PRACTICAL EXPERIENCE OF THE RUSSIAN VVER DESIGN ORGANIZATION IN THE USE OF PSA FOR VERIFICATION OF COMPLIANCE WITH SINGLE AND DOUBLE FAILURE CRITERIA

A. LYUBARSKIY, V. MOROZOV
JSC “Atomenergoproekt”
Russian Federation, Moscow
Email: Lyubarskiy_AV@aep.ru

I. KUZMINA
Consultant
Russian Federation, Moscow
Email: irina.kuzmina@yahoo.com

Abstract

JSC “Atomenergoproekt”, Moscow, is a Russian design organization, which is part of the integrated group of companies of ASE, and the main designer of AES-2006 with the VVER-1200 reactor. The AES-2006 project provides an enhanced level of safety through the introduction of innovative design solutions. JSC “Atomenergoproekt” extensively uses probabilistic safety analysis both for the selection of design solutions and for assessing compliance with the requirements of Russian and international standards, including those of the IAEA and the EU. The paper gives an overview of the results of the use of the PSA for assessing compliance of the design with the single failure and the ‘N + 2’ failure criteria. In addition, the paper discusses the requirements for PSA that are needed to perform such analyses.

1. INTRODUCTION

JSC “Atomenergoproekt”, Moscow, is a design organization that is part of the integrated group of companies of the “Atomstroyexport” (ASE). The first unit with NPP-2006M (“generation 3+” design) of JSC “Atomenergoproekt” is already operating at Novovoronezh NPP (NVNPP-2). A number of other units are at various stages of construction in Russia, Turkey and Bangladesh. The design provides an enhanced level of safety and efficiency through the use of innovative design solutions, namely, the combination of two-trains active safety systems (in some cases with additional redundancy of active elements within each train.) Figure 1 shows the diagram of the emergency core cooling system (ECCS) of NVNPP-2 as an example of a two-train system with internal redundancy.

FIG. 1. System diagram of ECCS (JNA)
At the same time, the design provides a two-train structure with regard to connections of active elements with support systems (power supply, control, information representation). Passive systems, along with active safety systems, participate in performing all basic safety functions providing a time window sufficient to connect additional facilities used in the design basis accidents. Nevertheless, taking into account the two-train structure of active safety systems, including emergency power supply systems, the justification for fulfilling a number of safety criteria requires additional consideration. It is necessary to take into account not only the states with the operation of the unit at power, but also the shutdown states of the unit, in which part of the safety systems can be disabled or can be taken out of service for scheduled maintenance.

In particular, it is required to justify compliance with one of the main safety criteria - the single failure criterion (SFC), as well as the "N+2 failures" criterion, which in fact is an extension of SFC.

According to section 2.1 of [1], SFC is formulated as follows: "An Assembly of Equipment satisfies the Single Failure Criterion (SFC) if it can perform its Safety Function despite a single random failure assumed to occur in any part of the assembly during any plant design condition in which the assembly is required to operate. This includes unrevealed pre-existing failures. Consequential failures resulting from the assumed single failure shall be considered to be an integral part of the single failure." However, according to 2.1.3.4F [1], failures of passive components may not be considered for SFC if they are designed, manufactured and assembled in accordance with the specified high quality requirements (e.g. pipelines, heat exchangers, tires, etc.).

According to paragraph 2.8.4.1.1.E [1], the criterion "N+2 failure" is formulated as follows: As Preventive Maintenance for some specific equipment performing Safety Functions is foreseen during plant Normal Operation conditions, the N+2 concept (unavailability due to maintenance plus SFC) shall be applied on a case by case basis depending on the level of function performed and on the design conditions for which the function may be required. In this formulation N is the minimum number of redundant elements required for the function being performed. At the same time, since this criterion refers to complex sequences exceeding the SFC conditions, its fulfilment can be demonstrated on the basis of a realistic (non-conservative) approach to safety analysis. Note that for AES-2006M, N = 1 (one element is needed for performing safety function).

The assessment of the design compliance with these criteria requires an analysis of the detailed list of postulated initiating events, and, more importantly, of all dependencies between structures, systems and components. The analysis should consider a huge number of combinations of failures and repair states of equipment and should take into account all explicit and implicit dependencies potentially leading to inability to perform critical safety functions. The probabilistic safety analysis (PSA) is an effective tool that allows the most complete and justified confirmation of the fulfilment of the above criteria. The approach and results of the analysis to confirm the compliance with the SFC and the criterion of "N+2 failure" performed at JSC "Atomenergoproekt", including the use of PSA models and results for the AES-2006M unit (exemplified by NVNPP-2) are briefly presented below.

2. OVERVIEW OF DETERMINISTIC ANALYSES OF THE DESIGN FOR JUSTIFICATION OF THE COMPLIANCE WITH SINGLE AND "N+2" FAILURE CRITERIA

In support for SFC, the NVNPP-2 design has the following features:

- Emergency shutdown of the reactor is carried out by an emergency protection system, designed with appropriate backup in the initiation and implementation parts.
- Residual heat removal is carried out by active safety systems (SS) consisting of two redundant independent trains, where all active components check valves inside each train are reserved (with the exception of diesel generators (DGs)).
- The localization function is performed by the passive component (primary containment) and the active ventilation system of the inter-enclosure space (2 trains), failures of which cannot be induced by the design basis accidents.
- A two-train sprinkler system, which operates automatically in the event of leakage under design conditions, removes heat and reduce pressure in the containment, and also helps to limit the release of radioactive products beyond the contaminant boundaries. Failures of this system cannot be induced by the design basis accidents.
- In accordance with 2.1.3.4F [1] and generally accepted practice, SFC does not apply to passive components such as reactor vessel and steam generator, refuelling pool, primary and secondary
containment. Also, failures of passive components (pipelines in the safety train) may not be taken into account when justifying the SFC, because they are assigned the 2nd safety class, according to Russian regulatory requirements [2] and they are under the workload only for a short period necessary for cooling of the unit (less than 24 hours) that altogether guarantees their high reliability.

— For DGs of the emergency power supply system (SAE), redundancy is not required, since, with deenergizing and failure of one DG, another DG remains in operation (there are no failures dependent on the design basic accidents).

— In operating states when the reactor head is removed (before combining the volumes of the reactor shaft and the refuelling pool to carry out the refuelling), there are two trains of the emergency and planned cooling system (EPCS) available, one of which performs the function of heat removal, and the second is in stand-by. In each train, the active parts are reserved. Scheduled maintenance (SM) of safety systems trains is not allowed in these states.

— During refuelling, when the volumes of the reactor and the refuelling pool are combined and scheduled maintenance on a safety system train is allowed, operator has sufficient time to connect alternative systems to compensate water losses.

Thus, it can be concluded that the structure of the safety systems in NVNPP-2 ensures the compliance with SFC.

In terms of compliance with the "N+2 failure" criterion, the following is envisaged in the NVNPP-2 design:

— When the unit is operating at power, scheduled maintenance of equipment of safety systems is not allowed. Therefore, in this state, the "N+2 failure" criterion is automatically satisfied.

— For various possible configurations of safety systems in the conditions of failures of individual systems, their trains or components, the design justifies the permissible time for performing repairs at power using the criterion of the minimum frequency of severe core damage, the value of which is significantly lower than 1E-06 per year. In this case, when a single train is put into unscheduled repair of a system, the redundant components in another train (with the exception of the DGs) ensure the compliance with the "N+2 failure" criterion without the use of passive systems. The design also includes functional redundancy, which allows performing the most important safety functions by different systems.

— In case of station blackout, heat removal from refuelling pool is done in a passive way, the water reserve (about 10 days) is sufficient to fulfil the autonomy criterion (6h), providing sufficient time for connecting an additional heat removal system from the refuelling pool based on an alternative independent from designed safety systems heat transfer circuit to the ultimate heat sink using mobile DG and dry cooling tower.

— Connecting a mobile DG also makes it possible to use a sprinkler system to reduce the pressure in the containment, however, there is no pressure increase in station blackout conditions, since no significant evaporation of the coolant occurs. In all cases, the function of heat removal from the reactor and the refuelling pool is carried out, the limitation of radioactivity releases is ensured by the contaminant, the integrity of which is maintained.

— In the state of shutdown for refuelling, planned maintenance on safety systems is allowed only when volumes of the reactor shaft and the pool are combined. In this case, failure of the second DG during loss of of-site power leads to a regime similar to that discussed above. In this case, the time reserve for fuel assemblies uncovery is at least 80h (about 10 hours before the boiling point), an additional system of heat removal from the pool will remove heat from the total volume of the reactor-pool, preventing the boiling away of the coolant.

Thus, the "N+2 failure" criterion is satisfied for all operational states.

3. EVALUATION OF COMPLIANCE WITH SINGLE AND "N+2" FAILURE CRITERIA USING PSA

The above justification for verifying the compliance with the criteria obviously does not guarantee the completeness of taking into account all possible dependencies, in particular, there is no explicit consideration of failures caused by initiating event, as well as there is no comprehensive analysis of dependencies from the
support systems (instrumentation and control, cooling water, power supply, ventilation systems) and between support that can violate the “N+2 failures” criterion.

The most effective way to verify the compliance of the design with the “N+2 failures” criterion is an analysis based on the PSA, which in this case should be developed for all operational states of the plant. It should be noted that the use of PSA in the context of verifying the “N+2 failures” criterion is fully acceptable, since complex sequences are subject to analysis.

One of the most important elements of probabilistic safety analysis is the construction of a logical model that takes into account all interrelations between systems and equipment, both intra-system and inter-system. The analysis of such a logical model using mathematical tools based on the application of Boolean logic allows identifying the minimum combinations of failures and operator errors sufficient to damage the core for the entire range of possible initiating events, including the events falling in the design extension conditions envelope. These combinations are usually called “minimal cutsets” (MCSs); they represent combinations of an initiating event, equipment failures and operator errors. In this case, if the calculation of the model is organized in such a way that there is no truncation on probability, it can be ensured that all MCSs containing at least two of the following: equipment failures and/or operator error and/or basic events representing maintenance unavailability are identified.

The analysis of the MCSs allows confirming:

- Compliance with the single failure criterion (in addition to the deterministic analysis) if it is shown that there are no MCSs containing initiating event and one equipment failure or one operator error.
- Compliance with the criterion “N + 2 failure”, if it is shown that there are no MCSs containing initiating event, unavailability of the equipment due to maintenance and repair (planned or not planned) and one equipment failure or one operator error.

The developed full-scale Level 1 PSA for NVNPP-2 [3] allowed revealing all MCSs containing up to four basic events.

Note, that MCSs with four basic events have to be reviewed because for non-symmetric PSA model some MCSs may include “conditional” basic events and those MCSs should be also analysed. For symmetric model consideration of MCSs containing three basic events is sufficient. MCSs containing more than four basic events are not of interest, since for them both criteria are obviously satisfied.

Table 1 summarizes the analyses of all MCSs containing up to four basic events (including the initiating event) [3].

<table>
<thead>
<tr>
<th>TABLE 1 RESULTS OF MINIMAL CUTSETS ANALYSES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Analysis of Minimal Cutsets</strong></td>
</tr>
<tr>
<td><strong>1. Review of MCSs containing only an IE</strong></td>
</tr>
<tr>
<td>The MCSs contain only the following initiating event caused by passive components failures directly leading to core damage: SGVR – steam generator rupture SCCR – steam generator header rupture RPRV – reactor vessel rupture These IEs are not part of the design envelope and do not require to be considered for compliance with SFC and “N+2 failure” criterion.</td>
</tr>
<tr>
<td><strong>2 Review of MCS containing two basic events</strong></td>
</tr>
<tr>
<td>The MCSs, in addition to the IE identifier, contain basic events with “RPS” symbols. Such basic events are part of a simplified model of the reactor scram system, calculated outside the framework of the PSA model. The reactor scram system is designed in such a way that there are no single and double failures for any IE, leading to system failure.</td>
</tr>
<tr>
<td>The MCSs, in addition to the IE identifier, contain basic events with common cause failures that represent at least two equipment failures.</td>
</tr>
<tr>
<td>The MCSs, in addition to the IE identifier, contain basic events with USBT symbols. Such basic events are part of a simplified model of a control system, calculated outside the framework of the PSA model. The USBT system is designed in such a way that there are no single and double failures for any IE, leading to its failure.</td>
</tr>
<tr>
<td><strong>3. Review of MCS containing three basic events</strong></td>
</tr>
<tr>
<td>The MCSs, in addition to the IE identifier, contain basic events with maintenance unavailability (identifier “M”) and passive components (filters, heat exchangers, buses, electrical assemblies). Failures of passive components may not be considered when compliance with SFC and “N+2 failure” criterion is verified.</td>
</tr>
</tbody>
</table>
4. Review of MCS containing four basic events

Other MCSs containing four basic events include: IE, unavailability due to maintenance and two additional components failure or human errors. There are no MCSs with “conditional” basic events because the model is developed as a symmetric model.

<table>
<thead>
<tr>
<th>Analysis of Minimal Cutsets</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>The MCSs include: design extension IE = “Steamline rupture and leak from primary to secondary circuit”, unavailability due to maintenance and single failure. Thus for these cutsets SFC is not fulfilled; however, for design extension conditions compliance with the criteria is not required.</td>
<td>Compliance with SFC and “N+2 failure” criteria is not required.</td>
</tr>
<tr>
<td>Other MCSs containing three basic events include: IE, unavailability due to maintenance and common cause failure.</td>
<td>SFC and “N+2 failure” criteria are satisfied.</td>
</tr>
</tbody>
</table>

Based on the results of the analysis presented in Table 1, it can be concluded that the analysis of MCSs confirms the compliance with the SFC and the "N + 2 failures” criterion in the NVNPP-2 design.

4. REQUIREMENT FOR IMPLEMENTATION OF PSA FOR RATIONALE OF CRITERIA

Summarizing the above, Level 1 PSA model for NVNPP-2 was used as a tool for the analysis of the compliance with SFC and “N+2 failure” criterion for all operating modes of the plant.

The analysis procedure included the following steps:

- Calculation of the PSA model without probability truncation limit in order to identify all MCSs containing up to four basic events (up to three basic events if the PSA model is symmetric).
- Analysis of the MCSs for the absence of cutsets violating SFC and "N+2 failure" criterion.

Obviously, the approach used to justify the implementation of SFC and “N + 2 failure” criterion for the design can only be applied if a Level 1 PSA for internal IEs including all operating states of the unit (at full power, reduced power, shutdown) is available. In addition, in the software used to build the PSA model, it should be possible to identify all the MCSs containing up to four basic events regardless their probability.

5. REFERENCES

[1] European utility requirements for LWR nuclear power plant, Revision D, October 2012