INTRODUCTION

Probabilistic approach to the safety of nuclear power plants is neither new nor homogenous method. It is a syntesis of various known and applied calculating techniques used also in deterministic safety assessment procedure. In the deterministic approach some abnormal initiating events are investigated and the response of the object to that event is analysed in conditions determining the mode and the range of action of particular a protection systems /the latter choosen by the designer on the basis of his subjective experience/. The assumptions about initiating event constitute the basy to the definition of the series of the so called design failures and in particular the maximum design failure. /Mc Cormick 1981/. The analysis of such failures is the basis for the evaluation of safety level of nuclear power plants in socialist countries /Edrenyi 1978/.

The probabilistic methods, instead of considering one or several failures choosen in subjective way take into account, in theory all possible initiating events and all possible sequences of events resulting from the initiating. The realistic treatment of such physical processes, is the essence of the probabilistic methods as opposed to the bounded sequence deterministic method, which introduces intentionally and consiously a series of factors increasing the pessimism of the reasearch results of the safety level. The comparision of safety estimation obtained in the above mentioned two ways is not usefull and even illogical, because of such specific differences between them.

In the cases of human safety endargement analysis or in the estimation of particular system reliability the probabilistic methods are unique in enabling the quantitative approach. The consideration of all possible initiatising events and, all their possible developments creates the basis for comparative approach to different systems and the designer can conduct the optimization of acceptable solution. /Kuraszkiewicz 1987, 1989/

THE BASES OF PROBABILISTIC ANALYSIS

The object and scope of probabilistic safety analysis can differ depending on the result of failure. The following three analysis levels have been adopted:

- the first level: the analysis covers all systems essential for
the operation of a nuclear power plant, identify all breakdowns or errors which may have as consequence a disturbance in the cooling system of the reactor core, the result, is a number of event sequences together with the estimation of probability for every sequence.

- the second level - on this level the mechanism of release of radioactive materials and the quantities of materials released are determined together with the determination of the state of the safety containment which is the last barrier in case of between the core and the environment failure. The results are the so called release categories from the safety containment determined by the probability of occurrence of the quantity of radioactivity released and characterized by the physical process of the release. /Nieshaus 1987 /

- the third level - at that level the analysis is concentrated on determination of the results of radioactive material release, together with the results reached during the preceding analysis it is possible to abain the probability of occurrence of the defined results of failure expressed in the form of enderament factor of type: summarized dose can absorbed by the human beings in the vicinity of power plant, the growth of cancer mortality, the number of lives lost as the results of the operation of radiation. The important practical problem in PSA analysis is the criterion for estimation if the defined risk level is acceptable. Risk is a synthetic indicator and thus a rather primitive one as the basis for the analysis aiming at the correction of decision making at the stage of engineering design or during the power plant operation. The probabilistic method applied in PSA conditions in particular during the reliability analysis and operation capability analysis of systems gives the extremely profound and valuable knowledge about the object performance. /Gesellschaft für Reactor Sicherheit 1981/ The full three step analysis to support the design decision making is not always necessary and can be limited to the first level. The described analysis conducted in the countries having a significant number of nuclear power plants yields practical results within limited financial and methodological resources engaged. /Wild 1983/

THE METHODOLOGY OF THE ANALYSIS OF THE FAULT TREES

Two basic fault trees concerning protection system of WWER - 1000 reactor have been worked out. For the purpose of safety estimation the tree has been constructed which has as the top event security break down consisting of the reactors shut down causal by not dropping two shut off rod failure assemblies. The first stage of the analysis is to find the set of cross sections of the tree and to eliminate events with the negligible probability of occurrence in comparison to the others. The next step in the construction of the set of boolean equations equivalent to each of the analyzed trees. To estimate the operation un capability of a power plant caused by improper safety system operation the tree having as the top event the partial drop of shut-off assemblies in conditions of proper power plant operation should be considered. The possibility of manual tripping of such by operator for action partial shut down was not considered. It is not possible to present here the full structure of the trees analysed because of place limitation.
According to the commonly applied methodology only the quantification of the trees is given below. The following probabilistic were determined in the order given:

- break down of elements
- human errors
- out of service caused by tests
- particular cross section of the tree
- top event

For the failures of system elements depending on time the probability of out of service was determined according to the equation

\[ q = \lambda \frac{T}{2} + \lambda T_R \]

\( \lambda \) - failure rate
\( T \) - the period between the system tests
\( T_R \) - the average period of the repair,

For the failures independent of time according to the model "no action for the order" the probability is given by:

\[ q = p + \lambda \frac{T}{2} \]

\( p \) - the probability of failure independent of time

To estimate the failures caused by human errors during systems tests the "Swan" formulae was applied. /Handbook for Human Reliability 1983/

\[ P_H = P \beta_H \]
\[ \beta_H = \frac{1 + 19p}{20} \]

where:

\( P_H \) - the probability that the error will occur more than once

\( P \) - the probability of the individual human error

The quantification of the top event was done by the first order estimation

\[ Q_T = \frac{N}{i} Q_i \]

where:

\( Q_i \) - the probability of \( i \)-th element of the set corresponding to the minimal tree cross section

\( N \) - the number of elements in the set of minimal free cross sections

CONCLUSION

The final results of the analysis for the considered two types of trees are gathered in the table 1
<table>
<thead>
<tr>
<th>Event</th>
<th>Correlated failure</th>
<th>Failure without correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A1</td>
<td>A2</td>
</tr>
<tr>
<td>Tree No 1</td>
<td>3.6</td>
<td>3.6</td>
</tr>
<tr>
<td></td>
<td>$10^{-4}$</td>
<td>$10^{-4}$</td>
</tr>
<tr>
<td>Tree No 2</td>
<td>4.2</td>
<td>4.1</td>
</tr>
<tr>
<td></td>
<td>$10^{-6}$</td>
<td>$10^{-6}$</td>
</tr>
</tbody>
</table>

The results obtained give some indication for further development of such type analysis. To diminish the uncertainty margins the improvement of data quality seems to be most important. This could be achieved by Expert System with the information about failures of elements in different objects. The data concerning the break down of particular devices are quoted in various positions and have values in certain ranges. The estimated values are often applied which lower the certainty of the final results. The use of proper Expert System seem to be motivated. The deterministic criteria used in Poland and in other countries grouped in the Council for Mutual Economic Aid /for instance the rule of single failure/ have important influence on the factors characterising the safety and the operation capability of nuclear power plants. The probabilistic estimations which make possible the evaluation of the safety in design stage and in operation should be introduced now.

REFERENCES

Gesellschaft für Reaktorsicherheit: 1981 Deutsche Risikostudie Kernkraftwerke, Verlag TBV Rheinländ
Kuraszkiewicz P., An instrument for the determination of the safety level of nuclear power plants. Nuclmat - 88, Nice
Niehaus F., 1987 Prospects for use of probabilistic safety criteria, SMiRT, Volume M, A.A. Balkema /Rotterdam/ Boston