Lessons learned in applying PSA methods to VVER-1000 design

G.V.Tokmachev and Y.V.Shvyryaev

In: Proceedings of the International Conference on Probabilistic Safety Assessment Methodology and Applications PSA'95. November 26-30, 1995, Seoul, Korea, Volume 2, pages 783-787, Korea Atomic Energy Research Institute, Seoul, 1995.

ABSTRACT

The paper discusses two important measures (reduce human error and reduce common cause failure) to be taken for advanced VVER-1000 based on the PSA for existing VVERs. It is found that almost all the contribution into core damage frequency of the existing VVER-1000 is the result of either human errors or common cause failures. To decrease their impact, functional diversity and passive systems are introduced for advanced VVER-1000.

Some issues related to testing&repair plant staff activities were also investigated within the framework of PSA projects. They are as follows:

- modelling of different testing&repair strategies in reliability model;
- modelling of long-term mission time (more than 24 hours) taking into account restoration of failed component and time window which is available until core damage.

These studies were performed using computer codes developed by Atomenergoproekt. Impact of test&repair on final results is discussed.

1.RESULTS OF PSA FOR THE EXISTING VVER-1000

Atomenergoproekt institute has performed a number of preliminary level 1 PSAs for different types of VVER-1000 reactors [1] from advanced VVER in design to the first VVER-1000 operated at Unit 5 of Novovoronezh NPP. These studies were done in cooperation with almost all Russian institutions working in the field of PSA. PSA results are used for NPP's safety level evaluation as well as for the identification of

design/procedure improvements needed.

PSAs level 1 of standardized V-320 NPPs with VVER-1000 reactors are performed for limited list of initiating events such as LOCAs, LOOP, secondary side ruptures, etc. which may arise while the plant is in power operation. Balakovo NPP and Rostov NPP were under consideration as reference plants. Quantification of core damage frequency was performed for two cases. In particular, for Balakovo-4 NPP the total core damage frequency is 7.0E-4 1/year if beyond design basis accident (BDBA) management is neglected. Should such measures be considered, the total core damage frequency decreases to the value of 5.0E-5 1/year. The main measures are supposed to be as follows:

- the use of feed and bleed mode;
- extension of emergency feed water system operation in open cycle by using service water inventory.

For both cases (with and without BDBA management) such initiating event groups as long-term loss of normal heat removal the secondary side, long-term loss of off-site power are the main contributors to core damage frequency. Should such initiating event occur, operator actions are required to fulfil safety functions as well as for accident management. Human errors made before accident initiation and human errors related to emergency control of plant were analysed with respect to NPP safety. So the human contribution to core damage frequency amounts to as high as 54% for the case of BDBA management. On the other hand BDBA management about 14 times could decrease the core damage frequency value. Thus the facts are that from the standpoint of safety, human reliability is of great importance for operational VVER-1000. Another dominant contributors to core damage frequency are common cause failures (CCF) giving about 44%.

2.RESULTS OF ADVANCED VVER-1000 PSA

2.1 Defences against CCF and human error

The results of preliminary PSAs were taken into account to develop advanced VVER-1000 design. So, it is found that almost all the contribution into core damage frequency is the result of either human errors or CCFs. This raises an important problem of inherent defensive measures against both human errors and common cause failures which should be applied in the advanced NPP design. Undoubtedly such problem should be solved to improve safety of NPPs. It is unlikely that root causes of all human errors and dependent failures will be eliminated by the inherent protection, but the ultimate aim is to ensure that such factors are not dominant contribution into the overall risk from severe accidents.

The concept of advanced VVER is realized based on two fundamentals:

- to remain the important features of the existing VVER-1000;
- to add passive features in such a way that all important safety functions are fulfilled by two diversified redundant systems, one of which is operated in passive mode.

So, most of the important features of NPPs with VVER-1000 reactors which have been already proven in the operating NPPs were implemented in advanced VVER-1000 as far as practically possible. Such concept makes it possible to use operational experience of VVER-1000 as well as analyses performed. The principle of using full-capacity active subsystems is applied in the advanced VVER-1000 to all important safety functions. All active safety systems are completely separated into four trains (plus train in comparison with operational VVER).

To decrease the human&CCF contribution to core damage frequency, some inherent safety features which will operate spontaneously during an accident (without the need for human action or actuation of elaborate engineered systems) are developed. Concerning the defence against human errors, main emphasis is laid on the use of passive safety systems as well as active systems almost not requiring the human actions to fulfil safety functions. The major design modification related to active systems concerns “semi-passive” actuation of some trains of active safety systems such as emergency injection system and emergency feed water system in case of an accident. One out of four trains of the emergency injection system cools normally spent fuel pond and two out of four trains of the emergency feed water system serves normally as steam generator blow down system. In case of an accident those

trains start to perform safety functions by opening of a single valve only.

Functional and/or design diversity has been applied for all the important safety related functions.

The following safety functions are subject to the diversity principles:

- reactor shutdown
- emergency core cooling
- emergency residual heat removal

One of the critical safety function is the shutdown of the reactor. This function is performed by any two systems affecting reactivity. The first one is mechanical rod insertion system, which efficiency has increased making it possible to ensure reactor subcriticality without introducing boron and cooling reactor to cold shutdown state. According to the advanced design the reactor shutdown function may also be performed by the passive system of fast boron injection, which consists of four tanks of highly concentrated boric acid solution. The tanks are connected to the primary circuit by high-speed valves, which have fail-safe design, and are located at the bypass of the primary coolant pumps, runout of which results in the fast injection of boron into the core.

The emergency core cooling function may be performed either by above-mentioned emergency injection system or by two-stage hydroaccumulator system. The first stage of the hydroaccumulator system is like the ordinary system of the existing VVER. The second stage is designed to supply core by water during 24 hours in the event of large LOCA keeping the fuel covered without external help. Residual heat generated in the core is removed by water flowing under gravity from large tanks positioned over the reactor vessel. In this case, spray system is intended to decrease pressure inside containment. Should the spray system fail, surplus steam may be removed from containment to atmosphere through filter system.

The emergency residual heat removal function may be performed by systems of either active or passive heat removal through the secondary side. The active systems consist of emergency feed water system and emergency steam condensing system which are intended to remove heat in close cycle. The backup passive system operates based on different operating principle that do not require a forced supply of electrical power or cooling medium for its functioning. Only a single change in the position of steam-operated valves is required to activate this system. Steam is continuously supplied from steam generators, and in case of pressure increase the valves are opened without human intervention or emergency power.

The passive heat removal system has a four-train structure. Each train consists of heat exchangers cooled by natural air intake, being continuously connected to one steam generator. In case of an accident the above-mentioned air side steam-operated valves to be opened by pressure increase. It starts natural air circulation using temperature differences and natural convection to draw cooling air through heat exchangers that in turn initiates the delivery of steam from the steam generator to heat exchangers and return of condensate which are also effected through natural circulation.

2.2 Main results

Total frequency of core damage of advanced VVER-1000 is 3.2E-7 1/year for long-term mission time (720 hours). LOCAs are the main contributors to core damage frequency because capacity of hydroaccumulators is sufficient only for 24 hours. However, should accident sequences be developed for 24 hours only, it is reduced core damage frequency by almost two orders of magnitude.

Core damage frequency value almost is not sensitive to human errors. Thus application of new design decisions ensures rise to a high safety level. It should be stressed, however, that above value was obtained for power operation mode only. Shutdown plant operating mode was not analysed. External initiating events such as fire, flooding, etc. were not taken into consideration either.

It should be noted that Russian Regulatory Body adopted two quantitative safety objectives for nuclear power plants in design [2]. According to the first quantitative safety objective, nuclear plants to be designed met the criterion that a probability of core damage should not be greater than 1E-5 per year. The second numerical safety objective is met if the probability of a severe accident with containment failure is less than approximately 1E-7 per year. With regard to quantitative criteria, we believe that PSA methods cannot be used to settle absolutely the question of adequate safety of a particular NPP because PSA still cannot give an accurate results, but probabilistic analysis must be added to deterministic to reach an overall conclusion and to identify weaknesses that might undermine the safety of a specific NPP.

3.SPECIAL MAINTENANCE STUDY

3.1 Issues related to testing&repair plant staff activities.

Results of PSA for the existing VVERs show that a topic of particular interest is man-machine interactions which addresses the problems of incorporating a full

assessment of human actions into safety analyses given the potential for operating stuff to err or to initiate system recovery and accident management. Therefore, work was directed towards developing methods for a systematic analysis of potential operator interventions. In particular, some issues related to testing&repair plant staff activities were investigated within the framework of PSA projects. They are as follows:

- modelling of different testing strategies in reliability model (staggered strategy, out of order tests);
- modelling of safety system reconfiguration in reliability model (allowed outage time, taking out of service more than one safety system train);
- modelling of different component repair (restoration) strategies for multiple component failure (for example, CCF);
- modelling of long-term mission time (more than 24 hours) taking into account restoration of failed component and time window which is available until core damage.

3.2 Software used.

Core damage quantification was performed using Risk Spectrum code developed by Relcom Technic AB (Sweden), but special studies were performed using APRA computer code package developed by Atomenergoproekt.

APRA is a complex of logically interconnected executable modules running in PC AT 386/486 “OS-2” environment. APRA uses success path diagram linked with fault tree models, which makes it possible to perform modularization followed by intermediate screening. APRA makes use of minimal cut set (MCS) method for Boolean reduction. Quantification is based on either simple analytical estimators for quick quantification of minimal cut set probabilities or system failure&repair time dependent behaviour modelling and procedure of integration using Monte-Carlo method. Besides, estimators based on Markovian equation approximation is used for post-accident configuration modelling.

3.3.Long-term mission time

Analysis of the accident sequences has been conducted either to a state of core damage or to a steady state in which the risk can be considered to be negligible. Such boundary definition assumption has resulted in post-accident scenarios of long durations to be modelled. In particular, for the case of LOCA, long-term mission time lasting as long as one month has been considered.

With regard to long-term accident sequences it seems to be necessary to allow for the possibility of recovery. It is very important to make sure that the

analysis is realistic. Recovery may consist of either restoration of the failed components or human action to apply accident management procedure. In the case of partial failure of redundant system, failed components may be restored until operable part of system fails (provided that capacity of the available trains is sufficient to meet success criteria). Besides, if accident sequence is supposed to be long-term one, the development of physical process is such that there is a time window which is available until core damage given a total loss of system of interest. The time delay before the occurrence of core damage always increases in proportion to time passed since the occurrence of system loss, since residual heat to be removed will decrease over time. In the case of long-term phase of accident, this delay may be sufficiently long to make it possible to prevent core damage by recovery.

In general, human intervention to apply accident procedure has been introduced into the event/fault trees in the same manner as success or failure of safety system. On the other hand, possibility of restoration of failed component during accident is taken into account on the level of minimal cut set quantification. This type of minimal cut sets is divided into two subtypes:

- MCS containing only failures during mission time;
- MCS containing also pre-accident failures.

As an example, estimators for MCSs of the former type are considered. It should be noted that component failures constituted MCS are also subdivided into two subsets: repairable and non-repairable ones. So, for long-term mission time $\mathbf{t_{mt}}$, probability **p** of MCS involving combination of **k** repairable and **(n-k)** non-repairable failures is calculated by the following formula:

$$p = \frac{\sum_{i=1}^{k}\left(\mu_i \cdot t_{mt}\right)}{n - k + 1} \cdot \prod_{i=1}^{k} \frac{\lambda_i}{\mu_i + \lambda_i} \cdot \prod_{i=k+1}^{n}\left(\lambda_i \cdot t_{mt}\right) \Big)$$

where

λ_i - failure rate of i-th component

μ_i - restoration rate of i-th component

In case of short mission time $\mathbf{t_{mt}}$, another estimator is used:

$$p = \prod_{i=1}^{n} \lambda_i \cdot t_{mt}$$

Quantification results show that probability of some accident sequence increases by 1-2 orders of

magnitude for long-term mission time (720 hours) compared with 24 hours even taking into account possibility of restoration of failed components. It is clear that ignoring of restoration would give very pessimistic results.

3.4 Restoration strategy

As a rule, the average component restoration time is estimated as the sum of the observed restoration times divided by the number of restoration actions that is determined based on operational experience. The restoration time includes detection and waiting times plus post-repair test duration. Such values are quite adequate for modelling of simple cases when restoration of single component is sufficient for system failure elimination. If these data are used for more complicated cases, care should be taken to avoid undercounting multiple component failure restoration time.

There is a potential problem in the attempt to use an existing data base on component restoration time to assess restoration time for multiple component failure (for example, CCF) because input statistical information is generally obtained for “convenience” repair of single failed component when time, man-power and spare part resources are sufficient. Examples are such real configurations as either three-train system consisting of components with two out of three success criterion or two-train group of four identical motor-operated valves (two normally closed sequential valves in each train), for which existing data seem not to be applicable directly. For the event of failure of above complete CCF group, it should be considered that failure detection and restoration of single component incorporated in CCF would not result in system availability. Should it be necessary to restore several components, different component repair strategies such as sequential or concurrent restoration can be modelled. It depends on such factors as maintenance crew readiness, spare parts availability, etc.

However, to meet success criteria, it is not generally necessary to restore all failed components. The primary event of a particular accident sequence MCS may be eliminated by restoration of part of failed component group and it may be sufficient to restore the sequence to a success.

Thus, process of restoration of multiple component failure should be modelled up to elimination of system failure. In this case, average restoration time for multiple failure is estimated as time to be necessary for restoration of the components of the required number of system trains. That is true for both pre-accident and post-accident plant states, but Technical Specifications requirements such as allowable outage time or minimal number of trains

to be available should be also taken into account to model the former plant state.

Sequential repair strategy is the most conservative one. It means that more than one component failed can not be restored simultaneously. Sequential repair strategy is real if repair resources are limited, i.e. several repair crews are not available to carry out concurrent repair actions; time in which decision can be made regarding optimum repair action location is not sufficient, etc. Choice of the next component to be restored depends on the strategy of failure detection. In the case of staggered detection, the component which failure is detected before is generally restored formerly. In the case of non-staggered detection, it is supposed that the choice of component to be repaired is random, after that the rest of failed components of this train are restored till total availability of the train. The average restoration time $\mathbf{t_r}$ for **k** trains out of **N** is given by

$$t_R = \frac{k}{N} \cdot \sum_i t_{r_i}$$

where summing up is performed over all components to be restored in **k** trains.

Concurrent restoration strategy is the most optimistic one. It means that restoration of all components failed is carried out simultaneously. It is certainly that such strategy is suggested to be based on unlimited repair resources. Nevertheless, modelling of concurrent restoration is useful for sensitivity analysis. The random time τ_R for repair of any train out of **N** trains accounting for concurrent restoration is

$$\tau\tau_R = \min_{1 \le i \le N} \max_{1 \le j \le k_i} \tau_{ij}$$

where

τ_{ij} - random restoration time of j-th component of i-th train

$\mathbf{k_i}$ - number of components failed in i-th train

Hence it follows that average restoration time $\mathbf{t_R}$ for train is given by

$$t_R = \left(\sum_{i=1}^{N} \mu_i \right)^{-1}$$

where μ_i - restoration rate of i-th train

Then, an appropriate way of using semi-Markov expressions for steady state case [3] is used to obtain μ_i values in terms of average component restoration times $\mathbf{t_{Rij}}$

$$\mu_i = \min\left\{ \frac{1}{t_{Rij}},\ \frac{1}{\frac{\ln\left[\frac{3}{2}\left(k_i+1\right)\right]}{k_i}\sum_{j=1}^{ki} t_{R_{ij}}} \right\}$$

where the first term represents the case of wide range of $\mathbf{t_{Rij}}$ values, and vice versa - the second term. The implementation of above estimators is supposed to be sufficient for engineering calculation, with total error not exceeding 10%.

Study of sensitivity of core damage frequency to repair strategy applied has not finished yet. Quantitative results will be obtained later.

3.5 Testing strategy

Impact of different testing strategies on core damage frequency was studied using APRA computer code package. Testing strategies modelled are as follows:

- non-staggered testing of redundant components;
- staggered testing of redundant components without extraordinary tests;
- staggered testing of redundant components Extraordinary tests of the non-tested components are performed following detection of failure of tested component.

Care was exercised when calculating the impact of testing strategies on CCFs as having the potential substantially to affect the final results. It should be stressed that a specific issue is estimation of latent period of common cause failures depending on the different factors such as following:

- application of staggered testing. For example, should staggered testing strategy without extraordinary tests be applied to three-train system, complete detection period of CCF of two components depends on specific components failed;
- test intervals applied to components to be included in the same common cause failure group. In practice, there are cases of different test intervals of identical valves belonging to the same common cause group;
- size of CCF event versus size of MCS. If the former exceeds the latter, partial detection of CCF, followed by restoration of the component, which failures have been discovered, can be insufficient to restore the

accident sequence to a success. In this case, detection interval for common cause failure event will be determined by test intervals of the rest of components failed.

With regard to allowable outage time for repair of safety system component failed in reactor power operation mode, additional time duration has been taken into account. This time interval is necessary to bring NPP into safety state given unsuccessful repair of failed component. Such time duration is estimated to be ten hours. Thus, to assess impact of allowable outage time on the core damage frequency, plus ten hours should be also taken into consideration. Besides, unscheduled reactor trip, followed by cooling down, can give itself additional contribution into the core damage frequency.

The calculation results demonstrate that application of staggered testing strategy with extraordinary tests may reduce unavailability considerably (1.5-6 times). On the other hand, the allowable outage time of a safety system train accepted at Russian NPPs with VVER-1000 reactors is not so important from the safety point of view. Therefore, PSA results were used to reissue Technical Specifications. At present, there is the following requirement to safety system tests&maintenance at all operational VVER-1000:

- each safety system train must be tested once a month. The trains are tested at staggered intervals, once every ten days, and, if there is a failure, the rest of trains are to be tested immediately;
- allowable time to repair of failed train may be 72 hours. The previous requirement was 16 hours.

ACRONYMS

BDBA	beyond design basis accident
CCF	common cause failure
LOCA	loss of coolant accident
LOOP	loss of off-site power
MCS	minimal cut set
NPP	nuclear power plant
PSA	probabilistic safety assessment

REFERENCES

[1] Y.Shvyryaev, V.Morozov, A.Barsukov, G.Tokmachev and A.Derevyankin, “The state and problems of PSA for WWER plants”, Proceedings of the IAEA Technical Committee meeting on Advances in Reliability Analysis and Probabilistic Safety Assessment, Budapest, Hungary, pp.72-80, September 7-11, 1992.

[2] Atomic Power Plants - General Safety Regulations(OPB-88), 1989, Doc.PN AE G-1 011-89, Moscow, SU Gosatomnadzor.

[3] A.I.Klemin, V.C.Emel’yanov and V.B.Morozov, “Quantification of Nuclear Facility Reliability. Markov Model”, Moscow, Energoatomizdat, 1982 (available in Russian).