Հավելված
ՀՀ կառավարության 2012 թվականի
նոյեմբերի 8-ի N 1411 - Ն որոշման

Design Safety Requirements to New NPP Unit(s)

CONTENTS

1. GENERAL PROVISIONS

The current regulation defines the basic criteria and rules of nuclear safety and radiation protection of nuclear power plants (NPP), as well as the administrative provisions and the technical requirements for ensuring NPP design safety.

Content, completeness and depth of the implementation of these requirements and measures shall comply with the national regulations in the field of nuclear energy, as well as other regulations and state standards and the validity of their application for specific NPPs shall be confirmed by the State Committee on Nuclear Safety Regulation during in the process of licensing (Regulation).

At lack of the required regulations, the proposed specific technical solutions are justified and established in the design in accordance with the achieved level of science and technology. The acceptability of these solutions is determined by the State Committee on Nuclear Safety Regulation in the process of licensing (Regulation).

This document does not cover all requirements associated with the safety of nuclear power reactors. Separate documents establish requirements related to selection of the reactor site, construction, plant operational safety and decommissioning.

These requirements are mandatory to all legal entities and physical persons implementing practices related to siting, design, construction, commissioning, operation and decommissioning of nuclear power units, and are applied on the territory of Armenia.

2. DEFINITIONS

The following terms with their corresponding definitions are used in this document:

Accident: means a deviation from normal operation involving release of radioactive products and/or ionizing radiation outside design boundaries specified for normal operation in amounts exceeding the established safe operational limits. An accident is characterized by an initiating event, human and hardware failures, and consequences.

Accident management means a set of actions to prevent escalation of an event into a severe accident, to mitigate the consequences of a severe accident; and to achieve a long term safe stable state.

Active component is a component whose functioning depends on an external input such as actuation, mechanical movement or supply of power.

Anticipated operational occurrence is an operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to systems and components important to safety or lead to accident conditions.

As Low As Reasonably Achievable (ALARA means making every reasonable effort, through design and operation, to maintain exposures to radiation as far below the dose limits as practical, taking into account the state of technology and socioeconomic factors)

Beyond Design Basis Accidents: event sequences that could lead to conditions beyond the design basis accident conditions, without significant core degradation and/or with significant core degradation (severe accidents), from which event sequences can be selected to identify and to implement those reasonably practicable provisions for their prevention and mitigation.

Common cause failure is failure of two or more structures, systems or components due to a single specific event or cause.

Confining safety systems, components are designed to prevent release of radioactive materials and radiation during accidents.

Conservative approach to analysis of accident causes, development and consequences means that values and limits admittedly resulting in the most unfavorable results are taken as parameters and characteristics.

Controlling safety systems, components are designed to initiate safety system actions, monitor and control them in the course of performance of their intended functions.

Design limits are values of parameters and characteristics of systems established by design for operational states and accidents.

Design-basis is the collection of information which identifies the specific functions to be performed by a structure, system, or component, and the specific values or ranges of values chosen for controlling parameters as reference bounds for design.

Design-basis accidents are accidents against which a nuclear power plant is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.

Diversity principle is the presence of two or more redundant components or systems to perform an identified function, where the components or systems have different attributes so as to reduce the possibility of common cause failure.

Emergency preparedness establishes the preparedness level and technical facilities used in actions for personnel and public protection in case of an accident.

Fail-safe design is the ability to ensure safety based on natural feedback and processes.

Functional isolation means prevention of influences from the mode of operation or failure of one circuit or system on another.

Hazard is a condition that potentially can cause a disease, injury or loss of human life, or damage to the facility or the environment.

Independence principle improves system reliability using functional and/or physical separation of trains, components for which failure of one train, component does not result in failure of another train, component.

Systems (components) important to safety are safety systems and systems for normal operation failure of which leads to deviation of normal operation, create obstacles for restoration of normal operation and can lead to design base or beyond design base accidents.

Nuclear power plant*, NPP* is a facility for generation of power (electric and/or thermal) with a nuclear reactor (reactors) and a set of systems, devices, components, buildings and personnel required for this purpose.

Normal operation is operation within specified by design operational limits and conditions.

Normal operating systems*,* ***components*** are systems, structures, components designed for normal operation.

Operation includes particularly start up of reactor into criticality, stable power operation, shut down of reactor, increasing and decreasing of reactor power, shut down state, maintenance, repairs and testing of unit and refueling outages.

Operational states define the status of the NPP under normal operation and anticipated operational occurrences.

Passive component is a component whose functioning does not depend on an external input such as actuation, mechanical movement or supply of power.

Personnel error is a single inadvertent wrong action upon controls, or a single omission of a proper action, or a single inadvertent action during maintenance of equipment and safety- significant systems, components.

Physical separation means separation by geometry (distance, orientation, etc.), by appropriate barriers, or by a combination thereof.

Postulated initiating event is a single failure of NPP systems, external event or operator error resulting in disturbance of normal operation that may lead to violation of limits and/or conditions of safe operation. The initiating event includes all dependent failures.

Protective safety systems, components are designed to prevent or limit failure of nuclear fuel, fuel cladding, piping and components containing radioactive materials.

Redundancy principle improves system reliability by provision of more than a single system, structure or component to perform a safety function.

Risk-informed approach is a process to assign priority and allocate resources in proportion to the relative significance of considered hazards for NPP safety.

Safety criteria are values of parameters established by regulations or license condition as limits for the conditions experienced during normal operation or design basis accidents.

Safety limits for nuclear reactors are limits upon important process variables that are found to be necessary to reasonably protect the integrity of certain of the physical barriers that guard against the uncontrolled release of radioactivity.

Safety-related SSC are SSC which are relied upon to function following design-based accidents to ensure that specific design limits are not exceeded and to limit the consequences of design-base accidents.

Safety systems*, structures, components* are systems, structures, components designed to perform safety functions.

Severe accident is an accident resulting in conditions outside the design basis of the plant, possible damage to the reactor core and potential release of radiation to the environment.

Single failure criterion states that a system shall perform its functions in case of any initiating event demanding its operation, and in case of a failure, independent from the initiator, of one of the active components or passive components having mechanical movable parts, or a single independent operator error.

Station blackout means the complete loss of alternating current (ac) electric power to the essential and nonessential switchgear buses in a nuclear power plant (i.e., loss of offsite electric power system concurrent with turbine trip and unavailability of the onsite emergency ac power system). Station blackout does not include the loss of available ac power to buses fed by station batteries through inverters or by alternate ac sources as defined in this section, nor does it assume a concurrent single failure or design basis accident.

Supporting safety systems, components are designed to provide safety systems with motive power, cooling fluid and other conditions needed for reliable performance.

Unidentified failure is the failure of a system, component that is not apparent at the time of its initiation during normal operation and cannot be identified by available inspection methods used according to regulations for maintenance and inspections.

3. SAFETY PRINCIPLES AND OBJECTIVES

The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation.

A nuclear power plant is assumed to be safe when its radiation impact in all operational states is kept at a reasonably achievable low level and is maintained below the regulatory prescribed dose limits for internal and external exposure of the personnel and population, and when in case of any accident, including those of very low frequency of occurrence, the radiation consequences can be mitigated.

Measures shall be provided to ensure that radiation doses to the public and to site personnel in all operational states, including maintenance and decommissioning, do not exceed prescribed limits and are as low as reasonably achievable.

The design shall have as an objective the prevention or, if this fails, the mitigation of radiation exposures resulting from design basis accidents and selected severe accidents. Design provisions shall be made to ensure that potential radiation doses to the public and the site personnel do not exceed acceptable limits and are as low as reasonably achievable.

Plant states that could result in high radiation doses or radioactive releases shall be restricted to a very low likelihood, and it shall be ensured that the potential radiological consequences of plant states with a significant likelihood shall be only minor.

For accidents without core melt, there shall be no necessity of protective measures for people living in the vicinity of the NPP.

Accidents with core melt which would lead to large early releases have to be eliminated by design provisions.

The plant shall comply with **design limits** governing the key physical parameters for each structure, system or component for operational states and design basis accidents. The design limits will be defined in guidance published by the regulatory body.

The plant shall meet the following main **nuclear and radiation safety criteria**:

- The annual effective dose to the public shall not exceed 0.1 mSv.
- The annual effective dose to plant personnel shall not exceed 20 mSv.
- The annual effective dose of the public from internal and external exposure beyond the boundary of the exclusion zone shall not exceed 1 mSv over the first year following a design basis accident.
- Accidents with core melt shall not lead to permanent relocation, long term restrictions in food consumption, or need for emergency evacuation outside the exclusion zone.
- The probability of reactor core damage or core melt during accidents shall be less than 10^{-5} events per reactor per year.
- The formation of a secondary critical mass in case of core damage and/or melt shall be ruled out by engineering decisions.
- The estimated probability of a large early release of radioactive materials to environment shall be less than 10^{-6} events per NPP unit per year.

3.1. Design for defense in depth

The defense in depth principle is the fundamental principle of safety for the NPP with implementation of several levels of protection including successive barriers against the release of radioactive substances to the environment and shall be used to demonstrate that the fundamental safety functions are correctly insured.

Design of a plant shall provide levels of defense aimed at preventing accidents and ensuring appropriate protection in the event that prevention fails. The design shall consider possibilities of multiple failures and the use of diversified means to fulfill the three basic safety functions.

Defense in depth includes multiple physical barriers to confine radioactive material at specified locations. The barriers consist of the fuel matrix, fuel cladding, the reactor coolant system pressure boundary and containment. The design shall prevent as far as practicable challenges to the physical barriers, failure of a barrier when challenged; and failure of a barrier as a consequence of failure of another barrier.

The first level of defense requires the prevention of transients, accidents and other deviations from normal operation. The plant must be designed, constructed, maintained and operated in accordance with high quality levels and proven engineering practices, selection and application of appropriate design codes and materials.

The second level of defense is to detect and intercept deviations from normal operational states in order to prevent anticipated operational occurrences from escalating to accident conditions. The plant shall include specific systems and operating procedures to prevent or minimize damage from such PIEs.

The third level of defense requires design features and operational procedures to control consequences of transients or accidents and to achieve a stable and acceptable plant state. Inherent or engineered safety features safety systems and procedures shall be provided that are capable of leading the plant first to a controlled state, and subsequently to a safe shutdown state, and maintaining at least one barrier for the confinement of radioactive material. Selected multiple failure events including possible failure or inefficiency of safety systems shall be considered on this level.

The fourth level of defence is to mitigate the consequences of accidents that result from failure of the third level of defence in depth. The most important objective for this level is to ensure the confinement function, thus ensuring that radioactive releases are kept as low as reasonably achievable. Practical elimination of situations that could lead to early large realizes of radioactive materials and control of accidents with core melt to limit realizes are the objectives of this level.

The fifth level requires mitigation of radiological consequences of significant releases of radioactive materials to protection of plant personnel and the public. An emergency control center and emergency plans and emergency procedures shall be developed to protect on-site and off-site personnel from potential radiological consequences of accidents.

The design shall be such that the first, or at most the second, level of defense is capable of preventing escalation to accident conditions for all but the most improbable PIEs.

The reduction of frequencies of occurrence of accidents (including core melt accidents) has to be obtained by reducing the frequencies of occurrence of initiating events and by further improving the availability of safety systems.

Accidents during shutdown states must be taken into account at the design stage.

The quality of design, manufacturing and construction is essential for safety in the frame of the first level of DiD. Quality must be obtained and demonstrated notably by an adequate set of requirements for design, manufacturing including test and inspections, construction , as well as by quality assurance. At the design stage consideration must be given to the inspectability and testability of equipment as well as to the possibility of replacement of some equipment, considering that maintenance and testing activities are essential to maintain the safety of the plant throughout operation.

3.2. Safety functions

The following fundamental safety functions shall be performed in operational states, in and following a design basis accident and, to the extent practicable, on the occurrence of those selected accident conditions that are beyond design basis accidents:

- Control of reactivity
- Removal of heat from the core
- Confinement of radioactive materials and control of operational discharges, as well as limitation of accidental releases.

A systematic approach shall be followed to identify the structures, systems and components (SSC) that are necessary to fulfill the safety functions. The capacity and reliability of SSC to perform safety functions shall be demonstrated by design descriptions, operational experience and analysis in the PSAR and FSAR. SSC needed to perform safety functions shall meet the appropriate safety requirements in Chapter 6 of these requirements.

3.3. Aging safety margins

Appropriate margins shall be provided in the design for all SSC important to safety so as to take into account relevant aging and wear-out mechanisms and potential age-related degradation, in order to ensure the capability of the structure, system or component to perform the necessary safety function throughout its design life.

Aging and wear-out effects in all normal operating conditions, testing, maintenance, maintenance outages, and plant states in a PIE and post-PIE shall also be taken into account. Provision shall also be made for monitoring, testing, sampling and inspection, to assess aging mechanisms predicted at the design stage and to identify unanticipated behavior or degradation that may occur in service.

3.4. Design to Prevention and Mitigation of Accidents

3.4.1. Prevention of postulated initiating events

Normal operation. The plant shall be designed to operate safely within a defined range of parameters (pressure, temperature, power etc.). The design shall be such that the response of the plant to a wide range of anticipated operational occurrences will allow safe operation or shutdown, if necessary, without the necessity of invoking provisions beyond the first, or at the most the second, level of defense in depth.

The potential for accidents to occur in low power and shutdown states, when the availability of safety systems may be reduced, shall be addressed in the design, and appropriate limitations on the unavailability of safety systems shall be specified.

The design shall establish requirements and limitations for safe operation, including:

- control system and procedural constraints on process variables and other parameters;
- requirements for maintenance, testing and inspection of the plant to ensure that structures, systems and components function as intended in the design, with the ALARA principle taken into consideration;
- clearly defined operational configurations, including operational restrictions in the event of safety system outages.

These requirements and limitations shall be a basis for establishing operational limits and conditions under which the operating organization will be authorized to operate the plant.

Design solutions to reduce the frequencies of initiating events have to be considered for all types of events which contribute to the total core melt frequency significantly. It is important to consider initiating events during all operating states, including full power, low power, and all relevant shutdown conditions.

Quality of design, manufacturing, construction operation and maintenance shall ensure that those malfunctions leading to the actuation of safety systems are unlikely.

Postulated initiating events. A full range of events shall be postulated in order to ensure that all credible events with potential for serious consequences and significant probability have been anticipated and can be withstood by the design of the plant. The PIEs should be selected to challenge all of the plant safety functions and SSC important to safety.

The PIEs to be used in the overall safety assessment of the plant may be limited to a number of representative event sequences. These sequences shall be bounding cases and provide the basis for quantitative design limits for structures, systems and components important to safety.

Fire. Structures, systems and components important to safety shall be designed and located so as to minimize, consistent with other safety requirements, the probabilities and effects of fires and explosions caused by external or internal events.

Non-combustible or fire retardant and heat resistant materials shall be used wherever practicable throughout the plant, particularly in locations such as the containment and the control room. Design shall include fire hazard evaluation. All rooms, buildings and structures shall be classified by explosion and fire safety levels. A fire hazard analysis of the plant shall be carried out to determine the necessary rating of the fire barriers.

Fire detection and fire fighting systems shall be provided. Fire fighting systems shall be automatically initiated where necessary, and systems shall be designed and located so as to ensure that their rupture or spurious /inadvertent operation does not significantly impair the capability of safety related SSC, nor simultaneously affect redundant safety systems (which would render ineffective the measures taken to comply with the single failure criterion).

The capability for shutdown, residual heat removal, confinement of radioactive material and plant monitoring from a location outside the main control room shall be maintained.

These requirements shall be met by suitable incorporation of redundant parts, diverse systems, physical separation and design for fail-safe operation.

Internal and external hazards. The potential for internal hazards such as flooding, missile generation, pipe whip, jet impact, or release of fluid from failed systems or from other installations on the site shall be taken into account in the design of the plant. Corresponding preventive and mitigating measures shall be provided to ensure that safety is not compromised. Since certain external events may initiate internal fires or floods, the interaction of external and internal events shall also be considered in the design.

If two fluid systems that are operating at different pressures are interconnected, either the systems shall both be designed to withstand the higher pressure, or provision shall be made to preclude the design pressure of the system operating at the lower pressure from being exceeded, on the assumption that a single failure occurs.

The design shall include due consideration of those natural and human induced external events (i.e. events of origin external to the plant) that have been identified in the site evaluation process. Natural external events shall be addressed, including meteorological, hydrological, geological and seismic events. Human induced external events arising from nearby industries and transport routes shall be addressed. In the short term, the safety of the plant shall not be permitted to be dependent on the availability of off-site services such as electricity supply and fire fighting services. The design shall take due account of site specific conditions to determine the maximum delay time by which off-site services need to be available.

Site related design considerations. In the design of a nuclear power plant, interactions between the plant and the environment, including meteorology, hydrology, geology and seismology, shall be taken into account. The seismic design of the plant shall provide for a sufficient safety margin to protect against seismic events and to avoid cliff edge effects.

The availability of off-site services such as the electricity supply, water supply, and fire-fighting services, shall also be taken into account. Nuclear power plants to be sited in volcanic areas shall be assessed with a view to identifying special design features which may be necessary as a result of the characteristics of the site.

3.4.2. Response to PIE

The plant design shall be such that its sensitivity to PIEs is minimized. The expected plant response to any PIE shall be that:

1. a PIE produces no significant safety related effect or produces only a change in the plant towards a safe condition by inherent characteristics; or
2. following a PIE, the plant is rendered safe by passive safety features or by the action of safety systems that are continuously operating; or
3. following a PIE, the plant is rendered safe by the action of safety systems that need to be brought into service in response to the PIE; or
4. following a PIE, the plant is rendered safe by specified procedural actions.

Where prompt and reliable action is necessary in response to a PIE, the necessary actions of safety systems shall be initiated automatically. Where prompt action is not necessary, manual initiation of systems or other operator actions are permitted, provided that the need for the action would be revealed in sufficient time and that adequate procedures are defined to ensure the reliability of such actions.

Operator actions necessary to diagnose the state of the plant and to put it into a stable long term shutdown condition shall be facilitated by instrumentation to monitor plant status and controls for manual operation of equipment.

Equipment necessary in manual response and recovery processes shall be placed at the most suitable location to ensure its ready availability at the time of need and to allow human access in the anticipated environmental conditions.

Common cause failures. The potential for common cause failures of safety-related systems and components shall be considered to determine where the principles of diversity, redundancy and independence should be applied to achieve the necessary reliability.

Single failure criterion. The single failure criterion shall be applied to each safety-related system incorporated in the plant design. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Single failures shall include spurious actions resulting from the design basis event. Single failures shall be considered to occur concurrently with all identifiable but non-detectible failures.

To test compliance with the single failure criterion, the safety system shall be analyzed in the following way. A single failure (and all its consequential failures and identifiable but non-detectable failures) shall be assumed in turn to occur for each element of the safety system until all possible failures have been analyzed. The analyses of each pertinent safety system shall be conducted in turn until all safety systems and all failures have been considered. In the single failure analysis, no more than one random failure is assumed to occur. Spurious action shall be considered as one mode of failure when applying the criterion to a safety system.

In the conduct of a single failure analysis, any potentially harmful consequences of the PIE for the safety system shall be assumed to occur. In addition, the worst permissible configuration of safety systems performing the safety function is assumed, accounting for maintenance, testing, inspection and repair, and allowable equipment outage times.

In the single failure analysis, it may not be necessary to assume the failure of a passive component designed, manufactured, inspected and maintained in service to extremely high quality, provided that it remains unaffected by the PIE. However, when it is assumed that a passive component does not fail, such an analytical approach shall be justified, with account taken of the loads and environmental conditions, as well as the total period of time after the initiating event for which functioning of the component is necessary.

Fail-safe design. The principle of fail-safe design shall be considered and incorporated into the design of systems and components important to safety for the plant as appropriate.

Equipment outages. The design shall ensure, by measures such as increased redundancy, that reasonable on-line maintenance and testing of systems important to safety can be

conducted without the necessity to shutdown the plant. Equipment outages, including unavailability of systems or components due to failure, shall be taken into account, and the impact of the anticipated maintenance, test and repair work on the reliability of each individual safety system shall be included in this consideration in order to ensure that the safety function can still be achieved with the necessary reliability. The time allowed for equipment outages and the actions to be taken shall be analyzed and defined for each case before the start of plant operation and included in the plant operating instructions.

3.4.3. Severe accident measures

Measures shall be taken for protection of confining safety systems from damage during severe accidents. Measures shall be taken to ensure that the radiological consequences of severe accidents are mitigated. Such measures include: engineered safety features; accident management procedures; and possibly off-site intervention measures. The design of severe accident features shall consider the principle that plant states that could result in high radiation doses or radioactive releases are of very low probability of occurrence, and plant states with significant probability of occurrence have only minor radiological consequences.

Consideration shall be given to the plant's full design capabilities, including the use of safety and non-safety systems beyond their originally intended functions and anticipated operational states; and the use of temporary systems. It shall be shown that such systems are able to function in the environmental conditions to be expected.

3.4.4. Emergency preparedness

Emergency plans for protection of plant personnel and the public in case of nuclear and radiological emergencies, including severe accidents shall be developed by the operating organization in coordination with off-site authorities. The plans shall be tested periodically to demonstrate their credibility.

The operating organization shall provide emergency management facilities and equipment to monitor the accident progression and manage the response. An on-site emergency control center, separated from the plant control room, shall be provided. Information about important plant parameters and radiological conditions in the plant and its immediate surroundings should be available there. The emergency control center should provide means of communication with the control room, the supplementary control room and other important points in the plant, and with the on-site and off-site emergency response organizations. Appropriate measures shall be taken to protect the occupants of the main control room, the supplementary control room and emergency control center against hazards resulting from nuclear and radiological emergencies.

4. SAFETY ASSESSMENT

In the design of a nuclear power plant, a comprehensive safety assessment shall be carried out to identify all sources of exposure and to evaluate radiation doses that could be received by workers at the NPP and the public.

The assessment shall include both a deterministic analysis of design basis and beyond design base accidents and a probabilistic assessment of severe accidents.

The safety assessment shall examine the following categories of initiating events:

- All planned normal operational modes of the nuclear power plant;
- Nuclear power plant performance in anticipated operational occurrences;
- Design basis accidents;
- Beyond design base accidents;
- Event sequences that may lead to a severe accident.

On the basis of this assessment, the robustness of the engineering design in withstanding postulated initiating events and accidents shall be established, the effectiveness of the safety systems and safety

related systems and components or systems shall be demonstrated, and requirements for emergency response shall be established.

The safety assessment shall be part of the design process, with iteration between the design and confirmatory analytical activities, and increasing in the scope and level of detail as the design program progresses.

The operating organization shall ensure that an independent verification of the safety assessment is performed by individuals or groups separate from those carrying out the design, before the design is submitted to the regulatory body.

On the basis of this analysis, the design basis for systems and components important to safety shall be established and confirmed. It shall also be demonstrated that the plant as designed is capable of meeting prescribed limits for radioactive releases and for potential radiation doses for each category of plant states, and that defense in depth has been affected.

The computer programs, analytical methods and plant models used in the safety assessment shall be verified and validated, and adequate consideration shall be given to uncertainties.

4.1. Deterministic safety Analysis

The plant states shall be identified and grouped into a limited number of categories according to their probability of occurrence. The categories shall cover normal operation (1), anticipated operational occurrences (2), design basis accidents (3), BDBA (4) and severe accidents (5). Acceptance criteria shall be assigned to each category such that frequent postulated initiating events (PIE) shall have only minor or no radiological consequences, and that events that may result in severe consequences shall be of very low probability.

Internal events. An analysis of the PIEs shall be made to establish internal events which may affect the safety of the plant. These events may include equipment failures or abnormal operation.

External events. The design basis natural and human induced external events shall be determined for the proposed combination of site and plant. All those events with which significant radiological risk may be associated shall be considered. A combination of deterministic and probabilistic methods shall be used to select a subset of external events that the plant is designed to withstand, and from which the design bases are determined.

Natural external events which shall be considered include those which have been identified in site characterization, such as earthquakes, floods, high winds, and extreme meteorological conditions. Human induced external events that shall be considered include those that have been identified in site characterization and for which design bases have been derived. The list of these events shall be reassessed for completeness at an early stage of the design process.

Station blackout. The external events shall include station blackout (SBO). The ability to withstand a station blackout event shall be included in the facility design. The facility shall be able to withstand for a specified duration and recover from a station blackout. The specified station blackout duration shall be based on the following factors:

- The redundancy of the onsite emergency ac power sources;
- The reliability of the onsite emergency ac power sources;
- The expected frequency of loss of offsite power; and
- The probable time needed to restore offsite power.

The reactor core and associated coolant, control, and protection systems, including station batteries and any other necessary support systems, must provide sufficient capacity and capability to ensure that the core is cooled and appropriate containment integrity is maintained in the event of a station blackout for the specified duration. The capability for coping with a station blackout of specified duration shall be determined by an appropriate coping analysis.

Combinations of events. Where combinations of randomly occurring events could credibly lead to anticipated operational occurrences or accident conditions, they shall be considered in the analysis. Certain events may be the consequences of other events, such as a flood following an earthquake. Such consequential effects shall be considered to be part of the original PIE.
Design basis accidents. A set of design basis accidents shall be derived from the listing of PIEs for the purpose of setting the boundary conditions according to which the structures, systems and components important to safety shall be designed.

Deterministic safety analysis shall include:

- confirmation of operational limits and conditions compliance with the design assumptions for normal operation;
- identification of the postulated initiating events characteristics, including those specific for the selected site;
- analysis and assessment of postulated initiating events' progression;
- comparison of analysis results of postulated initiating events' against the radiological acceptance criteria and the other design limits;
- confirmation of the design basis;
- substantiation of plant capabilities to manage all anticipated operational occurrences and design basis accidents through a combination of safety systems' automatic actions and required actions of the operating personnel.

Conservative approach must be applied for deterministic analyses.

4.2. PSA

Probabilistic safety analysis shall be carried out with the objective to:

- give confidence that the design will comply with the general safety objectives;
- demonstrate that a balanced design has been achieved; that no feature or PIE makes a disproportionately large or significantly uncertain contribution to the overall risk; and that the first two levels of defense bear the primary burden of ensuring nuclear safety;
- provide confidence that small deviations in plant parameters that could give rise to severely abnormal plant behavior ('cliff edge effects') will be prevented;
- provide assessments of the probabilities of occurrence of severe core damage states and assessments of the risks of major off-site releases necessitating a short term off-site response, particularly for releases associated with early containment failure;
- provide assessments of the probabilities of occurrence and the consequences of external hazards, in particular those unique to the plant site;
- identify systems for which design improvements or procedural modifications could reduce the probabilities of severe accidents or mitigate their consequences;
- assess the adequacy of plant emergency procedures; and
- verify compliance with probabilistic targets.

The probabilistic safety analyses shall include:

- all modes of operation, all postulated initiating events, including internal fire and flooding, severe weather conditions and seismic events;
- all possible important dependencies (functional dependencies, area dependencies and other interactions and impacts, leading to common cause failures);
- uncertainty analysis or sensitivity analysis of the results;
- realistic modeling of plant response, taking into account operator actions in accordance with operational and accident instructions;
- human error analyses, taking into account the factors which can influence the performance of operating personnel in all operational states and accident conditions.

Probabilistic safety analyses shall be performed according to state-of-the-art methodology, documented and maintained according to the quality management program of the operating organization.

Probabilistic safety analyses shall be used to support the deterministic assessments in the decision making for plant design and operation, for assessment of necessary changes of SSCs, operational limits and conditions, operating and emergency operating procedures and training programs of the operating personnel.

4.3. Severe Accidents Analysis

Severe accidents are low probability accident conditions, which lead to significant core degradation and jeopardize the integrity of barriers to the release of radioactive material.

Consideration shall be given to these severe accident sequences, using a combination of engineering judgment and probabilistic methods, to determine those sequences for which reasonably practicable preventive or mitigating measures can be identified.

Acceptable measures need not involve the application of conservative engineering practices, but rather should be based upon realistic or best estimate assumptions, methods and analytical criteria. On the basis of operational experience, relevant safety analysis and results from safety research, the analysis of severe accidents shall take into account the following:

- Sequences that may lead to a severe accident shall be identified using a combination of probabilistic methods, deterministic methods and engineering judgment.
- These event sequences shall then be reviewed against a set of criteria aimed at determining which severe accidents shall be addressed in the design.
- Potential design or procedural changes that could either reduce the likelihood of these selected events, or mitigate their consequences should these selected events occur, shall be evaluated and shall be implemented if reasonably practicable.

5. SAFETY CLASSIFICATION OF EQUIPMENT

All safety-related SSC, including software for instrumentation and control (I&C), shall be identified and classified on the basis of their function and significance to safety.

They shall be designed, constructed and maintained such that their quality and reliability is commensurate with this classification.

The method for classifying the safety significance of a structure, system or component shall primarily be based on deterministic methods, complemented by probabilistic methods and engineering judgment, with due account taken of factors such as:

- the safety function(s) to be performed by the item;
- the consequences of failure to perform a safety function;
- the frequency with which the item will be called upon to perform a safety function;
- the time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function.

Appropriately designed interfaces shall be provided between SSC of different classes to ensure that any failure in a system classified in a lower class will not propagate to a system classified in a higher class.

Equipment that performs multiple functions shall be classified in a safety class that is consistent with the most important function performed by the equipment.

If a SSC has been classified differently based on deterministic and probabilistic methods, the SSC shall be placed in the higher of the two classes.

Components or structures which form the interface between components belonging to different classes shall be assigned to the highest class.

Safety classes to which components belong and special rule requirements applied to them shall be indicated in the documents for design, manufacturing and delivery of SSC.

6. SAFETY REQUIREMENTS FOR SYSTEMS, STRUCTURES AND COMPONENTS

Design rules and limits. Engineering design rules for SSC shall comply with accepted national standard engineering practices, or standards and practices used internationally or established in another country and whose use is applicable and also accepted by the State Committee on Nuclear Safety Regulation.

Protective safety systems. The design shall provide for protective safety systems assuring reliable emergency shut-down and maintaining safe conditions of the plant in any normal operating modes and in case of design-basis accidents. Emergency shut-down systems shall have sufficient capacity and speed of response for normal operation and design-basis accidents. Emergency shut-down shall be assured regardless of whether electric power is available or lost. Protective safety systems shall include systems for emergency heat removal from the reactor system and containment and ensure their required capacity. The design shall justify the permissible number of protective safety system activation cycles over the plant life time (including spurious activations) in terms of effect on component service life.

The protective safety systems shall be designed for high functional reliability and periodic testability commensurate with their safety function(s). Redundancy and independence designed into the protective systems shall be sufficient at least to ensure that:

1. no single failure results in loss of protection function; and
2. the removal from service of any component or channel does not result in loss of the necessary minimum redundancy.

The protective safety systems shall be designed to ensure that the effects of normal operation, anticipated operational occurrences and design basis accidents on redundant channels do not result in loss of function; unless such a loss shall be demonstrated to be acceptable on some other basis.

All reactor designs shall include safety features to mitigate the consequences of an anticipated transient without a reactor scram (ATWS).

Supporting safety systems. Auxiliary services that support equipment forming part of protective safety systems or other systems important to safety shall be classified according to the significance of the systems they support. Their reliability, redundancy, diversity and independence and the provision of features for isolation and for testing of functional capability shall be commensurate with the reliability of the system that is supported.

Auxiliary services necessary to maintain the plant in a safe state may include the supply of electricity, cooling water and compressed air or other gases, and means of lubrication.

Systems shall be provided to transfer residual heat from SSC important to safety to an ultimate heat sink. This function shall be carried out at very high levels of reliability in all operational states and in design basis accidents. All such systems shall be designed in accordance with the importance of their contribution to the function of heat transfer.

The reliability of the systems shall be achieved by the use of proven components, redundancy, diversity, physical separation, interconnection and isolation.

Design basis natural phenomena and human induced events shall be taken into account in the design of the systems; and in the possible choice of diversity in the ultimate heat sinks; and in the storage systems from which fluids for heat transfer are supplied.

Adequate consideration shall be given to extending the capability to transfer residual heat from the core to an ultimate heat sink so as to ensure that, in the event of a severe accident, acceptable temperatures can be maintained in structures, systems and components important to the safety function of confinement of radioactive materials.

Equipment qualification. A qualification program shall be adopted to confirm that SSC important to safety can perform their functions throughout their design operational lives while being subjected to

the environmental conditions (of vibration, temperature, pressure, jet impingement, electromagnetic interference, irradiation, humidity or any likely combination thereof) prevailing at the time of need.

The environmental conditions to be considered shall include the variations expected in normal operation, anticipated operational occurrences and design basis accidents.

Consideration shall be given to aging effects caused by environmental factors (such as vibration, irradiation and extreme temperature) over the expected lifetime of the equipment. Where the equipment is subject to external natural events and is needed to perform a safety function in or following such an event, the qualification program shall replicate as far as practicable the conditions imposed on the equipment, either by test or by analysis or by a combination of both.

In addition, any unusual environmental conditions that can reasonably be anticipated and that could arise from specific operational states, such as in periodic testing of the containment leak rate, shall be included in the qualification program. To the extent possible, equipment (such as certain instrumentation) that must operate during a severe accident should be shown, with reasonable confidence, to be capable of achieving the design intent.

Protection from CCF. The NPP design shall consider and justify measures for prevention or protection of systems and components from common-cause failures. The potential for common cause failures of systems and components important to safety shall be considered to determine where the principles of diversity, redundancy and independence should be applied to achieve the necessary reliability.

Human engineering. The design shall be 'operator friendly' and shall be aimed at limiting the effects of human errors. Attention shall be paid to plant layout and procedures (administrative, operational and emergency), including maintenance and inspection, in order to facilitate the interface between the operating personnel and the plant. The working areas and working environment of the site personnel shall be designed according to ergonomic principles.

Consideration of human factors and the human–machine interface shall be included at an early stage and throughout the entire design process, to ensure an appropriate and clear distinction of functions between operating personnel and the automatic systems is identified. The human–machine interface shall be designed to provide the operators with comprehensive but easily manageable information, compatible with the necessary decision and action times. Similar provisions shall be made for the supplementary control room.

Verification and validation of aspects of human factors shall be included at appropriate stages to confirm that the design adequately accommodates all necessary operator actions.

The operator shall be considered to have dual roles: that of a systems manager, including accident management, and that of an equipment operator. In the systems manager role, the operator shall be provided with information that permits the following:

1. the ready assessment of the general state of the plant, whether in normal operation, during an anticipated operational occurrence or in an accident condition, and confirmation that the designed automatic safety actions are being carried out; and
2. the determination of the appropriate operator initiated safety actions to be taken.

As equipment operator, the operator shall be provided with sufficient information on parameters associated with individual plant systems and equipment to confirm that the necessary safety actions can be initiated safely.

Operator actions necessary for safe operation shall account for the time available for action, the physical environment to be expected and the psychological demands on the operator. The need for action on a short time-scale shall be kept to a minimum.
The design shall include means for prevention of single operator errors or mitigation of their consequences, including those during maintenance.

Avoiding multiple use of systems. Structures, systems and components important to safety shall generally not be shared between two or more reactors in nuclear power plants. Multi-purpose use of safety systems and components shall be specially justified, and it shall be demonstrated that combined functions will not result in violation of safety requirements and reduction of required reliability of systems (components) performing safety functions.

In the event of a severe accident involving one of the reactors, an orderly shutdown, cooling down and removal of residual heat shall be achievable for the other reactor(s).

System interaction. If there is a significant probability that systems important to safety will operate simultaneously, their possible interaction shall be evaluated. In the analysis, account shall be taken not only of physical interconnections, but also of environmental and other possible effects of one system's operation, abnormal operation or failure on the other.

Design to enable ISI/IST. SSC important to safety shall be designed to be calibrated, tested, maintained, repaired or replaced, inspected and monitored with respect to their functional capability over the lifetime of the plant to demonstrate that reliability targets are being met. The plant layout shall be such that access is provided for in-service inspection and in-service testing without undue exposure of the site personnel to radiation.

For safety-significant systems and components a direct and complete inspection shall be performed during the plant commissioning for compliance with design characteristics. Additionally, such inspections shall be performed periodically and after maintenance of these systems over the whole plant life-time period:

1. the design shall provide for possibility of diagnostics (tests) of safety systems and components belonging to classes 1 and 2, and possibility for their testing in conditions simulating an emergency situation to a maximum extent possible; and
2. frequency and allowed maintenance and testing time shall be justified in the design or approved according to a special procedure.

Design to enable decommissioning. The design shall incorporation features that will facilitate the decommissioning and dismantling of the plant. In particular, account shall be taken of:

- the choice of materials, such that eventual quantities of radioactive waste are minimized and decontamination is facilitated;
- the access capabilities that may be necessary; and
- the facilities necessary for storing radioactive waste generated.

Physical Plant Security and Safeguards. The licensee shall provide physical protection against radiological sabotage and against theft of special nuclear material. The licensee shall establish and maintain physical security in accordance with security plans approved by the regulatory agency. The scope of the program shall include:

- protection against radiological sabotage, including determined violent external assault, attack by stealth, or deceptive actions;
- protection against theft or diversion of strategic special nuclear material;
- protection of spent nuclear fuel and high-level radioactive waste; and
- protection of physical security information.

The physical protection system shall include provisions to:

- prevent unauthorized access of persons, vehicles and materials into material access areas and vital areas;
- permit only authorized activities and conditions within protected areas, material access areas, and vital areas;
- permit only authorized placement and movement of strategic special nuclear material within material access areas;
- permit removal of only authorized and confirmed forms and amounts of strategic special nuclear material from material access areas;
- limit authorized access and assure detection of and response to unauthorized penetrations of the protected area, and
- limit location of vital equipment only within vital areas, and storage of strategic special nuclear material only in a material access area.

The plant security system shall include provisions for:

- a security organization, including guards;
- access control subsystems and procedures;
- detection, surveillance and alarm subsystems and procedures, and
- contingency and response plans and procedures for responding to security emergencies.

Design for ease of egress in emergency. The nuclear power plant shall be provided with a sufficient number of safe escape routes, clearly and durably marked, with reliable emergency lighting, ventilation and other building services essential to the safe use of these routes. The escape routes shall meet the relevant international requirements for radiation zoning and fire protection and the relevant national requirements for industrial safety and plant security.

Alarm systems and means of communication shall be provided so that all persons present in the plant and on the site can be warned and instructed, even under accident conditions.

The availability of means of communication necessary for safety, within the nuclear power plant, in the immediate vicinity and to off-site agencies, as stipulated in the emergency plan, shall be ensured at all times. This requirement shall be taken into account in the design and the diversity of the methods of communication selected.

Preference for passive systems. Safety systems shall preferably rely on passive devices and the fail-safe design principle (safe geometry, safe parameters, self-control, temperature difference and natural processes).

Accounting for external effects in design. The plant design shall consider site-specific man-induced and naturally caused external events, as well as geotechnical characteristics of foundation materials. The design basis shall use site-specific parameter values to characterize external hazards. Man-induced external hazards with probability of occurrence below 10^{-7} events per year may be excluded from the design basis.

The assessment and design of protection from natural and man-induced external events shall consider loads due to the external hazards in combination with normal operating and transient loads.

Regardless of low levels of external impact intensity assumed in design basis, the design shall have the following provisions:

- seismic resistance to horizontal peak ground acceleration more than 0.4g. Seismic hazard at the site shall be defined on a basis of earthquake sources, determined site and site-specific response spectra, performance-based ground motion response spectra.
- the wind used in the design shall be the most severe wind that has been historically reported for the site and surrounding area with sufficient margin for the limited accuracy, quantity, and period of time in which historical data have been accumulated.)
- resistance to loads produced by explosive shock waves of not less than 10 kPa;
- resistance of safety-related buildings and structures to external fires – not less than 2.5 hours under an external thermal environment of up to 300^{o}C;
- spatial and physical separation of safety systems and their trains;
- resistance of protective structures for confining systems to impact loads from a commercial airliner during normal landing. Design shall include section as follows:
    1. missile effects on plant structures from aircraft impacts;
    2. fire effects from aircraft fires;
    3. requirements to protect plant SSCs important to safety from aircraft crashes.

SSC included in seismic Category I shall perform their safety functions during and after a seismic event, assuming ground motion equivalent to that of a safe shutdown earthquake (SSE).

Plant personnel shall be provided with protection from external factors. External loads on personnel shall be maintained within limits which do not degrade reliability (or welfare) of personnel.

The NPP design shall provide external event warning systems; recording of natural and man-induced external impacts; to determine if the maximum calculated level established by design basis is exceeded.

6.1. Reactor Core and Associated Features

Reactor core and associated reactor coolant system, reactor control and protection safety systems shall be designed with appropriate safety margins to ensure that the specified acceptable design limits for fuel damage are not exceeded during all operational states and design basis accidents with account taken of:

- design operating modes and their passing;
- thermal, mechanical and irradiation degradation of the core components;
- physical-chemical interaction of core materials;
- limiting values of thermal hydraulic parameters;
- vibrations and thermal cycles, material fatigue and aging;
- impact of coolant additives and radioactive fission products on the corrosion of fuel cladding;
- irradiation and other impacts that deteriorate mechanical characteristics of core materials and fuel cladding integrity.

The design of the reactor core shall specify the limits for damage of fuel elements (in terms of amount and degree) and the associated coolant radioactivity according to reference isotopes.

To ensure safe shutdown of the reactor, to maintain the reactor subcritical and to ensure adequate core cooling, the reactor core and associated internal components located within the reactor vessel shall be designed and mounted in such a way as to withstand the static and dynamic loads expected in all operational states and external events considered in the design.

Reactor core and its elements that affect reactivity shall be designed in a way that any reactivity change caused by the control rods as well as reactivity effects shall not lead to fuel damage that exceeds the specified design limits and shall not cause any damage to reactor coolant pressure boundary during all operational states and design basis accidents.

Design shall be such that in all design basis accidents with fast insertion of positive reactivity, specific energy threshold for fuel damage is not exceeded at any moment of the fuel cycle and fuel melting is excluded by insertion of the control rods. With respect to beyond design basis accidents, conditions for possible fuel melting or exceeding the specific energy threshold causing fuel damage shall be specified.

For all design basis accidents and for beyond design basis accidents changes in core geometry shall be limited thus ensuring conditions for long-term fuel cooling.

The combined reactivity coefficients of coolant density, of coolant-moderator and fuel temperature, and of reactor power, shall be negative within the whole range of the reactor coolant system parameters for all operational states and design basis accidents.

Design shall ensure minimization of possibilities for re-criticality and reactivity excursions following postulated initiating events.

Design of the reactor core shall reduce demands on the system for control of the neutron flux (distribution, levels and stability within specified limits) in all operational states.

Reactor core and associated coolant, control and protection systems shall be designed to enable adequate inspection and testing throughout the service lifetime of the plant.

The characteristics of nuclear fuel, the reactor structures and of the reactor coolant system components (including the coolant clean up system) shall prevent re-criticality in severe accidents, considering the operation of the other systems.

Fuel elements and assemblies, taking into account the uncertainties in data, calculations and fabrication, shall be designed to withstand irradiation and reactor core conditions in combination with all degradation processes that can occur in all operation states, such as:

- differential expansion and deformation;
- external pressure of the coolant;
- additional internal pressure due to fission products in the fuel element;
- irradiation of fuel and other materials in the fuel assembly;
- changes in pressures and temperatures resulting from changes in power;
- chemical effects;
- static and dynamic loads, including flow induced vibrations and mechanical vibrations;
- changes in heat transfer that may be a result of distortions or chemical effects.

The reactor core and associated coolant, control and protection systems shall be designed with safety margins to ensure that the specified acceptable fuel design limits are not exceeded.

6.2. Reactor Coolant System

The design of reactor coolant system shall include passive pressure relieving devices (safety valves) with sufficient relieving capacity to prevent exceeding the reactor coolant design pressure during all conditions of normal operation, abnormal operational occurrences and postulated accidents.

Components, pipelines and supporting structures of the reactor coolant system shall withstand all anticipated static and dynamic loads and temperature effects on the components during all postulated initiating events and external events such as seismic events.

Materials to be used for fabrication of the components of the reactor coolant system shall be selected so as to minimize the probability of crack propagation and neutron embrittlement, with account taken of the expected degradation of their characteristics at the end-of lifetime under the effects of erosion, creep, fatigue and chemical environment.

Reactor pressure vessel shall be designed and constructed to be of the highest quality with respect to material selection, design standards, capability of inspection and fabrication.

Design of the components contained inside the reactor coolant pressure boundary shall be such as to minimize the likelihood of failure and associated consequential damage to other items of the primary coolant system in all operational states and in design basis accidents.

Components of the reactor coolant pressure boundary shall be designed, manufactured and situated in a way allowing periodical inspections and tests to be carried out, throughout the service lifetime of the plant. Implementation of a material surveillance program for the reactor coolant pressure boundary shall monitor the effects on structural materials of various factors such as irradiation, stress corrosion cracking, embrittlement, and ageing and particularly in locations of high irradiation, and others.

Provisions shall be made in the design to regulate coolant inventory and pressure with adequate capacity for all operational states.

Design shall provide for systems to cleanup reactor coolant from radioactive substances, including activated corrosion products and fission products. Capacity of the necessary systems shall be based on the fuel design limits on permissible leakage with a conservative margin to ensure that the coolant activity is as low as reasonably practical and that sub-criticality is assured following anticipated operational occurrences and during accidents.

The reactor coolant system shall be designed to prevent the initiation of flaws (cracks) at its pressure boundary. If initiation were to occur, the design shall be such that flaws will propagate in a metallurgical regime characterized by high resistance to unstable fracture and rapid crack

propagation. Designs and plant states in which components of the reactor coolant pressure boundary could exhibit brittle behavior shall be avoided.

The design of components inside the reactor coolant pressure boundary, such as pump impellers and valve parts, shall minimize the likelihood of failure and consequential damage to other items of the primary coolant system in all operational states and in design basis accidents, with due allowance for deterioration that may occur in service.

6.3. Removal of Residual Heat

Plant design shall provide for redundant safety-related systems to remove, to an ultimate heat sink, the residual heat from the core and from SSCs important to safety, in all operational states and design basis accidents. All systems that contribute to the heat transfer (by conveying heat, by providing power or by supplying fluids to the heat transport systems) shall be designed and classified according to their safety significance. Systems interfacing directly with the reactor coolant system shall be Class 2. The portion of the RHR system that is not isolable from the RCS shall be classified as Class 1. Supporting safety-related systems such as component cooling water and service water shall be classified as Class 3.

Reliability of the systems shall be achieved by the use of proven components, redundancy, diversity, physical separation and isolation.

Natural phenomena and human induced events specific to the NPP site shall be taken into account in the design of the systems and in the possible choice of diversity in the ultimate heat sinks.

Adequate consideration shall be given to the residual heat removal from the reactor core and cooling of the localization system components in case of a severe accident.

6.4. Emergency Core Cooling

Core cooling shall be provided in the event of a loss of coolant accident so as to minimize fuel damage and limit the escape of fission products from the fuel. The cooling provided shall ensure that:

1. limiting parameters for cladding or fuel integrity (such as temperature) will not exceed acceptable values for design basis accidents;
2. possible chemical reactions are limited to an allowable level;
3. the alterations in the fuel and internal structural alterations will not significantly reduce the effectiveness of the means of emergency core cooling, and
4. the cooling of the core will be ensured for a sufficient time

Adequate consideration shall be given to extending the capability to remove heat from the core following a severe accident.

6.5. Control of the Technological Processes

NPP unit shall be provided with the following means to control and monitor the systems for normal operation and the safety systems:

1. main control room (MCR);
2. supplementary control room (SCR);
3. control systems for systems required during plant shutdown, refueling and normal operation;
4. control systems for safety-related engineered safety features required for accident mitigation;
5. independent means for information collection and storage.

The MCR shall provide possibilities for undertaking measures to maintain the plant in a safe state or to recover such state if needed in all operational states and design basis accidents.

Design shall be sufficient to maintain the MCR personnel health and availability, as well as proper functioning of the MCR, in all operational states and internal and external events.

MCR design shall provide for:

1. instrumentation to control the fission process, in all core states, and conditions in normal operation, including in subcritical state during refuelling;

2. position indicators of the reactivity control devices, automatic control of soluble neutron absorber concentration, and status indicators of all means for reactivity control;
3. a system for information support to the operators;
4. a safety parameter display system of the reactor installation.

Control signals of technological systems and components important to safety, formed by the automatic control system or by the MCR remote control switches, shall be automatically registered.

Any possibility of parallel actuation of control components, from the MCR and the SCR, shall be eliminated by technical means. Appropriate measures shall be taken to eliminate any possibility for failure of the control circuits of both MCR and SCR due to a common cause, in all postulated initiating events.

SCR shall be designed to protect the personnel in all conditions resulting from internal and external events and design basis accidents.

Control systems for normal operation shall control and regulate the technological processes, in all operational states, in conformity with the design specified indicators for quality, reliability and metrological characteristics, and shall encompass:

1. means for collecting, treating, documenting and storing of information, which to be sufficient for timely and unambiguous identification of the initiating events for anticipated operational occurrences and accidents, their progression, factual algorithms of operation of the safety systems and the components, which failures are initiating events for design basis and beyond design basis accidents, deviations from the design algorithms and personnel actions;
2. means for automatic control of reactor coolant activity, liquid and gaseous effluents to the environment, and radiation monitoring of plant compartments, and radiation protection and monitored areas, in all operational states and design basis accidents;
3. means for automatic control of the conditions for safe storing of nuclear fuel and radioactive waste, and for notification in case these conditions are violated;
4. means and methods for identification of the locations and quantities of coolant leakages;
5. means for reliable group and individual communications between the MCR, SCR and field operators.

Control systems for normal operation shall ensure the most favorable conditions to the operating personnel to take the correct decisions for plant management.

In the design of computer based control systems for normal operation:

1. special standards and proven practices shall be used in development and verification of the hardware, and especially of the software;
2. development and verification process shall be conducted in compliance with a quality assurance program;
3. level of reliability assumed in the safety analysis shall include a specified conservatism to compensate for the inherent complexity of the technology.

Control safety systems shall be designed to:

1. initiate automatically the operation of appropriate systems, including systems for reactor shutdown, in order to ensure that specified design limits are not exceeded as a result of anticipated operational occurrences;
2. detect the symptoms for design basis accidents and automatically actuate other safety systems necessary to limit the consequences within the design basis;
3. lock the switch-off capability of the operating personnel for at least 30 minutes after an automatic actuation;
4. be capable of overriding unsafe actions of the control systems for normal operation.

Design shall provide possibilities for manual remote actuation of the safety systems – and for the isolation of components at their location. A failure in automatic actuation circuits shall not impede the remote manual actuation and the implementation of the safety functions.

Design of control safety systems shall provide for: continuous automatic diagnostics of the systems operability; periodic testing from MCR and SCR of system channels; and diagnosis of the technological components,

Instrumentation shall be provided to monitor plant variables and the status of essential equipment over the ranges for normal operation, anticipated operational occurrences, design basis accidents and severe accidents; to allow projections of the locations and quantities of radioactive materials that could escape from the plant; and to permit classifying events for the purposes of emergency response. Instrumentation and recording equipment shall be adequate for determining plant status in a severe accident and for making accident management decisions.

6.6. Containment System

Reactor installation design shall include containment safety systems to ensure fulfillment of the established criteria for radioactive releases to the environment. Containment safety systems shall perform their functions in all postulated initiating events and mitigate the consequences of beyond-design basis accidents including severe accidents.

In establishment of containment functions, provisions shall include a leak tight structure, systems and means for control of containment parameters, for containment structure isolation, and for reducing the concentration of fission products, hydrogen and other substances that could be released in the containment atmosphere during and after design basis and severe accidents.

The containment structure and its components, including hermetic access doors, penetrations and isolation devices, shall be designed with sufficient safety margins on the basis of potential internal overpressure, underpressure and temperatures, dynamic effects such as missiles impact, reaction forces, and the effects of other potential energy sources anticipated to arise as a result of design basis accidents.

In calculating the necessary strength of the containment structure and its components, natural phenomena and human induced events shall be taken into consideration, as well as a combination of the effects of reactor coolant system break with maximum size and safe shutdown earthquake.

The containment structure and its components shall be designed and constructed to permit structural integrity testing during commissioning and performing of periodic leaktightness tests over plant lifetime. The design shall specify test requirements and the respective methods and means. Components located inside the containment shall retain their functional capability after the tests have been conducted.

Number of penetrations through the containment structure shall be kept to a practical minimum. All penetrations shall meet containment structure design requirements with account of possible mechanical, thermal, and chemical effects.

Elastic components of containment penetrations shall be designed to allow individual leak testing, independent of the containment leak rate detection (integral test).

To prevent radioactive releases outside the containment in case of a design basis accident, any containment penetrating line (part of the reactor coolant pressure boundary or directly connected to containment atmosphere) shall be reliably isolated by at least two isolation valves having independent automatic control, arranged in series and located outside and inside the containment structure as close to the containment structure as practicable.

Any containment penetrating line that is neither directly connected to the reactor coolant pressure boundary nor to the containment atmosphere shall be reliably isolated by at least one isolation valve outside the containment and located as close to the containment structure as practicable.

To secure personnel access to containment premises, provisions shall be made of lock and block doors as to secure at least one door in a locked position for all operational states and design basis accidents.

The design shall include arrangements to ensure capability of isolation devices to maintain their functionality in the event of a severe accident.

Containment design shall include measures and technical means to ensure sufficiently low pressure difference between the separate internal compartments so as not to challenge the integrity of

pressure bearing structure or of other systems with containment functions, taking into account the pressure and the possible effects resulting from design basis accidents.

6.7. Emergency Power Supply

An onsite electric power system and an offsite electric power system shall be provided to permit functioning of structures, systems, and components important to safety. The safety function for each system (assuming the other system is not functioning) shall be to provide sufficient capacity to assure that (1) specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded as a result of anticipated operational occurrences and (2) the core is cooled and containment integrity and other vital functions are maintained in the event of postulated accidents.

Electric power from the transmission network to the onsite electric distribution system shall be supplied by two physically independent circuits designed and located so as to minimize to the extent practical the likelihood of their simultaneous failure under operating and postulated accident and environmental conditions. A switchyard common to both circuits is acceptable. Each of these circuits shall be designed to be available in sufficient time following a loss of all onsite alternating current power supplies and the other offsite electric power circuit, to assure that specified fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded. One of these circuits shall be designed to be available within a few seconds following a loss-of-coolant accident to assure that core cooling, containment integrity, and other vital safety functions are maintained. An exception to the requirement for two circuits may be made for a reactor whose safety systems do not rely on offsite power.

The trip of a nuclear power plant can affect the grid so as to result in a loss of offsite power. Foremost among such effects is a reduction in the plant's switchyard voltage as a result of the loss of the reactive power. Less likely results of the trip of a nuclear plant are grid instability, potential grid collapse, and subsequent loss of offsite power due to the loss of the real and/or reactive power support supplied to the grid from the plant's generator. To mitigate these events provisions shall be included to minimize the probability of losing electric power from any of the remaining supplies as a result of, or coincident with, the loss of power generated by the nuclear power unit, the loss of power from the transmission network, or the loss of power from the onsite electric power supplies. The offsite power circuits shall be designed to be available following a trip of the nuclear power unit(s), to permit the functioning of system structures and components necessary to respond to the event.

Procedures should include the actions necessary to restore offsite power and use nearby power sources when offsite power is unavailable. As a minimum, the following potential causes for loss of offsite power should be considered: grid under-voltage and collapse, weather-induced power loss, and preferred power distribution system faults (including distribution system hardware, switching and maintenance errors, and lightning-induced faults) that could result in the loss of normal power to essential switchgear buses.

The onsite electric power supplies, including the batteries, and the onsite electric distribution system, shall have sufficient independence, redundancy, and testability to perform their safety functions assuming a single failure.

The design shall provide for EPS maintenance, periodic testing, tests and inspection of individual components, parts and trains during the whole service life in the process of operation and after maintenance.

The design shall specify reliability criteria, as well as quantitative reliability indicators of EPS and its individual components.

6.8. Auxiliary Systems

NPP design shall provide for supporting safety systems fulfilling auxiliary services on supply of safety systems with fluids and energy, and maintaining their operational conditions over a justified period of time in all operational states and design basis accidents.

Supporting safety systems shall be designed with adequate components' reliability and redundancy to ensure the necessary effectiveness on the assumption of a single failure, independent of the initial

state. Functional reliability of supporting systems shall be sufficient enough to meet the required reliability criteria of the respective safety system.

Systems' design shall provide possibility for testing of their functional capability and for failure indication.

Fulfillment of supporting functions shall have priority over supporting systems own protections, if this will not aggravate safety consequences. Design shall specify the non-isolable own protections of the components of the supporting safety systems.

Design shall make provisions for fire alarm and fire-extinguishing systems to prevent fire-induced common cause failures in safety systems and to automatically fulfill the specified functions.

Fire-extinguishing systems shall also be able to be manually actuated.

7. RADIOACTIVE WASTE MANAGEMENT

Radioactive waste (RAW) management systems shall be designed based on analysis and assessment of the composition and quantities of solid and liquid RAW and the gaseous radioactive substances generated in all operational states.

Systems for management of liquid and gaseous radioactive release to the environment shall be designed so that their quantities and concentrations are kept as low as reasonably achievable in all operational states and within the specified dose limits for the personnel and the population,
NPP design shall include systems for handling and temporary storage of RAW in a condition suitable for transportation and/or further treatment.

NPP design shall include facilities for temporary storage of solid RAW, equipped with remote means for manipulation.

RAW storage compartments shall be watertight and provided with systems for ventilation, decontamination, fire-alarm and fire-extinguishing.

The cleanup equipment for the gaseous radioactive substances shall provide the necessary retention factor to keep radioactive releases below the authorized limits on discharges. Filter systems shall be designed so that their efficiency can be tested, their performance and function can be regularly monitored over their service life, and filter cartridges can be replaced while maintaining the throughput of air.

8. FUEL HANDLING

SSCs for handling and storage of non-irradiated fuel shall be designed to:

1. prevent criticality by a sufficient margin, even under the most adverse states, by ensuring related physical means or processes, such as geometrically safe configurations, and characteristics of the components and medium;
2. permit appropriate fuel acceptance test, maintenance, periodic inspection and testing of components important to safety;
3. ensure control of the storage conditions;
4. minimize the possibility of damage or unauthorized access to nuclear fuel;
5. prevent fuel assembly drop during transportation;
6. prevent the inadvertent dropping of heavy objects upon the fuel assemblies.

SSCs for handling and storage of irradiated fuel shall be designed in compliance with the requirements to non-irradiated fuel and additionally shall have the following:

1. reliable systems for residual heat removal during all operational states and design basis accidents;

2. measures to prevent unacceptable handling stresses on the fuel assemblies;
3. means for safe storage of non-tight or damaged fuel assemblies or fuel elements;
4. systems for local ventilation and other means for radiation protection;
5. means for identification of the fuel assemblies.

For reactors using a water pool system for storage of irradiated fuel, the design shall provide for the following:

1. means to control the temperature, water chemistry and activity;
2. means to monitor and control the water level in the storage pool and to detect leakages;
3. measures to prevent emptying the pool as a result of syphon effect in the event of a pipe break;
4. means to control the concentration of the soluble neutron absorber.
5. mans for preventing the uncovering of fuel assemblies in the pool in the event of a pipe break (i.e. anti-siphon measures).

Capacity of the structures for storing of irradiated fuel shall be substantiated in the design considering the capability at any time to completely remove the fuel from the reactor core.

9. RADIATION PROTECTION

To ensure radiation protection, NPP design shall identify all real and potential sources of ionizing radiation and shall provide measures for ensuring the necessary technical and administrative control over their use.

The requirements with regard to the classification of zones and compartments, radiation monitoring, the individual protection means and the access control are established by a different regulation.

To keep the exposure of personnel and public as low as reasonably achievable during plant operation, the design of the reactor coolant system shall arrange for:

1. use of structural materials with minimum content of chemical elements with high activation cross-section and producing long-living radioactive corrosion products;
2. coolant purification from fission and corrosion products;
3. water chemistry control;
4. minimum length of the pipelines with a minimum number of isolation valves and connections;
5. leak-tightness testing of operating components;
6. decontamination of SSCs outer and inner surfaces;
7. prevention of uncontrolled radioactive leaks in the NPP premises.

The layout of the plant, its buildings and SSCs shall facilitate the operation, inspections, maintenance, repair and replacement of systems and components and shall limit the personnel exposure to ionising radiation.

The buildings, compartments and components, which may be contaminated with radioactive substances, shall be designed in a way that allows easy decontamination by chemical or mechanical means.

The personnel access to compartments of high dose rate or high contamination level shall be controlled by means of locking devices with interlocks and indication for actuation and unavailability.

Biological protection shall be designed in a conservative way, taking into account the build-up of radionuclides over the plant lifetime, the potential loss of shielding efficiency due to effects of interactions of neutron and gamma rays with the shielding, due to reactions with other materials, decontamination solution, and the expected temperature conditions in design basis accidents.

The choice of materials for the shield shall be made on the basis of the nature of the radiation, the shielding, mechanical and other properties of materials and space limitations.

Ventilation systems shall be installed to:

1. prevent spreading of gaseous radioactive substances in plant compartments;
2. reduce and maintain compartments' airborne concentrations below the established limits and as low as reasonably achievable in all operational states and design basis accidents;
3. cleanup the air in premises containing inert or harmful gases.

In designing a ventilation system, the following factors shall be taken into account:

1. mechanisms of thermal and mechanical mixing;
2. limited effectiveness of dilution in reducing airborne contamination;
3. exhausting of the air from areas of potential contamination at points near the source of contamination;
4. ensuring adequate distance between exhaust air discharge point and the intake point;
5. providing a higher pressure in the less contaminated zones in comparison with the zones of higher contamination level;
6. preventing the spread of fire-released smoke products to neighbouring compartments.

Design shall provide for ventilation and air cleaning systems before discharge of gaseous radioactive substances to the environment.

Filters of air cleaning systems shall be sufficiently reliable to perform their function with the necessary decontamination factor in all operational modes. The design shall provide means to test their efficiency.

Provisions shall be made in the design for an automated system for radiation monitoring at the workplace and at the NPP site, and a system for radiation monitoring at the radiation protection and the monitored areas. These systems shall ensure the collection and processing of information on the radiation conditions, on the effectiveness of protective barriers, on the radionuclide activity, and information necessary to predict changes in the radiation conditions in all operational states and accident conditions.

The equipment of the automated system for radiation monitoring shall enable the implementation of:

1. process radiation monitoring;
2. individual monitoring;
3. radiation monitoring at the workplace and at the NPP site;
4. area monitoring for limiting the spread of radioactive contamination.

The laboratory methods and technical means of the system for radiation monitoring at the radiation protection and monitored areas shall ensure measurement of the content of human induced radionuclides in soil, water, deposits, vegetation, water flora and fauna, and agricultural products.

10.EMERGENCY PREPAREDNESS

The operating organization shall provide emergency management facilities and equipment to monitor the accident progression and manage the response. An on-site emergency control center, separated from the plant control room, shall be established.

Information about important plant parameters and radiological conditions in the plant and its immediate surroundings should be available there. The control center should provide means of communication with the control room, the supplementary control room and other important points in the plant, and with the on-site and off-site emergency response organizations.

The centre shall receive information on unit's status during the phases of accident progression and on the radiological conditions at the NPP site and its surroundings.

Appropriate measures shall be taken to protect the occupants against hazards resulting from a severe accident.

11.QUALITY MANAGEMENT SYSTEM

A quality management system that describes the overall arrangements for the management, performance and assessment of the plant design shall be prepared and implemented. This programme shall be supported by more detailed plans for each structure, system and component so that the quality of the design is ensured at all times.

Design, including subsequent changes or safety improvements, shall be carried out in accordance with established procedures that call on appropriate engineering codes and standards, and shall incorporate applicable requirements and design bases. Design interfaces shall be identified and controlled.

The adequacy of design, including design tools and design inputs and outputs, shall be verified or validated by individuals or groups separate from those who originally performed the work. Verification, validation and approval shall be completed before implementation of the detailed design.

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ
ԿԱՌԱՎԱՐՈՒԹՅԱՆ ԱՇԽԱՏԱԿԱԶՄԻ
ՂԵԿԱՎԱՐ Դ. ՍԱՐԳՍՅԱՆ