III. OTHER PROVISIONS

THE NUCLEAR SAFETY COUNCIL

10882

The Nuclear Safety Council's Instruction IS-27, of 16th June 2010, on general nuclear power plant design criteria.

Article 2.a) of Law 15/1980, of 22nd April, Creating the Nuclear Safety Council, confers on this Public Entity the faculty to "prepare and approve instructions, circulars and guides of a technical nature relating to nuclear and radioactive installations and nuclear safety- and radiological protection-related activities" related to the safe operation, i.e. without undue risks for people or the environment, of nuclear and radioactive installations.

Royal Decree 1838/1999, of 3rd December, approving the Regulation Governing Nuclear and Radioactive Installations fundamentally regulates the administrative and procedural aspects for the granting of licenses. For technical aspects, in the absence of Spanish regulations, the different licenses have been based on the regulation from the country of origin of the design and the technical regulations developing said regulation. Article 8.3 of said Royal Decree establishes that "The Licensee must continuously strive to improve the nuclear safety and radiological protection conditions of its installation. In order to do so, it must analyse the best existing techniques and practices, in accordance with the requirements set by the Nuclear Safety Council, and implement those that are suitable in the opinion of said body", which introduces as a regulatory basis for the installation the continuous improvement of the safety of the installation and the CSN's authority to require the best practices and techniques to this end.

The general design criteria constitute the set of minimum requirements with which a nuclear power plant must be designed so as to be considered safe. The objective of the present Instruction is to establish said set of criteria. During its preparation, the regulations from the countries of origin of the technology of Spanish plants have been taken into account, in particular the contents of Appendix A of Portion 50 of Title 10 of the US Code of Federal Regulations and the equivalent regulations from the BMI in Germany, as well as those from the IAEA. Likewise, the experience gained in relation to the design of structures, systems and components (hereinafter, SSCs) has been taken into consideration. Up to now, the Nuclear Safety Council (CSN) has been evaluating and examining whether nuclear power plant licensees comply with these regulations in all phases of the life of the installations.

Additionally, the work that has been carried out in the Western European Nuclear Regulators Association (WENRA) in order to harmonise the regulations from the different countries has been taken into account in this Instruction. As a result of this effort, a set of common requirements, or reference levels, which must be reflected in national regulations, has been established. The development of a CSN Safety Instruction that takes these criteria into account has been considered necessary so as to give consistency to the process of regulatory development that has been undertaken by the CSN as a result of this harmonisation process.

By virtue of the all the above and in accordance with the legal authorisation envisaged in Article 2.a) of Law 15/1980, of 22nd April, creating the Nuclear Safety Council, modified by Law 33/2007, of 7th November, prior consultation of the affected sectors and after the appropriate technical reports, this Council, during its meeting on the 16th of January of 2008, has agreed the following:

First. *Object and scope of application.*

1. The purpose of the present Nuclear Safety Council Instruction is to set the general criteria that must be fulfilled in the design, manufacture, construction, testing and general operation of a nuclear power plant's structures, systems and components important to safety.
2. The present Instruction applies to licensees of Spanish nuclear power plants in relation to their operating licenses.

Second. *Definitions.*

The definitions of the terms and concepts contained in the present Instruction match those contained in the following Regulations:

Law 25/1964, of 29th April, on Nuclear Energy (BOE No 107, of 4th May 1964, second article).

Law 15/1980, of 22nd April, creating the Nuclear Safety Council (BOE No 100, 25th April 1980).

Royal Decree 1838/1999, of 3rd December, approving the Regulation Governing Nuclear and Radioactive Installations (BOE No 313, 31st December 1999).

Council of the European Union's Directive 2009/71/EURATOM, of 25th June 2009, establishing a Community framework for the nuclear safety of nuclear installations.

In addition, the following definitions apply within the context of the present Instruction:

Anticipated operational occurrences (also known as anticipated operational transients): Those operating conditions that deviate from normal operation and are expected to occur one or more times during the life of the nuclear power plant such as e.g. the loss of off-site power, a trip of the turbine or the isolation of the reactor. The criteria used to design the plant prevent these events from causing significant damage or giving rise to postulated accident conditions.

Design-basis accidents: The set of accident conditions against which a plant is designed. In these conditions, the criteria used for the design of the plant help to keep the deterioration of nuclear materials and the release of radioactive materials within authorised dose limits.

Design limits: A set of values that set limits for functional capacity and behavioural parameters and levels and are considered acceptable in that they guarantee the observance of safety limits.

Effective multiplication factor: The quotient of the neutron numbers of two successive neutron generations of the chain reaction.

Loss-of-coolant accidents: In the case of Pressurised Water Reactors (PWRs), those events where a break of the reactor coolant pressure boundary causes a rate of loss of coolant greater than the capacity of normal systems to make it up; in the case of Boiling Water Reactors (BWRs), they make the pressure of the containment impossible to control by the normal cooling systems thereof, whatever the size of the break, including those equivalent in size to the double-ended rupture of the pipe with the greatest diameter of the reactor cooling system.

Normal operation: All modes of operation in which the plant can routinely find itself, from a refuelling outage to full-power operation, are included in this concept.

Nuclear reactor: Any structure containing nuclear fuel arranged in such a way that a self-sustaining nuclear fission process can take place in it without the need for an additional neutron source.

Nuclear unit: Each of the nuclear reactor assemblies and associated systems existing in a single site.

Protection systems: This concept includes the reactor protection system and the systems or subsystems that activate the technological safeguards and enable the automatic performance of their safety functions.

Radioactive materials or substances: All those substances or materials containing one or more radionuclides and whose activity or concentration cannot be considered negligible from the point of view of radiological protection.

Reactor containment (or containment): One of the structures of a nuclear power plant that acts as a barrier, together with the fuel rods and the reactor coolant pressure boundary, for controlling the emission of radioactive material. The containment includes:

1. The containment structure and its access hatches, penetrations and ancillary systems,
2. The valves, pipes, closed systems and other components enabling to isolate the containment atmosphere from the outside, and
3. Those systems or portions of systems which, given their functions, extend the boundary of the containment structure and provide effective isolation (e.g. steam and feedwater lines).

Reactor coolant pressure boundary: The set of all components subjected to the pressure of the reactor and that belong to its cooling system or are connected to it. The pressure boundary includes:

1. Plants of American design:

For systems with pipes that penetrate into the containment, up to the outermost containment isolation valve.

For systems that do not penetrate into the containment, up to the second of the two valves that are closed during the reactor's normal operation.

For BWRs, the reactor cooling system includes up to the outermost containment isolation valve of the feedwater and main steam systems.

The relief and safety valves of the reactor cooling system.

2. PWR plants of German design:

The pipes that connect to the reactor cooling system, up to the first isolation valve.

The relief and safety valves of the reactor cooling system.

Safety limits: Those limits set for the values of significant process variables, which it has been proven are necessary to reasonably maintain the integrity of the physical barriers that protect against the uncontrolled off-site release of radioactivity.

Safety (or safety-related) structures, systems and components: Those structures, systems and components whose operation is given credit in the analyses of design-basis accidents to:

Lead the installation to a safe condition and keep it in said condition in the long term.

Keep the radiological consequences of anticipated operational occurrences and of design-basis accidents within their specified limits.

Single failure: An independent event that causes a component to loose its capacity to perform its safety function. Multiple failures that might occur as a result of a single event are considered a single failure. It is considered that electrical and fluid systems are designed to withstand a single failure if the system maintains its capacity to carry out its safety functions in case a single failure of any active component takes place (assuming all passive components work properly) or of any passive component (assuming all active components work properly).

Site area: A plot of land, delimited and owned by the licensee, where an authorised installation is located, the inside of which being subjected to a series of controls, limits and regulations.

Structures, systems and components important to safety. The following is included in this concept:

1. Those structures, systems and components whose malfunction or failure could lead to an undue exposure to radiation of site personnel or members of the public,
2. Those structures, systems and components that prevent anticipated operational occurrences from giving rise to accident conditions;
3. Those items that are aimed at mitigating the consequences of accidents caused by a malfunction or failure of structures, systems and components.

Third. *Criteria.*

In order to make the implementation and documentary control of design criteria easier for licensees, the nomenclature, numbering and divisions of the structure of Appendix A of 10CFR50, approved by the US Nuclear Regulatory Commission, are used in the present Instruction.

Part 1: General requirements.

Criterion 1. Design of safety functions.

1.1 The nuclear power plant must be capable of maintaining the following safety functions in conditions of normal operation, anticipated operational occurrence and design-basis accident:

1. Reactivity control.
2. Removal of residual heat from the nuclear fuel.
3. Radioactive material confinement.

1.2 The design of structures, systems and components (hereinafter, SSCs) important to safety must take the fail safe criterion into consideration i.e. in case of failure, SSCs must remain in the position most favourable for safety allowed by their design.

1.3 The design shall prevent that a failure in systems not important to safety might affect the performance of a safety function.

1.4 The actions and manoeuvres needed to perform safety functions must be carried out in an automatic manner or through passive means such that action by an operator is not required during the 30 minutes following an initiating event. If the design requires an operator to take actions during that period of time, the actions must be justified and must be included in operating procedures which operations personnel are drilled in periodically and, whenever possible, in a replica full-scope simulator.

1.5 The reliability of SSCs important to safety shall be achieved by choosing the most appropriate options in each specific case such as e.g. the use of intrinsic safety means, passive safety means, properly tested components, redundancy, diversity, or physical and functional separation.

1.6 SSCs important to safety must be designed, manufactured, assembled and tested as per quality standards that match the importance of the safety functions they perform. To this end, all SSCs important to safety must be identified and shall be classified according to their importance to safety.

1.7 The classification of SSCs important to safety shall be mainly based on deterministic methods, complemented when necessary with probabilistic methods and the opinion of experts.

1.8 The design of SSCs important to safety must take human factors engineering principles and techniques into account.

Criterion 2. Design bases for protection against natural phenomena.

SSCs important to safety must be designed to withstand the effects of natural phenomena without loosing the capacity to carry out their safety functions. The design basis for these SSCs must contemplate the following aspects:

1. The most severe natural phenomena that have taken place at the site and in the surrounding area throughout history must be properly taken into account, and a sufficient margin shall be included in the design to account for the limitations in the historic data as regards precision, quantity and period of time to which the information corresponds.
2. Plausible combinations of normal operation and accident conditions with the effects of natural phenomena must be taken into consideration.
3. The importance of the safety functions these SSCs must carry out must be taken into account.

Criterion 3. Fire protection.

SSCs important to safety must be designed and located such that the probability of fires or explosions and their effects are minimized, always in a manner that is consistent with other safety requirements.

Non-flammable and heatproof materials must be used provided it is feasible and particularly in essential areas of the plant such as the containment and the control room.

Fire detection and extinguishing systems of the appropriate effectiveness and capacity must be installed, which must be designed to minimise the adverse effects of fire on SSCs important to safety. Fire extinguishing systems must be designed such that, in case of rupture or improper operation of the system, the capacity of these SSCs to carry out their safety functions is not affected in any significant manner.

The plant must have the necessary protection measures to restrict the propagation of fires, guaranteeing that they are confined to fireproof areas.

Criterion 4. Environmental and dynamic-effect design bases.

4.1 The SSCs indicated below must be designed to withstand the effects derived from, and to be compatible with, the environmental conditions associated with normal operation, maintenance work, testing and design-basis accidents, including loss-of-coolant accidents, during the entire life of the plant.

– Safety-related SSCs,
– those SSCs, without being safety-related, whose failure under postulated environmental conditions could prevent the performance of the safety functions of safety-related SSCs, and
– that post-accident instrumentation that requires it in accordance with applicable specific regulations.

4.2 To achieve this goal, a qualification programme shall be adopted that confirms that the SSCs indicated in Section 4.1 can fulfil their function during their entire design life, taking both the environmental conditions expected during the operation of the plant and, where appropriate, those corresponding to anticipated operational occurrences and design-basis accidents into consideration.

4.3 The SSCs indicated in Section 4.1 must be conveniently protected against dynamic effects, including those due to projectiles, the whip effect in pipes, and discharges of fluid, that could take place owing to the failure of equipment, as well as against events and conditions that take place outside the plant. However, the dynamic effects associated with the postulated rupture of plant pipes may be excluded from the design basis if there are CSN-approved analyses that prove that the probability of such ruptures is extremely low in conditions consistent with the design basis of the affected pipes.

Criterion 5. Shared structures, systems and components.

In nuclear power plants having more than one unit at the same site, SSCs important to safety may not be shared amongst the different units unless it is proven that this does not significantly affect the SSCs' capacity to carry out their safety functions, including, in case of accident in one unit, that of carrying out the orderly shutdown of the remaining units.

Part 2: Protection against fission products by means of multiple barriers.

Criterion 10. Design of the reactor.

The reactor core and the cooling, control and protection systems associated therewith must be designed with margins large enough to ensure that the fuel's design limits are not exceeded during any normal operation condition, including the effects of anticipated operational occurrences.

Criterion 11. Intrinsic protection of the reactor.

The reactor core and the associated cooling systems must be designed such that the net effect of the intrinsic nuclear feedback tends to compensate fast increases in reactivity within the entire range of power operation.

Criterion 12. Suppression of reactor power fluctuations.

The reactor core and the cooling, control and protection systems associated therewith must be designed to ensure that either no power fluctuations leading to conditions in which the fuel's design limits are exceeded can occur or there are guarantees that these fluctuations can be detected and eliminated in a fast and reliable manner.

Criterion 13. Instrumentation and control.

13.1 The plant must have instrumentation suitable for monitoring the behaviour of the plant's main variables and systems within the ranges of expected values for normal operation conditions, for anticipated operational occurrences and for postulated accident conditions such that the plant may be operated in a safe and reliable manner.

13.2 The instrumentation shall include the variables and systems that might affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary and the containment and its associated systems. The plant must have the necessary means to automatically record the measured values of the variables that are important to safety.

13.3 The instrumentation shall be suitable for measuring the plant's variables and must be qualified to fulfil its function in the environmental conditions anticipated in conditions of normal operation, anticipated operational occurrence and postulated accident conditions.

13.4 The plant must have control systems and methods suitable for keeping the variables and systems within the prescribed operating ranges.

Criterion 14. Reactor coolant pressure boundary.

The reactor coolant pressure boundary must be designed, manufactured, assembled and tested such that there is an extremely low probability of abnormal leaks, fast-propagation failures or a catastrophic break of the boundary taking place.

Criterion 15. Design of the reactor cooling system.

The reactor cooling system and the ancillary, control and protection systems associated therewith must be designed with a margin large enough to ensure that the design conditions of the reactor coolant pressure boundary are not exceeded during any normal operation condition, including anticipated operational occurrences.

Criterion 16. Design of the containment.

The plant must have a reactor containment and the necessary associated systems to provide an essentially leaktight barrier that prevents the uncontrolled release of radioactivity into the environment. It must be guaranteed that the containment's design conditions important to safety are not exceeded during the period of time associated with the development of design-basis accidents.

Criterion 17. Electrical power systems.

17.1 The plant must have an on-site electrical power system and an off-site electrical power system enabling the operation of SSCs important to safety. The safety function of each system shall be that of providing, in case the other one fails, enough electrical power to ensure that:

1. In case an anticipated operational occurrence takes place, the fuel's design limits or the reactor coolant pressure boundary's design conditions are not exceeded, and
2. In design-basis accident conditions, it will be possible to cool the core and the integrity of the containment, and the rest of safety functions needed in these conditions will be maintained.

17.2 The sources of on-site electrical power, including batteries, and the on-site electrical distribution system must have the necessary independence, redundancy and test capacity to carry out their safety functions in case of single failure.

17.3 The supply of electrical power from the grid to the on-site electrical distribution system must be carried out through at least two physically independent circuits (although not necessarily running over separate paths), which shall have the following characteristics:

1. The circuits shall be designed and located such that the possibility of their simultaneous failure in normal operation conditions, as well as under postulated accident or environmental conditions, is reduced, provided it is feasible.

Having a common electrical park for the two circuits is considered acceptable.

2. Each of these circuits must be designed such that, in case of the simultaneous loss of the other circuit and all on-site electrical power sources, the circuit is immediately available as a ensure that the system is capable of fulfilling its safety function at all times.

17.4 The design of electrical power systems must include the necessary measures so that, in case of loss of the power generated by the nuclear power plant or of loss of on-site or off-site power, the probability of losing the electrical power supply from any of the remaining sources, as a result of or coincidentally with the initial event, is minimised.

Criterion 18. Inspection and testing of electrical power systems.

Electrical power systems important to safety must be designed to enable the periodical execution of inspections and tests of its relevant components and characteristics, such as the wiring, insulations, connections and cabinets, to verify the continuity of the systems and the state of their components. The systems shall be designed with capacity for the following to be periodically tested:

1. The operability and functional capacity of the systems' components, such as on-site power sources, relays, switches and busbars.
2. The operability of the systems as a whole.
3. The full sequence of actuation that starts the operation of the system under conditions as close as possible to design conditions, provided it is feasible. This includes the operation of the corresponding parts of the protection system and the transfer of electrical power between the plant's main generator, the off-site electrical system and the on-site electrical system.

Criterion 19. The control room.

19.1 The plant must have a control room from which the actions needed to run the plant in a safe manner in normal operation conditions and to lead the plant to a safe condition and keep it there when an anticipated operational transient or a design-basis accident takes place can be taken.

19.2 The design of the control room shall take human factors into account. The control room shall be provided with visual and, where appropriate, sound devices identifying the processes and conditions that have deviated with regard to their normal condition and may affect safety. The operator shall have all necessary information so as to be able to check the actuation and effect of automatic actions.

19.3 Events internal and external to the control room that might affect its continuous operation shall be identified, and the design shall include the measures that can be reasonable taken to reduce the effects of these events to a minimum. In particular, an appropriate protection against radiation must be provided such that the access to and occupation of the control room for the full duration of an accident is enabled.

19.4 Additionally, the control room must have control instrumentation and equipment with the following design characteristics:

1. Being located in a single place physically and electrically separated from the control room. If there is more than one location, the capacity of all the equipment to operate in an integrated manner must be proven by means of the appropriate procedures.
2. Having the capacity to take the plant to a hot shutdown in a sufficiently fast manner, including the capacity to keep the plant in safe hot-shutdown conditions.
3. Having the potential capacity to take the plant to the reactor's subsequent cold shutdown by using the appropriate procedures.

Part 3: Reactivity protection and control systems.

Criterion 20. Protection system functions.

The protection system must be designed to fulfil the following functions:

1. Automatically initiating the operation of the necessary systems, including reactivity control systems, to guarantee that, in case an anticipated operational occurrence takes place, the fuel's design limits are not exceeded.
2. Detecting the conditions that indicate that an accident has occurred and automatically initiating the operation of the systems and components important to safety that are required to mitigate its consequences.

Criterion 21. Reliability and possibility of testing the protection system.

21.1 The protection system must be designed such that it has a high functional reliability and a high capacity to be tested in operating conditions in a manner consistent with the safety functions it must perform.

21.2 The design of the protection system must include enough redundancy and independence so as to ensure that:

1. No single failure may cause the loss of the protective function.
2. Putting any component or channel of the protection system out of service may not lead to the loss of the minimum required redundancy unless it can be proven that the reliability of the system's operation is still acceptable in those conditions.

21.3 The protection system must be designed to enable to periodically test its full operation (from the sensing instrument that provides the input signal to the final actuator) during the plant's normal operation, including the capacity to independently test the channels in order to identify the failures and losses of redundancy that could have taken place. The exceptions to this criterion must be properly substantiated based on the specific characteristics of the system's design.

21.4 The protection system shall be designed such that the possibility that action by an operator might reduce the effectiveness of the protection system during normal operation and in case of anticipated operational occurrences is reduced to the minimum. However, the protection system shall not prevent operators from taking corrective actions in case a design-basis accident occurs.

21.5 The digital systems that are used to carry out the protective functions, or that might affect their performance, must have the following characteristics:

1. The systems shall be designed, built, verified, validated, tested and controlled as per the highest, internationally renowned quality standards in the nuclear field.
2. The entire system development process, including the control, testing and commissioning of design modifications, must be systematically documented and reviewed.
3. In those cases where the reliability of the systems against common-cause failures cannot be proven with a high degree of confidence, there will be an alternative method for guaranteeing the fulfilment of their safety functions.

Criterion 22. Independence of the protection system.

22.1 The protection system must be designed such that the protective function is not lost because of the conditions associated with natural phenomena, normal operation, maintenance tasks, testing and design-basis accidents unless it is proven that the reliability of the protective function is acceptable by using a different technical basis.

22.2 In order to prevent the loss of the protective function, design techniques, such as functional diversity or the diversity in the design of components and their operating principles, must be used provided it is feasible.

Criterion 23. Failure modes of the protection system.

The protection system must be designed such that it remains in the state that provides the greater safety, or which can be proven to provide acceptable safety, by using a different technical basis, in those cases where the following occurs:

a. The disconnection of the system,
b. The loss of electrical power,
c. The loss of instrument air supply,
d. The adverse environmental conditions that have been postulated.

Criterion 24. Separation of the protection system from any control system.

The protection system must be separated from the control systems such that, in case a component or channel of a control system fails or a component or channel of the protection system that is common to the control and protection systems fails or is put out of service, there is always a system satisfying all reliability, redundancy and independence requirements of the protection system that remains intact. The protection system's interconnection with control systems must be restricted so as to ensure that safety is not significantly affected.

Criterion 25. Requirements of the protection system in case of failures in the control of reactivity.

The protection system must be designed to ensure that the fuel's design limits are not exceeded in case of any single failure of the reactivity control systems, such as e.g. the uncontrolled withdrawal of control rods. The ejection or drop of control rods is not considered a single failure for the purposes of this criterion.

Criterion 26. Capacity and diversity of reactivity control systems.

26.1 The plant must have two independent reactivity control systems, which shall be based on different design principles.

26.2 One of the systems must use control rods, it being preferable that it is provided with an active device to insert the rods. The system must be capable of reliably controlling the changes in reactivity to ensure that the fuel's design limits are not exceeded in normal operation conditions, including anticipated operational occurrences, and having a margin suitable for the case of single failure of the system or of operational failures such as rod seizure.

26.3 The second reactivity control system must be able to reliably control the rate of change in reactivity derived from normal and planned changes in power level (including changes in xenon concentration) such that the fuel's design limits are not exceeded.

26.4 At least one of the systems must be capable of keeping the reactor core subcritical in cold conditions.

Criterion 27. Combined capacity of reactivity control systems.

Reactivity control systems, together, where appropriate, with the injection of neutron poison by safety systems, must be designed such that their combined capacity enables to reliably control the changes in reactivity in order to ensure that the capacity to cool the core is maintained in the conditions of design-basis accidents, and having a margin suitable for covering the possibility of control rod seizure.

Criterion 28. Reactivity limits.

28.1 The design of reactivity control systems must include limits for the increase and rate of increase of reactivity that can potentially take place, in order to ensure that the effects of postulated reactivity accidents are limited as follows:

1. They cannot damage the reactor coolant pressure boundary beyond limited local damages.
2. They do not affect the core, its support structures or other vessel internals in a manner big enough for the capacity to cool the core to be affected in any significant manner.

28.2 Postulated reactivity accidents must include, at least, the ejection of control rods (unless this can be prevented by positive means), the drop of control rods, the rupture of steam lines, changes in the temperature and pressure of the reactor coolant, and the injection of cold water in steam generators (PWRs) or the reactor vessel (BWRs).

Criterion 29. Protection against anticipated operational occurrences.

The protection system and reactivity control systems must be designed to ensure that there is a high probability that they will fulfil their safety functions in case an anticipated operational occurrence takes place.

Part 4: Fluid systems.

Criterion 30. Quality of the reactor coolant pressure boundary.

The components that are part of the reactor coolant pressure boundary must be designed, manufactured, assembled and tested as per the most stringent quality standards. The plant must have the necessary means to detect reactor coolant leaks and identify, provided it is feasible, the origin and location of the leaks.

Criterion 31. Prevention of the break of the reactor coolant pressure boundary.

31.1 The reactor coolant pressure boundary must be designed with a margin large enough so that the following aspects are guaranteed when it is subjected to the stresses corresponding to operation, maintenance, test and postulated accident conditions:

1. The materials that make up the barrier do not behave in a fragile manner.
2. The probability of the occurrence of a rapidly propagating fracture is minimised.

31.2 The design must consider the service temperature and other conditions to which the material of the boundary is subjected during operation, maintenance, testing, design-basis accidents and anticipated operational occurrences, as well as the uncertainties existing in the determination of the following parameters:

1. The properties of the materials.
2. The effects of irradiation on the properties of the materials.
3. Residual stresses, in stationary state and during transients.
4. The size of defects.

Criterion 32. Inspection of the reactor coolant pressure boundary.

The components that make up the reactor coolant pressure boundary must be designed such that the following is possible:

1. The periodic execution of inspections of and tests on the most important areas and characteristics in order to verify their structural integrity and leaktightness.
2. The implementation of an appropriate programme for monitoring the material of the reactor vessel.

Criterion 33. Reactor coolant replenishment.

33.1 As a protection against small breaks of the reactor coolant pressure boundary, the plant must have a system that provides the capacity to replenish the coolant that might leak from the reactor cooling circuit. The system's safety function must be that of ensuring that the fuel's design limits are not exceeded in case of coolant losses due to leaks in the circuit or to the rupture of small pipes or other minor components that are part of the pressure boundary.

33.2 The system must be designed to ensure that in both operation with on-site electrical power (assuming there is no off-site power) and operation with off-site electrical power (assuming there is no on-site power), the system's safety function can be fulfilled by using the same pipes, pumps and valves that are used to maintain the inventory of coolant during normal operation of the reactor.

Criterion 34. Removal of residual heat from the reactor core.

34.1 The plant must have systems for removing residual heat. The safety function thereof shall be that of transferring the decay heat of fission products and other sources of residual heat of the core with a heat removal rate high enough so that the fuel's and the pressure boundary's design limits that have been established as acceptable are not exceeded.

34.2 The capacity of these systems shall be large enough to remove the residual heat from the core after the shutdown of the reactor, as well as during and after an anticipated operational occurrence or a design-basis accident.

34.3 These systems must be provided with the appropriate redundancy in their components and characteristics and shall have the interconnections and leak detection and isolation capabilities needed to ensure that, in both operation with on-site electrical power (assuming there is no off-site electrical power) and operation with off-site electrical power (assuming there is no on-site electrical power), the system's safety function can be fulfilled assuming a single failure occurs.

34.4 Residual heat removal systems must be designed to allow the appropriate periodic inspections of the components that carry out safety functions in order to guarantee the integrity and capacity of the systems themselves.

34.5 Residual heat removal systems must be designed to enable the execution of the appropriate, periodic pressure and functional tests allowing to guarantee:

1. The structural integrity and leaktightness of the components that perform safety functions.
2. The operability and actuation of the active components that carry out safety functions.
3. The operability of the entire systems and, under conditions as close as feasible to design conditions, the functional capacity of the system and the operation of the associated cooling water system or systems.

Criterion 35. Emergency core cooling.

35.1 The plant must have a system that provides abundant cooling to the core in case of an emergency. The system's main safety function shall be that of transferring the heat of the core in case of the loss of reactor coolant with a removal rate enough to ensure that:

1. Damage to the fuel and cladding that could prevent the effective and continuous cooling of the core is prevented.
2. The reaction between the metal of the cladding and the water is kept down at insignificant levels.

35.2 The system must be provided with the appropriate redundancy in its components and characteristics and shall have the interconnections and leak detection and isolation capabilities needed to ensure that, in both operation with on-site electrical power (assuming there is no off-site electrical power) and operation with off-site electrical power (assuming there is no on-site electrical power), the system's safety function can be fulfilled assuming a single failure occurs.

Criterion 36. Inspection of the emergency core cooling system.

The emergency core cooling system must be designed to allow the appropriate periodic inspections of its most important components in order to guarantee the integrity and capacity of the system.

Criterion 37. Testing of the emergency core cooling system.

The emergency core cooling system must be designed to enable the execution of the appropriate, periodic pressure and functional tests allowing to guarantee:

1. The structural integrity and leaktightness of its components.
2. The operability and actuation of the system's active components.
3. The operability of the entire system and, under conditions as close as feasible to design conditions, the actuation of the full operational sequence that puts the system into operation, including the operation of the applicable parts of the protection system, the switch from normal to emergency electrical power and the operation of the associated cooling water system or systems.

Criterion 38. Removal of heat from the containment.

38.1 In case it is necessary, there must be a system or systems for removing the heat from the reactor containment. The safety function of these systems shall be that of reducing, rapidly enough and in a manner consistent with the operation of other associated systems, the

pressure and temperature of the containment after any design-basis accident and keeping these variables at acceptably low values.

38.2 Each system must be provided with the appropriate redundancy in its components and characteristics and shall have the interconnections and leak detection and isolation capabilities needed to ensure that, in both operation with on-site electrical power (assuming there is no off-site electrical power) and operation with off-site electrical power (assuming there is no on-site electrical power), the systems' safety function can be fulfilled assuming a single failure occurs.

Criterion 39. Inspection of containment heat removal systems.

Containment heat removal systems must be designed to enable the execution of the appropriate periodic inspections of its most important components in order to guarantee the integrity and capacity of the systems.

Criterion 40. Testing of containment heat removal systems.

Containment heat removal systems must be designed to enable the execution of the appropriate, periodic pressure and functional tests allowing to guarantee:

1. The structural integrity and leaktightness of their components.
2. The operability and actuation of the systems' active components.
3. The operability of the entire systems and, under conditions as close as feasible to design conditions, the actuation of the full operational sequence that puts the systems into operation, including the operation of the applicable parts of the protection system, the switch from normal to emergency electrical power and the operation of the associated cooling water system or systems.

Criterion 41. Cleanup of the atmosphere of the containment.

41.1 The plant must have the necessary systems to control fission products, hydrogen, oxygen and other substances that might be released inside the containment so as to carry out, consistently with the operation of other associated systems, the following functions:

1. Reducing the concentration of fission products that are released into the environment during design-basis accidents to such values that compliance with the established radiological limits is ensured.
2. Controlling the concentration of hydrogen, oxygen and other substances in the containment's atmosphere after a postulated accident in order to ensure that the integrity of the containment is maintained.

41.2 Each of the systems must be provided with the appropriate redundancy in its components and characteristics and shall have the interconnections and leak detection and isolation capabilities needed to ensure that, in both operation with on-site electrical power (assuming there is no off-site electrical power) and operation with off-site electrical power (assuming there is no on-site electrical power), the systems' safety function can be fulfilled assuming a single failure occurs.

Criterion 42. Inspection of containment atmosphere cleanup systems.

Containment atmosphere cleanup systems must be designed to enable the execution of the appropriate periodic inspections of its most important components in order to guarantee the integrity and capacity of the systems.

Criterion 43. Testing of containment atmosphere cleanup systems.

Containment atmosphere cleanup systems must be designed to enable the execution of the appropriate, periodic pressure and functional tests allowing to guarantee:

1. The structural integrity and leaktightness of their components.

2. The operability and actuation of the systems' active components.
3. The operability of the entire system and, under conditions as close as feasible to design conditions, the actuation of the full operational sequence that puts the system into operation, including the operation of the applicable parts of the protection system, the switch from normal to emergency electrical power and the operation of the associated cooling water system.

Criterion 44. Cooling water systems.

44.1 The plant must have a system or systems for transferring the heat from SSCs important to safety to an ultimate heat sink. The safety function of these systems shall be that of transferring the combined heat load of these SSCs in normal operation and postulated accident conditions.
44.2 Cooling water systems must be provided with the appropriate redundancy in its components and characteristics and shall have the interconnections and leak detection and isolation capabilities needed to ensure that, in both operation with on-site electrical power (assuming there is no off-site electrical power) and operation with off-site electrical power (assuming there is no on-site electrical power), the systems' safety function can be fulfilled assuming a single failure occurs.

Criterion 45. Inspection of cooling water systems.

Cooling water systems must be designed to enable the execution of the appropriate periodic inspections of its most important components in order to guarantee the integrity and capacity thereof.

Criterion 46. Testing of cooling water systems.

Cooling water systems must be designed to enable the execution of the appropriate, periodic pressure and functional tests allowing to guarantee:

1. The structural integrity and leaktightness of their components.
2. The operability and actuation of the systems' active components.
3. The operability of the entire systems and, under conditions as close as feasible to design conditions, the actuation of the full operational sequence that puts the systems into operation both for a reactor shutdown and in the case of a loss-of-coolant accident, including the operation of the applicable parts of the protection system and the switch from normal to emergency electrical power.

Part 5: Reactor containment.

Criterion 50. Design bases of the containment.

The structure of the reactor containment and its inner compartments, including access hatches and penetrations, must be designed such that they withstand with a large enough margin the calculated pressure and temperature conditions that would take place in case of a loss-of-coolant accident, without exceeding the containment's design leak rate. The determination of this margin must be based on the following considerations:

1. The effects of all possible energy sources that have not been contemplated when determining the maximum temperature and pressure conditions, including the energy contained in the steam generators and that generated by the metal-water reaction and other chemical reactions that could take place as a result of the postulated degradation of the operation of the core emergency cooling, without arriving at the total loss of this function.
2. The limitations in the experience and available experimental data relating to the knowledge of the phenomena that take place during the accident and the containment's response thereto.
3. The conservatism of the calculation models and input data that have been used.

Criterion 51. Prevention of the break of the containment.

51.1 The reactor containment boundary must be designed with a margin large enough to ensure that under operation, maintenance, test and postulated accident conditions the ferric materials that make up the boundary do not behave in a fragile manner and the probability of the occurrence of a rapidly propagating fracture is minimised.

51.2 The design must consider the service temperature and other conditions to which the material that makes up the boundary is subjected during operation, maintenance, testing, design-basis accidents, as well as the uncertainties existing in the determination of the following parameters:

1. The properties of the materials.
2. Residual stresses, in stationary state and during transients.
3. The size of defects.

Criterion 52. Capacity to conduct containment leaktightness tests.

The containment and other equipment that might be subject to test conditions must be designed so that the execution of leak tests at the containment's design pressure is possible.

Criterion 53. Inspection and testing of the containment.

The reactor containment must be designed to allow:

1. The execution of the appropriate periodic inspections of all its important areas, including penetrations.
2. The implementation of a suitable monitoring programme.
3. The execution, at the containment's design pressure, of periodic tests of the leaktightness of penetrations with resilient seals or expansion joints, unless it is proven under a different technical basis that this is not necessary to guarantee the containment's leak rate that was considered the hypothesis in the applicable safety analyses.

Criterion 54. Systems with pipes that go through the walls of the containment.

54.1 Systems having pipes that go through the walls of the containment must have containment isolation and leak detection capabilities, with a redundancy, reliability and capacity of action consistent with the importance to safety of the isolation of said pipes.

54.2 These systems must be designed with capacity to:

1. Periodically test the operability of containment isolation valves and their associated equipment.
2. Periodically verify that the leaks from containment isolation valves are within acceptable limits, unless it is proven under an appropriate technical basis that this is not necessary to guarantee the containment's leak rate that was considered the hypothesis in the applicable safety analyses.

Criterion 55. Isolation of pipes that belong to the reactor coolant pressure boundary and go through the walls of the containment.

55.1 Every pipe that belongs to the reactor coolant pressure boundary and goes through the walls of the containment must be provided with containment isolation valves that meet one of the configurations indicated below:

1. One closed, locked isolation valve inside the containment and one closed, locked isolation valve outside.
2. One automatic isolation valve inside the containment and one closed, locked isolation valve outside.
3. One closed, locked isolation valve inside the containment and one automatic isolation valve outside.
4. One automatic isolation valve inside the containment and one automatic isolation valve outside.

No standard check valve, i.e. that does not have an active, remote actuation mechanism, may be used as an automatic isolation valve outside the containment.

Configurations other than those indicated may be considered valid if it is proven under a different technical basis that the containment isolation devices in a pipe or a specific type of pipes, such as e.g. the instrumentation lines, are acceptable.

55.2 Isolation valves located outside the containment must be placed as close as possible to it.

55.3 Automatic containment isolation valves must be designed so that, in case of loss of the electrical power needed for them to actuate, they remain in the position most favourable for safety allowed by their design.

55.4 In order to guarantee an appropriate safety level, the additional requirements that are needed to minimise the probability or the consequences of an accidental rupture of these pipes or others connected to them must be implemented. Examples of these additional requirements are: the use of higher levels of quality in design, manufacturing and testing; additional capabilities to conduct inspections in service; protection against the most severe natural phenomena; and the use of additional isolation valves. In order to determine whether these additional requirements are appropriate, the population density, the physical characteristics and the land use characteristics in the site's surrounding area shall be taken into account.

Criterion 56. Isolation of pipes open to the atmosphere of the containment.

56.1 Every pipe that goes through the walls of the containment and directly connects to the atmosphere of the containment must be provided with containment isolation valves that meet one of the configurations indicated below:

1. One closed, locked isolation valve inside the containment and one closed, locked isolation valve outside.
2. One automatic isolation valve inside the containment and one closed, locked isolation valve outside.
3. One closed, locked isolation valve inside the containment and one automatic isolation valve outside.
4. One automatic isolation valve inside the containment and one automatic isolation valve outside.

No standard check valve, i.e. that does not have an active, remote actuation mechanism, may be used as an automatic isolation valve outside the containment.

Configurations other than those indicated may be considered valid if it is proven under a different technical basis that the containment isolation devices in a pipe or a specific type of pipes, such as e.g. the instrumentation lines, are acceptable.

56.2 Isolation valves located outside the containment must be placed as close as possible to it.

56.3 Automatic containment isolation valves must be designed so that, in case of loss of the electrical power needed for them to actuate, they remain in the position most favourable for safety.

Criterion 57. Isolation of pipes belonging to closed systems.

57.1 Every pipe that goes through the walls of the containment and does not belong to the reactor coolant pressure boundary or is not directly connected to the atmosphere of the container (closed systems) must have at least one containment isolation valve, which shall be automatic, or shall be closed and locked, or shall be able to be manually operated in a remote manner. No standard check valve, i.e. that does not have an active remote actuation mechanism, may be used as an automatic isolation valve.

57.2 Containment isolation valves belonging to closed systems must be located outside the containment and placed as close as possible to it.

57.3 Automatic containment isolation valves must be designed so that, in case of loss of the electrical power needed for them to actuate, they remain in the position most favourable for safety.

Part 6: Control of radioactivity.

Criterion 60. Control of the discharges of radioactive materials or substances into the environment.

60.1 The design of the nuclear power plant must include the means suitable for controlling the release of radioactive materials or substances in gaseous and liquid effluents and for managing the solid radioactive waste generated during normal operation of the reactor and during anticipated operational occurrences.

60.2 There must be a capacity large enough to retain gaseous and liquid effluents containing radioactive materials or substances, in particular for the case when adverse environmental conditions at the site might impose limitations on the off-site discharge of said effluents.

Criterion 61. Monitoring of radioactive discharges.

In order to detect the radioactivity that might be released during normal operation, anticipated operational occurrences and design-basis accidents, the plant must have the necessary means to monitor the atmosphere of the containment and that of spaces outside thereof containing components where fluids resulting from an accident might flow as well as effluent discharge paths and the plant site's surrounding area.

Part 7: Storage of fuel and radioactive waste.

Criterion 70. Storage and handling of fuel and radioactive waste.

Fuel storage and handling systems, radioactive waste handling systems and other systems that might contain radioactive substances must be designed to guarantee an appropriate safety level in normal operation, anticipated operational occurrence and postulated accident conditions. These systems must be designed with the following characteristics:

1. A capacity to allow the execution of the appropriate, periodic inspections and tests of their components important to safety.
2. A shielding suitable for protecting against radiation.
3. An appropriate containment, confinement and filtering capacity.
4. Residual heat removal capacity, which in the case of underwater storage, must be large enough to maintain the temperature of the coolant within a range of values compatible with the design of SSCs important to safety in all fuel storage operating conditions, and with test reliability and capacity levels that reflect the importance to safety of the removal of decay heat and residual heat in general.
5. In the case of underwater storage, a capacity to prevent a significant reduction in the fuel storage coolant inventory from occurring in accident conditions, such that fuel elements are kept flooded.

Criterion 71. Prevention of criticality during storage and handling of fuel.

71.1 Criticality during fuel storage and handling must be prevented by using physical systems or processes, preferably by means of the use of safe geometrical configurations.

71.2 The proper value of the effective multiplication factor (K effective) of fresh fuel storage racks loaded with fuel elements of the maximum reactivity and flooded with pure water must not exceed 0.95, with a 95% probability and a 95% level of confidence.

71.3 In the case that the optimum moderation of fresh fuel storage racks takes place in low moderation conditions (for equivalent reduced water densities), the K effective calculated in those conditions for racks loaded with maximum reactivity fuel elements may not exceed 0.98, with a 95% probability and a 95% level of confidence.

71.4 The design of spent fuel underwater storage racks shall meet the following conditions:

1. If credit is not given to the soluble boron of the storage, the calculated K effective of racks loaded with fuel elements of the maximum reactivity and flooded with pure water must not exceed 0.95, with a 95% probability and a 95% level of confidence.

2. If credit is given to the storage's reduction in reactivity caused by soluble boron, the calculated K effective of the racks loaded with maximum reactivity fuel elements must not exceed 0.95, with a 95% probability and a 95% level of confidence, when flooded with borated water, and must be below 1.0, with a 95% probability and a 95% level of confidence, when flooded with pure water.

These conditions shall not be applied to the fuel loaded in the spent fuel storage and/or freight containers when they are inside the spent fuel pool.

Criterion 72. Surveillance of fuel and waste storages.

Fuel and radioactive waste storage systems, and the associated handling areas, must have systems suitable for:

1. Detecting the presence of conditions that might lead to the loss of the capacity to remove residual heat or to excessive radiation levels.
2. Initiating the appropriate safety actions.

Fourth. *Infractions and sanctions.*

The present Nuclear Safety Council Instruction is binding in accordance with that established in Article 2.a) of Law 15/1980, of 22nd April, creating the Nuclear Safety Council, such that the failure to comply with it shall be punished in accordance with the provisions of Chapter XIV (Articles 85 to 93) of Law 25/1964, of 29th April, on Nuclear Energy.

Fifth. *Exemptions.*

Nuclear power plant licensees may request the CSN to exempted them from complying with some requirement of this Instruction, provided they prove the impossibility of complying therewith and include the corresponding proof and the alternative way in which the levels of nuclear safety and radiological protection provided by the requirement from which exemption is requested are maintained.

Sole Transitory Provision.

A six-month period from the publication of this Instruction is set for nuclear power plant licensees to include the criteria contained in it in their Safety Analysis Reports.

Other plant documents must be updated by following that indicated in this Instruction when they are reviewed in accordance with the facility's existing documentation management programmes.

Sole Repealing Provision.

Any rule of equal or lower level that opposes the present Instruction is repealed.

Sole Final Provision.

The present Instruction shall come into force on the day following that of its publication in the "Official State Gazette".

In Madrid, on the 16th of June of 2010.–Carmen Martínez Ten, the President of the Nuclear Safety Council.