NUKLEONIKA 2013;58(2):307–316

ORIGINAL PAPER

# The PSA analysis of PWR emergency coolant injection availability following SBLOCA

**Mieczysław Borysiewicz,
Katarzyna Bronowska,
Piotr Kopka,
Karol Kowal,
Tomasz Kwiatkowski,
Andrzej M. Prusiński,
Piotr A. Prusiński,
Grzegorz Siess**

**Abstract.** The aim of this article is to briefly introduce the probabilistic safety assessment (PSA) of nuclear power plants (NPPs), its scope, main concepts and application to a real case. The results of analysis presented here have been obtained by the Probabilistic Safety Analysis Group (GPSA) at the National Centre for Nuclear Research (NCBJ, Otwock) as a part of the work done for the Polish National Atomic Energy Agency (NAEA). As a reference, NPP Surry Unit 1 (USA), equipped with 800 MWe Westinghouse triple-loop PWR (pressurized water reactor), has been chosen. The emergency coolant injection (ECI) function availability following the small break loss of coolant accident (SBLOCA) was thoroughly analyzed. The approach and data, which were adopted for the selected part of the SBLOCA sequences, were those used in the U.S. NRC Reactor Safety Study (WASH-1400). As a result of this study, the SBLOCA event tree, including ECI systems, i.e. high pressure injection system (HPIS) and auxiliary feedwater system (AFWS) reliability models, was developed and quantified. The probability of each accident sequence was evaluated using Saphire v.8, the PSA software by U.S. NRC. The choice of the software was based on earlier PSA software study. The failure probability of at least one of the considered safety systems – P(FAIL) is equal to 5.76E-3 and the most pessimistic accident branch (unavailability of both HPIS and AFWS) is about 0.05% of P(FAIL). These results were obtained based on assumption that the SBLOCA has occured. The most significant failure components are those corresponding to charging pumps unavailability, loss of electric power and human errors.

**Key words:** probabilistic safety assessment (PSA) • small break LOCA (SBLOCA) • emergency coolant injection (ECI) • high pressure injection system (HPIS) • auxiliary feedwater system (AFWS)

M. Borysiewicz✉, K. Bronowska, P. Kopka, K. Kowal, T. Kwiatkowski, A. M. Prusiński, P. A. Prusiński, G. Siess
Nuclear Energy Division,
National Centre for Nuclear Research (NCBJ),
7 Andrzeja Sołtana Str., 05-400 Otwock/Świerk, Poland,
Tel.: +48 22 718 0132, Fax: +48 22 779 3888,
E-mail: manhaz@cyf.gov.pl

Received: 19 October 2012
Accepted: 19 March 2013

## Introduction

The primary issue, when nuclear power plant (NPP) is designed, licensed and operated, is to carry out its safety assessment. For that reason safety assessment reports (SARs) have to be prepared. It is a common practice in many countries that SARs are issued in successive and complementary parts. The SAR represents an important communication between the operating organization and the regulatory body, and it forms an important part of the basis for licensing an NPP and an important part of the basis for the safe operation of the plant. For many years, the SARs were based on empirical and deterministic studies with the use of results of experiments and conservative simulations, covering thermal-hydraulic issues, structure mechanics, neutron kinetics and radiation protection.

Nowadays the probabilistic safety assessment (PSA) is considered to be an important tool for a comprehensive safety analysis of nuclear power plants accounting for the variety of initiating events that can be caused by a random component failure and human error, as well

as internal and external hazards (fires, flooding, etc). The PSA is complementary to deterministic safety assessment (DSA) in its scope and provided results [3].

PSA provides a methodological approach to identification of accident sequences leading to core damage and radioactivity releases from the plant containment that can follow from a broad range of initiating events and it includes a systematic and realistic determination of accident frequencies and consequences [1]. With PSA it is easier to identify and thus to avoid common cause failures, when one fault can cause more than one negative effect or to check if the engineered redundancy is really effective, i.e. whether the unavailability of separate technological trains designed for the same purpose may be affected by failures of common components, harsh work environment, faulty, maintenance procedure or external events.

Although this approach is well known since the 1970s [8], its importance for the NPPs safety assessment has been recognized very recently by the majority of nuclear regulatory bodies and operators all over the world. It has been also considered by the national regulation as the required element of the SAR for the NPPs to be located in Poland [7].

## The PSA methodology

The comprehensive PSA analysis is usually partitioned into three levels. Level-1 PSA is to estimate the probabilities of accident sequences making use of the reliability estimations of reactor safety systems and their components, whose functionality is crucial in case for the analyzed accident. As a result, the frequency of a core damage (CDF) can be assessed [4]. Level-2 PSA models: phenomena that could occur following core damage; challenges to the containment integrity; transport of radioactive material in the containment and estimates the frequency; magnitude of a release of radioactive material to the environment [5]. Level-3 PSA models the consequences of a release of radioactive material to the environment and estimates the risks to public health and societal risks such as the contamination of land or food. This paper is devoted only to certain safety systems considered at PSA Level-1.

The PSA Level-1 analysis workflow is illustrated in Fig. 1. At first, the plant design information, i.e. the component (equipment) characteristics or human actions are collected and then all the potential events that could initiate an accident should be outlined. The occurrence probability of an accident has to be assessed. Afterwards, the success criteria for every single safety system required to mitigate an accident are identified and all the potential sequences in the accident progress are predicted. These sequences are then depicted in the form of an event tree (ET). In order to quantify the event tree, it is necessary to develop fault trees (FTs), by identification of basic events (BEs), i.e. equipment failures and human errors, that could cause a failure of the safety system, and their relations. The deep study should base on the information about failures, troubles, etc. obtained from the operating experience and those gathered in dedicated databases. As a result of PSA Level-1, the core damage frequency (CDF) for each

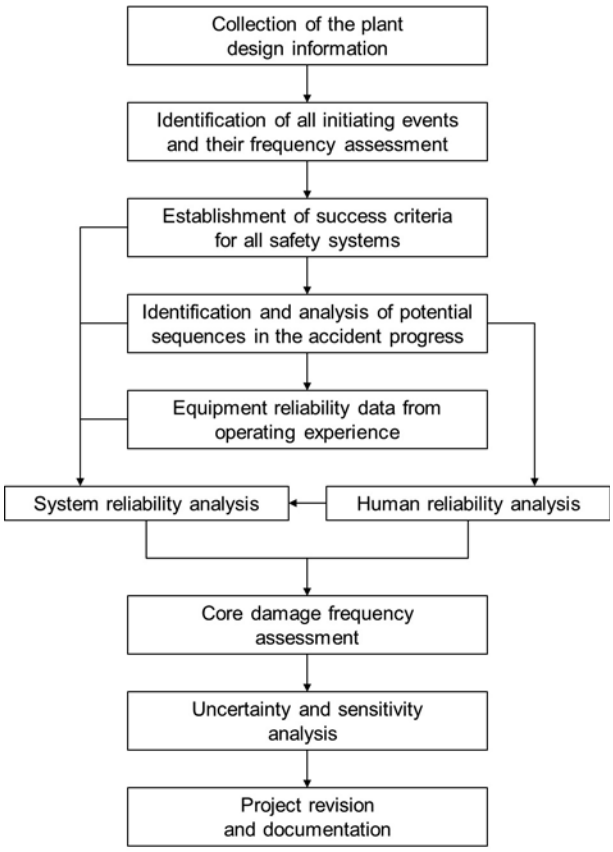


**Fig. 1.** Workflow of PSA Level-1.

accident sequence is assessed. Summing them up, one evaluates the total CDF in case of postulated initiating event. After all, the results should undergo uncertainty analysis in order to prove their level of confidence. Finally, one needs to gather all the information in the form of project documentation [4].

### Methodology of the event tree construction

The PSA Level-1 procedure starts from the definition of an accident, then the relevant engineered safety features (ESFs) – risk mitigation barriers, have to be identified. By the definition ESF is a function or action that can be performed using one or multiple safety systems. Actually, almost each safety system is playing more than one role, depending on time and type of an accident, which means it can be used by different ESFs while different accident scenarios. Since some relations between systems exist, they have to be also taken into account. After that, the structure of event tree (ET), which describes all possible accident sequences, can be developed (Fig. 2). The consequences of initiating event depend on success or failure of relevant safety systems, what is depicted as a form of tree branches on ET. The upper branch is for the success and the lower one for failure. The tip of each branch represents the plant state, as a result of the initiating event and a particular combination of subsequent events.

To evaluate the probability of a certain accident mitigation sequence to occur, one needs to estimate the reliability of each ESF or relevant safety systems. For this purpose, the fault trees (FT) are created.

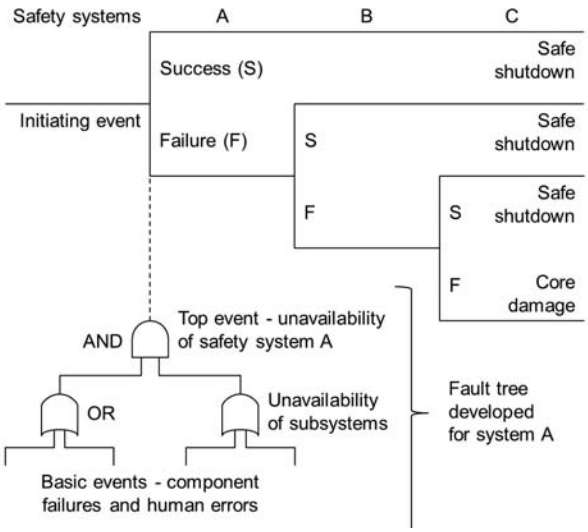


**Fig. 2.** Framework of PSA Level-1.

## Methodology of the fault trees construction

The idea of fault tree construction is to evaluate the probability of considered system unavailability. It should be noticed that unavailability does not necessarily mean total loss of system capabilities, but rather – reduced functionality or its flexibility required to perform its role properly enough to achieve success criteria. The unavailability is a failure branch by means of event tree (ET) and top event in case of fault tree (FT) [4].

It enables to calculate the probability of the top event based on probabilities of basic events and the Boolean algebra, in the sense of creation logic sums and products according to the relations between events. By applying Boolean operations, the irreducible logical expressions can be obtained, corresponding to the various shortest ways by which the analyzed system can fail to perform its functions. These expressions are known as minimal cut sets (MCSs) and play an important role in understanding how the whole system functions. They are used afterwards to compute the contribution of every single basic event (and the following branch) to the final accident scenario.

Depending on the assumptions or software applied, the set of FT elements may be different. Nevertheless, the most significant are those shown in Fig. 3. Although they are very basic, some explanations are necessary at least for the two latter ones. The undeveloped event is a kind of event that could be further developed, but its probability is known and its expansion is neither possible due to lack of full set of data nor the development itself would contribute to the project much. In that case also the level of project details must be considered, basing on engineering judgment. The second one is a transfer to subtree and it is used when the main FT has to be sliced into smaller pieces. It is necessary when FT becomes too big or unclear to read due to the number of branches.

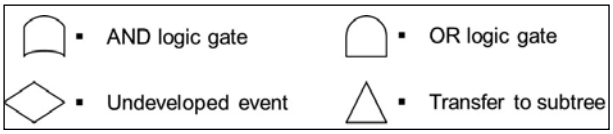


**Fig. 3.** Basic fault tree elements.

## The frequency assessment and failure modes

When the ET and all related FTs are developed and quantified, one is ready to start the analysis. There are various methods to find unknown probabilities and their level of confidence. With the log-normal distributions defined and assigned, the distributions then are propagated to yield the system distribution and range. The most viable approach to distribution or uncertainty propagation is to use computerized Monte Carlo (MC) techniques. For each fault appearing in the Boolean expression for a system FT, a particular failure rate is obtained by a random sampling of the appropriate log-normal probability distributions. These failure rates are then used to compute a value for the top event characteristic (e.g. unavailability) as discussed in the results section later on. This process is repeated for a large number of trials to obtain a distribution of top event characteristics. In the present study 10 000 such trials were run for each system.

Nevertheless, when the analysis is done, one can finally check the system in the sense of the so-called component failure modes. The main safety idea implemented by nuclear industry is to avoid the situations, when the failure of a single component can cause unavailability of the whole safety system. For that reason, one designs backup circuits (or loops) able to play the same role independently, but not necessarily in the same way. Such design is called redundant and the situation, when more than one of the redundant circuits (or loops) fail to operate at the same time, is called double, triple etc. failure mode.

Another issue to evaluate are the so-called common cause failures, which describe such a situation, when a single component fault can affect more than one independent safety line. Lack of independency leads to reduction of redundancy factor and, in turn, the safety.

One of the most significant contributor to the unavailability of safety system is human error as it was proved in this study. The problem with human errors is that it is difficult to assess them with a high degree of confidence, though different techniques and methods were and are developed until today. It is enough to mention robust studies based on human error analysis and reliability assessment (HEART) or technique for human error rate prediction (THERP) approaches. These errors may come from either lack of experience or due to routine, either due to increased stress or lack of motivation etc. That is why it is necessary to find a rational optimum for human work conditions. For that reason, more conservative approach is applied than in the case of equipment.

## The loss of coolant accident (LOCA)

In this PSA Level-1 study the loss of coolant accident (LOCA) has been chosen as an initiating event. LOCA is commonly thought of as being initiated by the break or rupture of a pipe in the reactor coolant system (RCS). RCS ruptures which result in loss of coolant accidents can be categorized as a function of rupture location. According to WASH-1400 [8], the significant LOCAs

can be covered by six categories, depending on size and break location with respect to the RCS main circulating water pumps, pressurizer and steam generator. In this study the small break LOCA, in the range of diameters $d = 0.01$–$0.05$ m, located at the one of reactor cold legs, has been analyzed. As the reference NPP Surry Unit 1 (USA), equipped with 800 MWe Westinghouse triple--loop PWR, has been chosen.

Although the size of the rupture seems not to lead to core damage itself, its location makes a difference. Taking the very end of cold leg into account as a break point, one assumes the most conservative approach. It is more difficult to bypass the flow via the safety systems in case of LOCA occurring at the end of cold leg than in the other parts of RCS, since all the safety (refilling) systems are placed before and not after the leakage point. As it is discussed further on, in some unfortunate cases even that small rupture may lead to undesired situation when reactor core is uncovered and starts to melt.

During small break LOCA, the pressure in RCS falls down slower than in case of a large break, running at first high pressure injection system (HPIS) and stabilizing the pressure at a higher level than that at which the low pressure injection system (LPIS) begins to operate. In order to shut down the reactor safely, the operator must then reduce the temperature and pressure to be able to use LPIS. For that reason, the additional heat sink is required. This is normally achieved with the help of the steam generators, the auxiliary feedwater system (AFWS) and by opening the relief valves on the secondary side. Alternatively, the operator can manually break the isolation of a loop in the main feedwater system (secondary side) and use the turbine condenser as a heat sink directly [6].

## PWR emergency coolant injection

The SBLOCA, considered in this study, can potentially lead to a wide range of accident sequences. The probability of each sequence and its consequences depends on the success or failure of various safety systems, installed in the nuclear power plant to perform ESF. There are several ESFs in PWR, whose implementation is crucial in case of losing water from the RCS. Each of these functions has a special assignment related to mitigation of the SBLOCA consequences, and when taken together, are designed for preventing reactor core damage. In this study only one of them, the ECI, implemented by HPIS and AFWS, was thoroughly analyzed in case of the SBLOCA located at the one of reactor cold legs. The ECI is designed to provide quickly sufficient emergency coolant to flood the reactor core with borated water following a LOCA in the RCS. Operability requirements for ECI safety systems are dependent on the size and location of the RCS break. The SBLOCA, even at the most pessimistic location meaning the reactor cold leg, requires only one of the three HPIS pumps to be maintained [8].

### High pressure injection system (HPIS)

The main purpose of ECI is to replace the coolant lost following a LOCA, so that the core cooling is maintained. The HPIS provides a high pressure source of water to the RCS in the event of small and medium-size breaks. For large LOCA, when the loss of pressure is more rapidly, its functions takes over the LPIS. Another function of HPIS is to push a 12% boric acid solution to the RCS after the reactor shut down in order to keep the negative reactivity and prevent an uncontrolled neutron flux excess [8].

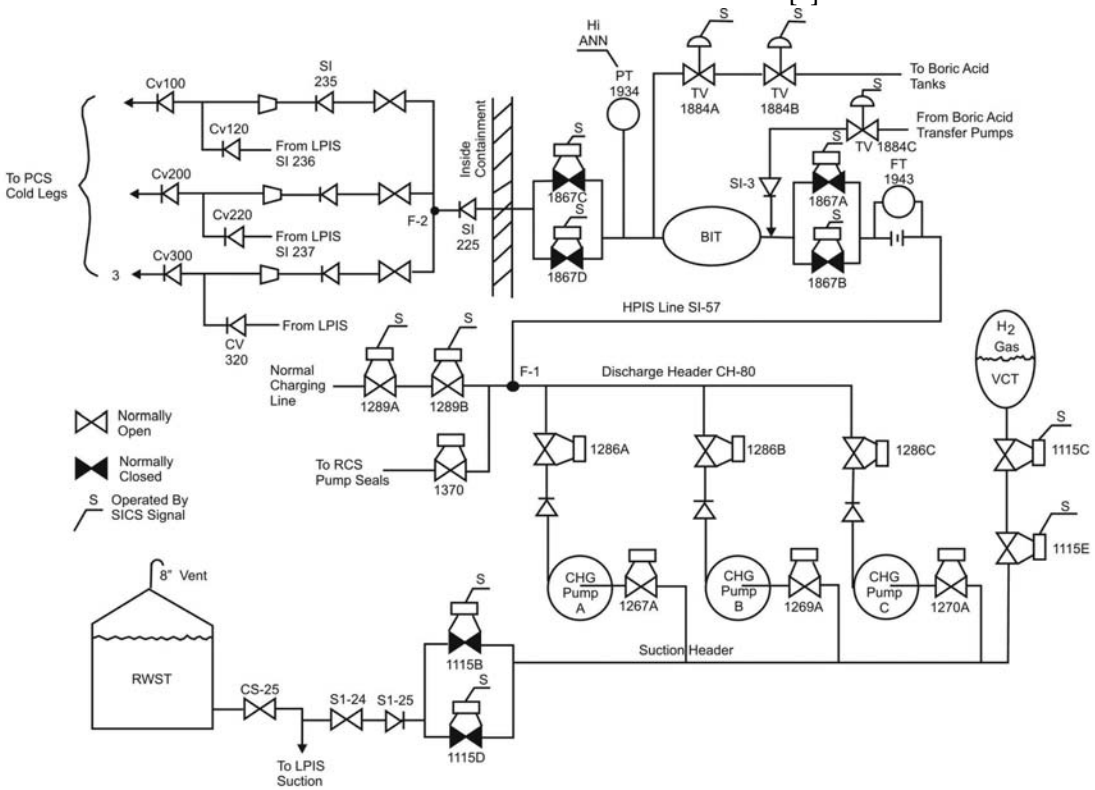


**Fig. 4.** Simplified HPIS system diagram [8].

There are two configurations of the HPIS. One of them is designed for the normal and the other for the emergency state of NPP. During the normal operation, one operating charging pump (CHG Pump A) draws water from volume control tank (VCT) and discharges it to the RCS through the open valves 1289A and 1289B (Fig. 4). The other two of the three HPIS charging pumps (CHG Pumps B and C) are on standby. At the same time, a small amount of water is served from RCS through the chemical and volume control system (CVCS), whose function is to purify the coolant using special filters, demineralizers and other chemical equipment. Then, the coolant returns to the VCT. In addition, the HPIS system supplies a small flow of high pressure water to the seals of the RCS pumps in order to cool them down. This flow continues even during LOCA.

The emergency operation of HPIS is initiated by the safety injection control system (SICS), which responds to signals from the RCS pressure transducers. When pressure drop in RCS is identified, the SICS actuates HPIS reconfiguration process. For this purpose, the parallel supply valves 1115B and 1115D must be opened to provide water supply from the external refueling water storage tank (RWST). Then, the two standby charging pumps are started. After that, the VCT isolation valves 1115C and 1115E must be closed, as well as the normal charging line valves 1289A and 1289B. In order to discharge the flow through the boron injection tank (BIT) to the RCS cold legs the two pairs of parallel valves, 1867A and 1867B (at the BIT inlet), as well as 1867C and 1867D (at the BIT outlet), must be opened by the SICS signal.

Closure of the boric acid recirculation line trip valves (1884A, B and C) is also required for proper HPIS operation in the emergency regime and it is actuated by SICS. Continuous recirculation of boric acid solution is justified only during normal operation, when there is no flow through the BIT. The boric acid recirculation serves in that case to assure that BIT is full, and to help prevent boron precipitation by keeping the solution mixed. The additional protection against boron precipitation and thus the valves plugging is the strip heaters isolation. Since the boron precipitation, which can lead to valves plugging, occurs at a temperature below 328 K, the strip heaters isolation is used for piping and valves in this part of the system. Moreover, the temperature alarms and backup heaters are provided to prevent heat tracing circuit failures.

The requirements for successful HPIS operation relay also on efficient cooling of the charging pump seals and lubrication oil. It depends, in turn, on the availability of charging pump support subsystem (CPSS), which consists of two redundant pumps dedicated to the seals cooling and two others, also redundant, pumps to lubrication oil cooling. Therefore, it has to be also taken into account in HPIS reliability analysis.

Another aspect of HPIS efficiency is the availability of electrical power, whose supply is necessary, e.g. for motors of the charging pumps. The emergency power system (EPS), which is responsible for the electrical energy distribution after the main generator closure, consists of: two sources of off-site AC power, two diesel generators and two sources of DC power in the form of 125 V batteries. In addition, it is formed into redundant, independent trains A and B, which consist of several buses with different voltages, adapted to equipment that must be operable.

Both trains can be powered by the off-site and on-site (diesel generators) sources. If the train A is damaged or there is a loss of power on its particular buses, the HPIS equipment can be switched to the appropriate buses of the train B. Failure of both redundant trains of the EPS will result in failure of the HPIS. Therefore, the failure probability of particular power buses is an input to the evaluations for the HPIS system unavailability.

### Auxiliary feedwater system (AFWS)

Although, the success criterion of the ECI in case of SBLOCA is the flow capacity of at least one HPIS charging pump, the auxiliary feedwater system (AFWS) reliability was also analyzed in this study. The function of this system is to provide auxiliary feedwater to the secondary side of the steam generator during the main feedwater source unavailability. This situation takes place also after the reactor shutdown and the main turbine closure in the wake of the SBLOCA identification. Although, in this case the nuclear chain reaction is no longer maintained, decay heat is still produced and must be removed.

The AFWS consists of three pumps, two electric and one turbine driven, which can be started either automatically or manually (Fig. 5). The electric pumps are started automatically in the case of SICS signal presence, off-site power loss, main feedwater pumps failure or low water level in a steam generator. The turbine one is started automatically only in two cases, when low water level in steam generator is detected or loss of off-site power occurs. Each of these pumps can draw the water from the external reservoir with a capacity of over 400 $m^3$ via separate suction line. Then, the water is delivered redundantly by two headers, and each of the three steam generators can receive condensate from either of them. There are also two additional water sources with a capacity of about 1000 and 1500 $m^3$, but to make them available the manual valve operation is required.

The decay heat mentioned above, is quite high only at the short time upon the reactor closure. After the first hour of the reactor shutdown, it decreases from around 7% down to only 2% of the initial power, and after the first day it is even lower than 0.5%. For that reason, the AFWS system has been designed to remove decay heat during the first eight hours after reactor closure. It should be noted that the system is characterized by the high level of redundancy and the design assumptions, when taken into account, can lead to conclusion that the AFWS is a highly reliable system.

However, there are some interfaces with another systems like the EPS or the SICS, which can affect the AFWS unavailability. Furthermore, for certain actions (e.g. additional water source valve-in) the manual valve operation is required. For this reason, the AFWS system seems to be sensitive for human errors, which should be examined particularly.

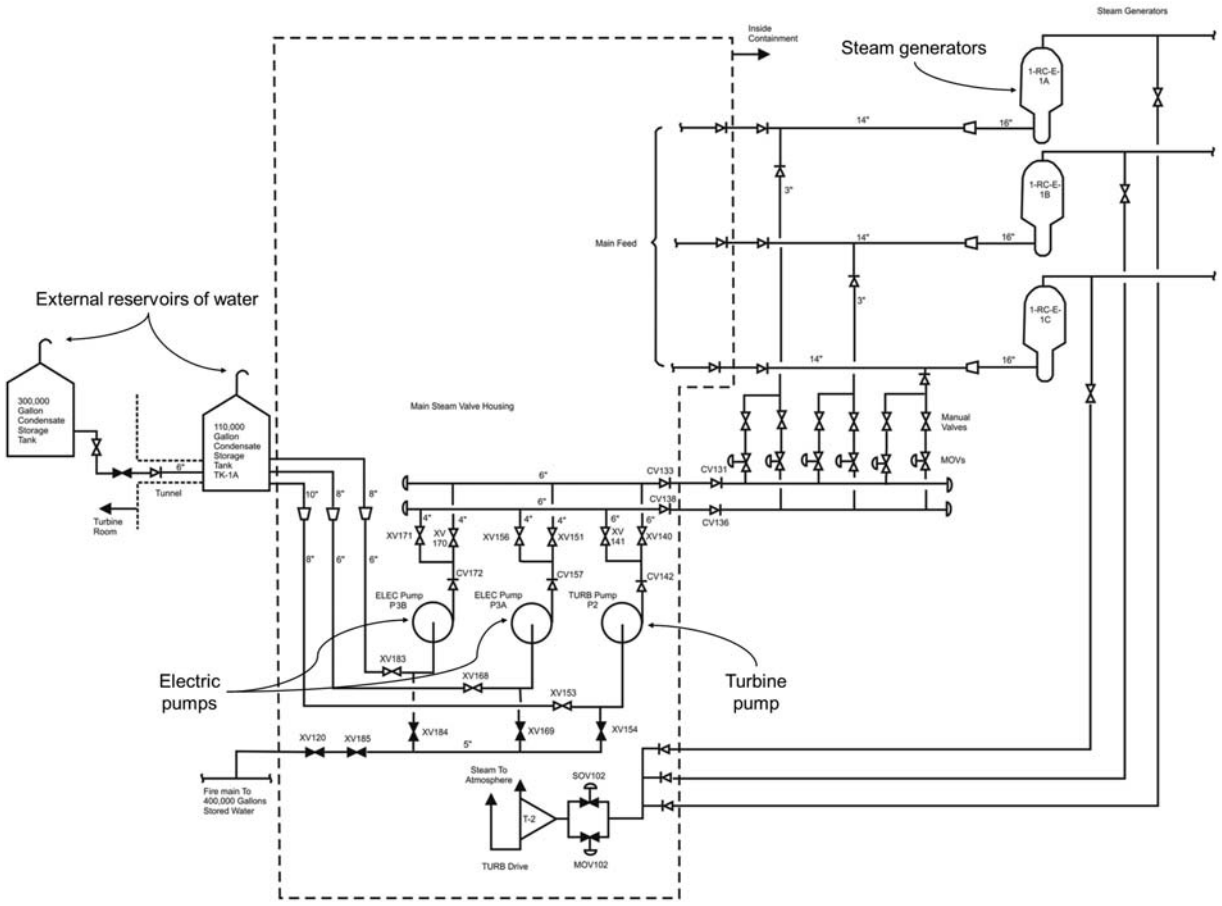


**Fig. 5.** Simplified AFWS system diagram [8].

## Results and discussion

The fault trees of the considered safety systems have been developed to determine all possible ways leading to their unavailability. For this purpose, faults of the basic elements of the systems like pipes, valves, pumps, controls and instrumentation were thoroughly analyzed using detailed plant design information.

In addition to component failure modes, human errors and common failures were also considered in this study. Furthermore, the fault tree analysis for both HPIS and AFWS included identification and examination of their interfaces with the other systems like electrical power. For this reason, the analysis of some equipment required consideration of the electrical power sources availability, components of the control circuit failures, SICS interface signal, etc.

After that, the qualitatively significant failures were identified and grouped into: single failures (e.g. single check valve fails to open), double failures (e.g. the failure of both parallel valves at the same time), triple failures (various triple failure combinations), as well as the charging pumps and theirs motors failures. Then the quantitative fault trees evaluation was prepared based on reliability data of basic elements and their logical connections, corresponding to the technical design of considered safety systems. The fault trees were evaluated using Saphire v.8, the PSA software by U.S. NRC (United States Nuclear Regulatory Commission). The choice of the software was based on earlier PSA software study [2].

### HPIS fault tree analysis and quantification

The function of HPIS in the case of SBLOCA, that occurred at one of the three reactor cold legs, is to deliver a sufficient amount of borated water to the two others during the first 30 min. Therefore, the unavailability of this system can be defined as failure to deliver sufficient borated water to cold legs 2 and 3 when LOCA at cold leg 1. This is also the top event definition of the HPIS fault tree (Fig. 6). However HPIS is a rather complex system and more than one fracture point can be identi-

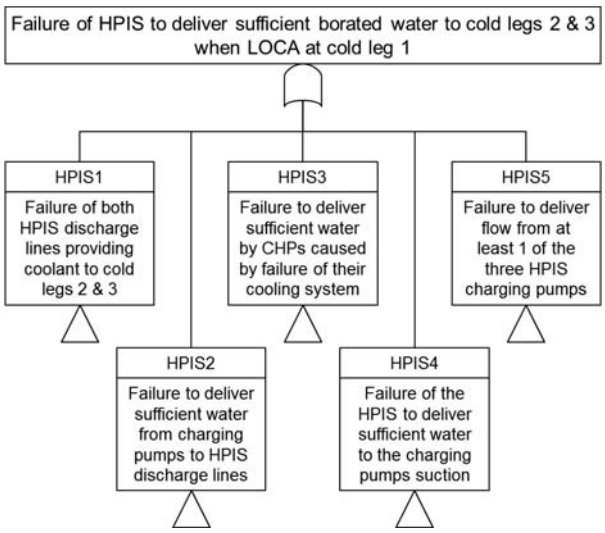


**Fig. 6.** The main contributions of the HPIS fault tree.

fied. Usually, in such cases, the whole system is divided into the major functional parts whose failures lead to the overall unavailability of the system. It forms the first branching of the system fault tree.

The five possible ways corresponding to failures of different HPIS parts and leading to its unavailability were identified in this study and depicted in Fig. 6. The first part of the system (HPIS1) are the three discharge lines, located inside the containment and providing borated water directly into the cold legs of the reactor coolant system (Fig. 4). Assuming LOCA at one of the cold legs, there are only two possible ways by which the water can be supplied. Thus, the simultaneous failure of both HPIS discharge lines, providing water to the cold legs free of LOCA, leads to loss of the HPIS functionality. The probability of this event P(HPIS1) is equal to 7.29E-6. This value was calculated based on the analysis of failure frequency of the valves placed on the discharge pipelines (Fig. 4). Human errors associated with manual control of some valves and their maintenance are also included.

Assuming that there is no failure of HPIS discharge lines, one can analyze availability of the second section of the system (HPIS2) which starts from the charging pumps (point F-1 in Fig. 4) and ends inside the containment (point F-2 in Fig. 4). Probability of failure to deliver sufficient water through this section P(HPIS2) is equal to 1.98E-03. This event may be caused by such failures like rupture of the HPIS line SI-57, rupture of the boron injection tank (BIT) or boron precipitation, which leads to plugging the valves.

The third branch of the HPIS fault tree (HPIS3) are failures of the charging pumps caused by their cooling system unavailability. It covers all potential problems with cooling of the seals and lubrication oil, including insufficient electrical power on the CPSS busses. The probability of such an event P(HPIS3) was assessed as 7.78E-5.

Another issue is the failure to deliver sufficient water from the RWST to the charging pump suction (HPIS4). The probability of this event P(HPIS4) is equal to 1.43E-3. This value was calculated based on the analysis of failure frequency of the valves placed on the pipelines between the RWST and the charging pumps. Ruptures of the pipes and leakage of the RWST itself was also considered here.

The last branch of the HPIS fault tree (HPIS5) relates to unavailability of the three charging pumps at the same time caused by factors other than the problems with their cooling, e.g. failures of their motors or the lack of electrical power. The probability of this event P(HPIS5) is equal to 1.67E-3.

Summing up the probabilities of events HPIS1, HPIS2, HPIS3, HPIS4 and HPIS5 one can obtain the total HPIS failure probability P(HPIS) which is equal to 5.17E-3. In Fig. 7 percentage of these five HPIS fault tree contributors is presented. The whole fault tree for HPIS consists of 217 elements and the following basic events were identified as the most significant contributors to the HPIS failure:

– failures of CHP motors (~ 10%),
– parallel valves failures (~ 7%),
– human errors related to manual valves position switch (~ 6%).

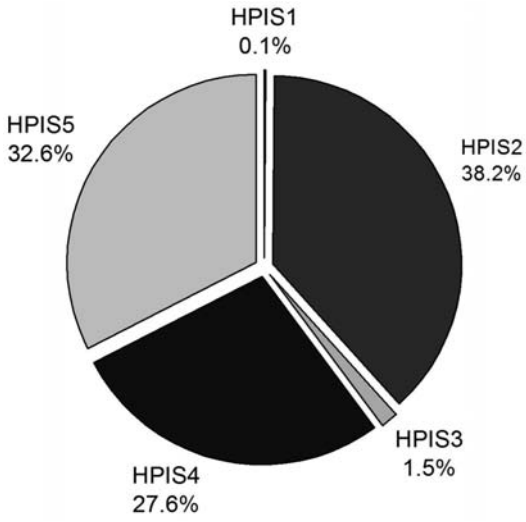


**Fig. 7.** Percentage of HPIS fault tree main contributors.

P(HPIS) was initially calculated based on the assumption, that the probability of each basic event is given by a specific point value. However, in a real case the frequency of both equipment failures and human errors is specified by statistical distributions. In order to improve the results a log-normal distribution was assumed for all basic events in the HPIS model. Relevant parameters of the probability distribution for each event were adopted based on the data from WASH-1400. Then, the Monte Carlo simulation was run 10 000 times. Every time the probabilities of particular basic events were chosen randomly from the range defined by their distributions which gave in result 10 000 different values of P(HPIS). Thus, the probability of failure of the HPIS system P(HPIS) can be treated as a random variable. This was shown in Fig. 8 where on the y-axis the num-

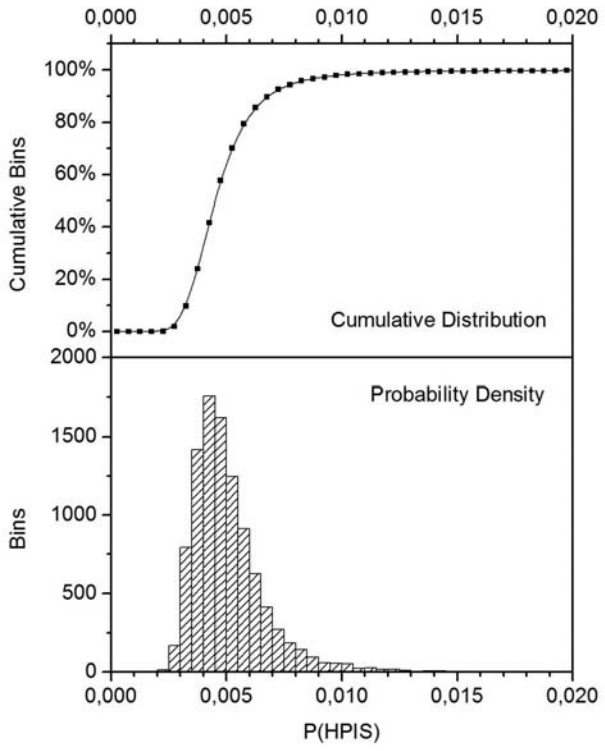


**Fig. 8.** Probability density and cumulative distribution of P(HPIS).

**Table 1.** Final results of the Monte Carlo simulations for P(HPIS)

| | |
|---|---|
| Mean value | 5.17E-3 |
| Median value | 4.75E-3 |
| 5th % value | 3.26E-3 |
| 95th % value | 8.18E-3 |
| SD[a] | 2.19E-3 |

[a] SD – standard deviation.

ber of Monte Carlo bins is presented vs. probability of system failure. Final results of the MC simulations for P(HPIS) are collected in Table 1.

## AFWS fault tree analysis and quantification

In case of AFWS, the failure criteria were defined as insufficient auxiliary feedwater delivered to at least one steam generator during the first 8 h. For this case, a slightly different approach was introduced, by means of single, double and triple failures investigation and their influences on AFWS unavailability. The analysis proved that triple failures give the biggest feedback to the system that is over 95% of the top event probability (Fig. 9). The point value of the AFWS system failure P(AFWS) was calculated as 5.92E-4. However, in order to find the uncertainty of this value the P(AFWS) was treated as random variable, which is shown in Fig. 10 where on the y-axis the number of Monte Carlo bins is presented vs. probability of the AFWS system failure. Final results of the MC simulations for P(AFWS) are collected in Table 2.

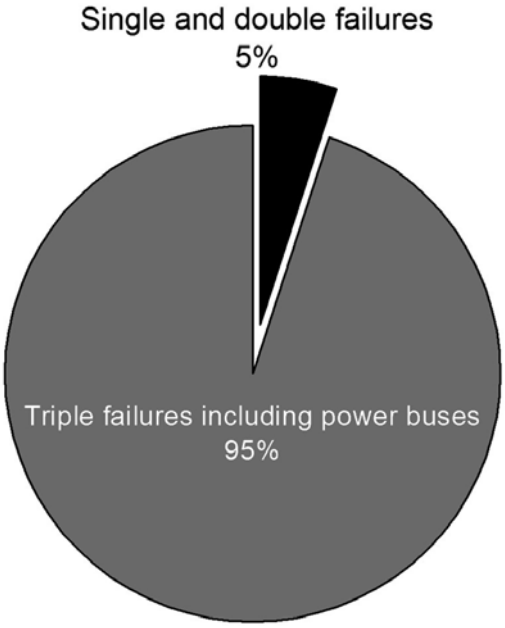


**Fig. 9.** Percentage of AFWS fault tree main contributors.

**Table 2.** Final results of the Monte Carlo simulations for P(AFWS)

| | |
|---|---|
| Mean value | 5.91E-4 |
| Median value | 3.99E-4 |
| 5th % value | 1.23E-4 |
| 95th % value | 1.53E-3 |
| SD[a] | 8.61E-4 |

[a] SD – standard deviation.

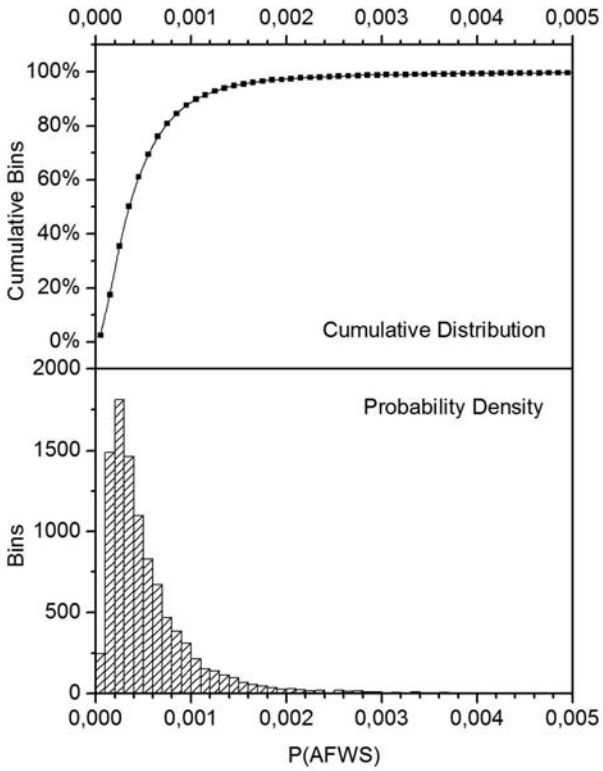


**Fig. 10.** Probability density and cumulative distribution of P(AFWS).

The triple failure actually stands for unavailability of all 3 AFWS pumps (Fig. 5). It should be noticed however that those pumps are not of the same kind. Two of them are electrical (and powered by two independent trains) and one turbine (driven by steam). The situation when all of them are detached from the system seems to be unlikely. The results of the analysis reveals the following conclusions. The probability of situation where there is no flow from the turbine pump is equal to 7.18E-3, while no flow from both of the electric pumps at the same time is just 7.76E-5. However, in case of electrical pumps, one should take into account also the common mode failures. Such a situation could be the case when both electrical pumps are out of power due to one common cause that eliminates two independent power buses. The probability of that case is estimated as equal to 3.7E-2, which makes it actually the main contributor to AFWS failure.

## SBLOCA event tree construction

As a result of this study, the SBLOCA event tree, including ECI systems (HPIS and AFWS) reliability models, has been developed and quantified. The probability of each accident sequences was also evaluated. The most probable accident sequence is the optimistic one called SUCCESS, corresponding to availability of both HPIS and AFWS systems (Fig. 11). The total failure probability of at least one of the considered safety systems P(FAIL) is equal to 5.76E-3 and the most pessimistic accident branch FAIL3 (unavailability of both HPIS and AFWS) is about 0.05% of P(FAIL). Moreover, the Monte Carlo simulations were performed in order to assess the uncertainty of P(FAIL). Results of these

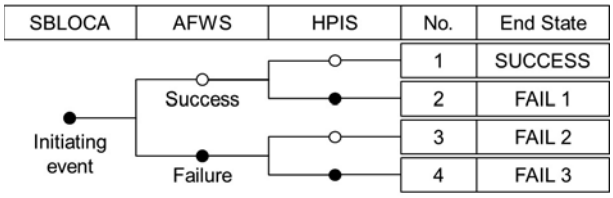


**Fig. 11.** The SBLOCA event tree, including ECI systems reliability.

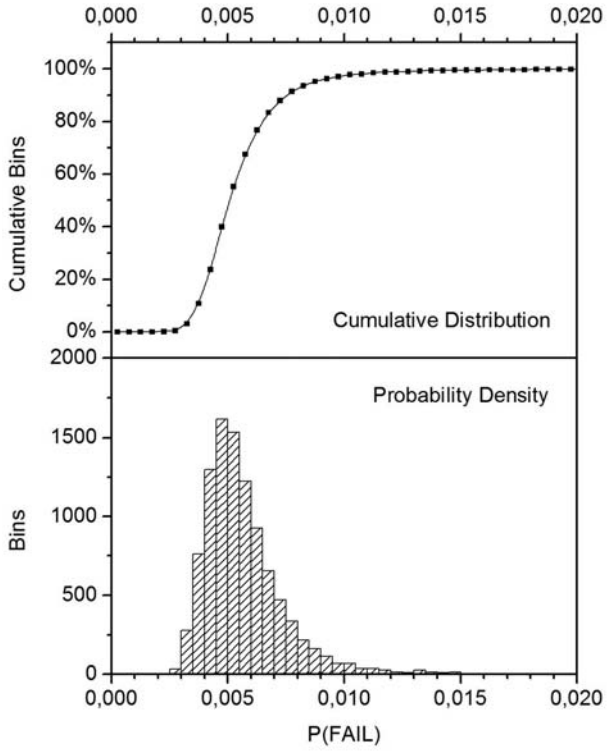


**Fig. 12.** Probability density and cumulative distribution of P(FAIL).

**Table 3.** Final results of the Monte Carlo simulations for P(FAIL)

| | |
|---|---|
| Mean value | 5.74E-3 |
| Median value | 5.32E-3 |
| 5th % value | 3.66E-3 |
| 95th % value | 8.95E-3 |
| SD[a] | 2.20E-3 |

[a] SD – standard deviation.

calculations are presented in Fig. 12 and Table 3. The most significant failure components are those corresponding to charging pump unavailability, loss of power and human errors. Moreover, the obtained results are consistent with those published by the U.S. NRC in the WASH-1400.

**Acknowledgment.** The authors of this paper are pleased to acknowledge the support of the U.S. NRC and PAA (National Atomic Energy Agency, Poland) that provided the necessary PSA software. Special thanks should be directed also to Prof. W. Wiślicki – Head of the Świerk Computing Centre project. The work was supported by the EU and MSHE grant no. POIG.02.03.00-00-013/09.

## Abbreviations

AC – alternating current
AFWS – auxiliary feedwater system
BE – basic event
BIT – boron injection tank
CDF – core damage frequency
CHP – charging pump
CPSS – charging pump support subsystem
CVCS – chemical and volume control system
DC – direct current
DSA – deterministic safety assessment
ECI – emergency coolant injection
EPS – emergency power system
ESF – engineered safety feature
ET – event tree
FT – fault tree
GPSA – Probabilistic Safety Analysis Group
HEART – human error analysis and reliability assessment
HPIS – high pressure injection system
LOCA – loss of coolant accident
LPIS – low pressure injection system
MCSs – minimal cut sets
MC – Monte Carlo
NAEA – National Atomic Energy Agency
NCBJ – National Centre for Nuclear Research
NPP – nuclear power plant
PSA – probabilistic safety assessment
PWR – pressurized water reactor
RCS – reactor coolant system
RWST – refueling water storage tank
SAR – safety assessment report
SBLOCA – small break loss of coolant accident
SICS – safety injection control system
THERP – technique for human error rate prediction
U.S. NRC – United States Nuclear Regulatory Commission
VCT – volume control tank

## References

1. Borysiewicz M (2010) The PSA (Probabilistic Safety Assessment) technique in defining safety regulations for nuclear power plants. IEA POLATOM, Otwock-Świerk, http://ncbj.gov.pl/raporty/
2. Borysiewicz M, Potempski S, Prusiński P, Wasiuk A (2010) Evaluation of software for analysing event/fault trees from the nuclear power plant PSA point of view. IEA POLATOM, Otwock-Świerk, http://ncbj.gov.pl/raporty/
3. IAEA (1999) Basic safety principles for nuclear power plants. IAEA INSAG-12. International Atomic Energy Agency, Vienna
4. IAEA (2010) Development and application of Level-1 Probabilistic Safety Assessment for nuclear power plants. IAEA SSG-3. International Atomic Energy Agency, Vienna
5. IAEA (2010) Development and application of Level-2 Probabilistic Safety Assessment for nuclear power plants. IAEA SSG-4. International Atomic Energy Agency, Vienna
6. Pershagen B (2009) Light water reactor safety. Pergamon Press, Nyköping

7. Regulation of the Polish Council of Ministers of 31 August 2012 on the scope and methods of safety analyses performed before applying for an authorization of a nuclear facility construction, and the scope of the preliminary safety assessment report for the nuclear facility. Dz U (Law Gazette) 2012 no 0 item 1043 (in Polish)

8. US Nuclear Regulatory Commission (1975) Reactor Safety Study – An assessment of accident risks in US commercial nuclear power plants. US NRC NUREG 75/014. Washington, DC