V.Morozov, G.Tokmachev

Risk based definition of TS requirements for NPPs with VVER type reactor

IAEA Technical Committee Meeting Advances in Safety Related Maintenance", IAEA-J4-97-TC-771, Vienna, September 1997

Abstract

The main regulations in safety related maintenance for NPPs in Russia are defined as a part of Technical Specifications (TSs). It includes limiting conditions for operation (surveillance requirements, allowed outage time, et.). In Russian practice the two levels of TSs are presented: general TSs that have been established as a master documents for similar designed NPPs and plant specific based on operation practice of each NPP unit.

Paper presents the brief review of submissions to TS changes for NPPs with VVER type reactor were issued by AEP PSA team since 1990 year. Besides it provides an approach allows to justify the optimum values for both Limiting Conditions of Operation (LCO) and Surveillance Test Intervals (STI) based on relevant probabilistic tool (Minimal Cut Sets method as well as Marcovian Chains are applying).

Introduction

Since 1988 AEP has performed a number of probabilistic risk studies for different VVER type NPPs. The results of these studies in addition to the purpose of design and operation improvement were used also as a base for definition of limiting conditions for both general and plant specific TSs.

Quantification of the risk probabilities associated with loss of critical safety functions for different test interval and allowed outage time values provided the base for choice of limiting conditions in general TSs for VVER-1000/320 (this document was developed by AEP, VNIIAES, ODB Gydropress and Kurchatov institute).

Mentioned risk calculations used conservative generic reliability data and model assumptions to obtain conservatism in results which is important for such type of documents.

The best estimate results could be obtained by performing more detail studies for specific NPP units. For this studies the risk measure usually associates with core damage frequency. It means that plant specific PSA models and data base should be used. AEP performed this type of studies for Kola Unit 3,4 and Kalinin Unit 1 and 2 NPPs. The periodicity of component testing and AOT as well as repair strategies were under consideration. For decision making regarding TS optimisation an acceptance of risk increase over 10% of nominal level for the TS changes was assumed. However regarding to Kalinin NPP, the risk level was demonstrated even to improve. Such results was achieved by extending of AOT in exchange for reducing a number of long-term surveillance test intervals as well as implementing staggered testing strategy.

It should be underlined that above mentioned studies based on PSA approach and used corresponding computer codes. An experience shoes, however, that for complete optimisation, including changes in surveillance requirements, AOT and repair strategies together, existing PSA codes (RISK SPECTRUM, IRRAS, PSA PACK, et.) can not provide an adequate model response to all possible variables, as they suggest a limited number of fixed component reliability models that do not depend on actual operation history.

Taking this into account an original approach was developed to solve the task in a complex form. According to it optimisation procedure includes quantification of a set of two concurrent characteristics: core damage frequency and frequency of unscheduled unit shutdowns as well as comparison of values obtained for different alternatives. For this purpose a method that summarise the advantages of Minimal Cut Set methodology and Marcovian Chains can be used.

The paper in addition to description of studies and results that used traditional PSA tools also presents a basis of methodology seems to be able to provide complex optimisation process for TS decision making.

1.General description

Unplanned maintenance (states #1,2,3 on the graph) refers to corrective maintenance required to restore equipment to service following a critical failure that makes it unavailable. Planned maintenance period (state #7 on the graph) is used to conduct both preventive maintenance and minor corrective maintenance items on

noncritical faults that can be deferred. Both are constrained by the AOTs in the Technical Specifications

2. Kalinin NPP specific study

In 1988 Kalinin NPP requested a study to be performed by Atomenergoproekt institute to resolve safety system testing and AOT issue. The problem was that it was required that safety systems had to fulfil the single criterion during maintenance action as well. If not, a plant was forced to shutdown due to a Technical Specifications requirement which were based on deterministic analysis and engineering judgement.

The only method to eliminate latent failures was to run available trains of safety systems during the whole repair of failed component. In this case failures of available components ware supposed to be directly revealed by instrumentation or process symptoms. However, such procedure led to overheating of emergency cooling water caused by a long-term pump operation in the recirculation mode as well as useless losses of diesel fuel.

Another restriction of TSs was to limit AOT by 24 hours. It was not suitable for operators because the component restoration times should include detection plus waiting times as well as post-repair test time. It should be noted that delay time during which repair is unlikely to be performed because of the time required for detection and repair initiation may be considerable. As a matter of fact, repair initiation time can include administrative time, component cooldown time, decontamination time, and time waiting for tools and spare parts needed for repair.

Thus, to meet TSs requirements, occurrence of frequent unscheduled reactor trips, followed by cooling down, would be evident that could give itself an additional contribution into the core damage frequency.

It was decided that new requirements would be justified and provided to the NPP which allowed to the operator more flexibility and which removed the pessimism from the previous requirements.

Impact of different testing strategies and AOT values on core damage frequency was studied using VNF computer code based on event tree / fault tree linking method. That code makes it possible to take into account the time dependent

effects such as staggered testing scheme, repair time distribution censored by AOT value, etc.. The study was limited by full power reactor operation mode and internal initiating events.

Data collated from NPPs of so-called “small series” (Novovoronezh unit 5, South Ukraine NPP and Kalinin NPP) were used to derive input reliability values such as failure rates and mean times to repair. Initiating event frequencies used were generic.

With regard to allowable outage time for repair of safety system component failed in reactor power operation mode, additional time duration was taken into account. This time window was necessary to bring NPP into safety state given unsuccessful repair of failed component. Such time duration was 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.

Risk level in terms of core damage frequency was demonstrated to improve from 1.6E-3 per year to 6.8E-4 per year in case of implementing technical specification modification recommended. Such result was achieved by extending of AOT in exchange for reducing a number of long-term surveillance test intervals, implementing surveillance tests of untested motor- and air-operated valves as well as the fact that staggered tests over redundant trains were arranged for availability benefit.

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, extending of the allowable outage time of a safety system train accepted at Kalinin NPP was not so important from the safety point of view.

PSA results were used to reissue Technical Specifications. At present, there is the following requirement to safety system tests & maintenance at Kalinin NPP:

- 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 in 4 hours;
- allowable outage time of failed train may be 72 hours including the above-mentioned 4 hours.

3 Kola Unit 3 and 4 specific study

In the early 90's, reliability analysis of safety systems for Kola unit 3 and 4 was performed to validate STIs and AOTs. The impact of STIs and AOTs on safety function performance was estimated. Those safety functions were to:

- maintain the reactor subcriticality
- maintain primary reactor coolant inventory
- remove residual heat via the secondary circuit at high and low pressure in the primary circuit
- remove heat from containment
- scrub radioactivity from containment atmosphere

Kola plant specific reliability data was used for the study. The component reliability data base for all mechanical and electrical components in safety systems at Kola Units 3 and 4 covered 6 reactor-years of operational experience. A total of 613 components such as pumps, motor-operated valves, check valves, safety valves, relief valves, air-operated valves, control valves, fans, diesel generators, invertors, rectifiers, circuit breakers were under consideration. Over 230 events were collated from early 1986 through 1988.

Both front-line and support systems which should perform the above-mentioned safety functions were analysed. Study was performed using APRA computer code package developed by Atomenergoproekt. APRA uses success path diagram linked with fault tree models, which makes it possible to perform modularization followed by intermediate screening. VNF computer code is a part of APRA. APRA makes use of minimal cut set (MCS) method for Boolean reduction.

For decision making regarding TS optimisation, risk values in terms of probabilities of unfulfilment of safety functions were derived. An acceptance of risk increase over 10% of nominal level for the TS changes was assumed.

It was concluded that the increase of AOT from 24 to 72 hours would not effect significantly on the probability of safety function fulfilment, given an extraordinary test of the other two trains would be carried out and their availability would be confirmed. According to Technical Specifications implemented in Kola

NPP based on the reliability study, a functional test of safety system trains is to be staggered among the three trains. The procedure calls for testing all redundant components in case of any failure discovered.

Model description

The subject of interest is a stochastic process represents changes in unscheduled plant configurations $\{E_i\}$, $i=1...N_1$ during period of normal operation between two consequent outages. As the transfers from one configuration to others could be caused by component unavailability at specific time points (at the end of surveillance tests of safety trains) vector $X=\{x_1....x_{N2}\}$, represents component status ($x_j=1$ when j-component is out of service or failed and $x_j=0$ when component is available) should be also considered in the model. In other words the pair $\{E(t),X(t)\}$ reflects completely all factors need for probabilistic estimations. Assuming a constant failure rate for all components

$S(t)= \{E(t),X(t)\}$ can be addressed to a specific class of random processes known as renewal processes or processes of Semi-Marcov type.

The main feature of this process type is that it has renewal point at every time of configuration transfer. It means that the discrete random sequence $S(\theta_1),...,S(\theta_k)...$, where $\{\theta_k\}$ are transfer time point, is a discret Marcov chain, embedded to random process S(t).

The basis of Marcov chain modeling is a definition of transition condition probabilities for $\{E^{k+1},X^{k+1}\}$ given $\{E_k,X_k\}$, where $\{E_k,X_k\}$ denotes $S(\theta_k)$ i.e. just before k-th transient:

$P\{E^{k+1},X^{k+1}, \theta_{k+1}/ E^k,X^k,\theta_k\}$.

To do above all factors that affect on state transients need to be described explicitly. This is given below.

The state life-time and transient moments

The end of life-time for each state E_i is defined by three concurrent alternatives:

- start of next to θ_k test;
- demand to change plant configuration by external causes;
- exhaustion of. AOT defined for current configuration.

The moment of a test start $\tau(\theta_k)$ is a random value due to random nature of θ_k, though the test moments themselves form the regular sequence. For given θ_k $\tau(\theta_k)$ can be found as a constant value. For example if the tests are performed with period of ΔT_{ST}, $\tau(\theta_k)$ is expressed by formulae:

$$\tau(\theta_k) = \text{ENTIER}\left[\left[\frac{\theta_k}{\Delta T_{ST}}\right]+1\right]\Lambda T_{ST}$$

Demands to change configuration can be caused by failures in normal operation systems or (and) initiating events occurrence. All these events are considered in the model external factors. Assuming the Poison law for such events the cumulative distribution for the random time to demand in the state E_i can be written as:

$$F(\theta) = 1 - exp\left\{-\sum_{m\neq i}\vartheta_{im}\theta\right\}, \text{ where}$$

ϑ_{im} - frequency of events that demand the transfer from E_i to E_m.

The later factor is a constant value, representing limiting condition for configuration E_i or its actual duration.

Summarizing above, the next to θ_k transient moment θ_{k+1} can be written:

$$\theta_{k+1} = \sum_{i=1}^{N_1}\alpha_i \, min\left\{\tau(\theta_k), \theta_k + \theta, \theta_k + T_i\right\},$$

where

$\tau(\theta_k)$ - denotes the closest to θ_k test start time,

θ- random time to event that demands the transfer to E_m;

T_i - AOT for current configuration E_i;

α_i - characteristic random value for i-th configuration:

$$\alpha_i = \begin{cases} 1, \text{ when } E^k(\theta_k) = E_i \\ 0, \text{ when } E^k(\theta_k) \neq E_i \end{cases}.$$

Transfers and transfer conditional probabilities

Number of the next (after current E_i) configuration is affected by the following factors:

- external causes that break the plant configuration E_i (discussed above);

- events that can be realized after component testing (genera.ted by the random process itself.

The later factor do not affect on the state life time. However it expresses limiting conditions which define the new configuratios and AOTs given several failure combinations, that could be defined at the test.

These events normally express component failures in one, two or three safety trains. The typical limiting conditions are:

- failure of the one train leads to transfer to train repair configuration with large AOT (up to 72 hours);
- failure of the two trains leads to transfer to multiply repair configuration with small AOT (a few hours);
- failure of the three trains demand to shutdown the plant using normal operation systems.

Let $\{A_l\}$, $l=1...N_E$ to be a set of such events. They suppose to be mutual exclusive. Each A_l can be expressed by the sum of elementary component vector events:

$$A_l = \sum_{r \in R_l} X_r .$$

It is convenient to consider A_j as a event that demands to transfer to E_j. Formally A_j could equals to zero event for some of E_j, with no transfers due to test. So, knowing (E^k,X^k) at the moment θ_k, just before leading the k-th configuration, it is possible to define probability distribution of the (E^{k+1},X^{k+1}) for the infinite interval $(\theta_{k+1}d\theta)$:

$$P\left\{E_j^{k+1}, X_p^{k+1}, \theta_{k+1} d\theta \;/ E_j^k, X_p^k, \theta_k\right\} =$$

$$= \pi_{iT}^{(\theta_k)} \delta_r^j \pi_{iD_j}^{(\theta_k)} \cdot P\left(X_{P_j}^{k+1} \theta_{k+1} \;/ X_{P_j}^k \theta_k\right) \cdot \left[F\left(\theta_{k+1} + d\theta\right) - F\left(\theta_{k+1}\right)\right];$$

where δ_r^j is characteristic value, equals to 1, when $X_r \in A_j$ and 0 when $X_r \notin A_j$,

$\pi_{iT}^{(\theta_k)}$ *and* $\pi_{iD_j}^{\theta_k}$ were introduced earlier.

The central point of equation ( ) is a second term.

To quantify it the two factors should be considered:

- restoration effect at the time point θ_k;

- component failures during the interval $[\theta_k\theta_{k+1}]$.

If Ei corresponds to configuration of one (or two) trains this event occurs at θ_k and therefore vector Xr_j will transfer to another vector $X_{\tilde{r}_j}$ at time point θ_k just after the configuration change. So, the two vectors $X_{\tilde{r}_j}^{\theta_k}$ *and* $X_{\tilde{P}_j}^{\theta_{k+1}}$ should differ only by failures of the part of components. Suppose that for transfer from $X_{\tilde{r}_j}$ to X_{P_j} components of 1,2,...k numbers should change their status from 0 to 1, i.e. fail and the status of others is not changed.

In this case taking into account exponential distribution of component reliability

$$P\left[X_{P_j}^{k+1}(\theta_{k+1}) \ / X_{jr}^{k}(\theta_k)\right] = P\left[X_{P_j}^{k+1}(\theta_{k+1}) \ / X_{j\tilde{r}}^{k}(\theta_k)\right] =$$

$$= \prod_{m=1}^{k}\left\{1 - exp\left[-\lambda_{mj}(\theta_{k+1} - \theta_k)\right]\right\},$$

where λ_{mj} - a failure rate of component m under plant configuration E_i. If however there is at least one component, which status in X_{P_j} is 0, but in $X_{\tilde{r}_j}$ is 1, then

$$P\left[X_{P_j}(\theta_{k+1}) \ / X_{j\tilde{r}}\right] = P\left[X_{P_j}(\theta_{k+1}) \ / X_{jr}\right] = 0.$$

In general the described above allows to define transition failure probabilities and therefore other desirable probabilistic characteristic of Marcov chain $[E_k,X_k,\theta_k]$. However for practical application some simplifications should be introduced to the model in order to decrease the space size.

An important sequence model was then developed from the same 6,000 sequences saved to the sequence database. This set was then examined to ensure that it provided representative sequences for cases in which a train of a system is unavailable for planned maintenance. For example, because the component cooling water (CCW) system has sucl low risk importance at STPEGS, the saved sequences did not contain a representative set of sequences with failed trains of CCW. To identify sequences for evaluation of CCW system planned maintenance, a special sensitivity case was developed by setting a train *o′* CCW split fractions to .5. This added another 645 sequences to the sequence database with train B CCW failed. This version was then used to address all maintenance states in which CCW is being

maintained.