EVALUATION OF THE SAFETY OF THE OPERATING NUCLEAR POWER PLANTS BUILT TO EARLIER STANDARDS

S. MENTESEOGLU

Department of Nuclear Engineering, Çekmece Nuclear Research and Training Centre,
P.O. Box 1, Atatürk Havalimani, 34831 Istanbul, TURKEY

SUMMARY:
The objective of this paper is to provide practical assistance on judging the safety of a nuclear power plant, on the basis of a comparison with current safety standards and operational practices. For nuclear power plants built to earlier standards for which there are questions about the adequacy of the maintenance of the plant design and operational practices, a safety review against current standards and practices can be considered a high priority. The objective of reviewing nuclear power plants built to earlier standards against current standards and practices is to determine whether there are any deviations which would have an impact on plant safety. The safety significance of the issues identified should be judged according to their implications for plant design and operation in terms of basic safety concepts such as defence in depth and safety culture. In addition, this paper provides assistance on the prioritization of corrective measures and their implementation so as to approach an acceptable level of safety.

OBJECTIVES OF SAFETY REVIEW:
The approach to safety that should be taken for existing nuclear power plants does not differ, in principle, from the safety approach applied to new plants. Fundamental safety principles must be demonstrated for all reactors, existing and future, to achieve the basic nuclear safety objective of protecting individuals, society and the environment from harm by establishing and maintaining in nuclear installations effective defences against radiological hazards.

The safety significance of identified issues may be judged according to their impact on the defence in depth and safety culture of the plant. The concepts of defence in depth and safety culture establish a rational framework of the fundamental safety principles for achieving the safety objectives. Therefore, the assessment of plant safety should be based on the effectiveness of the defence in depth capability of the plant design and operation.

Generally, the level of safety of a specific plant built to earlier standards is acceptable if:
1- it is established on a verified design basis which provides appropriate defence in depth;
2- the risk of intolerable consequences for the plant, for humans and for the environment is sufficiently low;
3- all factors contributing essentially to safety are continuously checked according to applicable current standards, methods and practices with the characteristics of the respective plant taken into account.
A plant built to earlier standards is judged to be acceptably safe if:

1- All issues in the HIGH and MEDIUM category, as defined in Table 1, have been resolved, or at least reduced to negligible importance for plant safety after all reasonable, practical, prompt or interim corrective measures have been taken, and also all reasonably practical measures have been defined to address safety issues of the LOW category,

2- The total mean core damage frequency and the expected frequency of severe off-site radioactive releases comply with national safety goals, if established.

SAFETY JUDGEMENTS:
Judgement is the central element of any safety assessment process, and is applied broadly in almost all aspects of nuclear power plant design, construction and operation. Simply stated, judgement is the process by which information is gathered and assessed so that decision can be made. In the area of nuclear power plant safety, judgements and safety conclusions about the state of the current knowledge base involve the careful balance of risk and benefits based on defence in depth practices and safety culture mentality (Table 2).

PREPARATION JUDGEMENTS:

1- Information gathering and scope of the review:
The initial organization of any safety review consists of a stock taking of the state of the plant built to earlier standards. The judgements made during the preparation phase concerning the scope of the review for the particular plant will consider what information is available and what information is needed such as:

- Licensing basis and plant history
- Modifications and backfits completed, ongoing or planned
- Results of routine inspection activities
- Probabilistic safety assessment evaluations
- Programmes to systematically review events at the site and in the country
- Results of trend analyses as a straightforward calculation of the number of occurrences of particular types of system or component failures, transients and plant trips.

During the development of the scope of review, particular attention should be given to those topics for which the standards were not as well developed at the time of the design. Such topics usually involve design basis events, external hazards (earthquakes, floods, winds, etc.), redundancy, physical separation, diversity and the impact on the overall plant safety caused by the potential of common cause failures, protection, ageing, severe accidents and accident management, human factors and safety management principles. In the past, less attention was given at the design stage to low power and shutdown conditions.
Information may be missing regarding the design of components or systems, accident analysis or practices such as the maintenance procedures. A judgement will then be made to determine whether new information must be obtained for conducting the safety assessment, or whether the lack of information may be treated as a safety issue and resolved during the assessment of other safety issues.

To ensure that the safety assessment is both comprehensive and complete, sufficient information must be gathered to identify differences from the agreed current standards and practices. Information should also be assembled regarding the plant specific operating experience and system availability, to determine whether that experience justifies any differences from current standards and practices.

2- Applicable standards and practices:
Where a country has a mature nuclear industry and regulatory body, it is expected that national standards for the safe use of nuclear power which are recognized by the wider international community are in place. In such cases, the current national standards would be appropriate for the plant safety review.

Where there is neither a mature regulatory process nor an imported technology, then some other comprehensive safety standards can be obtained and adopted by the country as the basis for the plant review. The safety standards to be applied should be suitable for the plant type under evaluation and consistent with the IAEA NUSS Codes and Guides, and the Basic Safety Principles for Nuclear Power Plants of INSAG-3.

During the organization of the review, the plant operator and the regulator determine whether particular standards need to be defined as 'necessary'. The 'necessary' standards establish requirements which must be satisfied, while the remainder of the standards and practices provide guidelines that allow judgements to be used for interpretation and the development of a wide range of acceptable alternatives. For example, many countries consider the temperature limits to prevent brittle fracture of light water reactor pressure vessels as 'necessary' standards.

Standards for operational processes and practices continue to evolve. Consequently 'operational safety' issues (process and safety culture concerns) are often distinguished from engineering issues (design basis and hardware concerns).

3- Acceptance criteria:
The current standards and practices specify particular acceptance criteria which are intended for prospective applications. In the safety review process for nuclear power plants, the acceptance criteria appropriate for the assessment phase are those acceptable limits contained within the current standards and assessment methods, or alternatively proposed by the plant operator, which the regulator agrees with and will rely on to ensure public safety.
The plant operator can consider the operational criteria in the assessment methods to include additional margins for operational flexibility. The regulator usually considers the complete set of acceptance criteria and operational criteria, as proposed by the plant operator, to confirm that there are adequate safety margins beyond the acceptable limits to allow for uncertainties and provide defense in depth.

In some cases, the operational criteria and acceptance criteria may be identical, particularly for the safety assessment of plants built to earlier standards. Many standards include sufficient background information for the plant operator and regulator to agree to alternative acceptance criteria. In some circumstances, it may be appropriate to consult with the source of standard or practice to clarify the purpose of the acceptance criteria in order to ensure that the safety significance judgements are competent. The plant operator and the regulator need to clearly understand any differences between the acceptance criteria and operational criteria that will be used for the safety assessment. Safety goals can be used effectively to judge the relative significance of safety issues and to prioritize corrective measures. Currently there is no internationally agreed policy on the use of universally accepted safety goals, although some Member States have developed their own safety goals.

**ASSESSMENT JUDGEMENTS:**

An effective approach is to organize the assessment on the basis of discrete 'safety issues' (deviations from the current safety standards or operational practices, or weaknesses in plant design or practices identified by plant events, with a potential impact on defence in depth, margins to safety or safety culture).

**1- Identification of Safety Issues:**

Plant specific issues are safety concerns which are applicable to the specific situation of a nuclear power plant. They are identified during examination of the detailed design and from the operational experience of the plant that is being evaluated. In international practice, plant specific issues and generic issues are usually treated differently. Generic safety issues are defined as those issues that involve broad safety concerns that may affect the design, construction or operation of several plants or a plant type. Specifics issues identified for individual but similar units may indicate a safety concern generic to all units of the plant type. The list of generic issues for a plant review is usually very broad and based on different source of international and national experience.

PSA insights and operational experience are significant sources for plant specific and generic safety issues, and important sources of potential safety issues for the comprehensive safety assessment of a particular plant. These sources include any pending plant improvements, particularly those that are being implemented as corrective measures.
Design issues include those derived from specific details of support systems and balance-of-plant systems that are not supplied by the reactor vendor and that are not subject to generic review. Other issues may result from details of equipment locations and cable routing that affect susceptibility to common cause failures or external events.

Operational issues may be identified from specific operational, testing and maintenance practices, equipment performance and trend analysis, performance indicators, management, training and quality assurance (Table 3).

2-Safety Issue Categorization:

Issues can best be managed by organizing them into 'categories'. The categorization of an individual safety issue depends on judgements of its impact on plant safety. The levels of defence are implemented firstly to prevent damage to the barriers and the plant, and secondly to mitigate the consequences of any damage. Therefore, the impairment of defence in depth for a given issue involves a judgement of the effectiveness of the performance of the primary safety functions: controlling the reactivity, cooling the fuel and confining the radioactive materials (each barrier needs to be evaluated separately). These functions may be affected individually or in combination.

Typically, more than one issue which can affect the primary safety functions of protecting the barriers against challenges to the plant will have been identified. Within the deterministic safety review, all relevant safety issues which can affect a primary safety function under different conditions need to be considered. They include:

- Controlling the reactivity by shutting down the reactor and maintaining safe shutdown conditions during normal operation and in transient and accident conditions.

- Cooling the fuel in all conditions during normal operation, during transients, after loss of coolant accidents (LOCAs) and during shutdown or refueling;

- Containing the radioactive material during normal operation and under accident conditions.

The judgement process involves the appropriate application of deterministic review, operational process review and probabilistic assessment to complement the judgements, for both individual issues and collective issues. Judgements will also be made on how the deterministic and operational process review and probabilistic assessment have been applied, how the assessment will be performed, and when several issues are considered collectively, how the issues interact.

The assessment process for the operational performance of a plant will draw on operational experience, both national and international, and identify solutions and actions taken elsewhere to deal with similar deficiencies. Judgement is required on the adequacy of organization, management accountabilities, event analysis, operational and technical staff competence, safety culture, engineered systems design and control, emergency arrangements, quality assurance, maintenance, etc.
Probabilistic analyses are useful for assessing the significance of safety issues. APSA should be plant specific, sufficiently broad in scope, and of a sufficient level of detail. Limitations and uncertainties in the PSA models, data and assumptions need to be considered carefully and documented. Furthermore, PSA analyses are difficult to apply to some issues, particularly issues related to safety culture and quality of material, equipment and plant structures. The detailed review of each potential safety issue, using all appropriate tools, will provide a sufficiently deep understanding of the safety concern as a basis to determine whether and how to develop corrective measures. The ranking of issues according to their safety significance is considered to be a reference basis for safety improvements until the issue is solved or the remaining risk is judged to be acceptable. The ranking of an issue must be reconsidered if new insights on the safety concern reveal a serious safety problem. Potential safety issues need to be carefully tracked during the safety assessment process by both the plant operator and the regulator, so that any interim corrective measures are appropriately reconsidered when final corrective measures are selected for implementation.

IMPLEMENTATION JUDGEMENTS:

1- Corrective Measures:

Once the significance of each safety issue and the collective impact on safety of a plant built to earlier standards have been evaluated, corrective measures will be developed to resolve the issues. The purpose of this phase is for the plant operator and regulator to agree on an optimum set of feasible corrective measures, such as:

- Operational restrictions
- Reduction of loads to equipment
- Modification to procedures, operator training, maintenance practice, test intervals, management
- Upgrading of the capacity, reliability and redundancy of existing equipment
- Qualification of equipment for extended functions
- Development of procedures
- Installation of new equipment (safety systems, support systems, fire barriers, etc.).

To ensure that the corrective measures are effective, it is most important that the root cause of the issue be clearly understood. In some cases, there may not be enough information available to develop a corrective measure that will fully resolve the issue. Further analyses may be appropriate to resolve the issue by clarifying the design basis, defining the root cause more exactly, or establishing a monitoring or surveillance programme to ensure that the root cause is properly addressed. In such cases, there must be sufficient information to ensure safe plant operation while additional analyses or information are being developed. These circumstances and practices are very common during the review of emerging generic issues such as ageing effects. If the root cause of an issue is not clearly understood, an interim corrective measure may need to be implemented.
There is a difference between corrective measures for design and operational issues. Design issues can often be effectively overcome by upgrading; however, it is also broadly recognized that it is not always feasible or cost-effective for plants built to earlier standards to fully meet current international practice in design standards. Conversely, corrective measures for operational safety issues can usually be implemented effectively in plants regardless of their age.

Once the plant operator and regulator agree on the corrective measures to resolve the issues, those decisions need to be carefully documented to provide an auditable record for peer review and future reference. Therefore, clear design basis records are an important precondition and provide important information if the implementation plan needs to be changed or new safety issues arise in the future.

2- Prioritization of Corrective Measures:
Corrective measures, both design and operation, need to be prioritized to ensure that limited resources are carefully planned and scheduled for upgrading of plants built to earlier standards. The priorities for corrective measures are based on progression of importance. The highest priority is given to those measures which will achieve or restore the most important defence in depth features in design and operation that were applicable at the time of first licensing; a moderate priority is given to those measures that enhance the preventive plant capabilities; and the lowest priority is given to those measures for enhancement of the mitigative plant features.

3- Implementation Plan:
The implementation of corrective measures basically consists of two phases:
Immediate actions and a schedule of subsequent actions to complete resolution of all issues. The schedules for the immediate and interim corrective measures should be separated from those for longer term corrective steps in order to ensure that any conditions necessary for safe plant operation have been fulfilled. Milestones need to be clearly established in the plan so that progress towards completion of the corrective measures can be carefully monitored, and potential impediments to successful implementation (e.g. resource limitations or availability of equipment) can be identified and promptly resolved.

An implementation plan needs to be developed and maintained by the plant operator to ensure that completion of all corrective measures is achieved on a schedule consistent with the assumptions in the prioritization, and to ensure that the implementation processes of the corrective measures do not adversely interact to detract from plant safety. The implementation plan needs to recognize that there will be an optimum approach to the implementation of changes in the plant design and operation in terms of their sequence and related effects.

A detailed implementation plan developed by the plant operator will reflect:
- controls for plant modifications
- work layout and process efficiencies
- project funding and management
- the necessary plant conditions to complete the changes
- procurement of materials
- inspection requirements
- personnel training and qualification

The implementation plan needs to address the impact of the collective hardware changes on the safety culture and management systems. The priorities of the individual corrective measures can be used if there are conflicting demands on resources, personnel, technical specialists and materials.

When an implementation plan has been established and agreed upon, the plant operator is expected to monitor the progress of the work to ensure that it is proceeding in accordance with the plan and the accepted priorities and schedules. Changes to the implementation plan should be developed periodically, in consultation with the regulator, by assessing the status of incomplete task, their original purpose and priority, new tasks, and the overall impact on plant safety of all the pending tasks.

**JUDGEMENT EXAMPLES :**

1- **External Hazards:**

Description: Current standards would consider an increase of the horizontal ground acceleration for the safe shutdown earthquake from 0.1g to 0.17g.

The initial seismic design of the plant considered two seismic levels:

Operational based earthquake 0.05g

Safe shutdown earthquake 0.1g

In the late 1960s, there were no design basis spectra available. A simplified soil model was used for the soil-structure interaction analysis. Most of the seismic design effort concerned the reactor building and the other nuclear auxiliary buildings (containing radioactivity). The electrical building was originally designed for vertical loads only.

**SAFETY SIGNIFICANCE**

Safety function capability :  INADEQUATE

Without an analysis to demonstrate the functional capability of the systems, it would probably be judged that the safety function could not be assured.

Event frequency:  UNLIKELY

The occurrence of an safe shutdown earthquake is considered to be 1.E-4 reactor-year.

Potential consequences:  INTOLERABLE
The consequences of an safe shutdown earthquake are dependent on the real capacity of the structures to withstand them, but a conservative judgement would assume that such an event would lead to radiological releases beyond the design basis.

Category of issue: MEDIUM
Corrective measures:
0.17g requalification of the electrical building, making strict use of current methods and criteria, was considered impossible. Two options were considered:
Erection of a new building designed according to the most recent practices with the function of guaranteeing the safe shutdown of the plant after earthquake;
Use and/or development of advanced and innovative methods in order to decrease the conservatism inherent in the design methods.
Without conducting a detailed cost-benefit analysis, the decision was made to develop the second option for the following reasons:
- The cost of a new system was thought to be very high;
- There were no senior experts in seismic engineering available;
- There were no advanced computer codes available;
- Feedback of experience for structures exposed to real earthquakes was available.
It was first decided to develop a site dependent design response spectrum, using records of earthquakes of the same intensity obtained for similar soil conditions. Complementary soil characteristic measurements allowed for a more accurate soil model.

REFERENCES:
### Table 1: Safety Significance Categories

<table>
<thead>
<tr>
<th>Safety Significance Category</th>
<th>Defence in depth classification criteria</th>
<th>Actions required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LOW</strong></td>
<td>An issue which may have a small impact on plant safety</td>
<td>Plant operation can continue without the need for interim corrective measures. Corrective measures may be considered and implemented within a specified time schedule if shown to be reasonably practicable.</td>
</tr>
<tr>
<td></td>
<td>• A barrier is affected by the issue -or- • One or more levels of defence are affected by the issue but the primary safety function capability to protect the barrier(s) is still considered robust for certain accident sequences in the design basis envelope or adequate for certain accident sequences beyond the design basis envelope. -or- • The issue causes a new initiating event or an increase of the frequency of certain initiating events and challenges to safety, systems and personnel, leading to a small impact on the risk. -or- • The level of operational performance and safety culture warrants improvement.</td>
<td></td>
</tr>
<tr>
<td><strong>MEDIUM</strong></td>
<td>An issue that has a significant impact on plant safety</td>
<td>Some interim corrective measures are usually necessary in the short term. Plant operation may continue for some limited time, depending on the risk after implementation of the interim corrective measures. Cost effective permanent corrective measures should be implemented.</td>
</tr>
<tr>
<td></td>
<td>• A barrier is degraded by the issue. -or- • One or more levels of defence are significantly affected by the issue but the primary safety function capability to protect the barrier(s) is adequate for certain accident sequences in the design basis envelope or is inadequate for certain accident sequences beyond the design basis envelope. -or- • The issue causes a new initiating event or an increase of the frequency of certain initiating events and challenges to safety, systems and personnel, leading to a significant impact on risk. -or- • The level of operational performance and safety culture is inadequate.</td>
<td></td>
</tr>
<tr>
<td><strong>HIGH</strong></td>
<td>An issue that has a significant impact on plant safety</td>
<td>Immediate corrective measures are necessary to reduce the risk, and plant shutdown should be considered. If immediate corrective measures cannot reduce the risk, the plant may need to be shut down until interim or permanent corrective measures which will reduce the risk are implemented.</td>
</tr>
<tr>
<td></td>
<td>• A barrier is seriously degraded by the issue. -or- • One or more levels of defence are lost because of the issue so that the primary safety function capability to protect the barrier(s) is inadequate for certain accident sequences in the design basis envelope or is inadequate for certain accident sequences beyond the design basis envelope. -or- • The issue causes a new initiating event or an increase of the frequency of certain initiating events and challenges to safety, systems and personnel, leading to a major impact on risk. -or- • The level of operational performance and safety culture is unacceptable.</td>
<td></td>
</tr>
</tbody>
</table>

---

*a* The phrase "certain accident sequences in the design basis envelope" means the design basis accidents for current design practices, which may be more comprehensive than those of the original design basis, including small break loss of coolant accidents and related boundary conditions, the range of anticipated operational occurrences, startup, shutdown and refueling operations.

*b* Although the levels of defence associated with the primary safety function capability already include elements of operational safety, the operational performance should emphasize the safety significance of shortcomings in human involvement. The terms used in this table are defined as: warrants improvement --- improvements in operational performance are warranted in relation to procedural compliance; inadequate --- poor procedural compliance or procedural quality; unacceptable --- a significant shortfall in procedural compliance and quality.
Table 2. The safety review process.
Table 3. Decision Matrix Glossary

**EXPECTED initiating events**
Events which might reasonably be expected in the life of the plant, i.e. a frequency of $>3 \times 10^{-2}/\text{reactor-year}$, which is generally consistent with the approximate range of the frequency for anticipated operational occurrences.

**POSSIBLE initiating events**
Events which have a greater than 1% chance of occurring over the life of the plant, i.e. a frequency of $\geq 3 \times 10^{-4}/\text{reactor-year}$, which is generally consistent with the approximate range of the frequencies of design basis accidents.

**UNLIKELY initiating events**
Events which have a less than 1% chance of occurring over the life of the plant, i.e. a frequency of $<3 \times 10^{-4}/\text{reactor-year}$ ---not normally included in DBAs.

**REMOTE initiating events**
Events which are very unlikely to occur, i.e. a frequency of $\leq 10^{-6}/\text{reactor-year}$.

**TOLERABLE consequences**
Consequences which will lead to some plant damage. Release of radioactive material may result in off-site doses not exceeding the order of a few milisieverts (1 mSv is the annual dose limit for the public).

**SIGNIFICANT consequences**
Consequences which will be serious, but contained damage to the plant, possibly involving core damage. Release of radioactive material may result in off-site doses up to the order of about 10-100 mSv.

**INTOLERABLE consequences**
Consequences which will result in severe core and plant damage. Release of a large fraction of the radioactive material of the order of tens of thousands of terabequerels or more of iodine, which might result in acute and certainly delayed health effects.

**ROBUST primary safety function**
Robust performance means that the primary safety function for EXPECTED and POSSIBLE initiating events can still be achieved with redundancy and diversity comparable to the design basis, and sufficient margin for the design capacity and protection against common cause failure. The degree and kind of redundancy, diversity and margin may or may not be the same as in new plants.

**ADEQUATE primary safety function**
Adequate performance means that the primary safety function could be achieved with questionable capacity only, or without the complete redundancy, protection against common cause failure, diversity and safety margin associated with current standards and practices.

**INADEQUATE primary safety function**
Inadequate performance means that the primary safety function cannot be achieved, or is unlikely to be achieved.