5

Low Power and Shutdown PSA for the Nuclear Power Plants with WWER440 Type Reactors

Zoltan Kovacs
RELKO Ltd, Engineering and Consulting Services
Slovakia

1. Introduction

Two nuclear power plants (NPPs) are in operation in Slovakia equipped with WWER440/V213 type reactors. The Jaslovske Bohunice V2 NPP has two reactors in operation, the Mochovce NPP has also two reactors in operation and another two reactor units are under construction which will be given into operation in 2013. Full power and shutdown level 1 and level 2 probabilistic safety assessment (PSA) as part of the plant safety report were performed for these plants by the RELKO PSA team.

The role of PSA for NPPs is an estimation of the risks in absolute terms and in comparison with other risks of the technical and the natural world. Plant-specific PSAs are being prepared for the NPPs and being applied for detection of weaknesses, design improvement and backfitting, incident analysis, accident management, emergency preparedness, prioritization of Research & Development and support of regulatory activities.

There are three levels of PSA, being performed for full power operation and shutdown operating modes of the plant:

- Level 1 PSA: The dominant accident sequences leading to the core damage are identified and the core damage frequency is calculated. The strengths and weaknesses of the safety systems and procedures to prevent the core damage are also provided as results.
- Level 2 PSA: The ways in which radioactive releases from the plant can occur are identified and the magnitudes and frequency of release are calculated. Detailed analyses of the containment are performed. Safety measures are proposed to minimize the release of radioactive materials into the environment after a severe accident.
- Level 3 PSA: The public health and other societal risks such as contamination of land or food are estimated. Damage to people (number of fatalities, the number of injured, reduction of life expectancy) and damage to property (loss of agricultural products and of natural resources, destruction, the cost of relocating the population and decontaminating effecting areas, etc.) are identified and safety measures are proposed to be implemented to minimize the risk. The Nuclear Regulatory Authority does not require the level 3 PSA for NPPs in Slovakia, however, the performance of analyses is strongly recommended.

There are two basic types of the plant outage: unplanned maintenance outages due to the repair of the components and planned refuelling outages. The differences are in:

- Safety systems availability,
- Duration of outage,
- Neutron and thermal-hydraulic conditions,
- Reactor coolant system (RCS) and containment configuration.

For the unplanned shutdowns, the operation can continue after several hours. In general, for these shutdown modes it is not necessary to achieve the cold shutdown state or to open the reactor vessel. Preparing of the action schedule is required for each shutdown of the unit, where the individual actions done by the personnel are indicated.

During these outages the reactor subcriticality is achieved by the insertion of all control rods into the core. Operational records of the WWER440 type reactors have shown us, that there are several events during the year where it is necessary to decrease the power for urgent repairs. The unplanned unit trip also occurred.

The outage of the reactor is planned once per year for the refuelling. These are the planned yearly outages for the refuelling of the reactor and the general plant maintenance. The reactor is cooled down to cold state and the reactor vessel is open. Only a fraction of the fuel is replaced by the new fuel (typically about 25% of the total number) in the short refuelling outage. The rest of the fuel elements remains in the reactor vessel during the outage. The refuelling is performed according to the approved refuelling program. These are the planned outages for the refuelling of the reactor and extended plant maintenance.

Long refuelling outage is performed every fourth year, and involves in-service inspection of the reactor vessel. The difference between the short and the long outage is mostly in the scheduled inspection of the reactor vessel. However, the whole reactor core is transferred to the spent fuel pool.

The risk from nuclear power plants was assumed for many years to be dominated by the risk during full-power operation. The deterministic licensing process, the PSA focused on full power. It seemed clear that shutdown was the safe condition.

After all, the reactor is shutdown, the decay heat is low, substantial time is available for recovery, and many recovery options are possible. On the other hand, a growing number of incidents during shutdown, some of them leading to substantial loss of reactor coolant through draining, began to focus attention on the possibility of significant risk during shutdown conditions. In fact, although decay heat is low, it can still be substantial and must be removed.

In addition, much equipment is unavailable due to maintenance, there may be unusual plant configurations, automatic safety features may be disabled, and manual response is required (often with little guidance from procedures and training). Also, knowledge of timing and success criteria is limited.

During last few years, operational experience and performance of the low power and shutdown PSA highlighted the magnitude of the risk contribution from those, previously considered safe operating modes. This risk was found to be significant. Many studies such as the shutdown PSA for PWR in Western Europe (France and Switzerland) and WWER plants in Central Europe (Slovak, Hungary and Czech Republic) as well as latest industry events, such as Paks NPP shutdown fuel damage accident, demonstrated that the core damage frequency (CDF) from an accident occurring during shutdown or low power operation modes was higher (up to 100% of CDF for some plants) than the one at power.

This risk is not related to the plant design. It is rather related to the unavailability of equipment due to maintenance activities undertaken during an outage, presence of

additional (contractor) personnel who may not be fully aware of the safety issues, presence of additional heavy loads and flammable materials, etc. All of these items increase the risk during plant outage.
Adequate planning and preparation of activities during outages can reduce both the probability and the consequences of possible events. In other words, there are a lot of possibilities for safety improvements in those operating modes. To decide what kind of improvements are the best on safety and cost beneficial grounds, a variety of analytical approaches could be used.
One of these is administrative control based on the experience of individuals involved in the outage planning. While any careful analysis will find ways to improve safety during outages, it is felt that this approach would not be best suited to very well handle a more complex interface, since critical configurations may not always be recognised.
Another approach is a PSA-type modelling, which considers a variety of interactions and dependencies of important systems. Performance of PSA for shutdown and low power operating modes (SPSA), may support the enhancement of the safety during plant outage, and may contribute to reduction of the outage duration. Thus a detailed analysis of shutdown operation may:

- contribute to a more economical plant operation,
- improve plant safety and
- decrease the consequences of incidents.

The full power PSA is no longer representative of the actual plant risk profile during the operational condition when the configuration of safety and support systems has changed extensively. This usually happens when the reactor power is below a certain level and automatic actuation of safety systems is being interlocked. Therefore, contribution of the risk during plant outage deserves a special attention and a shutdown PSA appears to be an ideal tool to improve safety during plant outage.
This chapter gives the view of level 1 and 2 SPSA modelling issues and results for the Slovak NPPs. The lessons learned in this area are presented and the PSA applications are described. The PSA models were developed in the RISK SPECTRUM PSA code.

2. Modelling issues related to Level 1 SPSA

The level 1 PSA study of the plant calculates the CDF and identifies the dominant initiating events (IE) and accident sequences that contribute to the core damage. The main modelling issues related to SPSA are described in this part of the chapter:

- Plant operating modes and plant operational states,
- Initiating events,
- Screening analysis,
- Modelling of accident sequences (fault trees and event trees),
- Human reliability analysis (HRA),
- Quantification of accident sequences and
- Application of SPSA.

2.1 Plant operating modes and plant operational states

The definition of the plant operating mode varies from country to country. The Slovak plants have adopted the USA definitions. There are seven operating modes, numbered 1 to 7. These are:

1. Full power operation,
2. Reactor criticality,
3. Hot shutdown,
4. Semi-hot shutdown,
5. Cold shutdown – reactor vessel is closed,
6. Cold shutdown – reactor vessel is open and
7. Empty reactor vessel (the fuel is removed from the reactor vessel and located to the spent fuel pool).

Understanding of plant operating modes and its characteristics in terms of systems available and the general plant conditions is essential for the development of the low power and shutdown PSA model. Operating modes are also highly important for defining the interface between power PSA and low power and shutdown PSA. For an integrated PSA model of a plant, it is significant to adequately define the interface between power PSA and low power and shutdown PSA. This interface does not necessarily coincide with the definition of the operating modes. Typically, the full power PSA considers 100% nominal power.

In terms of the thermal hydraulic response to an initiating event, there is not much difference between 100% power and lower power levels, expect that at lower power levels the time available for selected corrective actions may be somewhat greater. The 100% power case is therefore conservatively a representative of the whole spectrum of power levels.

When the reactor power reaches a certain power level, the automatic actuation of the safety systems is disabled. Depending on the reactor design, and in some cases on operating practice, this could be between 0-10% nominal power. This point is the natural interface between the full power PSA and SPSA (see Fig. 1).

While the reactor is on low power, even without automatic actuation of safety systems, the power PSA models (with appropriate modifications) could be used to determine the risk level. This is generally true also for the hot stand-by mode.

Once the reactor is in the shutdown mode, and especially when the decay heat is removed via residual heat removal system (RHR), the state of the plant is such that most of the power PSA models are not applicable without major modifications.

Plant operating modes are important from the standpoint of the conduct of the plant operation. For a SPSA the plant operating modes do not mean much. Due to extensive changes in plant configuration during a shutdown period, it is necessary to define plant operational states (POSs) which will properly reflect the plant configuration during an outage evolution.

The POS is used to define boundary conditions within which there would be no changes in major characteristics which are important for PSA modelling.

The POS is defined as a period during a plant operating mode when important characteristics are distinctively different from another plant operating state. The important characteristics describing a plant operating state are:

- RCS temperature and pressure,
- RCS water level (inventory),
- Decay heat removal,
- Availability of safety and support systems,
- Containment integrity,
- System alignments and
- Reactivity margins.

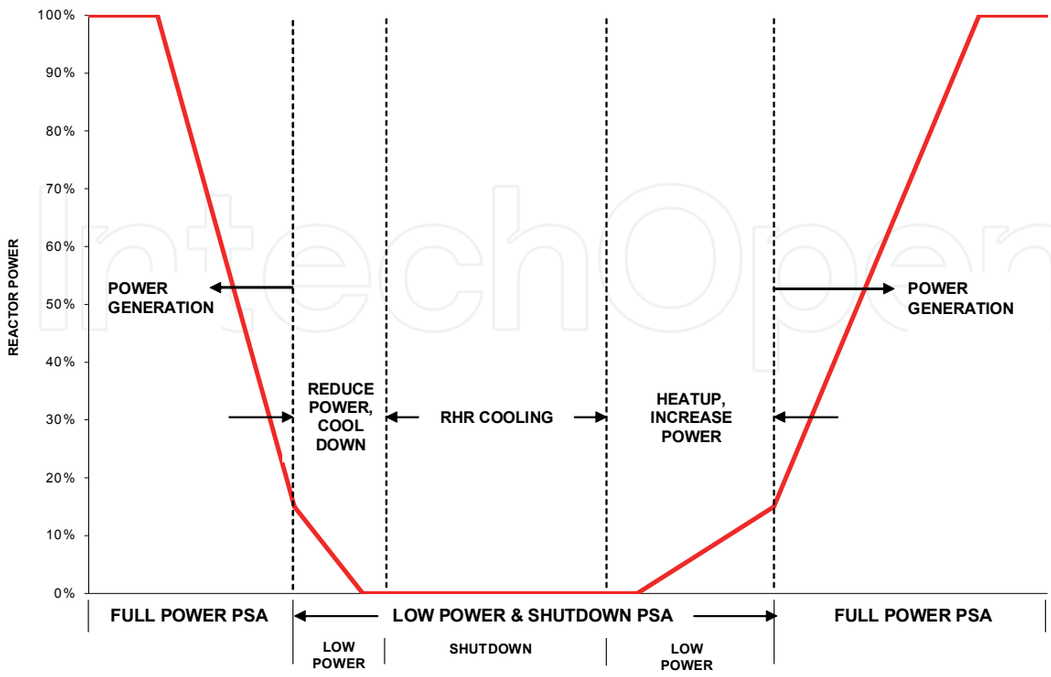


Fig. 1. Full power, low power and shutdown PSA

Some or all characteristics indicated above should be considered in defining the plant operational states. It is obvious that defining the POSs for every possible plant condition may result in a very large number of POSs. The attempt to define all the POSs which are relevant for SPSA could result in several hundreds POSs. One of the initial activities related to defining the POSs is their grouping to reduce the number of POSs to a manageable level. The grouping process shall consider issues like specific success criteria, typical IEs and system availability. The actual practice varies among PSA practitioners, but the general guidance is always to distinct POS in their main characteristic. A typical number of POSs considered in SPSA varies from 10 to 15. Newer studies tend to have more POSs than the early ones. It should bee noted that the scope and objectives of a SPSA have a dominant effect on the selection of the POSs.

Examples of POSs for a WWER440 type reactor are shortly described below:

1. POS1. The reactor is sub-critical. The RCS pressure is between the nominal pressure and 4 MPa. The RCS temperature is between nominal and 180°C. All trains of the safety systems are available (exceptions are allowed by the limiting conditions of operation). All SGs are connected to the reactor vessel. The primary to secondary side heat removal operates in the steam-water regime using the auxiliary feedwater system and steam removal via the steam dump station to the condenser initially and via the technological condenser at the end of POS. In this POS the containment is closed.
2. POS2. RCS temperature is below 180°C but above 100°C. The RCS pressure is 1-4 MPa. All trains of the safety systems are available (exceptions are allowed by the limiting conditions of operation). Some ESFAS signals are disconnected when the RCS temperature is below 180°C. All SGs are connected to the reactor vessel. In the first part of this POS the secondary side heat removal is in the steam-water regime. At the end of

POS the RHR is working in the water-water regime, RHR pump is running and the heat removal is performed via the technological condenser. At the end of this POS the containment is open.

3. POS3. The RCS temperature is between $T_{brittle\ fracture}$ and 40°C. The HPSI pumps are disconnected. These pumps are available in this POS for the accident mitigation only under the conditions defined in the limiting conditions of operation. However, exceptions are possible in case of the severe accidents (for example if primary bleed and feed is needed). One train of the safety systems is unavailable due to preventive maintenance. Two SGs are connected to the reactor vessel for residual heat removal in natural circulation, one loop is in reserve mode of operation (with one main isolation valve (MIV) fully closed and one MIV fully open). The RHR is working in the water-water regime and the heat is removed via the technological condenser.
4. POS4. The RCS temperature is 40°C. The RCS pressure is the atmospheric pressure. The reactor vessel is being open (drainage of vessel level is needed). One train of the safety systems is in the planned maintenance. Two SGs are connected to the reactor vessel; one SG is in the reserve mode. The RHR is working in the water-water regime and the heat is removed via the technological condenser. The water level is increased in the refuelling cavity in the end of POS.
5. POS5S. The RCS temperature is 40°C. The RCS pressure is the atmospheric pressure. The reactor vessel is open and the refuelling cavity is filled to the refuelling level. One train of the safety systems is unavailable due to the planned maintenance. Two SGs are connected to the reactor vessel; one SG is in the reserve mode. The RHR is working in the water-water regime and the heat is removed via the technological condenser.
6. POS5L. RCS temperature is 40°C. RCS pressure is the atmospheric pressure. The reactor vessel is open and the refuelling cavity is filled to the refuelling level. All fuel elements are located into the spent fuel pool. One train of the safety systems is unavailable due to the planned maintenance. This POS occurs only once per four years during the long refuelling outage. This POS contains all steps of POS5S. In addition, the reactor vessel inspection is being performed.
7. POS6. The RCS temperature is 40°C. The RCS pressure is the atmospheric pressure. In this POS the reactor vessel is being closed (drainage of the reactor vessel level is needed). One train of the safety systems is in the planned maintenance. Two SGs are connected to the reactor vessel; one SG is in the reserve mode. The RHR is working in the water-water regime and the heat is removed via the technological condenser.
8. POS7. The RCS temperature is between $T_{brittle\ fracture}$ and 40°C. The RCS pressure is between the atmospheric pressure and 2 MPa. There is a peak pressure of 3.5 MPa during a pressure test. The HPSI pumps are disconnected. These pumps are available for the accident mitigation only under the conditions defined in the limiting conditions of operation. Exception is possible during the severe accident (for example if primary bleed and feed is needed). Initially two SGs are connected to the reactor vessel; one SG is in the reserve mode. The RHR is working in the water-water regime and the heat is removed via the technological condenser. At the end of POS the RCS is heated by five main coolant pumps and the containment is closed.
9. POS8. The RCS pressure test is performed at the pressure of 13.7 MPa. Also the high pressure dynamic test at the pressure of 17.2 MPa is being performed (once per four years or if new welding is performed in the RCS). The RHR is stopped. If the pressure

test is not successful the plant is returned to POS7. Given the test successful the plant goes to POS9 and the containment is closed.

10. POS9. RCS temperature and pressure is gradually increasing to 200°C and to 12.26 MPa. The RCS coolant is heated by the main coolant pumps. At 180°C the interlocked ESFAS signals are becoming available. All trains of the safety systems are available (exceptions are based on the limiting conditions of operation). The primary to secondary side heat removal is performed in the steam-water regime by the AFW system. All SGs are connected to the reactor vessel.
11. POS10. The reactor is on the power. The RCS pressure is nominal. The temperature is increasing from 200°C to 260°C. All trains of the safety systems are available (exceptions are based on the limiting conditions of operation). At the RCS temperature of 245°C another ESFAS signals are becoming available. At the end of POS the reactor power is 2% of the nominal power.

Examples of POS duration in hours per year are presented in Table 1. Power 1 and 2 is duration of low power operation.

POS	Planned refuelling outages	Unplanned outages +	Planned and unplanned outages
Power 1	18.47	2.91	21.38
POS 1	13.71	3.68	17.39
POS 2	8.96	3.75	12.71
POS 3	34.58	23.61	58.19
POS 4	206.91		206.91
POS 5S	224.66		224.66
POS 5L	1 094.29		1 094.29
POS 6	259.77		259.77
POS 7	107.51	1.89	109.40
POS 8	19.05	0.40	19.45
POS 9	29.41	3.19	32.60
POS 10	79.82	6.61	86.43
Power 2	123.88	7.69	131.57
POS 1-10	Σ_j = 984.38/1854.01*	Σ_j = 43.13	Σ_j = 1027.51/1897.14*
Power 1-2	Σ_j = 142.35	Σ_j = 10.60	Σ_j = 152.95

+) Unplanned outages caused by component/system failures and initiated reactor shutdown to corresponding POS.

*) The first number is applicable for short refuelling outage; the second number is applicable for long refuelling outage.

Table 1. Duration of POS

2.2 The initiating events

Defining a list of initiating events is the major step, which influence the whole SPSA development process. While the main aim is similar to power PSA, actual initiators considered in a SPSA are different from those of the power PSA. The profile of initiators also

highly depends on the actual outage considered (lengths and type; forced, refuelling, etc.). Three broad categories of internal initiators are typically considered in a SPSA, and they are as follows:

- Loss of cooling,
- Loss of coolant (LOCA) and
- Reactivity events.

LOCA represents a group of events which result in loss of heat removal from the core. When the core is cooled by the RHR system, its failure is the main initiator in that group.

Loss of coolant events are a challenge to the RCS integrity in the same way as during full power operation. However, the profile and the causes of LOCAs are significantly different in the shutdown mode. In the shutdown mode breaks of pipes and reactor vessel rupture are still possible, but the dominant sources for LOCAs are the drain-down events, including inadvertent opening of valve and similar, both drain-downs to the plant rooms inside the containment or to another system (intersystem LOCA outside the containment) should be considered in a SPSA. Cold over-pressurisation events which are challenging the integrity of primary circuit may be broadly grouped with this category.

Reactivity events are a specific category due to their specific issues and consequences. Reactivity accidents can lead to a local or a full core criticality. Examples like boron dilution, unintentional withdrawal of control rods or refuelling errors are considered in the SPSA. Experience has shown that many such events occurred at NPPs, and their frequencies are high, though the consequences are low (recoveries are possible in many of those events). Some phenomena, like unborated slug of water entering the core and its consequences, are still being analysed.

Like in a full power PSA, hazards can be divided into two groups, internal hazards and external hazards. Internal events include fires, floods and events like drop of heavy loads. These events in comparison to power state are differently treated in a SPSA due to their specific attributes. Internal fire can have higher frequencies in comparison to the power operation. The possible fire locations increase during an outage due to maintenance activities. A fire during an outage is usually initiated by some repair work like welding, while fires during the power operation are usually initiated by electric circuits. Flooding has increased frequency due to maintenance activities where floods would be caused by opening isolation valves and similar activities. Drop of heavy load is an event which is seldom considered in the power PSA but it could have significant impact on the SPSA results. Numerous operations with overhead cranes has actually been analysed in several studies, although the results were not found to dominate the risk profile.

In addition, the external hazards must be taken into consideration: aircraft crash, external meteorological conditions, seismic events and impact of the neighbouring industry.

2.2.1 Grouping of the IE

The initiating event grouping was performed based on the qualitative criteria. Some modifications in grouping are possible later when the frequency of the initiating events is calculated and accident sequence modelling and fault tree modelling is performed.

The qualitative criteria applied for grouping at this stage are the following:

- In order to take benefit from the existing event trees and fault trees, the initiating event groups were selected as much as possible consistently with the list of the initiating event groups for the full power PSA.

- Plant response and core cooling requirements associated with each of the LOCA categories are conservatively assumed to be the same as for the full power conditions. However, this assumption was revised within the system analysis task as one train of the safety systems is unavailable in some POSs. Core cooling requirements can also be relaxed taking into account that at the shutdown conditions the residual heat rate of the core is lower than at the full power conditions.
- Frequency of the initiating events was not taken into account in the first step of grouping. Some of the groups can be screened out due to an extremely low frequency of the events (provided that they do not lead to a severe plant degradation, i.e. they are not expected to have a high risk impact).
- Some of the events with different consequences (risk impact) were assigned to the same group when the consequences did not differ very much. In this case the group is defined based on the event with the highest consequences.
- When the consequences of the events (groups) are expected to be different at least in one POS, such events (groups) are listed separately. However, for some POS these differences may be negligible and many events can be grouped together.
- All events grouped together are not necessarily applicable to the same POS.

Special cases of the event defined as a group representative may have a slightly different consequences. Bounded events have also different consequences than the event defined as a group representative as well as a different origin (contrary to the special cases). List of the events provided as examples is not necessarily exhaustive. Other events that are not indicated as a special cases or examples are expected to be exhaustive.

Further grouping was possible based on the result of data quantification and system analysis tasks. Initiating event frequency was one of the aspects on which further grouping could depend. Generally, it was assumed that the initiating events or IE group could be conservatively included into another group with similar but worse consequences if its frequency was not higher than the frequency of the main event representative for the group. This assumption was verified and the grouping confirmed when the initiating event frequency was finally determined.

Combination of the individual groups was also possible when the plant response and mitigation system requirements were defined more precisely.

2.2.2 Assignment of IE to POS

The first stage of POS assignment was done mostly on the basis of possibility of an occurrence. For instance, the breaks were not considered unless there was an overpressure in the circuit, the human errors associated with a maintenance were not considered unless some maintenance activities were conducted in the specific POS, etc.

In general, the assignment of an applicable POS to the initiating event group was carried out by the considering each event included into the group. In many cases the applicability of POS was dependent on the particular scenario either through a particular plant configuration or through specific maintenance activities associated with a certain POS.

In general, the frequency of IE was not taken into account in the POS assignment process. However, in some cases the frequency was considered in a qualitative way.

For some POS the risk impact of the event was expected to be very low either due to a low frequency or small consequences or both. However, only a qualitative and subjective judgement could be provided to justify such observations. Therefore, the event credibility level is not indicated in the POS assignment results.

However, a credit was given to the fact that during a specific POS the conditions for IE may change (e.g. the pressure is decreasing to atmospheric, so the credibility of a LOCA is diminished). Another aspect that was addressed explicitly was the case when an event was applicable to a part of POS only (but not a negligible part). This aspect was also subsequently considered in an estimating of IE frequency.
Since the selection of POS for IE calculation also depends on the expected frequencies and consequences, another stage of grouping was needed in a co-operation with other PSA tasks. In this stage a consideration was given to the assumptions taken during the accident sequence modelling and to the frequency estimation.
For some POS to which an initiating event was applicable the consequence of this event was considered negligible. The accident sequence task revealed such cases and these events were screened out for these POS. Typical examples of such screening include: events related to loss of the reactor core cooling in POS5S (because of a large inventory of the water in the reactor refuelling pool) and in POS8 (because the system does not need any cooling and the RHR is switched off) or the loss of working cooling pump in any POS (because of a relatively low decay heat generation in the spent fuel pool (exception is POS5S).
Initiating events were considered for the deletion if they lead to the core damage in a time period greater than 24 h. However, it should be noted that simply exceeding this 24 h window was not, by itself, considered to be sufficient reason for deleting initiating events.
Frequency of the events during particular POS was not taken into account in the initial stage of the grouping and POS assignment tasks. For some assigned POS an initiating event (or even a whole group of events) was screened out later due to a low frequency (provided that it was not expected to have a very high risk impact).
The duration of some POS is very short comparing with other POS, so an initiator or even the whole group can be screened out on that basis as well (see Table 1). Example for IE assignment to POS is provided in Table 2.

IE group	Event description	POS number									
		1	2	3	4	5S	5L	6	7	8	9	10
RT(RBD)	Rapid boron dilution			▨					▨	▨	▨	▨
RT(SBD)	Slow boron dilution	▨	▨	▨					▨	▨	▨	▨
RAT	Uncontrolled reactivity addition											▨

▨ Applicable to the POS ☐ Non-applicable to the POS

Table 2. IE assignment to POS – reactivity events

2.2.3 IE frequency calculation

The basic principles for calculation the IE frequencies are the same as for the full power PSA. However, the determination of the IE frequencies for shutdown events is much more plant specific due to configuration, maintenance practices and other issues. In SPSA the frequency of an IE is dependent on POS, and it must be determined for every POS individually.

There are three basic approaches to calculate the IE frequency in a given POS:

- calculation of frequency based on plant specific data,
- calculation of frequency by quantifying a logical model of an initiator and
- considering the full power PSA frequencies of IE with additional recalculation.

Determination of the IE frequencies based on actual operating experience (plant specific data) could be the most accurate approach but in the same time it is the most difficult one. A thorough evaluation of the records on various occurrences during outages is essential in determining the IEs frequencies. It is very important that the evaluation of experience is performed together with the plant personnel who could correctly interpret the information contained in the historical records. The outage schedule as well as POS defined in the previous step should be evaluated to identify the possibility of the occurrences of each specific IE in every POS.

The SPSA studies found that human interactions are a high contributor to the frequencies of many IEs. HRA is used for IE frequency calculation. The IE frequencies considered in the full power PSA may be only the starting point in defining the IE frequencies for SPSA. Many of the full power IEs are not directly applicable and the frequencies may be significantly different during an outage.

In many SPSA studies the frequencies for LOCAs are just adopted from the full power PSA. Such approach causes some controversy as whether:

- LOCAs frequencies should be modified to reflect that the systems are operating at much lower pressure (some analysts argue that non-pressurised primary piping will have the reduced pipe ruptures failure rate).
- LOCAs frequencies should not be modified to be conservative.
- In fact, the contribution to CDF from LOCAs caused by pipe rupture is found to be negligible in the SPSAs. LOCA caused by human errors is much more important.

The following approaches were applied for initiating event frequency calculation:

1. For the initiators that were quantified based on the plant operational history the applicable events are uniformly distributed across all applicable POS. For the time dependent events uniform distribution of the events is assumed within the applicable time period. The following formula is applied for the annual frequency calculation:

$$f_{i,k} = (N_i/T) \times (t_k/\Sigma t_j)$$

where

$f_{i,k}$ - frequency of initiating event „i" per reactor year per POS „k",
N_i - number of the applicable operating events reported during exposure time period T,
T - exposure time in reactor years,
t_k - duration of POS „k", hours,
Σt_j - total duration of applicable POS, hours.

2. For the events that were quantified based on full power data it is assumed that the initiating event frequency per hour of the full power operational states is the same for the applicable shutdown states. The following formula is applied for the annual frequency calculation:

$$f_{i,k} = f_{i,FP} \times t_k/T_{FP}$$

where

$f_{i,k}$ - frequency of initiating event „i" per reactor year per POS „k",
$f_{i,FP}$ - frequency of initiating event „i" per reactor year for full power operational states (generic or based on full power operational statistics),
t_k - duration of POS „k", hours,
T_{FP} - exposure time for full power operation in hours per reactor year.

3. Human reliability analysis is applied for several initiators that involve human actions and never occurred in the plant. These included the initiating events related to the cold over-pressurization, man induced LOCA and boron dilution. In the most cases there is the inadvertent actuation leading to the initiating events. The frequency is calculated based on HRA. In general, the probability of the inadvertent actuation is calculated from the following formula:

$$P_{IC} = P_I \times P_C$$

where P_{IC} is the probability of not corrected inadvertent actuation, P_I is the probability of the inadvertent actuation and P_C is the conditional probability that the error is not corrected. The commission error probability or probability of the inadvertent actuation (opening) is P_I = 3.0E-3, the conditional probability that the error is not corrected P_C = 0.1. The probability of the inadvertent actuation is P_{IC} = 3.0E-4.

4. Bayesian approach is applied to calculate the initiating event frequency for the events which never occurred in the plant and the IE frequency can not be calculated using HRA. After updating the prior frequency by the plant specific frequency the posterior frequency is received.

2.3 The screening process

IE with available recovery times longer than 24 hours could be screened out without much danger of leaving out important results. IE with very short recovery times, which are those earlier in an outage and which involve very specific system availability, shall not be screened-out because of their generally high importance.
Screening process can be performed in two phases:

- After screening-out the clearly unimportant events, the draft event trees can be developed for remaining sequences.
- The remaining sequences then could be analyses qualitatively or/and quantitatively.

The main idea of the whole process is to select events of higher safety significance and to reduce the level of details in modelling work for sequences with lower safety impact. The final step in the screening process is re-grouping of POSs and initiators. The result of the whole process is a list of safety important POSs and IE groups. The SPSA requires iterative processing for re-defining and re-grouping POSs and IEs several times during the process.
Development of detailed accident sequences (including supporting TH analysis, HRA, etc.) is the most labour intensive part of the SPSA. Its aim is to focus on essential issues only. Establishment of a systematic screening procedure is the best way of removing unimportant accident sequences.

2.4 The accident sequences

2.4.1 The fault trees

The fault tree models developed for the full power PSA could be used, with exceptions, as a basis for SPSAs as well. Revision of the models is necessary due to the following reasons:

- system is operational in shutdown (it is in the standby mode during power operation),

- system actuation is manual (it is automatic during power operation),
- mission time is different,
- system success criteria changes with POS,
- redundancies are different in different POSs,
- recovery possibilities are different and
- system alignment is different for individual POSs.

2.4.2 The event trees

The accident sequence modelling is usually performed using event trees. The event trees developed for full power PSA may be modified for use in SPSA. The modification will typically include removal of some headings (i.e. reactor trip) and relaxation of the others due to lower decay heat levels. Some new headings may be added to reflect operator actions which may not be possible during power operation.

Shutdown state also has some specific characteristics which are not modelled in the full power PSA. Operation of the RHR system and related operator responses often requires development of new sequence models. A longer time is available to operators to recover from initial failures. Possibilities to establish non-conventional accident mitigation (as an example, supplying water into the open reactor vessel) require from the PSA analysts to consider options which have not been addressed in the full power PSA.

2.5 The human reliability analysis

Human reliability analysis is the most important issue in a SPSA. Both the plant outage and the start-up activities involve a large number of operator actions, functional tests and maintenance activities. All of those have to be correctly introduced in a SPSA.

In a SPSA different types of human actions are considered:

- human actions before initiating event, affecting availability of equipment,
- human actions as an IE,
- procedure based post-accident human interactions to terminate an IE,
- human recovery actions to recover the failed equipment or to terminate an event.

Compared to the full power PSA, human interaction analysis in a SPSA is much more complex since they require identification of actual ways the work is being done and consideration of interactions which are not obvious.

The following issues needed to be addressed when evaluating the human interactions during outage safety analysis:

- operating procedures,
- supervision on maintenance activities,
- appreciation of risk during shutdown and
- comprehensive and appropriate training.

The following steps are important for considering human interactions:

- identify all possibly important human interactions during plant outage,
- screen these human interactions and prioritise them from the risk perspective, and
- collect information from plant experience during shutdown operating mode, and establish human error data base.

During an outage, the dependencies between human errors tend to be much more complex than during power operation. Testing and maintenance activities during shutdown operation create new dependencies which need to be identified and documented. Cross-

connections and support system status may cause hidden dependencies which need to be taken into account.

2.6 Quantification of accident sequences

Quantification of accident sequences is performed for all POSs. First, the total CDF is presented for an average refuelling outage, short refuelling outage and long refuelling outage. Then, the dominant initiating events, accident sequences, minimal cut sets and dominant categories of the basic events are identified. Results of the importance and sensitivity analyses are also summarized.

The task is similar to quantification in the power PSA. However, the sources of data as well as the procedure to develop a data base may be different. Data for component unavailability for SPSA have significantly different emphases than for the power PSA. While in the power PSA the unavailability of safety components are (often) dominated by the failures in stand-by, in SPSA they are clearly dominated by maintenance unavailability. Maintenance schedules and actual duration of various tests and maintenance actions are carefully evaluated to determine the actual equipment availability. Quantification of accident sequences, uncertainty and sensitivity analysis follow the same methodological approach as for the full power PSA. Due to various influences, it was shown that the SPSA results typically have higher uncertainties.

The dominant initiating events identified for all POSs are presented in Table 3. This is graphically depicted in the pie chart in Fig. 2. Instantaneous CDF for each POSs is presented in Fig. 3. The dominant contributions to the total CDF are from POS6, POS4, POS7, POS5S, POS3 and POS5L. The combined contribution of these POSs is 98.1% of total CDF.

No.	Initiating event	Description	CDF [1/y] mean value	Contribution to total CDF (%)
1	LOSW(OP)	Loss of service water	1.14E-5	20.5
2	LNC(GP)	Loss of natural circulation - gas penetration	1.12E-5	20.3
3	L(MI-SL)	Man-induced small LOCA	9.81E-6	18.0
4	LOP	Loss of offsite power	7.77E-6	14.1
5	LRHR	Loss of residual heat removal	5.95E-6	10.8
6	COVPR	Cold over-pressurisation	1.87E-6	3.4
7	LVBB	Loss of vital 6 kV bus bar	1.43E-6	2.6
8	LNC(OD)	Loss of natural circulation - over-draining	1.32E-6	2.4
9	LBA(B)	Leakage in the spent fuel pool	1.32E-6	2.4
10	LNVBB	Loss of non-vital bus bar	1.27E-6	2.3

Table 3. The dominant IE for all POSs

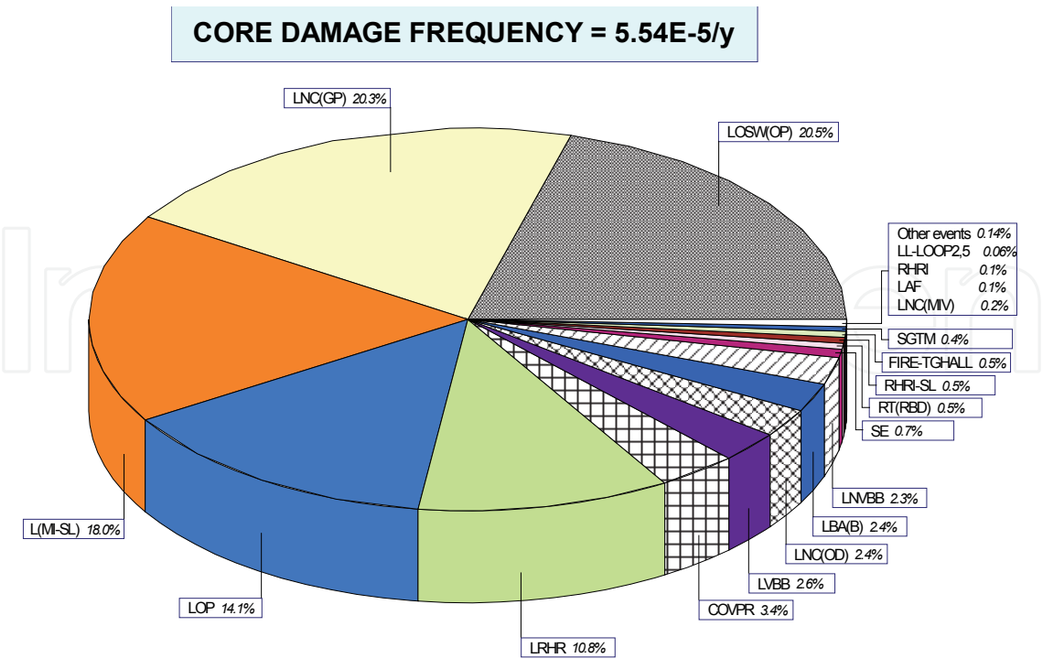
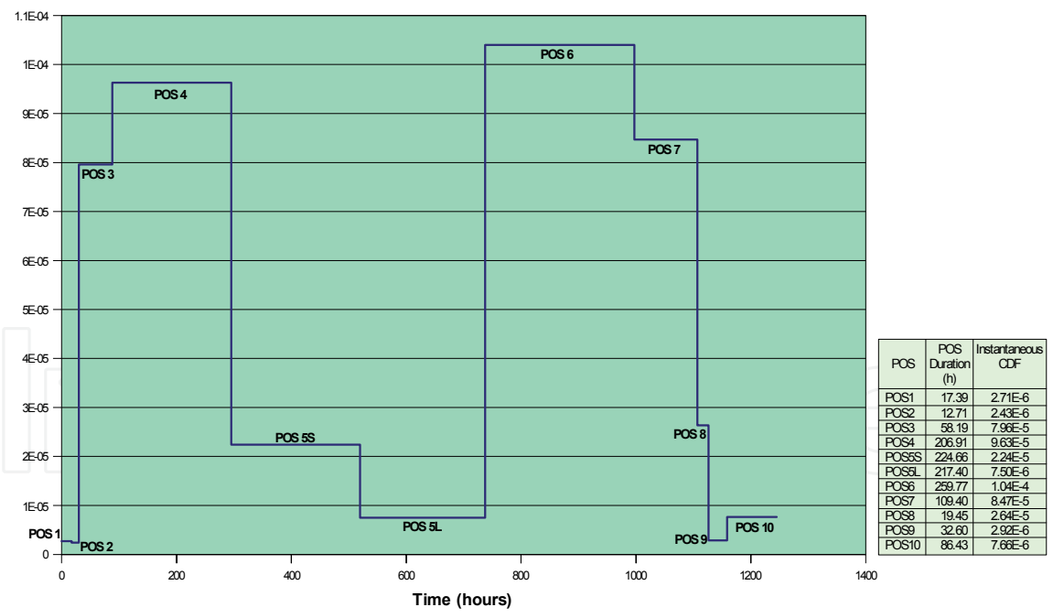


Fig. 2. The average core damage frequency with dominant IE for a WWER440 plant for all POSs



POS	POS Duration (h)	Instantaneous CDF
POS1	17.39	2.71E-6
POS2	12.71	2.43E-6
POS3	58.19	7.96E-5
POS4	206.91	9.63E-5
POS5S	224.66	2.24E-5
POS5L	217.40	7.50E-6
POS6	259.77	1.04E-4
POS7	109.40	8.47E-5
POS8	19.45	2.64E-5
POS9	32.60	2.92E-6
POS10	86.43	7.66E-6

Fig. 3. Instantaneous CDF for each POS

2.7 Application of SPSA

The following applications of SPSA model and results are considered:

- outage planning and scheduling,
- optimization of operating and maintenance procedures,

- optimization of limiting conditions of operation,
- accident procedures, emergency planning and
- making decision on hardware modification.

The Equipment Out Of Service (EOOS) risk monitor is developed for the J.Bohunice V2 plant plant in Slovakia. The monitor is used by operator and schedulers of maintenance (see Fig. 4, 5 and 6).

An example for SPSA application is described for the preventive maintenance strategy of the safety systems in the plant: 1) the maintenance activities are performed in operating mode 5 (reactor cavity not flooded) and 6 (the reactor cavity is flooded), 2) only a single train is under preventive maintenance, 3) the second safety train is available based on limiting condition of operation, 4) the third safety train can be or can not be available, the availability is not required by limiting condition of operation, 5) the systems that could be used for decay heat removal and accident mitigation should be available to the maximum extent possible but this is not the case in the plant. Recommendation for changes from SPSA: 1) planned maintenance activities will begin when the reactor cavity is flooded, 2) availability of all three safety trains will be required by limiting conditions of operations, 3) one train out of three is allowed to be unavailable due to preventive maintenance.

3. Modelling issues related to Level 2 SPSA

3.1 The plant damage states

The level 1 PSA sequences are terminated and the level 2 PSA sequences are started with the core damage. The interface between the level 1 and level 2 PSA is accomplished through the definition of plant damage states (PDS). The PDS defines the plant state at the beginning of the core damage and defines the conditions necessary for conducting severe accident progression analysis. PDS are developed as an initial step to a level 2 PSA. The status of some safety systems may not be identifiable from the level 1 PSA models. So, their availability during various core damage sequences must be addressed by means of an extension to the level 1 system models. In the level 2 PSA, post core damage recovery actions (using the existing system in automatic or manual mode) are also identified.

The criteria for binning the level 1 sequences into the plant damage states are based on the following five characteristics of each sequence:

- IE,
- Time to core damage,
- Status of high pressure and low pressure safety injection system,
- Status of containment spray system and
- Status of containment isolation.

The PDS are further grouped based on POS of the plant at power operation and during refuelling outage. Several POS groups (G0 – G4) were introduced to facilitate the PDS grouping process:

G0: Full power operation

G1: POS1, 9 and 10, which are essentially similar to the full power operation. Both the RCS and the containment are normally closed.

G2: POS2, 3, 7 and 8 in which the RCS is closed but the containment is open.

G3: POS4, 5S and 6, in which both the RCS and containment are open. The fuel is located in the reactor vessel.

G4: POS5L, which is a special case because the fuel is relocated to the spent fuel pool.

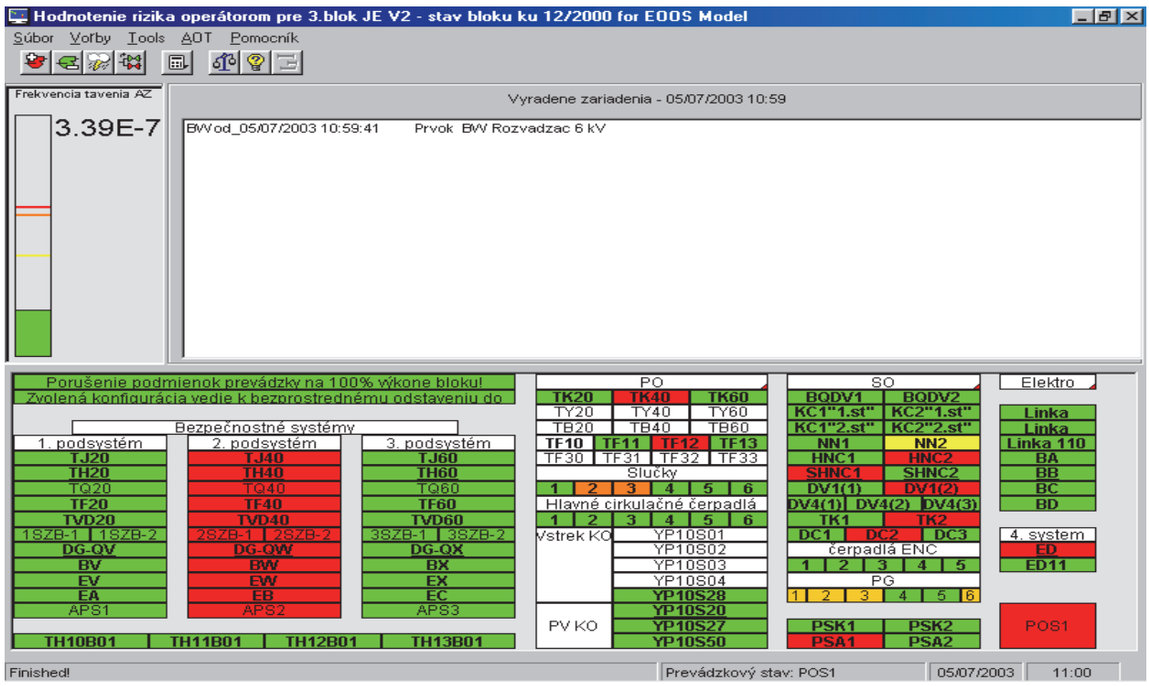


Fig. 4. Risk monitor for the operator (components in red colour are unavailable, CDF = 3.39E-7/y)

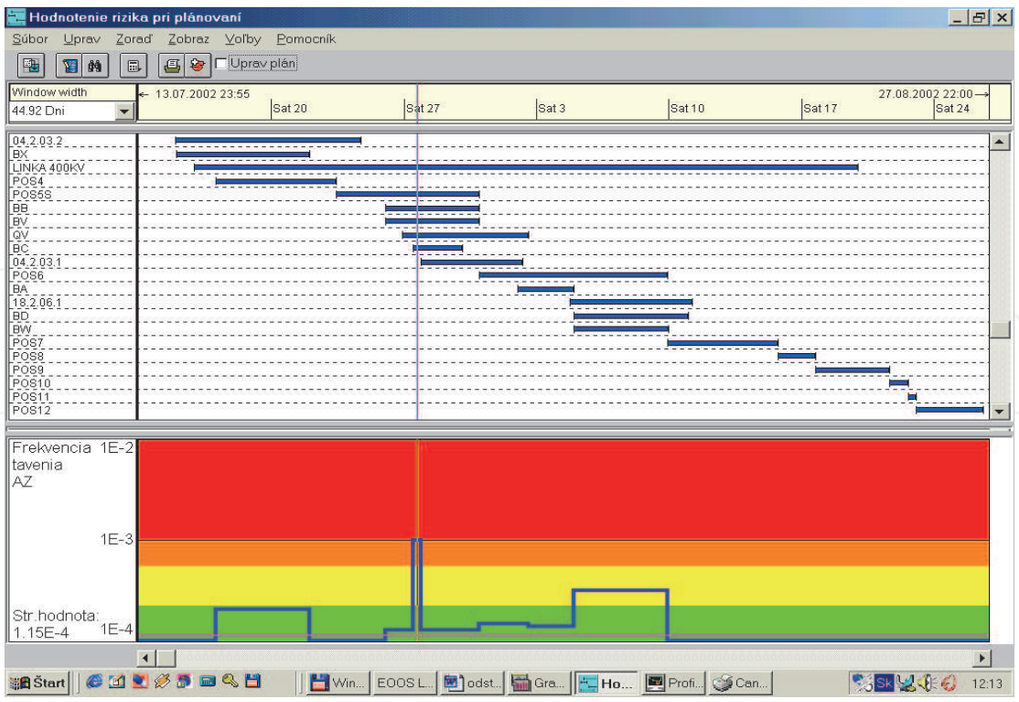


Fig. 5. Risk monitor for planning of maintenance activities (high risk profile)

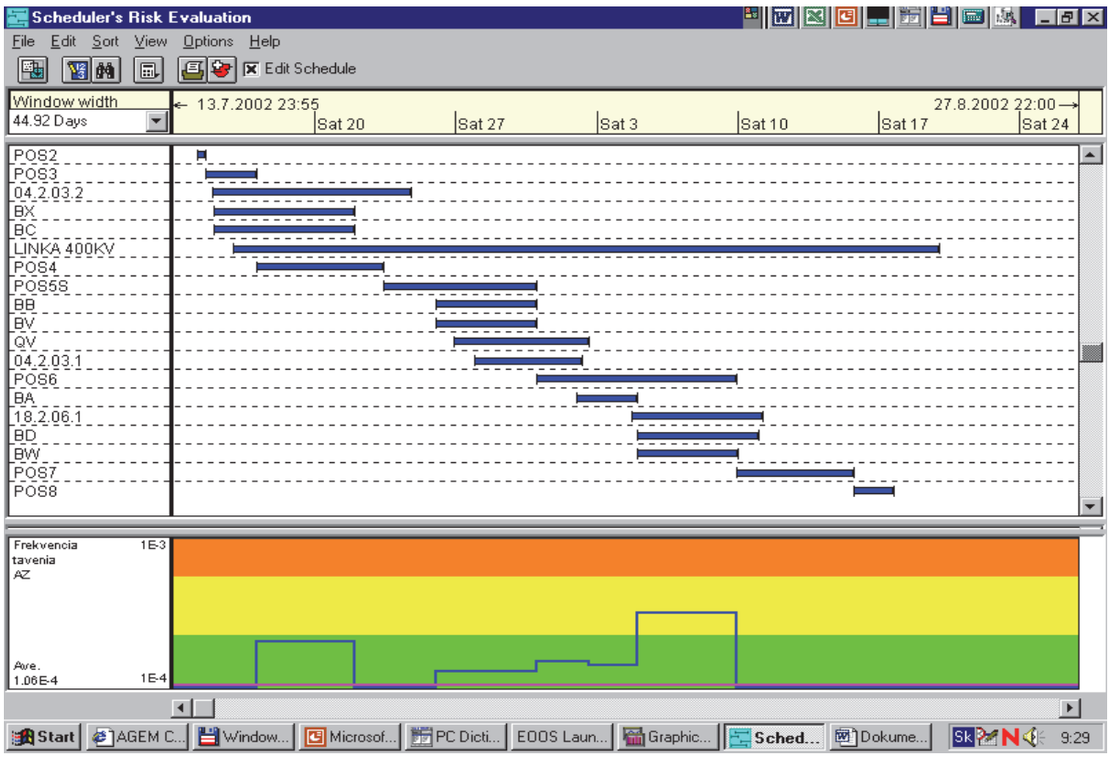


Fig. 6. Risk monitor for planning of maintenance activities (low risk profile)

3.2 Accident progression analysis

The MELCOR code is used to model all aspects of the severe accident progression, including:

- reactor coolant system thermal-hydraulic response to the initiating event prior to the core damage,
- core heat up, fuel degradation and material relocation within the reactor vessel,
- possible failure of the reactor vessel pressure boundary, and subsequent release of molten fuel and core debris to the containment,
- thermal and chemical interactions between the core debris and containment structures, such as concrete floors, and the containment atmosphere, and
- containment behaviour (including its pressure and temperature history, hydrogen mixing and combustion, and the effect of the operation of containment safeguard systems).

This code provides an integrated framework for the evaluating the timing of key accident events, thermodynamic histories of the reactor coolant system, core and containment, and corresponding estimates of fission product release.

3.3 Containment performance analysis

Deterministic calculations of severe accident progression generate pressure and temperature histories within the containment during the various accident sequences. To determine whether the containment pressure boundary will be able to withstand the loads, quantitative estimates of its structural performance limits must be generated.

Challenges to the containment integrity can take many forms. Therefore, the analysis of containment performance limits must address several topics. Typically, the following containment challenges are considered:

- internal, rapid and slow pressurization transients greater than nominal design conditions,
- high temperatures,
- thermal-mechanical erosion of concrete and steel structures (if contact with ejected core debris is possible),
- impact from internally-generated missiles and
- localised dynamic loads, such as shock waves, hydrogen detonation, etc.

In some instances, these challenges may exist simultaneously. For example, high temperatures often accompany high pressures.

Engineering calculations of structural response to these types of challenges are performed as part of the level 2 PSA. Quantitative failure criteria are developed as the primary reference for estimating the likelihood of containment failure for a wide spectrum of accident sequences. These criteria are based on plant specific design and construction data and represent realistic material response properties.

3.4 Construction of the containment event trees

Probabilistic model in the form of containment event trees (CET) is constructed for the evaluating the containment performance. The model is displaying the alternative accident progressions that may evolve from a given core damage sequence or a plant damage state.

The initiating event of the containment event tree is the PDS. During the construction of CET the following issues are taken into consideration:

1. Important time phases of severe accident progression. Different phenomena may control the nature and intensity of challenges to the containment integrity and the release of radionuclides as an accident proceeds in time. The following time frames are identified:
   - After the core damage begins, but prior to failure of the reactor vessel lower head. This period is characterised by the core damage and radionuclide release from the fuel while core material is confined within the reactor vessel. Hydrogen detonation is possible.
   - Immediately following reactor vessel failure. The level 2 PSA analysis concludes that many of the important challenges to the containment integrity occur just following reactor vessel failure. They often occur as a direct consequence of the release of molten core materials from the reactor vessel to the reactor cavity.
   - Long term accident behaviour. In the absence of the heat removal to the environment, the loads may steadily increase to the point of containment failure in a long term.
   - It must be noted that release is possible also from the containment which remains intact via the normal leakage.
2. Probabilities associated with events in the CETs are of different types: failure probability of safety system, probability that a human will not perform specific activity or probability of accident phenomena (for example hydrogen burn). Probabilities in the first two cases are developed in similar manner as in the level 1 PSA. The last one represents uncertainty in the occurrence or effects of severe accident phenomena. In this case, the split fraction associated with this event is not based on reliability data. Rather,

it is a reflection of the uncertainties in the engineering analyses required to characterise hydrogen generation, release, distribution and combustion. The probabilities are obtained using decomposition event trees.

3. Recognition of the interdependencies of phenomena. Most severe accident phenomena and associated events require certain initial or boundary conditions to be relevant. For example, a steam explosion can only occur if molten core debris comes in contact with the water. Therefore, it may not be meaningful to consider ex-vessel steam explosions during accident scenarios in which the reactor cavity is dry at the time of vessel breach. Logic models for evaluating containment performance capture these and many other such interdependencies among severe accident events and phenomena.

3.5 Source terms

Estimation of the magnitude of fission product release to the environment (i.e. source terms) are a major product of a level 2 PSA. Plant specific source terms were evaluated for the Slovak plants.

The following source terms categories are defined:

1. STC1 - containment intact, containment spray available, no vessel failure,
2. STC2 - containment intact, containment spray unavailable, no vessel failure,
3. STC3 - containment intact, containment spray available, core cooling recovery after vessel failure,
4. STC4 - containment intact, containment spray unavailable, core cooling recovery after vessel failure,
5. STC5 - containment intact, containment spray available, no core cooling recovery after vessel failure,
6. STC6 - containment intact, containment spray unavailable, no core cooling recovery after vessel failure,
7. STC7 - very early containment failure before vessel failure,
8. STC8 - release from the spent fuel pool,
9. STC9 - early containment failure at vessel failure, no core cooling recover after vessel failure,
10. STC10 - late containment failure after vessel failure, core cooling recover after vessel failure,
11. STC11 - late containment failure after vessel failure, no core cooling recover after vessel failure,
12. STC12 - late containment failure without vessel failure,
13. STC13 - containment not isolated, containment spray unavailable, vessel failure
14. STC14 – containment not isolated, containment spray unavailable, open reactor vessel, no vessel failure,
15. STC15 - containment not isolated, containment spray unavailable, open reactor vessel, vessel failure,
16. STC16 - containment bypassed after SGTR,
17. STC17 - containment bypassed after interfacing LOCA.

3.6 Large early release

The effective doses are identified from the source term for the public. Based on the effective doses the countermeasures are implemented, as for example evacuation. Based on an

estimate of the effective dose that could be avoided by implementing a particular countermeasure, the lower and upper emergency reference levels are defined. Below the lower level, introduction of the countermeasure would not be justified because of the harm that it would cause. The upper level is the dose level at which every effort should be done to introduce the countermeasure, except in exceptional circumstances. It is set at ten times the dose of the lower level.
The lower and upper levels for sheltering are a dose of 5 mSv and 50 mSv respectively. For evacuation, they are 50 mSv and 500 mSv. These are higher than the recommended dose limit for routine exposure, which is 1 mSv per year for the public. This is because the dose levels are not intended to represent the boundary between what is 'safe' and what is 'unsafe', but to represent an acceptable balance between the harms and benefits of an action.
In case of fission product release the release is large if more than 1% caesium is released to the environment from the core inventory. It can correspond to the dose of 50 mSv/y for the public. Large early release is a release to the environment before implementation of required countermeasure (before evacuation). For the purpose of the WWER440 units it is considered that the evacuation can not be performed until 10 h from the beginning of the accident. The release until 10 h is the early release.
For the groups G0, G1 a G2 the Large early release frequency (LERF) is given as sum of frequencies of the following source term categories: STC7 + STC9 + STC13 + STC16 + STC17. For group G3 the LERF is given by STC14 and STC15 (the reactor vessel is open, the containment is open). For group G4 the LERF is given by STC8 (the spent fuel pool is outside the containment).

3.7 Results

The source term category 14 for group G3 is presented in Table 4 for illustration of the results. The fission product groups Xe, I and Cs are presented in table with the corresponding frequency.

Source term category	Frequency 1/y	Beginning of the release	Xe [%]	I [%]	Cs [%]
14	4.08E-6	Early	94.8307	86.0377	83.8331

Table 4. The source term categories for group G3

The risk of fission product release from the spent fuel pool is very small in operating mode 7. The source term category frequency is 3.0E-9/y. However, the quantity of fission products in the source term is extremely high because the pool is located outside the containment and the spray system has no impact on the fission products which can be released into the environment. The fuel inventory is also higher in comparison with the core inventory.
The LERF for each group G0-G4 is less than 1.0E-5/y. The requirement of the Nuclear Regulatory Authority is met.

4. Conclusion

The level 1 shutdown risk of the WWER440/V213 plants presented in the form of CDF was higher than the risk coming from the full power operation. Safety measure were implemented which significantly decreased the CDF. After implementation of the proposed

changes the same level of risk is achieved for shutdown operating modes as for the full power operation.

The changes in the limiting condition of operation are the most important from the shutdown risk reduction point of view. In operating mode 5 and 6 only one train of safety system was required to be available. Now the limiting conditions of operation require the availability of safety system trains to the maximum extent possible. It was also recommended that the preventive maintenance for all three trains of safety systems should be done only in operating mode 6, when there is high water level in the reactor refuelling cavity and more than 30 h are required to core uncovery after loss of residual heat removal.

Symptom-based emergency operating procedures (SB EOPs) for shutdown operating modes, developed by Westinghouse and implemented in the Slovak NPPs, also significantly reduce the risk.

In addition, risk reduction factor of automatic operation of low pressure safety injection pumps during shutdown operating modes is also high.

The level 2 shutdown risk in POSs with open reactor vessel and open containment was also higher than the full power risk. The reason was in high core damage frequency in plant operational state during shutdown (groups G2 and G3). The proposed safety measures decreased the risk arising from the high core damage frequency. So, also the level 2 risk is decreased. Further decrease of the level 2 risk can be achieved after planned implementation of Severe accident management guidelines (SAMGs) for shutdown operating modes, being developed by Westinghouse.

The risk of fission product release from the spent fuel pool is very small in operating mode 7. The source term category frequency is 3.0E-9/y. However, the quantity of fission products in the source term is extremely high because the pool is located outside the containment and the spray system has no impact on the fission products which can be released into the environment. The fuel inventory is also higher in comparison with the core inventory.

The full power, low power and shutdown PSA models of the Slovak NPPs are periodically updated. Risk monitors are used to generate the risk profiles and to maintain the risk on the acceptable level for all operating modes. SB EOPs and SAMGs from Westinghouse guarantee high reliability of operators in post-accident situations.

5. References

US NUCLEAR REGULATORY COMMISSION (1989): Severe accident risks: an assessment for five U.S. Nuclear Power Plants - NUREG-1150, USNRC

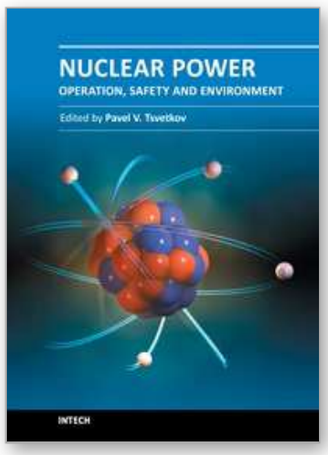
Kovacs, Z. et al. (2002): Post-reconstruction Shutdown Level 1 PSA Study for Unit 1 of J. Bohunice V1 NPP, Summary Report, RELKO Report, No. 0R0400, Bratislava

Kovacs, Z. et al. (2008): Full Power and Shutdown Level 2 PSA Study for Unit 1 of Mochovce NPP, Main Report, RELKO Report, No. 5R0506, Bratislava

OECD (2007): Recent Developments in Level 2 PSA and Severe Accident Management, NEA/CSNI/R

IAEA SAFETY STANDARD SERIES (2008): Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear, DS349, Vienna

IAEA SAFETY STANDARD SERIES (2002): Probabilistic Safety Assessment of NPPS for Low Power and Shutdown Modes, TECDOC-1144, IAEA, Vienna



Nuclear Power - Operation, Safety and Environment

Edited by Dr. Pavel Tsvetkov

ISBN 978-953-307-507-5
Hard cover, 368 pages
Publisher InTech
Published online 06, September, 2011
Published in print edition September, 2011

Todayâ€™s nuclear reactors are safe and highly efficient energy systems that offer electricity and a multitude of co-generation energy products ranging from potable water to heat for industrial applications. At the same time, catastrophic earthquake and tsunami events in Japan resulted in the nuclear accident that forced us to rethink our approach to nuclear safety, design requirements and facilitated growing interests in advanced nuclear energy systems, next generation nuclear reactors, which are inherently capable to withstand natural disasters and avoid catastrophic consequences without any environmental impact. This book is one in a series of books on nuclear power published by InTech. Under the single-volume cover, we put together such topics as operation, safety, environment and radiation effects. The book is not offering a comprehensive coverage of the material in each area. Instead, selected themes are highlighted by authors of individual chapters representing contemporary interests worldwide. With all diversity of topics in 16 chapters, the integrated system analysis approach of nuclear power operation, safety and environment is the common thread. The goal of the book is to bring nuclear power to our readers as one of the promising energy sources that has a unique potential to meet energy demands with minimized environmental impact, near-zero carbon footprint, and competitive economics via robust potential applications. The book targets everyone as its potential readership groups - students, researchers and practitioners - who are interested to learn about nuclear power.

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen

IntechOpen