10. SYSTEM ANALYSIS

Several projects related to the safety analysis of the Ignalina NPP or its safety systems have been performed. The joint Lithuanian - Sweden Barselina project - the first probabilistic assessment for RBMK type reactors - was conducted [63]. A peer review of this Ignalina PSA project was conducted by Pacific Northwest National Laboratory. The hardware required to use US Nuclear Regulatory Commission computer code for conducting probabilistic risk assessment was purchased and delivered to the Ignalina Safety Analysis Group. A plant analyzer and computer workstation were delivered to the ISAG, with additional hardware to support the extension of the Ignalina plant analyzer to multiple simultaneous users. An evaluation of the RBMK-1500 accident confinement system [64] was performed by a joint team from Ignalina Safety Analysis Group and the Department of Nuclear Engineering, University of Maryland. The study of the RBMK-1500 ACS was performed using the state-of-the-art codes RELAP5 and CONTAIN, and is the first study that analyzes not only short-term, but also long-term (up to 24 hours) aspects of LOCA transients for primary system and the ACS.

An in-depth safety assessment of the Ignalina NPP was undertaken and as a result a Safety Analysis Report has been produced [62] and reviewed [65]. 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 NSA provided 8.5 million ECU to fund the external assistance work.

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. All recommendations were accepted by the Ignalina NPP and included in new Safety Improvement Program [66]. Implementation of all improvements will greatly improve the safety level of Ignalina. Main SAR results are presented in Sections 10 and 11 of this Source Book.

As to 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 include 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 [67]. 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 1and 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 NPPs that in theory were 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.

10.1 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. EBRD has already funded through the Safety Improvement Program of Ignalina NPP [22] a feasibility study for a second shutdown system. Several options were investigated in this study and a second shutdown system with ball-type absorbers was proposed. Ignalina plant staff engineers have visited the United Kingdom and convinced that operating model of the shutdown system with ball-type absorbers does not exist, in spite of statements that such system are used at British plants. Development of a new shutdown system which has no predecessors would require inadmissible long period of time which is commensurable with plant operation lifetime. This drastically change the opinion of Ignalina staff about the shutdown system with ball-type absorbers and thus such an option was not accepted by the Ignalina NPP on October 9-13, 1995 in the Vienna meeting where design options for second shutdown systems for RBMK reactors [68] were discussed. Therefore, the plant asked an European Commission to initiate an additional project and provide financial support to perform a feasibility study of a second shutdown system for Ignalina NPP, taking into account experiences on the development of independent shutdown systems for RBMK reactors.

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 walkdowns of the installed system and met with Ignalina plan personnel involved in operation and maintenance of the CPS. These walkdowns 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 walkdowns, limited as they were due to lack of the wiring diagrams and schematic, confirmed the basic design concerns of the SAR team. The walkdowns 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 [63]:

- 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. In particular, the ISP recommends that before either unit restarts from its 1997 maintenance outage the following items related to CPS should be resolved:

- single Failure Analysis of the control and protection system should be completed,
- design and procedural modifications required to compensate for control and protection system deficiencies should be identified and implemented.

A number of issues concerning CPS, that were raised by SAR and RSR teams have been resolved by the Ignalina NPP and, in the opinion of VATESI, the planning of compensatory measures for lack of scram diversity has reached an acceptable stage to permit restart. Ignalina NPP plans to introduce an independent high pressure scram parameter aimed at removing residual concerns about ATWS scenarios during the next outage. The other follow-up actions to resolved critical CPS issues are further discussed in detail together with related EPPS critical issues in the next Section.

10.2 EMERGENCY PROCESS PROTECTION SYSTEM

The Emergency Process Protection System 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.

INPP has been fully responsive to these recommendations and initiated the effort to perform a detailed and comprehensive Single Failure Analysis [69] 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 [66] 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 [70]:

- 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 [63]. 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 [65] 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 [71] 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 1kΩ 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 [71]. 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 that "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 [72]. 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 following Postulated Initiating Events (PIE):

1. Loss of coolant accidents occurring in all zones and including rupture of fuel channels (PIE 1)
2. Flow stop in the fuel channels (PIE 2)
3. Loss of external power (PIE 3)
4. Loss of feedwater (PIE 4)
5. Trip of 2/2 main turbines (PIE 5)
6. Rupture of main or auxiliary feedwater headers (PIE 6)
7. Rupture of ECCS headers (PIE 7)
8. Ruptures or loss of flow in the CPS cooling system (PIE 8)
9. Failure of the de-aerators (PIE 9)
10. High rate of change in power in the start-up mode (PIE 10)
11. High rate of change in power in the power mode (PIE 11)
12. Overpower (PIE 12)
13. Decrease in drum separator level (PIE 13)
14. Over-pressure in the drum separator (PIE 16)
15. Low flow (PIE 17)
16. Manual trip of the reactor (PIE 18)
17. Decrease level in ECCS accumulators (PIE 19)
18. Increase in drum separator level (PIE 20)
19. Loss of 2/2 main turbine load (PIE 21)

- 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 Nuclear Power Plant 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. Ignalina therefore plans to design a permanent fix and implement it at the next scheduled outage.

10.3 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 [72] 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 letter 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 heatup. 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 recirculation 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 diagnosting 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 walkdown 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.

10.4 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. A description of the ACS is given in Section 6.3. 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 depressurization 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 m^3 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,
- Deminiralized 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. It was also recommended that before either units restarts from its 1997 maintenance outage planning should be completed and development started on a safety case for the Accident Confinement System.

Ignalina NPP has placed a contract with Lithuanian Energy Institute to assist in preparation of the safety case for Accident Confinement System. The intention of the developed work plan is basically in line with the recommendations of the Ignalina Safety Panel. The plan has been reviewed by Western experts and further recommendations were made to address relevant technical matters in sufficient detail. The work has started and will be finished by the end of October 1998.

10.5 FEEDWATER AND STEAM SUPPLY SYSTEM

The results of system analysis for the following systems are discussed in this Section:

- Deaerating and Feedwater System,
- Auxiliary Deaerator Makeup Supply System,
- Steam Supply and Pressure Relief Systems.

The Deaerating and Feedwater System is used first of all for normal operation. Secondly, its safety function under various accidental conditions is to provide water with suitable subcooling to the main and auxiliary feed water pumps. After a large or medium break-LOCA it provides water to the main feedwater pumps for the first two minutes, as MFWS is used as the third 50 % train of short term ECCS. After any LOCA it provides water to the emergency feedwater pumps if those are demanded to supplement the ECCS pumps in the long term mode. After any transient it provides water to the auxiliary feed water pumps as preferred providers of long-term makeup.

The main SAR finding are:

- the main feed water pumps will be tripped on low discharge header pressure within a few seconds of MCP pressure header rupture. They cannot fulfill their short-term safety function under this event,
- the Deaerating and Feedwater System and its support systems are not qualified against external events or against dynamic loading while performing safety functions. Furthermore, the main and auxiliary feed water pumps are susceptible to failure following certain feedwater line and possible steam line breaks,
- there are positions in the feedwater line where a break would disable all the main feedwater pumps,
- there is no evidence that the main and auxiliary feed water pumps would operate satisfactory under decreasing deaerator pressure conditions,
- long term heating and pressurization of the deaerator cannot be guaranteed. It has not been demonstrated that the specified auxiliary feed water pump maximum cooldown rate of 120 ^{o}C/h would not be exceeded.

The Auxiliary Deaerator Makeup System is a safety system with two main safety functions - to provide makeup water to the deaerator after a reactor trip to supply the auxiliary feedwater pumps and to provide makeup water to the ACS after LOCA to supply ECCS pumps. The main SAR system analysis findings on this system are as following:

- single failures in active components will not result in unavailability of the Auxiliary Deaerator Makeup System during first 24 hours after accident. After that time the capacity of the bypass line from the Utilization of Liquid Radioactive Waste Pumps will be sufficient,
- the system can be disabled by single pipe rupture,
- the bypass line from the Utilization of Liquid Radioactive Waste can manually be actuated to deliver cooling water with sufficient flow rate after 30 min.,
- the Auxiliary Deaerator Makeup System is vulnerable to fire accidents, which could disable the system.

The main steam pipelines downstream of the drum separator divide pipelines to two parts: live steam pipelines and hot steam pipelines. Live steam pipelines form closed loops which are the pressure relief devices - MSVs and SDV-A valves. Hot steam pipelines go ultimately to the turbines, but contain the SDV-D valves for normal operation and the main steam isolation valves. The SDV-D bleed steam to heat the cold deaerator makeup water when the turbines are tripped. The main SAR findings are:

- accident analysis shows that the relief valves are sufficiently sized to keep over-pressure after design basis transients to within 15 % of the normal working pressure of the primary circuit,

- there are no important single failures which could disable either the pressure relief or steam supply function,
- the systems are not seismically qualified nor are they qualified against dynamic loading,
- there is no equipment qualification program for the systems, and one should be developed.

Summarizing this Section, it is necessary to notice that the system analysis for the Deaerating and Feedwater System and Auxiliary Deaerator Makeup System show the weaknesses in system capabilities. The limit of operation of the Deaerating and Feedwater System with regard to break sizes in the primary circuit is not assessed. The Auxiliary Deaerator Makeup System can be disabled by single failure or manual interaction. The safety case for the steam lines concludes that there are sufficient relief valves to keep over-pressure after transients to within 15 % of the nominal pressure. System analysis does not cover the main steam isolation valves nor dynamic loads in the case of overfilling of the drum separators.

10.6 SUPPORT SYSTEMS

The primary safety functions are supported by many other systems which have the following basic functions: supply electric power or compressed air to equipment and instrumentation, provide raw and processed information to the operator, provide alternative sources of cooling water for fuel under post-accident conditions, provide cooling water to equipment, provide ventilation, etc. The results of the system analysis for following support systems are discussed in this Section:

- Electric Power Supply System,
- Service Water System,
- Intermediate Circuit,
- Purification and Cooling System,
- Ventilation System.

A detailed Engineering Assessment of the Electric Power Supply System has been carried out by SAR and in particular in-depth demonstration of compliance with the corresponding IAEA safety guide [73]. The high degree of redundancy in the Electric Power Supply System provides assurance with respect to reliability of the power supply. One exception from sound trainwise design was found in the automatic transfer of Instrumentation and Control and other loads between redundant uninterruptible power sources. The resulting dependency between buses must be assessed and eliminated, wherever possible. RSR recommended that Ignalina NPP perform an evaluation of the effect of persistent degraded voltage or AC-frequency to determine minimum voltage/frequency levels required to close breakers and operate equipment. The results should be used to determine if the 50 % nominal voltage or 46 Hz AC-frequency setpoints provide adequate protection of vital equipment.

The Service Water System represents a vital and common support system for a number of operational and safety systems. The SAR indicates there is the lack of segregation of the service water distribution within the whole plant. The Service Water System is built in two trains. The system function is not proven to be single failure tolerant, if an initiating event starts within the Service Water System, which may cause shut-down due to loss of operational function or flooding, but which simultaneously degrades the status of the SWS for the support of safety functions such as ECCS, ACS or AFWS. The SAR gives no evidence that the plant could be cooled down without Service Water System under the existing components specification, system configuration and operational procedures in force. The ECCS, AFWS and PCS rely directly or indirectly via IC on Service Water System. There is a potential for the plant to survive the losses of Service Water System and Intermediate Circuit. The credibility of the mutual support of the neighboring units has still to be demonstrated, with regard to tolerable downtime/periods of loss of service water for different front line systems. The loss of Service Water System can be caused by fire and seismic events. Improvements made during the last two years are not considered or assessed homogeneously within the SAR. The system analyses have to be adapted to the recent plant configuration.

The Intermediate Circuit consists of two separate circuits for different cooling functions. Redundancy is built in for pumps and heat exchangers to the Service Water System. Both circuits have single trains of piping and connections to the corresponding components to be cooled. IC-1 provides cooling to the Purification and Cooling System among others and has safety functions for low pressure residual heat removal. IC-2 is used for cooling non-safety components, but also for safety related cooling of ECCS and AFWS pumps. The dependence of ECCS on the availability of the ICC-2 is a high order critical issue. A failure of ECCS consequential to loss of IC-2 has to be postulated forming part of the design basis. No evidence is given in the SAR that the cooldown of the plant can be achieved without cooling of bearings and seals of the multistage ECCS pumps.

Besides the operational functions such as cleaning up and purging of primary coolant, the following characteristics and safety related functions are recognized to be the Purification and Cooling System: extension of the pressure boundary outside he ACS and low pressure residual heat removal. The PCS under normal operation receives water from the pressure headers of both loops to clean up to the required water quality. In case of breaks of the pipelines of the PCS system, it has to be isolated to limit the amount of primary water escaping from the pressure boundary. During reactor cooldown the

system is actuated to perform its residual heat removal function. According to Engineering Assessment of the system, pipe ruptures in the PCS are mitigated by relieving to the ACS and by subsequent automatic closure of the isolating valves. However, the consequences of pipe breaks in the PCS and the design requirements of the mitigative systems as well as residual heat removal function have not be assessed in the SAR system analysis.

The SAR has shown that there are more than 250 ventilation sub-systems for various purposes at the power unit. The safety task of the ventilation systems are to prevent contamination of indoor and ambient air by radiological and explosive substances, to provide airflow towards more contaminated premises only and to provide conditions for the operation of the plant safety functions. The ventilation systems were installed before there were requirement for such systems to operate despite natural phenomena such as high wind, earthquake and flood. It therefore is not proven to withstand such natural phenomena. An obvious weakness in ventilation is related to the availability of reliable ventilation and thus habitability of the main and emergency control rooms in case of external events. However, the SAR assessment has not demonstrated that ventilation will fulfill its safety functions following an accident when additional equipment will be operated and escaping steam will tend to increase both temperature and humidity in the reactor building.

Summarizing the assessment of the support systems it is necessary to mentione that system analysis identified few high priority non-compliance's related to vulnerability due to lack of physical separation or inadequate fire protection, lack of redundancy and failure of passive piping. Individually, these deficiencies do not in themselves represent major safety problems. However, the large number of low priority findings indicates a reduction in defense in depth provided by automatic systems, and potentially leads to an increased reliance on the operator.