exposure after steam rupture events. First of all an additional early reactor trip and emergency coolant injection for all break locations, based on the dP/dt measurements in steam separators should be installed. This modification will be implemented in the immediate future at the Ignalina NPP. The SAR also recommended as a safety enhancement measure to keep the number of pre-existing fuel rod failures as low as achievable. Means to rapidly remove the contaminated water from compartments that are in direct communication with the environment will be developed and implemented.

Downcomer breaks outside the ACS do not result in violation of safety criteria. However, reactor hall over-pressure protection may not be sufficient to prevent the release of contaminated coolant to the environment and provisions to improve the reactor hall over-protection will be installed during implementation of the SIP-2.

4.2.3 Reactivity Initiated Accidents

Reactivity initiated accidents are accidents which are induced by postulated faults in the CPS. In accordance with regulatory requirements [10] the following reactivity initiated accidents should be analyzed for nuclear power plants with RBMK-type reactors:

- continuous single rod withdrawal,
- continuous rod bank withdrawal,
- rod ejection,
- rod drop,
- faulty actuation of reactor emergency protection,
- refueling error including improper fuel placement,
- inadvertent emergency core cooling system actuation,
- voiding of or gas ingress into control rod channel cooling system.

In the SAR the following cases were analyzed:

- withdrawal of a single rod in the center of the core and at the periphery at full power (4200 MW) and during start-up (240 MW),
- withdrawal of a group of three rods in the center of the core at full power and during start-up,
- voiding of CPS including:
 - * loss or interruption of water supply to the upper storage tanks,
 - * various CPS coolant flow blockages,
 - * air entrapment in the CPS circuit following outage.

Initial conditions have been defined to account for most unfavorable operational conditions. Perturbed axial and radial power distributions have been defined which maximize the effect of the reactivity insertion. For dynamic simulations, power setback signal, the first neutronic trip signal and any trip signal based on process parameters were neglected.

For the single rod or group of three rods withdrawal accidents both at full power and during start-up no safety problems arise because the absolute power remains low and the maximum values of key safety parameters are maintained well below their limiting values. The analysis covers reactivity insertion for high and low rod worth's. The consequences of high reactivity insertion are limited due to the generation of early trip signals, which terminate the transient earlier than in cases with low reactivity insertion. Also, neglecting the first shutdown signal does not create problems concerning the safety limits.

Total voiding of the CPS channels in the reactor at operational conditions can cause a reactivity insertion of up to 4-5 β . The highest reactivity insertion is obtained for low values of the operational reactivity margin, i.e. when most of the rods are withdrawn from the reactor. The worst case of CPS voiding is a loss of coolant above the reactor core, producing a draining of all CPS channels. The water level in the channels decrease by gravitational forces, thus the process is not very fast. Due to different types of control rods and different control rod insertion depths, the flow velocities differ significantly in the different channels. Thus, the reactivity insertion is non-uniform in the CPS channels. In addition, the reactivity insertion is not very fast. The fastest possible complete voiding of CPS channels in the core occurs in about 10 seconds, while the slowest voiding occurs in about 50 seconds. Multiple scram signal are generated and if the reactor shutdown function is available on demand, no safety limits are exceeded.

Assessments of reactivity initiated accidents show that the Ignalina NPP is adequately protected against this type of accidents. The fuel channels remain adequately cooled both in cases where all systems operate as designed, and when additional equipment or component failures are postulated to coincide with the initiating event. Multiple signals are available either to reduce the reactor power or to shut down the reactor. The main issue is detector coverage, which is shown to be adequate for central and peripheral, single and multiple control rod withdrawals as well as CPS voiding accidents. The single failure criterion is applied through the loss of signals due to the loss of one detector group of six. The loss of a group of detectors does not significantly impact detector coverage because there are many redundant signals based on the remaining detectors, i.e. acceptable consequences are obtained whether or not these signals are available.

4.2.4 Anticipated Accidents Without Scram

Anticipated Transients Without Scram (ATWS) are accident sequences involving a non-LOCA transient of moderate frequency (about 1.0/ year, e.g. turbine trip) or infrequent incidents (about $3 \cdot 10^{-2}$ /year, e.g. reactivity events) and failure of automatic reactor scram. Major objectives of ATWS analyses are to demonstrate that the pressure boundary of the reactor coolant will not fail, the pressure suppression system will not fail, safe long term

shutdown is reached and heat removal capacity is sufficient. The ATWS are commonly considered as design basis accidents or as accidents to be dealt with in the licensing process for Western reactors. For RBMK reactors ATWS are not design basis accidents and no previous analyses of such accidents were performed. The ATWS studies in the Ignalina SAR are the first of the kind for RBMK reactors. These analyses have a different purpose from DBA studies. The purpose of the ATWS studies in this project is to identify the need for possible future design modifications to the shutdown system, to determine the minimum time available for accident mitigation and to make a step towards developing accident management measures and procedures. The ATWS scenario can lead to unacceptable consequences. The failure probability of the overall scram system is the major concern at Ignalina NPP. According to the assessment the failure probability may be $4 \cdot 10^{-4}$ per demand or higher. The magnitude of this failure probability highlights the importance of the ATWS issue for Ignalina NPP. Four different Anticipated Transients Without Scram were addressed in SAR:

- maximum reactivity insertion by continuous single rod withdrawal at full power and during start-up,
- partial loss of flow due to MCP failure,
- loss of main heat sink (loss of both turbines with loss of condenser vacuum),
- loss of preferred AC power.

The analyses were carried out using the following initial and boundary assumptions: All systems that affect the reactor power and are not active during normal reactor operation are assumed unavailable. This applies to the 24 FASS rods, 24 LSR rods and the CPS operation modes BAZ and AZ-1. All systems active during normal operation remain functional during the accident as long as they are not affected by the consequences of the accident, e.g. LAC system, pressure and level controllers. Systems that do not affect the reactor power and are poised to be activated by the accident, e.g. relief valves, ECCS, are assumed available. The base-case simulation is performed until one of the following conditions is reached:

- the plant achieves a new steady state,
- acceptance criteria are violated,
- conditions are encountered in the simulation that cannot be reliably described by the available mathematical models.

Results provided by the base-case simulation include list of all available scram actuation and power set-back signals as well as the minimum time available for accident mitigation. The issues addressed in the analysis include:

- the ability of fuel channels to withstand a local power rise due to rod withdrawal and sensitivity of protective systems for this postulated events,
- thermal-hydraulic stability under reduced flow rates and high power levels,
- rate of pressure rise when steam generation rates exceed steam relief rates,
- time necessary for reaching critical values of safety parameters,
- plausibility of effective operator intervention.

The following conclusions were drawn regarding the ATWS sequences for the Ignalina NPP. Continuous withdrawal of one control rod with ATWS from full power are controlled by local automatic control/protection system. Total reactor power is kept nearly constant, while the maximum local power excursion at full power was 175 %. Detector coverage is such that the reactor setback or trip signals are generated within about 10 and 16 seconds of the start of rod motion for start-up and full power levels, respectively. Redundant trip signals are generated within a short time span, so single failure of trip signal are inconsequential. At powers below the normal operating range acceptance criteria in fuel channels are not violated.

Failure of one MCP is inconsequential because the flow from the operating pumps compensates for the trip of 1 out of 3 MCPs in one circulation loop. The local automatic control/protection system maintains the plant within a safe range of operation. Flow instability is not encountered even when the power is not reduced. The acceptance criteria for fuel and pressure boundary are met. This conclusion applies to the whole normal operation range from 1000 MW to 4200 MW. There is adequate time for operator action.

During reactor operation at full power a turbine trip with loss of main heat sink leads to failure of the pressure boundary within about 3.5 minutes (likely between core outlet and MCP suction header) because steam production exceeds the steam removal capacity of 2 SDV-A and 12 MSRVs. Total reactor power is maintained nearly constant by local automatic control/protection system. However, eight different power reduction signals were

identified before pressure boundary failure. Effective operator intervention, i.e. manual scram is possible. If this ATWS were to occur at some steady state operation power level higher than 2650 MW, the sequence of event will remain the same, only there will be more time available for operator intervention. The relief capacity is sufficient at reactor power level below 2650 MW, so the manual scram is a highly probable terminator of transient, since long delay can be tolerated.

Loss of preferred AC power results in constant reactor power due to functioning of the local automatic control/protection system. Due to costdown of the MCPs and loss of main feedwater steam production rises considerably and will be in excess of the steam removal capacity of the 14 discharge valves (2 SDV-A and 12 MSRVs). Flow instability could occur after 10 seconds and dangerous cladding and pressure tube wall temperatures after 40 seconds. The acceptance criterion for main coolant circuit pressure of 10.4 MPa is violated after about 1 minute. Multiple pressure tube ruptures are likely to occur. Although the operator may be able to manually insert control rods, this may not prevent a pressure boundary failure.

The results of ATWS studies demonstrate the lack of inherent safety features in the RBMK design. The power is not reduced by means of inherent physical processes such as steam generation. The reactivity loss due to fuel temperature rise (Doppler effect) is not effective enough to prevent major damage of the core. The local automatic control/protection system assumed available under analysis rules turns out to be detrimental in some cases since it tries to maintain the power level.

The apparent lack of the effective inherent safety features in RBMK reactors leads to one high priority recommendation, that a second fast acting, independent and fully diverse reactor shutdown system needs to be installed. The second shutdown system has to be designed to ensure its functionality at conditions prevailing during and after the accident, and to provide safe long term reactor shutdown. Development of second reactor shutdown system is under progress, but its implementation requires 3-4 years. Compensatory measures which have the potential to reduce the overall risk are implemented at Ignalina NPP until a second shutdown system is in place.

5. FOLLOW-UP SAFETY ANALYSES

In the view of the results of the accident analysis, assessment of capabilities of the existing systems and of safety management practices produced in the SAR [2], and with expeditious implementation of all of modifications, procedures, and processes identified in the report, the SAR team supported the Ignalina NPP management convincing that:

- an adequate safety case for continued operation of Ignalina NPP had been demonstrated,
- the safety case would be adequate to the point of first gas gap between pressure tubes and graphite stack closure, which would be the life-limiting factor, and
- the plant's safety standards and practices had been assessed and recommendations for improvements had been made and accepted by the Ignalina NPP.

Recommendations for safety enhancement measures stated in the SAR [2] include not only hardware implementation at the Ignalina NPP but also further analysis to be performed. The most important recommended safety analyses are as follows:

- Safety Case for CPS/ECCS
- Safety Case for the structural integrity of the ACS
- Safety Case for the structural integrity of the Reactor Cooling Circuit (RCS), including assessment of waterhammer effect on ECCS/GDH check valves and connected pipelines
- Support analysis for the compensatory measures for CPS deficiencies
- Justification of omission of an assessment of accident at shut-down reactor
- Justification for category of accidents initiated by equipment failure omitted from analysis
- Analysis of reactivity initiated events for core with new fuel design
- Safety Cases in support for the implementation of early reactor trips and ECCS actuations (based on low flow in one GDH, low reactivity margin, and dP/dt in steam separator signals)
- Partial ATWS analyses
- Accident analysis in the long term including accidents during reactor shut-down, internal area events and external events
- Strategy for local flow degradation in intermediate and long term development

Some of these analyses are already completed, development of others are under way. Below are presented brief summary of analyses completed recently.

5.1 SAFETY CASE FOR CPS/ECCS

Ignalina NPP has been fully responsive to these recommendations and initiated the effort to perform a detailed and comprehensive Single Failure Analysis [14] and prepare a safety case. The work was performed by a team of analysts from the Lithuanian State Information Technology Institute, with significant technical input from the Instrumentation and Control Department at Ignalina NPP, and with external guidance from Swedish experts (ES-Konsult AB). The scope of the analysis produced focuses (as originally intended) on single failures arising from internal faults within the CPS-EPPS-TITAN systems and associated support systems (e.g. power supplies, ventilation). Very detailed analysis has been performed to find out whether failure of a single component could cause a loss of safety function. Due to potential for severe consequences the shutdown function is of utmost importance. External faults (such as fire and seismic) while acknowledged to be important, are being dealt with via other Ignalina safety improvement program [15] efforts currently under way and are not as extensively dealt with in the study.

The review of this study consisted of detailed review of the Single Failure Analysis documentation by a team consisting of members of the original Ignalina RSR team including experts from the Ignalina Safety Analysis Group and Western organizations. Summarizing the major conclusions and findings [16]:

- The review found that the Single Failure Analysis (SFA) was carried out in compliance with the recommendations of the RSR and Ignalina Safety Panel (ISP) and used the required IAEA safety guides and standards. The study considered 21 postulated initiating events which place a wide spectrum of demands on the proper functioning of the CPS/EPPS. The RSR reviewers looked at CPS/EPPS logic dealing with all 21 PIEs. The 21 PIEs chosen, were developed from the list used in the Barselina PSA Report [4]. The body of the analysis systematically looked for undetectable (latent) faults and documented the results via failure modes and effects analysis tables. The RSR reviewers were provided with all documentation requested, and answers to all technical questions, and were able to duplicate much of the analysts work. This provided high confidence in the integrity of the analysis.
- Original RSR concerns [3] regarding safety impact of AZ-1 reset logic and EPPS 40 second logic pulse/reset have all been fully resolved and the reviewers conclude there are no single failures or safety concerns.
- The RSR review of the SFA identified the issue of non-compliance with current standards [17] for analog signal isolation between CPS measurement channel signals and the TITAN system. This was expected from past safety reviews of RBMK-type reactors. The SFA clearly notes that the current analog signal interface circuits are designed to preclude a fault originating in the CPS from propagating back to the TITAN system. The circuit design uses only a 1k Ω resistor to isolate the CPS from faults originating in the TITAN system. This design is not in conformance with generally accepted Western nuclear safety standards [17]. The interfaces between CPS/EPPS and TITAN involve circuits of an older design which do not possess current day analog signal isolation devices. However, based upon information provided by the INPP it is clear that the impacts of such adverse interactions will be no more severe than the loss of a single CPS/EPPS channel - in the worst case. In view of this, the RSR reviewers have concluded the design meets the single failure criteria and is acceptable. The RSR reviewers, however, recommend that future modifications designed to improve the reliability of the CPS/EPPS (such as the DAZ system being implemented to address one of the RSR recommendation) address the most current industry standards for analog signal isolation.
- The RSR review of digital signal isolation based primarily on solid state optical isolators is acceptable and is in conformance with generally accepted Western nuclear safety standards.
- The physical separation between inputs and isolated outputs on the Relay Type "RES 8" is not in conformance with generally accepted Western nuclear safety standards. This lack of physical separation is not a new issue. The RSR review of digital signal isolation based on conventional relay circuits concludes their usage is marginally acceptable.
- The EPPS logic extensively uses "energize to trip" logic, whose availability is significantly less reliable than "de-energize to trip" logic typically used in Western designed NPPs. The availability of "energize to trip" logic, whose failures are not self-annunciating, is very sensitive to the thoroughness of the testing programs designed to detect latent faults. In this area, the Single Failure Analysis results are very sensitive to assumptions regarding the adequacy of the testing programs. The RSR reviewers performed a limited review of the test procedures for the most sensitive logic (e.g. loss of off-site power) and found that INPP

apparently has sufficiently comprehensive programs in place in this area. The RSR reviewers were not able to completely review all areas - but from what was observed have confidence such programs exist and that these are being carried out at a frequency specified in the Technical Specification [6]. This was verified by a sample review of INPP testing records. The issue of “energize to trip” logic was thus concluded to be resolved as far as single failures are concerned. The RSR reviewers, however, recommend that future modifications designed to improve the reliability of the CPS/EPPS utilize “de-energize to trip” logic.

- The RSR reviewers thoroughly reviewed all 21 postulated initiating events evaluated in the CPS/EPPS Single Failure Analysis. This included detailed technical review of the submittal materials, issuing requests for further back-up documentation and schematics, and meeting several times with the analysts who prepared the study. Based on these reviews and the further responses provided by the INPP, the RSR reviewers concluded that the SFA submittal demonstrates that there are no single internal failures capable of defeating the overall CPS/EPPS functioning for the Postulated Initiating Events.
- An electrical interface circuit related single failure mode was identified in the course of the RSR review, which is potentially capable of defeating the proper functioning of the CPS/EPPS for two postulated initiating events. The circuits in question are a series of coincidence circuits (“TEZ K” modules) taken from un-isolated redundant trip channel local coincidence signals. They are brought together at one point for the purpose of performing cross-channel checks on the failure of AZ-3/AZ-4 (PIE 14) and local emergency protection (PIE 15). The coincidences were installed for diagnostic/alarm purposes - but a fault on the “TEZ K” module circuit board integrated circuits will fail all trip channels used. The un-isolated circuits were only found on the logic for protection against PIEs 14 and 15, and there is no indication the problem is present on logic for protection against other PIEs. The RSR reviewers thus recommend that Ignalina NPP study this circuit further and recommend a suitable measure to eliminate the potential single failure in this area.

The review concluded that the Single Failure Analysis was a thorough, comprehensive analysis which exhaustively pursued the existence of potential single failures capable of defeating the overall functioning of the combined CPS/EPPS. The effort which was carried out by Ignalina NPP and their contractors was fully responsive to the recommendations of the RSR and Ignalina Safety Panel and has increased the level of confidence that the CPS/EPPS constitutes a strong line of defense. Such confidence could not be demonstrated without carrying out this work. While the reviewers conclude that the examination of the CPS/EPPS was comprehensive, this must not be interpreted to imply that the reviewers can state with absolute certainty that there are absolutely no other single failures present in the CPS/EPPS design. The reviewers do believe that there are no other obvious single failures which have not been considered based on the design information reviewed. During the course of the review, several single failures were identified and the Ignalina NPP is addressing the resolution of these. This outcome is not unexpected and is typical to safety investigations performed and reviewed for nuclear power plants throughout the world. The work was done under considerable time pressure and there was no time for the reviewers to validate all of the information of the plant that was used in the analysis. Of the single failures identified, only one was found to be potentially able to fail a system. However, justification was made by Ignalina NPP that an immediate solution is not necessary. This was supported by several arguments: the low probability of the relevant initiating events, the low probability of the single failure, very mild consequences of possible transient and the reasonable likelihood of compensating operator actions due to the slow development of the consequences. VATESI’s conclusion is that operation of the plant for short term time is permissible, but that a systematic approach to a physical resolution is required. Required hardware modification have been installed at during 1998 outage.

5. 2 SAFETY CASE FOR INTEGRITY OF THE ACCIDENT CONFINEMENT SYSTEM

The purpose of the project was to perform a detailed structural analysis of Ignalina NPP ACS. The realization of calculations of strength of ACS structure was demanded by the Panel of Safety of Ignalina NPP, on the basis of the recommendations SAR [2] and RSR [3]. Such analysis usually covers all design accidents and is an obligatory component of western SAR. For the performance of these requirements were formulated the following purposes:

- Documenting and verification of the project of system.-Reconsideration of the descriptions of systems, which were performed in SAR
- Reconsideration of design calculations, which were performed by Sverdlovsk and calculations of Ignalina NPP ALS structural integrity, which were performed by Lithuanian Energy Institute earlier
- Planning and realization of test on ACS density of Units 1 and 2, performance of measures for reduction of the leak, especially, for the unit first

- Planning and realization of check of reinforcement bars for the most loaded constructions of ALS compartments
- Performance of the analysis of structural integrity on the real data of reinforcement bars and design pressure
- Documenting and check of an assessment of distribution of fission products on ACS compartments
- Performance of calculations of doses for design basis accidents

The complex analysis of safety of Ignalina NPP ACS, including analysis of experience of operation, engineering assessment, thermal-hydraulic and structural analysis is performed. The obtained results of calculations, results of the performed non-destructive testing and carried out experimental tests on an determining of the mechanical characteristics of concrete and reinforcement bars have not revealed essential lacks which because of would be impossible the further operation of ACS of Ignalina NPP unit 1. The structural integrity of ACS during maximum design basis accident by results of the nonlinear analysis will not be violated. For increase of a level of safety of ACS the recommendations is given.

5.3 SAFETY CASE FOR INTEGRITY OF THE REACTOR COOLANT SYSTEM

The main objective of the Reactor Cooling System Safety Case is to perform the detailed structural analysis of the MCC of Ignalina NPP according to the requirements of the Safety Panel of Ignalina NPP, expert groups of SAR and RSR. For performance of these requirements the following purposes are formulated:

- Development and documenting, determination of limits of the MCC and in-service inspection of the MCC;
- Development of the list of priority problems, which should be solved in the course of the project. Drawing up of the list of critical components of the MCC;
- Documenting and checking of the project of the system. Review the descriptions of systems developed in SAR by the Task Group 1;
- The analysis of the program and the results of the in-service inspection;
- Review of the original design stress calculations;
- Strength and integrity calculations of pressure tube;
- Performance of the structural analysis of the MCC of Ignalina NPP based on the real data and detailed consideration of the requirements of the in-service inspection;
- MCC components finite element stress analysis according to ASME requirements;
- Assessment of the waterhammer effect on ECCS/GDH check valves and connected pipelines.

The most important conclusions on the reactor cooling system safety case of Ignalina NPP are discussed below. In the case of discrepancy to the requirements of the regulating documents are given the recommendations for their elimination.

- The results of the performed finite element analysis of Ignalina NPP reactor cooling system critical components according to the ASME III subsection NC under the conditions of normal operation, hydraulic tests and maximal calculational earthquake show, that there exist the sufficient safety margin of the strength and strength. Thus, their conformity to the categories of the design and operational criteria of ASME III requirements is shown.
- Non-fulfillment of the nonductile fracture criteria was obtained for the postulated corner crack in downcomer nozzle in the regime of pressing, carried out when temperature is 55 °C. Relating to this, it is necessary to prepare technical conditions for the performance of pressing of MCC having the increased temperatures and to develop the technical means for the non-destructive control of the possible defects of such type.
- The maximal bending stresses during the seismic influence resulting from the maximal calculational earthquake existing in the central (side) supports of the drum-separators, are received in the result of linear calculations, exceed the allowable value 2,59 times. It means, that the axial moving of the drum-separators will result in plastic deformations in the central (side) supports. The conservative linear calculations were performed for the potential failure of the horizontal support, when the calculational stresses in the most loaded downcomers do not exceed the ultimate strength of the material. On the whole the structural integrity of the construction of supports of DS can be considered as being acceptable.
- For the conditions of the hydraulic tests of the feedwater nozzle, do not satisfy ASME III subsection NB requirements for primary membrane local stresses P_1 . They by 29% exceed the yield strength of the material and equals to 59 % from the ultimate strength in hydraulic test temperature. These membrane local stresses are located in the middle of the wall. In the most loaded places of a nozzle appear plastic deformations and

these places can be subjected to a low-cyclic fatigue. It is recommended to carry out the calculation of the DS feedwater nozzle for low-cycle fatigue.

- Because of the fact, that during the hydraulic tests the overload of a DS nozzle (feedwater nozzle) was obtained, it was recommended to reconsider an opportunity to reduce frequency of realization and/or the pressure of hydraulic tests.
- During waterhammer event on ECCS/GDH check valve, stresses in the elbows of the pipelines of lower water communication pipelines (LWCP) will cause plastic deformations. In a case of waterhammer on the check valve of GDH it is necessary to perform the control of LWCP end connected to pressure tube and the elbows of the pipelines of LWCP, and the connection of LWCP to pressure tubes.

The carried out complex analysis of the most important for safety components of the reactor cooling system of Ignalina NPP has not revealed shortcomings, which could become the reason for not allowing the further operation. The RBMK-1500 reactor cooling system of Ignalina NPP principally corresponds to ASME standards.

5.4 SAFETY CASE FOR ADDITIONAL REACTOR SHUTDOWN SYSTEM

A good example both of significant safety improvement in frame of implementation of SIP-2 and state-of-the-art codes applications for safety management of Ignalina NPP is development and implementation of an additional shutdown system DAZ. In accordance with this Ignalina Safety Panel recommendation VATESI has required Ignalina NPP to develop and implement a compensatory measures for Control and Protection System before Unit 1 will be allowed to restart from its 1998 outage. The Lithuanian Energy Institute performed an analysis that supports the selection of the input process parameters and setpoints values as well as developed accident analysis for the Ignalina DAZ system. It was shown that in case of transients with failure of the existing CPS but with activation of DAZ system reactor is adequately protected and any safety criteria are not violated.

Pressure behavior in the main circulation circuit in case of loss of off-site power supply with failure of the existing Control and Protection System but with activation of DAZ system is presented in Fig. 3. In this case pressure in the reactor coolant circuit is far below of limit pressure 10.4 MPa. Therefore, after implementation of DAZ system at the Ignalina plant ATWS would be moved from the beyond design basic accidents to design basic accident class.

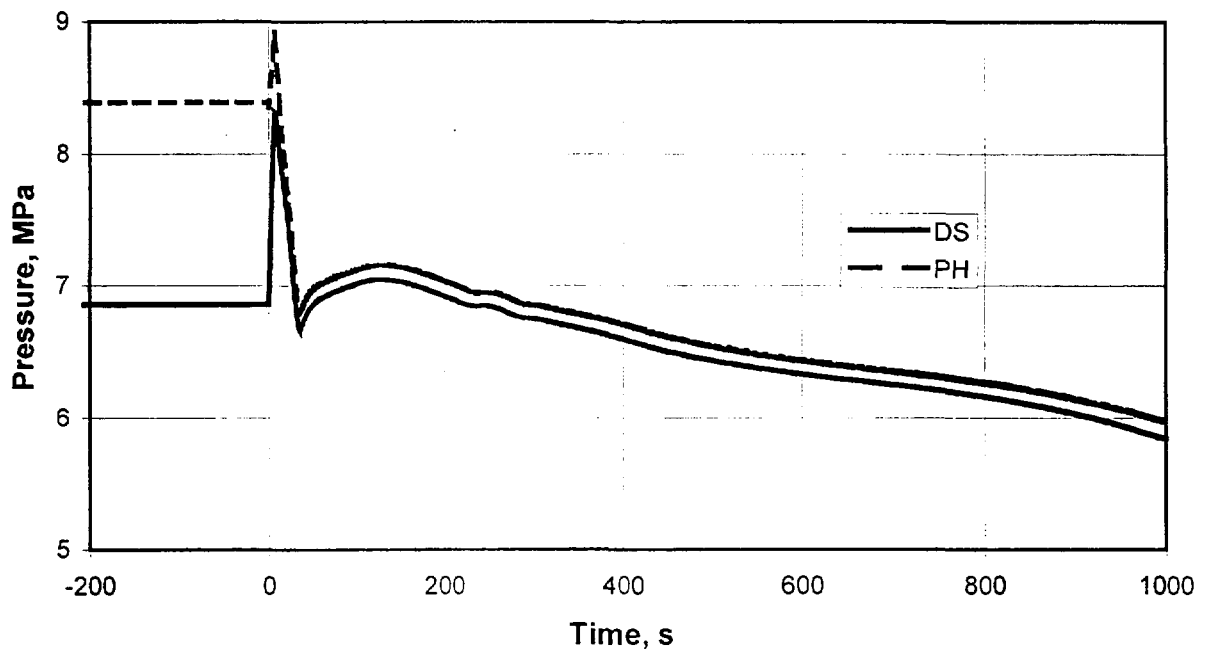


Fig. 3 Loss of off-site power supply with failure of existing Control and Protection System and activation of DAZ system. Pressure in the main circulation circuit

6. CONCLUSIONS

The INPP is unique among all RBMK type reactors in the scope and comprehensiveness of international studies which have been conducted to verify its design parameters and analyze its level of risk. Right from the start when Lithuania assumed control of the INPP (after the demise of the Soviet Union in 1991) the plant, its design and operational data has been completely open and accessible to western experts. Initially effective assistance in the nuclear safety field was provided by Sweden, subsequently most states having significant nuclear expertise contributed.

International assistance took several forms, a very valuable mode of assistance utilized the knowledge of international experts in extensive international study programs whose purpose was: a) collection, systematization and verification of plant design data, b) analysis of the level of risk, c) recommendations leading to improvements in the level of safety, d) transfer of state of the art analytical methodology to Lithuanian specialists. The major large scale international studies include:

- Barselina – A probabilistic risk analysis study conducted by Sweden, Lithuania and Russia.
- SAR – A very extensive international study funded by a grant from EBRD. Its purpose is to provide a comprehensive overview of plant status with special emphasis placed on its safety aspects. Specialists from the Ignalina NPP, Russia, Canada and Sweden contributed.
- RSR – An extensive review of the SAR by an independent group of international experts. Specialists from the U.S., United Kingdom, France, Germany, Italy, Russia and Lithuania contributed.

The noted studies provides a verified, state of the art base of knowledge which makes it possible to assess the present level of plant safety, compare this level with other reactor plants and plan improvements in plant hardware and operational procedures which enhance the level of safety. INPP is the only RBMK plant for which this information is available. Note, that statements made re. plant safety in this summary are based on the consensus reached in this area by the international expert community. A significant conclusion stated in the SAR is that none of the analyzed safety concerns require the immediate shutdown of the plant.

However, in spite that lot of safety improvements and analyses have been performed at the Ignalina NPP, much should be done in the nearest future.

References

1. Safety Report of Ignalina NPP with RBMK-1500 Reactors. RDIPE Report, Moscow, 1988 (In Russian)
2. In-Depth Safety Assessment of Ignalina NPP. Final Report, December 1996
3. Review of the Ignalina Nuclear Power Plant Safety Analysis Report. Final Report, June 1997
4. The Barselina Project Phase 4 Summary Report, December 1996
5. Evaluation of the RBMK-1500 Accident Confinement System. Report No. MD-NUME-96-09, September 1996
6. Technological Specification for Operation of Ignalina NPP with RBMK-1500 type reactor, Visaginas, Report O-380, 1998
7. Localization of accident products system of Ignalina NPP. Explanatory note to design. VNIPIET Report A07.062.000.113, Sverdlovsk, 1976 (In Russian)
8. In-Depth Safety Assessment of Ignalina NPP. Guidelines for Production and Review of Safety Analysis Report, June 21, 1994
9. IAEA Safety Practice Series No. 50-P-1. Application to the Single Failure Criterion, Vienna: IAEA, 1990
10. Typical Contents of Technical Justification of Nuclear Power Plant Safety. TS TOB AS-85 G-1-001-85, Moscow, 1987 (In Russian)
11. Nuclear Safety Regulations for NPP Reactors, VD-B-001-0-96, Vilnius, 1997 (In Lithuanian)
12. Sanitary Rules for Design and Operation of Nuclear Plant. SP AS-88/93, Moscow, 1993 (In Russian)
13. Code on the Safety of Nuclear Power Plants: Design. Safety Series No. 50-C-D, Vienna: IAEA, 1988
14. CPS and ECCS Single Failure Analysis for Unit 1. Final Report, August 1997
15. INPP Safety Improvement Program No. 2. April 7, 1997

16. Review of the Ignalina Nuclear Power Plant Reactor Control and Protection System Single Failure Analysis, September 1997.
17. IAEA Safety Series No. 50-SG-D3, Protection Systems and Related Design Features in Nuclear Power Plant, Vienna: IAEA, 1990