System Reliability Analysis and Probabilistic Safety Assessment to Support the Design of a New Containment Cooling System for Severe Accident Management at NPP Paks

Tamas Siklossy*[a], Attila Bareith[a], David Hollo[a], Zoltan Karsa[a], Gabor Lajtha[a], Jenő Nigicser[a], Peter Siklossy[a]

[a] NUBIKI Nuclear Safety Research Institute, Budapest, Hungary

Abstract: Based on the severe accident management related proposals of the post-Fukushima Targeted Safety Reassessment of Paks NPP, implementation of an independent heat removal system was envisaged to ensure long term containment cooling under severe accident conditions. Safety assessment was performed in support of the planned plant modification using preliminary design documentation. Quantitative system reliability targets were specified as a first step of the analysis. System reliability assessment was performed for the cooling system. The adequacy of system design was evaluated from reliability point of view by comparing the results of system reliability analysis with the preset unavailability target. The cooling water of the planned containment heat removal system is ensured by taking water from the emergency core cooling system (ECCS) sumps. To provide redundancy in cooling water supply, two ECCS lines are to be interconnected along the suction line of the containment heat removal system pumps. The effects of the planned new interconnection between the ECCS lines on ECCS functionality and on core damage frequency were also analyzed and evaluated. The paper gives an overview of the safety assessment, and it discusses the findings of the analysis, together with the proposed improvements and their impact on plant risk.

Keywords: PSA, System Reliability Analysis, Severe Accident Management, Aggravating Effects, Containment Cooling System.

1. INTRODUCTION

Based on the severe accident management related proposals of the post-Fukushima Targeted Safety Reassessment (TSR) of Paks NPP [1], implementation of an independent heat removal system was envisaged to ensure long term containment cooling under severe accident conditions. The main purpose of the system is to prevent containment overpressurization due to slow pressure build-up under severe accident conditions as well as to ensure containment integrity in case large amount of steam was generated due to external cooling of the reactor pressure vessel. In the resolution of the TSR the Hungarian Atomic Energy Authority prescribed the implementation of several corrective measures to reduce plant vulnerability to severe accidents. The majority of these actions had been identified by the licensee during the reassessment process, one of them being the construction of a new containment cooling system, which was the subject of this study. In a feasibility study it was examined in detail how the steam generated within the containment in the course of a severe accident can be condensed by means of a heat removal loop constituting a closed system with the containment to successfully perform the depressurization function. Besides pressure reduction in the containment, the planned system is to provide water supply for external cooling of the reactor pressure vessel by condensing the steam generated thereof, and transferring the heat outside the containment.

2. OBJECTIVES

Safety assessment had to be performed in support of the planned plant modification using preliminary design documentation [2]. Amongst others, system reliability analysis and probabilistic safety assessment were required to support the design of the new containment cooling system.

One main objective was to evaluate the adequacy of system design from reliability point of view. To fulfil this objective, quantitative system reliability requirements were specified as the first step of the analysis, by taking into account the quantitative criterion on the frequency of large releases prescribed in Hungarian nuclear safety regulations, as well as the range of severe accidents in which the operation of the planned system would be beneficial. Subsequently, system reliability assessment was performed for the cooling system. The adequacy of system design was evaluated from reliability point of view by confronting the results of system reliability analysis with the preset unavailability target.

A further main objective was to assess and evaluate the changes to the core damage frequency due to the planned cooling system. Aggravating effects induced by the interconnection between two independent ECCS lines to provide redundancy in cooling water supply had been identified. Consequently, changes in the efficiency of mitigating plant transients that require the operation of the ECCSs had to be assessed.

As to the scope of the analysis, internal failures were considered. The new containment cooling system fulfils its function when the containment is closed, so, based on the approach followed in Level 2 PSA [3], it seemed appropriate to limit the scope of the system reliability analysis to full power operation only. On the contrary, in the assessment on aggravating effects of the planned new interconnection between the ECCS lines low power and shutdown states of a typical refueling outage had to be dealt with.

3. SPECIFICATION OF QUANTITATIVE SYSTEM RELIABILITY TARGET

Quantitative system reliability targets were specified as a first step of the analysis. These targets are concerned with an acceptable level of likelihood of system failure to perform the intended containment depressurization function under severe accident conditions. A threshold on system unavailability was defined for this purpose.

3.1. System Purpose and Functionality

The aim of the Severe Accident Management upgrades implemented in Paks NPP is to prevent the progression of severe accident sequences and, eventually, to ensure a long-term stable state of the plant. Severe accident management strategies have been developed to prevent the occurrence of severe accident sequences identified in the Level 2 PSA study or to mitigate the consequences of these sequences so that significant radioactivity releases can be avoided.

The implementation of the strategy consists of two key elements; the implementation of Severe Accident Management Guidelines, and the installation of equipment for severe accident management including:

- external cooling of the reactor vessel;
- installation of passive autocatalytic recombiners for hydrogen removal during severe accidents;
- reinforcement of the spent fuel pool cooling system against loss of coolant;
- use of a dedicated diesel generator to supply power to severe accident management hardware components;
- implementation of a dedicated instrumentation system for severe accident management.

Based on the severe accident management related proposals of the TSR for Paks NPP, implementation of an independent heat removal system was envisaged to ensure long term containment cooling under severe accident conditions that was presented in Section 1.

The new containment cooling system can be considered as the last item in the series of severe accident management related technological improvements. This system is essential to the long term cooling of

the core and the core debris, and to ensure a stable, safe state of the containment, when all ECCS lines and the containment spray system are unavailable and recovery is not successful.

3.2. General Considerations on System Reliability

According to the design specifications, system startup as well as all necessary interventions during system operation have to be performed as operator actions taken in a manipulator container located next to the so-called localization tower. Hence, no automatic actuations are planned to be implemented. During a severe accident the vicinity of the manipulator containment may be contaminated due to containment leakage. It should also be noted, that redundancy and diversity to ensure high system reliability are not required.

Based on the aforementioned considerations, the quantitative system reliability target of a severe accident management system can be set at a much lower level than that of a safety system with a high level of redundancy applied to accident mitigation system. Taking into account the severe accident conditions that are assumed in the design basis of the system, a realistic target on the system failure probability cannot be lower than 0.1.

Besides, the actual plant state (e.g. availability of electrical power) and environmental conditions (e.g. radiological consequences in the vicinity of the manipulator container) during a severe accident also play an important role in the realistically achievable reliability level of the system. A scenario specific analysis was out of the scope of the study. Such an analysis would have required detailed modelling of the operating conditions and effectiveness of the planned system in accordance with the different circumstances imposed by numerous different Level 2 PSA sequences. As a conservative simplifying assumption, the most severe accident and the corresponding environmental conditions that are included in the design basis of the system were taken into account in determining the quantitative system reliability target. The fact that a significantly higher level of system availability may also be required and achieved under less severe conditions was borne in mind throughout the whole assessment process.

3.3. Effects of the System on the Progression of Severe Accidents and on the Large Release Frequency

It could be settled that the new containment cooling system should be able to protect containment integrity, and hence prevent large radioactive releases during a severe accident that occurs at full power operation of the plant. Based on the design specifications of the system and the Hungarian nuclear safety regulations (see Section 3.4.), severe accidents initiated by internal initiating events were considered in defining the probabilistic requirement. All severe accident sequences in the Level 2 PSA [3] were looked at, and the effect of the system on mitigating large radioactive releases was assessed first qualitatively then quantitatively. To this end, sensitivity assessment was performed for all containment states defined in the Level 2 PSA on a case by case basis by changing system unavailability in the PSA model. Table 1 summarizes the effect of the cooling system unavailability on the frequency of the different containment states. The last row of the table shows how much risk reduction can be achieved in terms of the total frequency of large releases avoided by using the new cooling system.

Table 1: The Effects of the Cooling System Unavailability on the Containment State Frequency

Containment State	Containment Cooling System Unavailability					
	0	**0.1**	**0.2**	**0.3**	**0.5**	**1**
Catastrophic Containment Failure, Rupture	$1.81 \cdot 10^{-8}$	$1.88 \cdot 10^{-8}$	$1.95 \cdot 10^{-8}$	$2.02 \cdot 10^{-8}$	$2.17 \cdot 10^{-8}$	$2.52 \cdot 10^{-8}$
Containment bypass	$4.09 \cdot 10^{-8}$	$4.09 \cdot 10^{-8}$	$4.09 \cdot 10^{-8}$	$4.09 \cdot 10^{-8}$	$4.09 \cdot 10^{-8}$	$4.09 \cdot 10^{-8}$
Early containment failure	$1.80 \cdot 10^{-7}$	$1.80 \cdot 10^{-7}$	$1.80 \cdot 10^{-7}$	$1.80 \cdot 10^{-7}$	$1.80 \cdot 10^{-7}$	$1.80 \cdot 10^{-7}$
Late containment failure	$7.92 \cdot 10^{-8}$	$1.42 \cdot 10^{-7}$	$1.97 \cdot 10^{-7}$	$3.09 \cdot 10^{-7}$	$4.63 \cdot 10^{-7}$	$6.66 \cdot 10^{-7}$
Increased late containment leakage	$6.00 \cdot 10^{-10}$	$5.51 \cdot 10^{-9}$	$1.04 \cdot 10^{-8}$	$1.53 \cdot 10^{-8}$	$2.51 \cdot 10^{-8}$	$4.97 \cdot 10^{-8}$
Late containment failure, containment spray system operates	$1.15 \cdot 10^{-8}$	$1.15 \cdot 10^{-8}$	$1.15 \cdot 10^{-8}$	$1.15 \cdot 10^{-8}$	$1.15 \cdot 10^{-8}$	$1.15 \cdot 10^{-8}$
Total	$\mathbf{3.30 \cdot 10^{-7}}$	$\mathbf{3.95 \cdot 10^{-7}}$	$\mathbf{4.59 \cdot 10^{-7}}$	$\mathbf{5.77 \cdot 10^{-7}}$	$\mathbf{7.42 \cdot 10^{-7}}$	$\mathbf{9.73 \cdot 10^{-7}}$
Large releases prevented in total	$\mathbf{6.43 \cdot 10^{-7}}$	$\mathbf{5.78 \cdot 10^{-7}}$	$\mathbf{5.14 \cdot 10^{-7}}$	$\mathbf{3.96 \cdot 10^{-7}}$	$\mathbf{2.31 \cdot 10^{-7}}$	**0.00**

3.4. Establishing the System Reliability Target

The requirements of the Hungarian Nuclear Safety Code (NSC) were taken into account to define an acceptable level of unavailability for the containment cooling system. The NSC requirement 3.2.4.0900. prescribes that for all initial operating conditions and effects, excluding sabotage and earthquake, the aggregated frequency of severe accident event sequences resulting in large or early releases shall not exceed 10^{-5}/a. Besides, by all means of reasonable plant modifications and interventions, 10^{-6}/a shall be targeted. The fulfilment of the criteria shall be demonstrated by Level 2 PSA.

According to the Level 2 PSA results, the large release frequency is $1.82 \cdot 10^{-6}$/a in those plant operational states when the containment is open. If the containment is open, the new containment cooling system is ineffective, so the total large release frequency ($2.79 \cdot 10^{-6}$/a without crediting the planned system) cannot be reduced below 10^{-6}/a, even by not assuming any system failure. Consequently, a system reliability requirement could not be defined solely on the basis of the Hungarian nuclear regulations. However, a probabilistic safety target that seemed to be a realistic expectation to ensure an adequate degree of safety enhancement was set by considering the following aspects:

- system purpose and functionality,
- the frequency of those sequences leading to large or early release that may be prevented by the system,
- the ratio of the frequency defined in the previous bullet to the total frequency of severe accident sequences leading to large or early release.

The frequency of those large or early release sequences that may be prevented by the system is $6.43 \cdot 10^{-7}$/a. Hence, these sequences give 64,3% of the 10^{-6}/a value that should be targeted according to the NSC. If this ratio can considerably be reduced thanks to the use of the system, then the system may be regarded as sufficiently reliable. This is because the large or early release frequency would then be determined mostly by event sequences that the system cannot affect. Also, the frequency of the remaining containment states would not have to be decreased significantly below 10^{-6}/a. What was regarded as a "considerable" frequency reduction could only be decided arbitrarily. Risk reduction was regarded acceptable, if the ratio of the frequency of the large or early release frequencies preventable by the system to the total large or early release frequency would be reduced to 25%. Moreover, 10% was defined as a ratio that should be aimed at by enhancing system reliability through appropriate design. Based on the aforementioned considerations and the results presented in Table 1, the probabilistic safety target for the system unavailability was defined as 0.3 (corresponding to the ratio reduction to 25%), but the value of 0.16 (corresponding to the ratio reduction to 10%) should be aimed at.

4. SYSTEM RELIABILITY ANALYSIS

The following tasks were performed as part of the safety analysis of the new containment cooling system:

- The reliability of the cooling system was quantified by means of system reliability analysis considering internal random failures.
- System unavailability related to the cooling function was compared with the preset unavailability target (see Section 3).
- The adequacy of system design was evaluated from reliability point of view based on the results of the comparison.
- Modifications to the design were proposed as it was seen necessary.

4.1. System Description

4.1.1. Basic Technical Information

The initial design information used as input to the system reliability analysis included a description of

- system design basis;
- structure of the system;
- system operation under conditions considered in the system design basis;
- planned periodical tests;
- location of the equipment that should be operated by the plant personnel;
- differences among the units.

As an example of such inputs, the system structure and operation are shortly summarized hereby. Figure 1 shows a simplified piping and instrumentation diagram of the cooling system.

The planned new cooling system is to be connected to 2 sump lines ((10,40)TJ(21,31) and (20,30)TJ(11,21)) below the containment sump valves. The two suction lines are planned to be interconnected between two motor-operated valves ((10,20,30,40)TQ41S(201,202)) and the parallel circulating pumps ((10,20,30,40)TQ42D(001,002)). The two pump discharge lines are to be unified (TQ44 pipeline) after the check valves ((10,20,30,40)TQ44S(001,002)) in these lines. Testing of the pumps is going to be performed by means of a separate pipeline (TQ43), that includes a manually operated valve ((10,20,30,40)TQ43S001)).

The TQ44 pipeline is going to enter the E004 turbine hall at an elevation of -6.5 m after the (10,20,30,40)TQ44S201 motor driven valves. Then the pipeline leaves the main building after bypassing the reactor hall. By going up along the wall to the roof of the localization tower, it is to reach the (10,20,30,40)TQ45W(001,002) air cooling equipment installed on the localization towers. The air cooling equipment is going to consist of 10+10 ((10,20,30,40)TQ45D(001-010) and (10,20,30,40)TQ45D(011-020)) ventilators. The cooled water is to enter compartment A624 through the TQ45 pipeline and reach the distributor pipeline. A motor operated containment isolation valve ((10,20,30,40)TQ45S201) and a check valve inside the containment ((10,20,30,40)TQ45S002) are to be installed in pipeline TQ45. The injected water is to flow onto grilles before the bubbler trays at an elevation of +44.9 m, then to other grilles placed 3 m from each other. This process partitions the cooling water to drops.

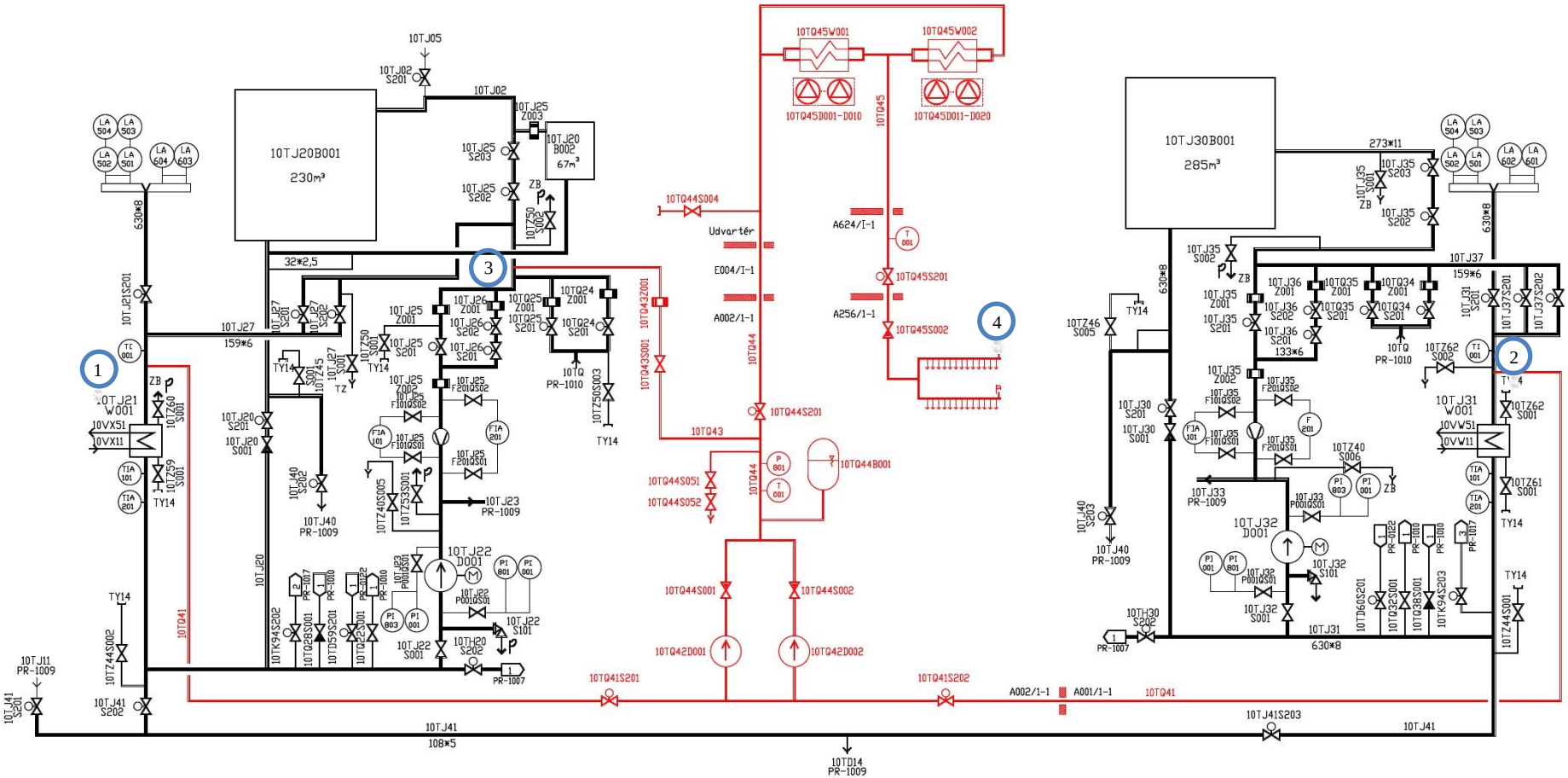

Figure 1: Preliminary P&ID of the cooling system at unit 1 of NPP Paks

4.1.2. Definition of System Function

Based on the supplied design information, the safety function considered in system reliability analysis was defined as follows:
The operation of the containment cooling system is successful, if the system ensures heat removal from the containment atmosphere for 168 hours so that containment overpressurization is prevented. 168 hours of operation was chosen on the basis of the assumption that beyond 168 hours other interventions can also be performed to make up for the functional failure of the cooling system, if it occurs. This time interval should be sufficient to enable preparations for such alternative interventions. After one week, the containment can withstand the effects of a short term loss of system function without being overpressurized.

4.2. System Reliability Model Development and Quantification

This section presents the process and the results of fault tree modelling and input data assessment performed in system reliability analysis. The most important analysis assumptions are also highlighted.

4.2.1. Fault Tree Analysis

The system can fulfil its intended function, if certain conditions are ensured. The list of necessary and sufficient conditions makes up the system success criteria. These success criteria define the minimum:

- number of operating system trains,
- system configuration and operation mode,
- mission time

that are necessary to successfully fulfil the system function.

The system fault trees were developed in the following two steps:

- failure mode, effect and criticality analysis (FMECA),
- delineation of system fault trees based on the results of FMECA.

4.2.2. Human Reliability Analysis

It was conservatively assumed that the system would not be capable of fulfilling its function if the manual valve ((10,20,30,40)TQ43S001) on the recirculation line was left unintentionally open after testing. This failure mode was considered as a pre-initiator (type A) human error in the analysis. Quantification of human error probability for this event was based on the approach used in the internal events PSA of NPP Paks [4]. The analysis pointed out the importance of ensuring low failure probability for mispositioning the manual valve after testing. This can only be assured, if the plant personnel can ascertain the closed position of the manually operated valve with high reliability. To achieve this goal it was suggested to

- clearly indicate and emphasize the need to check valve position and use a check list in the test procedure,
- to re-check valve position by an independent check, and make a record of it,
- use a valve position indicator on the control panel of the manipulator container.

By crediting the above-mentioned conditions, a human error probability of 10^{-2} was applied in the analysis for the type A human action in question.

The following severe accident management actions as post initiator (type C) human actions and the failure thereof were identified (for the base case scenario):

- electric power supply has to be ensured from a dedicated severe accident management diesel generator, by performing several subtasks as:
    - transportation of a container including a mobile 6/0.4 kV transformer next to the manipulator container,
    - setting up a mobile cable interconnection between the diesel generator and the transformer,
    - setting up a mobile cable interconnection between the transformer and the manipulator container,
    - startup of the diesel generator.
- manual startup of the containment cooling system from the manipulator containment,
- continuous control of system operation, e.g. changes in configuration if a ventilator or pump has to be turned off, or started.

The Success Likelihood Index Method (SLIM) [5] was used for quantifying these human failure events. The following performance shaping factors were considered as the most important ones for these human actions:

- environmental conditions;
- time constraint / emergency stressor;
- task complexity;
- human-machine interface;
- training and qualification of personnel;
- teamwork;
- procedures.

4.2.3. Modelling Dependent Failures

Functional (structural) dependence, human interaction dependence and residual dependence as common cause failures were considered in the assessment. Functional and human interaction dependence was modelled explicitly, and the simplest parametric model, the *β-factor* model was applied to common cause failure quantification. The following common cause failures were implemented into the PSA model:

- all TJ(11,21,31)S201 motor operated valves fail to open;
- all TQ42D(001,002) pumps fail to start or fail to continue running;
- all diesel generators dedicated to accident conditions fail to start or fail to continue running;
- all TQ45D(001-020) ventilators fail to start or fail to continue running.

4.2.4. Reliability Data Assessment

Assessment of input data was primarily based on component type specific reliability data taken from the internal events PSA of Paks NPP as well as on data supplied by the system designer. The existing PSA data base was not found applicable to the severe accident generators and to other, low power mobile diesel generators used for severe accident management. Hence, the reliability data of these diesel generators were assessed by combining data supplied by the designer, reliability data for the emergency diesel generators from the plant PSA, as well as data taken from NUREG/CR-6928 (see [6]).

4.3. Safety Evaluation

4.3.1. Reliability of System Function

The system unavailability was quantified and the most important risk contributors were determined by solving the system fault tree for the loss of system function top event. Point estimates of system

unavailability were computed. In addition, importance, sensitivity and uncertainty analyses were performed to gain further insights useful for a better characterization of risk and for recommending safety improvements. The RiskSpectrum PSA software was the basic tool used for quantification.

According to the PSA results, the point estimate of mean unavailability for the defined system function is 0.326. The most dominant risk contributors are Type C human errors, especially the failure to ensure electric power supply to the system from the severe accident diesel generator. Moreover, failure to manually start up the containment cooling system from the manipulator containment and failure to continuously control of system operation have significant effects on the results too. Besides, mechanical and electrical failures also have a considerable contribution to system unavailability. The lack of system redundancy and the expected mission time of 168 hours result in single-event minimal cut sets having a relatively high failure probability.

As part of sensitivity analyses, the reliability of the system was assessed by making the following assumptions:

- electric power supply can also be ensured from the severe accident diesel generator designated to the neighboring twin unit,
- fixed power cable interconnection is established between the severe accident diesel generator and the manipulator container,
- combination of the above two options, i.e. electric power supply can be ensured from the severe accident diesel generator designated to the neighboring twin unit AND fixed power cable interconnection is established between the severe accident diesel generator and the manipulator container.

4.3.2. Evaluation of Results

The results of system reliability analysis were compared with the preset unavailability target. This comparison shows that the unavailability of the system (0.326) slightly exceeds the target value (0.3). However, according to the results of the sensitivity analyses, the system can meet the preset probabilistic safety target, if:

- electric power supply can also be ensured from the severe accident diesel generator designated to the neighboring twin unit, the human interventions needed for this operation in case of diesel generator failure are properly described in the relevant procedures, and adequate training is provided for the responsible plant personnel (unavailability: 0.291),
- fixed cable interconnection is established between the severe accident diesel generator and the manipulator container (unavailability: 0.237).

In summary: although quantitative system reliability requirements could not be defined on the basis of the NSC, it was found feasible to establish an arbitrary reliability target for ensuring a sufficient level of risk reduction and to meet this target with appropriate system design. It is also noted that even the targeted lower unavailability of 0.16 was found achievable by implementing all the safety enhancement proposals conceptualized in the study.

The following modifications were proposed to the design based on the lessons learned from system reliability analysis:

- Special care should be taken to elaborating those sections of the emergency operating procedures that will prescribe the startup and the operation of the new containment cooling system. The training of the plant personnel is also a very important precondition for ensuring the required level of functional reliability.
- If the relevant 6 kV non-safety busbars are available during a severe accident, then the system can be powered by these busbars. So it is not necessary to use the emergency diesel generator in this case. The possibility and conditions for using this type of power supply arrangement should be described in the relevant operating procedures and included in the training program.

- Fixed power cable interconnection is proposed to be established between the severe accident diesel generator and the manipulator container.
- It is proposed to enable electric power supply from the severe accident diesel generator designated to the neighboring twin unit. The sequence of actions to be taken by the plant personnel to make use of this power supply source in case of diesel generator failure should be proceduralized and trained.
- Implementation of some designated automatic actuations is suggested, so that the system can start automatically when the containment pressure exceeds a certain threshold. A designated number of ventilators or even a circulating pump should be turned off if the pressure is below a certain limit. Also, the backup circulating pump or a ventilator should be started if the other pump or a ventilator fails to start or continue running.
- It is proposed to ensure the operation of the system from a location that is better protected against the effects of radioactive radiation.

5. AGGRAVATING EFFECTS OF THE PLANNED SYSTEM ON PLANT SAFETY

As noted in Section 2 and described in detail in Section 4.1.1, the two ECCS lines are to be interconnected along the suction line of the containment heat removal system pumps. The effect of this planned interconnection on the Level 1 PSA results has been analyzed and evaluated as follows.

5.1. Qualitative Analysis

Due to the interconnection of the two ECCS lines, the failure of one ECCS line may weaken the ability of the other line to inject water to the primary circuit. In extreme cases, i.e. in some special system configurations the entire amount of primary coolant may be lost. A systematic approach was used to assess such aggravating effects by considering all the possible influencing factors. If all the valves in the new cooling system are in normal closed position, dependence between the two ECCS lines can be virtually excluded. Therefore, valves that can be left unintentionally in open position were identified as the first group of aggravating factors.

There are 4 connection points between the new cooling system and the low pressure ECCS lines, all of which can be isolated from the ECCS. These locations are depicted by blue circles in Figure 1. All possible system interconnections that can be established by the combination of false positions of isolating valves were mapped. Hydraulic characteristics that determine the flow rate and flow direction through the newly established interconnections were determined. In addition, the following factors were identified that can influence the possibility and the disadvantageous consequences in terms worsening the plant capability to avoid of core damage:

- the position of the valves determining the flow paths established by the low pressure ECCS;
- the operability of pumps in plant systems that can be affected by the flow paths due to mispositioned valves;
- the plant operating mode (full power or shutdown).

Initially, several event sequences with negative outcome were identified. Most of them could be screened out from further detailed analysis based on some assumptions justified in the study. The only screened in event sequence with negative outcome relates to a situation where the water recirculated through the containment sump gets to a low pressure ECCS tank, fills the tank up, and then the coolant is lost by pouring on the floor of the ECCS room. All the identified event combinations with aggravating effects were defined as accident scenarios. These scenarios were found reasonable to be subject to assessment by PSA. From among the total 8 scenarios interpreted in detail, the first 6 are related to full power operation as well as to low power operational states where the primary coolant temperature exceeds 150°C. The remaining two scenarios characterize sequences with primary coolant temperature below 150°C.

5.2. Modification of the PSA Model

All scenarios selected for modeling in PSA result mainly in loss of recirculation through the sump. Hence, all these scenarios were modelled at fault tree level. The PSA event trees and initiating events did not require any modifications. Failures reflecting each scenario were modeled in separate fault trees. These newly developed fault trees were linked to the fault trees in PSA representing the failures of recirculation through the sump with a logical OR gate.

5.3. Input Data Assessment

Modelling was largely based on using numerous fault tree parts that were already available in the Paks PSA. To model the selected scenarios, four basic events had to be newly introduced into the PSA model. All of these events represent a pre-initiator (type A) human action, namely leaving a valve open unintentionally. Three (10TQ41S201-RES, 10TQ41S202-RES and 10TQ43S001-RES) out of these four failures represent independent human errors relevant to the related valves. The fourth error is a common error for connection points 1 and 3 in Figure 1, and it represents the failure to restore valves to closed position after the periodic test of the system. Based on the same assumptions presented in Section 4.2.2., failure probability of 10^{-2} was assigned to these Type A human failure events.

5.4. Findings

The change in core damage frequency was quantified by taking into account the aforementioned modifications. Quantification was performed for each internal initiating event, for some designated initiating event groups as well as for all initiating events together. Based on the aggregated results, the average core damage frequency is $5.79 \cdot 10^{-6}$/a by considering the aggravating effects of the new containment cooling system. This reflects a $3.03 \cdot 10^{-9}$/a (i.e. 0.05%) increase in the core damage frequency as compared to the baseline PSA results. Table 2 summarizes core damage frequency relevant to considering as well as neglecting the aggravating impacts of the system for all initiating event groups.

Table 2: Change in Core Damage Frequency due to the Planned Modification

Initiating Event Groups	CDF (1/a)		Change in CDF	
	considering the modification	neglecting the modification	1/a	%
ABC	$1.112 \cdot 10^{-6}$	$1.113 \cdot 10^{-6}$	$1.118 \cdot 10^{-9}$	0.101
DE	$2.098 \cdot 10^{-6}$	$2.100 \cdot 10^{-6}$	$1.892 \cdot 10^{-9}$	0.090
FJLM	$9.866 \cdot 10^{-7}$	$9.866 \cdot 10^{-7}$	$9.300 \cdot 10^{-12}$	0.001
GHI	$6.513 \cdot 10^{-6}$	$6.513 \cdot 10^{-6}$	0.000	0.000
K	$9.432 \cdot 10^{-7}$	$9.432 \cdot 10^{-7}$	$1.390 \cdot 10^{-11}$	0.001
Total	$\mathbf{5.791 \cdot 10^{-6}}$	$\mathbf{5.794 \cdot 10^{-6}}$	$\mathbf{3.033 \cdot 10^{-9}}$	**0.052**

The results indicate that the implementation of the new containment cooling system causes a negligible change in core damage frequency. Sensitivity and importance measures for Type A human errors related to leaving valves unintentionally open are significant. If the probability of these human errors is assumed to be higher by an order of magnitude, the increment in core damage frequency would increase to 5%. The RIF relevant to the corresponding model parameter is 6.2. Consequently, these pre-initiator actions have a significant effect on the results, so it is important to ensure that at least the same level of human reliability can be credited with high confidence that was assumed in the analysis. Further remarks on this issue are similar to the ones discussed in Section 4.2.2.

6. CONCLUSIONS

Safety assessment was performed in support of a planned plant modification at NPP Paks. This modification is the implementation of a new heat removal system that should ensure long term containment cooling during severe accidents.

Quantitative system reliability targets were specified as a first step of the analysis. Since no quantitative system reliability requirement could be defined on the basis of the Hungarian nuclear safety regulations, a probabilistic safety target was determined as a realistic expectation to ensure an adequate level of safety enhancement. This probabilistic safety target was set as 0.3 for the expected value of system unavailability. In addition, 0.16 was defined as a lower level target value that should be aimed at by appropriate system design.

System reliability analysis was performed for the cooling system. Internal failures were considered in the analysis. The analysis results were compared with the preset unavailability target. According to the comparison, the unavailability of the system (0.326) slightly exceeds the probabilistic safety target (0.3). However, it was found feasible to meet the pre-defined probabilistic target, if modifications are made to system design. The lower unavailability target of 0.16 was also found achievable by implementing all the safety enhancement proposals conceptualized in the study.

The effect of the planned new interconnection between the ECCS lines on ECCS functionality and Level 1 PSA results was also analyzed and evaluated. It can be concluded from the results, that the implementation of the new containment cooling system causes a negligible increase in core damage frequency. Sensitivity and importance measures for Type A human errors related to leaving valves unintentionally open are significant.

Acknowledgements

This work has been greatly supported by the National Research, Development and Innovation Fund in the frame of the VKSZ_14-1-2015-0021 Hungarian project.

References

[1] *"Targeted Safety Review. Summary of the Final Report. Paks Nuclear Power Plant Ltd. Units 1-4."* MVM Paks Nuclear Power Plant, Paks, Hungary (2011).

[2] Bareith, A., Hollo, D., Karsa, Z., Nigicser, J. and Siklossy, T. *"Safety Assessment of the Cooling System Designed to Mitigate the Slow Overpressurization of the Containment, System Reliability Assessment and Analysis of the Modification induced Impact on Safety"* NUBIKI Report No. 202-703-00/2, Budapest, Hungary (in Hungarian) (2017).

[3] Bareith, A., Karsa, Z., Lajtha, G. and Téchy Zs. "*Update of the Containment Event Trees and the release categories of the Level 2 PSA.*" NUBIKI Report No. 212-216-00/1, Budapest, Hungary (in Hungarian) (2012)

[4] Bareith, A., et al. "*Probabilistic Safety Assessment of the Paks NPP. Detailed Description of the Human Reliability Assessment.*" NUBIKI Report No. 222-318-00/A5, Budapest, Hungary (in Hungarian) (2017)

[5] Embrey, D.E. *"SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgment."* NUREG/CR-3518. US Nuclear Regulatory Commission, Washington DC (1984)

[6] "*Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power."* NUREG/CR-6928, Idaho National Laboratory (2007)