The CSN provides users of this website with an unofficial translation of the law in question. You are therefore advised that this translation is for your information only and may not be entirely up to date when you consult it. For official texts, look up the law in the Boletín Oficial del Estado, where you can find laws in any of the official languages of the State of Spain.

CSN

El CSN pone a disposición de los usuarios de esta web una traducción no oficial del texto de la norma de referencia. Se advierte, por tanto, de su carácter puramente divulgativo, y de la posibilidad de que no se encuentre debidamente actualizada en el momento de su consulta. El texto oficial es el publicado en el Boletín Oficial del Estado en cualquiera de las lenguas oficiales del Estado español.

NUCLEAR SAFETY COUNCIL

2039 *Nuclear Safety Council Instruction IS-37, of January 21st 2015, on the analysis of design basis accidents at nuclear power plants*

Article 2.a) of Law 15/1980, of April 22nd, creating the Nuclear Safety Council (CSN), attributes to this Public Body powers to «draw up and approve instructions, circulars and guidelines of a technical nature relating to nuclear and radioactive facilities» in relation to the safe operation of nuclear and radioactive facilities, that is without undue risk for persons or the environment. This article also incorporates promotion of the participation of stakeholders and the public in the process of drawing up these instructions.

The present Instruction is part of the process of development of standards dealing with nuclear safety and radiological protection carried out by the CSN. This process is also part of the objective of homologating the regulatory practices of the different international regulatory bodies, which takes as a reference the requirements generated within the International Atomic Energy Agency (IAEA) and the so-called reference levels established by the Western European Nuclear Regulators Association (WENRA).

This Instruction develops the contents of the nuclear power plant accident analyses, thereby contributing to compliance with Council Directive 2009/71/EURATOM of June 25th 2009, establishing a community framework for the nuclear safety of nuclear facilities, modified by Council Directive 2014/87/ EURATOM of July 8th 2014, article 6 of which obliges the national legal framework to require that the licensees »periodically evaluate and verify and permanently improve, to the extent that is reasonably feasible, the nuclear safety of the nuclear facilities, this to be done in a systematic and verifiable manner. The above shall include verification of the application of measures for the prevention of accidents and attenuation of their consequences, including verification of the application of the provisions of defence in depth».

The accident that occurred at Fukushima nuclear power plant in Japan has underlined the transcendental importance of aspects relating to the capacities and resources necessary to manage accidents beyond the design basis of the facility. The current wording of the thirteenth article of this Instruction, «Design extension», is consistent with the actions implemented to date, inasmuch as it requires the analysis of scenarios not contemplated in the design of the facility and determination of the possibility of improving it or establishing prevention and mitigation measures in order to contribute to reducing risk.

In the absence of other technical standards, the regulatory practice applied to date as regards the analysis of accidents and the relationship with the design basis of safety-related structures, systems and components has consisted of verifying compliance with the technical standards required in the country of origin of the technology, with whatever specific adaptations have been considered necessary. The present Instruction contributes to establishing an in-house standards framework while also ensuring compatibility with the practices applied to date and providing support for the design bases of the nuclear power plants currently in operation.

Throughout the different articles there is a detailed description of the deterministic methodology supporting the design of the operating nuclear power plants. The basic principles of defence in depth, the maintenance of safety margins and the limitation of the permissible magnitude of damage depending on the frequency with which it might be exceeded are reaffirmed. Developed around these principles is a systematic approach aimed at establishing the contents and scope of accident analysis; the concept of the postulated initiating event and its classification is dealt with; acceptance criteria are assigned for each class; the operability requirements applicable to systems and components and assumed initial and bounding conditions are analysed, in order to generate the set of design basis events for these structures, systems and components; and the concept of design extension is analysed as an element improving the safety of the facility.

Finally, the Regulation on Nuclear and Radioactive Facilities, approved by Royal Decree 1836/1999, of December 3rd, establishes a series of requirements relating to the safety assessment that includes documentation on the analysis of accidents and their consequences, in both the request for the building permit, Title II, Chapter III, and the

request for the operating permit, Title II, Chapter IV.

In compliance with the legal qualifications contemplated in article 2.a.) of Law 15/1980, of April 22nd, creating the Nuclear Safety Council and following consultation with the affected sectors and corresponding technical reports, this Council has agreed as follows during its meeting of January 21st 2015:

One. *Objective and scope of application*

The present Instruction is issued with the objective of developing the provisions of article 17 e) 3 and article 20 a) 3 of the Regulation on Nuclear and Radioactive Facilities, which require an analysis of foreseeable accidents and their consequences as documentation linked to the granting of nuclear power plant construction and operating permits.

The following are objectives of accident analysis:

a) Verify maintenance of the safety functions of the facility, through a study of the capacity of the facility to accommodate the postulated events making up the design basis of the safety-related structures, systems and components, in accordance with the applicable acceptance criteria.

b) Contribute to determination of the minimum conditions required as regards the operability and functional capacity of the structures, systems and components, as well as the ranges of values of the process variables and parameters within which operation of the facility is safe.

c) Verify that the consequences for the health of persons and the environment of the initiating events postulated from any operating condition of the facility are acceptable in accordance with the applicable radiological protection requirements.

d) Verify that the magnitude of the damage accumulated as a result of the postulated accidents is below the acceptance criteria established in accordance with their frequency.

e) Verify the safety of the design of the facility through minimisation of the frequency of initiating events, maintenance of defence in depth and maintenance of suitable safety margins.

This Instruction shall be applicable to the holders of construction and operating permits for nuclear power plants.

Accidents implying the use of beyond design basis hypotheses and not being subject to design extension in accordance with article thirteen are not included within the scope of this Instruction.

Two. *Definitions.*

The definitions of the terms and concepts contained in the present Safety Instruction correspond to those contained in the following standards:

– Nuclear Energy Act, Law 25/1964, of April 29th

– Law 15/1980, of April 22nd, creating the Nuclear Safety Council

– Royal Decree 1836/1999, of December 3rd, approving the Regulation on Nuclear and Radioactive Facilities

– Royal Decree 783/2001, of July 6th, approving the Regulation on the Protection of Health against Ionising Radiations.

– Royal Decree 1546/2004, of June 25th, approving the Basic Nuclear Emergency Plan.

In addition to the above, certain terms are used that in the context of this Instruction are to be understood as follows:

Accident analysis: Set of studies, contained in the Safety Assessment of the facility and reference documents, aimed at demonstrating that the operation of the nuclear facility in response to foreseeable operating events and accidents is in keeping with the required levels of safety.

Uncertainty assessment: Study and qualification of the uncertainty associated with safety variables, on the basis of the processes used for their estimation. This treatment makes it possible to determine the distribution of the probability of error for these variables or a level of error.

Exclusion zone: Area surrounding a nuclear power plant that is under the control of

the plant operator and in which the licensee is authorised to establish all activities, including the exclusion or removal of persons and objects present in the area. This area may be crossed by a road, railway or water course, as long as they are not so close to the facility as to interfere with its normal operation and that appropriate and effective measures are adopted to control the traffic on such road, railway or water course in the event of an emergency, in order to protect public health and safety. Residences will normally be prohibited within the exclusion zone. In any event, residents shall be rapidly evacuated if necessary. Activities not related to the operation of the plant may be allowed within the exclusion zone, subject to the pertinent limitations, as long as they do not pose any significant risk for public health and safety.

Design basis: This is the set of information that identifies the specific functions performed by a structure, system or component at the facility, along with the values (or range of values) of the parameters relating to this function and selected as bounding conditions for the design. These values may be: conditions deriving from practices commonly accepted to achieve functional objectives or requirements deriving from analyses (based on calculations or experiments) of the effects of the postulated accident for which the structure, system or component is required to fulfil its function.

Licensing basis: This is the set of obligatory requirements, regulatory commitments and exemptions deriving from both the initial standards and those incorporated subsequently. The licensing basis is included in the official operating documents of the plant, the conditions associated with their approval and the operating permit, as well as in the commitments of the licensee of the facility to ensure compliance with the design basis of safety systems (including the modifications performed).

Bounding condition: Value, time-dependent or otherwise, imposed upon the process variables of a calculation model.

Initial condition: Initial value imposed upon the process variables of a calculation model.

Passive component: Component that does not require moving parts or changes in its configuration, status or properties to perform its function.

Defence in depth: This consists of the hierarchical deployment, at different levels, of various structures, systems and components and procedures to prevent the escalation of foreseeable operating events or accidents and to maintain the effectiveness of the physical barriers fulfilling safety functions and located between a source of radiation or radioactive materials and the workers, members of the public or environment.

Diversity: Redundant systems (see redundancy) having different operating characteristics are said to be diverse. This makes it possible to reduce the possibility of a failure caused by a factor potentially affecting both systems in the same way (common cause failure).

Safety significant items: This includes the following:

1. Those structures, systems and components whose malfunctioning or failure could give rise to an undue exposure to radiation for the site personnel or members of the public.
2. Those structures, systems and components that prevent foreseeable operating events from giving rise to accident conditions.
3. Items designed to mitigate the consequences of accidents caused by the malfunctioning or failure of structures, systems or components.

These items are sub-divided into «safety elements» and «safety significant elements».

Safety element (or safety-related element): An element to whose operation credit is given in design basis accident analyses in order to:

1. Take the facility to a safe condition and keep it in this condition in the long term.
2. Limit the radiological consequences of foreseeable operating events and design basis accidents to within the specified limits.

Safety significant element: An element that is not part of a safety element but:

1. To whose operation credit is given to mitigate foreseeable operating events or accidents, or which is used in the emergency operating procedures.
2. Whose failure might prevent safety elements from performing their safety function.
3. Whose failure might cause the actuation of a safety element.

Design extension: Set of measures forming part of the defence in depth of the facility and whose objective is to improve the safety of the plant by reinforcing its capacity to withstand situations more demanding than those considered in the design basis, as well as to reduce radioactive emissions to the environment. Consideration is given to two categories of design extension conditions (DEC):

DEC-A: when it is possible to prevent severe damage to the fuel, both in the core and in spent fuel storage systems.

DEC-B: when severe damage to the fuel is postulated.

Concurrent failure: a failure additional to and independent from the postulated failure, applied to a component in the same system or in another.

Single failure: An independent event that causes loss of a component for the performance of its safety function. Those multiple failures that might occur as a result of a single event are considered single failures. Electrical and fluid systems are considered to be designed to withstand single failures if the system maintains its capacity to perform its safety functions in the event of a single failure of any active component (assuming that all the passive components operate correctly), or of any passive component (assuming that all the active components operate correctly).

Safety function: functions aimed at preventing the postulated accidents or at mitigating their consequences, the result being the protection of the workers, public and the environment against undue risks caused by radiation.

Safety limits: Limits established for important process variables that have been proven to be necessary to reasonably maintain the physical barriers that protect against the uncontrolled release of radioactivity off site.

Licence limit: Numerical value established with respect to a process variable, used in accident analysis, that guarantees conservatively or with a sufficient degree of probability and confidence the verification of an acceptance criterion. The licence limit may coincide with the safety limit or introduce conservatism additional to it.

Deterministic methodology: An accident analysis methodology characterised by establishing acceptance criteria in terms of the maximum acceptable damage for a postulated initiating event frequency. Normally, conservative hypotheses will be adopted for the mapping of each design basis event as regards the operability of the systems, without consideration of the probability of their failure.

Conservative deterministic methodology: A deterministic methodology that uses conservative initial and bounding conditions, as well as codes giving rise to conservatively biased predictions.

Realistic deterministic methodology: A deterministic methodology characterised by the use of best estimate codes. Realistic methodologies are further divided into those that make use of conservative initial and bounding conditions and those that perform a statistical treatment of the uncertainties associated with these conditions and of the calculation models used, with intermediate approaches also possibly applied. In any case, the overall conservatism of the results obtained must be guaranteed.

Controlled shutdown: Process of shutting down and cooling down the facility during which the limits of the operating specifications may have been exceeded or the deployment of the emergency procedures may have been required to mitigate the consequences.

Orderly shutdown: Process of shutting down and cooling down the facility, scheduled or otherwise, automatic, emergency or forced, during which the limits of the operating specifications have not been exceeded, although the automatic actuation of the protection or safeguards systems and manual operator actions may have been required.

Redundancy: Availability of alternative structures, systems or components (similar or different), such that any one of them may undertake the required function independently of the operational status or failure of the others.

Operational dose restriction: Dose value that, if exceeded during the operation of the facility, implies specific decision-making and actions. This value is lower than the legal public dose limit and than the maximum value established by the Administration, in accordance with article 6, Title II of the Regulation on the Protection of Health against Ionising Radiations (RPHIR), in the process of optimising the radioactive effluents of nuclear power plants.

Safe situation: For the purposes of article eleven, «design basis event acceptance criteria», a safe situation is considered to be that in which the acceptance criteria applicable to the postulated initiating event are verified.

Design basis event: For each postulated initiating event, the set of hypotheses and initial and bounding conditions that make it possible to ensure the enveloping nature of all the evolutions foreseen for the initiating event in question.

Postulated initiating event: An event defined during design as being capable of giving rise to foreseen operating events or accident conditions. The primary cause of a postulated initiating event may be the failure of an item of equipment or an operator error, either inside the facility or outside, caused by mankind or by natural events.

Foreseeable operating event: An operating condition that deviates from normal operation and that is expected to occur one or more times during the lifetime of the nuclear facility. The criteria used in designing the facility mean that these events do not cause significant damage to safety significant elements or give rise to accident conditions.

Safe shutdown earthquake: Earthquake of maximum intensity considered in the design of the plant and allowing the latter to be taken to the safe shutdown condition in the event of such earthquake occurring.

Mission time: Period of time during which a system or component has to operate in order to perform its function satisfactorily.

Analytical value: Value adopted by certain variables and parameters of the data of a calculation model. In determining this value, consideration shall be given to all uncertainties and biases, including those deriving from its supervision in the facility.

Calculated limit value: Calculated value of safety variables, obtained through the use of accepted methodologies, and giving rise to the minimum licence limit margin.

Safety variable: Variable for which an acceptance criterion has been established in accident analysis.

Low population density zone: Area encompassing or surrounding the exclusion zone and containing residents in a number and density such that there is a reasonable probability of suitable measures being adopted successfully for their protection in the event of an accident involving severe damage to the fuel.

The low population density zone should be located inside the preferential attention area defined in the Basic Nuclear Emergency Plan (PLABEN).

Three. *Responsibilities of licensee*

The licensee shall be responsible for the following:

A. The completeness, rigour and accuracy of the contents of accident analysis for his facility, as well as the maintenance, custody and accessibility of the documentation constituting such accident analysis in keeping with Nuclear Safety Council Instruction IS-24, of May 19th 2010, regulating the filing and retention periods of nuclear facility documents and records.

B. Consistency between the design basis of safety significant structures, systems and components and corresponding accident analysis.

C. Operation of the facility under conditions covered by accident analysis.

Four. *Contents of accident analysis*

In the case of the postulated initiating events contemplated in the design basis of the facility, the accident analysis shall contain at least the following set of studies:

A. Description of analysis methodology used,
B. Detailed listing of postulated initiating events,
C. Classification of postulated initiating events,
D. Identification and definition of design basis events,
E. Set of hypotheses regarding failures and operability of systems and components,
F. Initial and bounding conditions and actuation setpoints of safety systems,
G. Applicable acceptance criteria,
H. Results analysis.

It shall also incorporate a study of extension of the design, as described in article thirteen.

Five. *Analysis methodology.*

The methodology required for the performance of the accident analysis shall be deterministic in nature and shall be made up of analytical tools, models and design procedures. This methodology shall be duly documented. The development, validation, maintenance, revision and application of the methodology shall be compliant with the applicable licensing basis, in keeping with technical standards and best practices and subjected to an appropriate process of quality assurance (process internal to the licensee or required by the latter of his contractors).

Modification of the methodology shall be carried out in accordance with the provisions of CSN Instructions of IS-02, on documentation dealing with refuelling outages at light water nuclear power plants, and IS-21, on the requirements applicable to modifications at nuclear power plants.

Six. *Postulated initiating events.*

Accident analysis shall identify the set of postulated initiating events that might affect the safety of the facility from any operating condition.

A. In order to determine this set of initiating events, accident analysis shall:

1. Identify the radioactive materials present at the facility and their location.
2. Identify the physical barriers included in order to contain the dispersal of radioactive material or to protect against the ionising radiations given off by it.
3. Identify the failure mechanisms of these barriers and scenarios compatible with the design of the facility that might give rise to their failure.
4. Postulate initiating events for each scenario.
5. Conservatively estimate the frequency of occurrence of the postulated initiating events.

B. In determining the set of postulated initiating events, consideration shall be given to events such as pipeline breaks, equipment failures and operating errors, as well as to events occurring as a result of them. The list of events to be considered shall be specific to each facility and may be affected by modifications to the design of the plant or other circumstances. Appendix I contains a set of events to be considered under this heading for the purposes of illustration.

Seven. *Classification of postulated initiating events.*

Each postulated initiating event shall be classified on the basis of its frequency of occurrence.

For determination of this frequency, use may be made of the reference standards, probabilistic methods, operating experience, qualified databases, expert judgement or, in general, any method that reflects the state of the art in this area.

A. The postulated initiating events shall be classified as follows:

1. Category I: normal operation of the facility and other events having a frequency of more than 1/reactor-year, which will be accommodated by the facility control and limitation systems and by routine operator operations.
2. Category II: foreseeable operating events with a frequency of occurrence of between 1/reactor-year and 0.1/reactor-year.
3. Category III: foreseeable operating events with a frequency of occurrence of between 0.1/reactor-year and 0.01/reactor-year.

4. Category IV: accidents not foreseeable during the lifetime of the facility but whose consequences could give rise to the emission of important quantities of radioactive material. In view of the severity of these accidents, they are limiting events that the design of the systems, structures and components must be capable of addressing.

B. Alternatively, classifications different from that indicated in the previous paragraph may be established, which must at least differentiate between normal operation, foreseeable operating events and accidents.

C. When contemplated in the design of the facility, the classification may be drawn up taking into consideration the frequency of the postulated initiating event, the probability of operating under the postulated conditions and the probability of failure of the safety systems whose operation is required.

D. Whatever the type of classification, if events are reclassified there shall be confirmation that the accumulated frequency of the postulated initiating events belonging to the new category in which the reclassified event is included will not exceed the upper limit established for it. If this were the case, the postulated initiating events or a sub-group of such events should be relegated to a lower category.

Eight. *Design basis events.*

For each postulated initiating event, the combination or combinations of the hypotheses and initial and bounding conditions that, for each operating situation, give rise to the most severe conditions that the structures, systems and components required will have to withstand shall be determined. For the determination of the initial conditions of category II, III and IV initiating events, consideration shall be given to the event's leading to one of the operating evolutions contemplated in category I.

Consideration shall also be given to the credible combinations of internal and external events included in the design basis of the facility that, given their magnitude and effects, might give rise to a postulated initiating event or increase the seriousness of its consequences. Probabilistic methods and expert judgement may be used for the selection of credible combinations.

Given that these events encompass other similar events of lower severity, they shall constitute the design basis for safety structures, systems and components; in each case it will be necessary to identify the initiating event or events that serve as the design basis and that determine the loads to which such structures, systems and components are subjected, their functional capacity and their operability requirements, as appropriate.

Nine. *Hypotheses regarding the failures and operability of systems and components in design basis event analysis.*

For each initiating event the accident analysis shall describe the set of hypotheses assumed regarding the failures, operability and capacity of the systems and components and the operator actions required.

A. In the case of non-safety related systems and components, the condition of inoperability will be assumed if it is more limiting for the case under analysis than that associated with the response expected by design. Nevertheless, by means of the corresponding justification to be incorporated in the description of the event, credit may be given to these systems and components when their inoperability is detectable, the probability of random failure during the event is highly unlikely and inoperability is not a result of the event itself.

In addition, when used as a back-up protection, these systems and components shall be subject to adequate surveillance programmes or requirements.

B. As regards the demands made of safety systems or components, failures additional to and independent from the initiating event itself shall be imposed. It will not be necessary to impose more than one failure or inoperability on the set of systems, components and operator actions unless this is required in some other way, the operating status of the facility so determines or it is a result of the design characteristics of the structures, systems or components of the facility.

C. It will not be necessary to assume the failure of a passive component, as long as it is possible to justify that the failure of this component is highly unlikely and that it is not affected by the postulated initiating event and, furthermore, this should be justified taking into account the loads and environmental conditions and the total time interval as from the initiating event during which the operation of this component is necessary. In this respect, highly reliable single active components that do not require external forces for their actuation may justifiably be assimilated to passive components.

D. With the limitations established in the previous paragraphs, accident analysis shall demonstrate that there is a sufficient degree of redundancy and diversity, such that a single failure in safety systems and components does not compromise any safety function, in which respect the analysis shall contemplate the entire set of all possible initiating event combinations, including the spurious actuation of systems and components and the single failure of the set of safety systems and components of which demands are made. When the initiating event affects a redundant system carrying out a safety function, it will not be necessary to postulate the failure of the other single or multiple redundancies as a single additional failure, unless this is the consequence of or responds to a common mode failure.

E. The postulated failures will not be considered additional failures as long as they are the result (or have one same common cause as their origin) of the initiating event, the postulated failure or the very evolution of the accident.

F. In the case of category II, III and IV events, no operator action will be postulated in the thirty minutes following the onset of the event. If such actuation were exceptionally required, then in addition to being included in suitable procedures ensuring a high degree of reliability of the action, the capacity to perform it shall be validated, along with the actuation times involved, conservatively determined through the use of techniques reflecting the state of the art.

G. For the analysis associated with any initiating event requiring actuation of the reactor quick shutdown system, the value of negative reactivity corresponding to the highest value control rod shall be subtracted from the value for the system, unless it is demonstrated that its impact on the dynamics of the event is irrelevant. In any case, demonstration of the shutdown margin will require the hypothesis of a seized control rod to be taken into account.

H. The capacity to fully insert the control rods shall be demonstrated for any postulated initiating event, including manual tripping, arising as a result of the safe shutdown earthquake.

Ten. *Initial and bounding conditions and actuation setpoints of safety elements.*

Accident analysis shall include a description of the set of initial and bounding conditions used, including the analytical values of the actuation setpoints of safety elements and their determination.

A. Determination of the initial and bounding conditions and actuation setpoints of safety elements is part of the analysis methodology.

B. The initial and bounding conditions or any sub-set thereof shall adopt values enveloping the authorised operation. Methodologies using a statistical treatment of the uncertainties associated with these conditions, in part or in full, shall be required to demonstrate their conservatism.

C. The safety limits, the limiting conditions for operation and their applicability, as reflected in the Technical Specifications, shall be established such that consistency is maintained with the analytical methodology used to obtain them, with safe operation being guaranteed in all cases.

D. The assignment of the instrumentation and safety element actuation setpoints considered in the analyses, on the basis of the values controlled by the Technical Specifications, shall be accomplished using a methodology that takes into account all the existing uncertainties.

Eleven. *Design basis event acceptance criteria.*

A. The following acceptance criteria shall be verified in order to demonstrate the safety of the facility:

1. The radiological consequences for the public shall be as low as reasonably possible and below the following limits:

1.1 Category I: The doses affecting the members of the public as a result of the release of radioactive material shall not lead to the dose limits established in the regulation on the protection of health against ionising radiations (RPHIR) being exceeded.

1.2 Category II: The doses affecting the members of the public as a result of the release of radioactive material shall not lead to the dose limits established in the RPHIR being exceeded.

1.3 Category III: The emissions of radioactive material may give rise to the dose limits for members of the public established in the RPHIR being exceeded beyond the boundaries of the exclusion zone, but the reference values established in the Basic Nuclear Emergency Plan (PLABEN) for the adoption of urgent protection measures will not be exceeded.

1.4 Category IV: The off-site emissions of radioactive material shall not give rise to a situation in which a person located at the boundary of the exclusion zone for 2 hours or in the low population density zone throughout the time taken for the radioactive cloud to pass may receive an effective dose of more than 250 mSv. Fractions of this limit may be applied, depending on the frequency of the accident or the methodology used. In addition, adequate measures shall be available to ensure that the control room personnel do not receive a dose of more than 50 mSv at any time during the accident.

If a classification other than that mentioned in article seven A is used, the limits of the new classification shall be adapted to what has been set out in the previous paragraphs, taking into account the frequency of the initiating events for each category.

Equivalent dose limits may be used when this is contemplated by the methodology used, which shall guarantee similar levels of protection.

2. Events classified as category I shall be accommodated by the normal operation of the facility with a sufficient margin, such that the automatic or manual actuation of the protection system is not required. Category II events shall allow for the orderly shutdown of the facility and its return to operation without safety restrictions following the clearing of the original cause of the event and of the damage. Category III and IV events shall allow for the controlled shutdown of the facility.

3. The minimum degree of integrity of the barriers against the release of radioactive material shall be specified on the basis of the category assigned to the initiating event and with sufficient margin, such that the radioactive material released does not compromise the dose limits established in A.1.

The acceptance criteria associated with the integrity of the barriers shall be established with respect to those variables that govern the physical processes affecting them. Nevertheless, depending on the analytical methodologies, substitute variables may be used as long as they guarantee the minimum barrier integrity required if not exceeded. The establishment of safety limits shall be supported by experimental results, complemented where appropriate by analytical studies incorporating an adequate analysis of the existing uncertainties. The ageing of the affected structures may be contemplated, where appropriate, in defining the acceptance criteria. For the purposes of illustration, Appendix II includes a set of parameters and variables habitually used to establish acceptance criteria in barrier integrity analysis.

4. The capacity of the structures, systems and components, and the reliability of operator actions fulfilling a safety function, shall be preserved in those events in which their actuation is required, assuming any combination of worst single failure when it does not, in itself, constitute a postulated initiating event.

5. No initiating event shall evolve into another of higher category without the existence of another failure additional to the single failure considered.

6. The stable final condition of the facility, following an initiating event, shall guarantee compliance with the basic safety functions: subcriticality, cooling of nuclear fuel and confinement compatible with compliance with the applicable radiological criteria.

7. Criticality accidents shall verify the dual contingency criterion, according to which these accidents cannot occur unless two unlikely and independent changes in the process conditions take place simultaneously. In any case, the safety limits established for criticality shall be verified.

8. The licensing limit may not be exceeded for any postulated initiating event whose evaluation methodology does not include the performance of an uncertainty analysis to obtain the calculated limit value. In the case of evaluation methodologies that include the analysis of uncertainties, a margin shall be established with respect to the licensing limit for each postulated initiating event, in terms of the probability of the licensing limit not being exceeded, with a given degree of confidence. Unless otherwise required, a probability value of 95% with a degree of confidence of 95% is considered acceptable. In remaining cases in which the established limits are exceeded, it shall be demonstrated that the damage caused is acceptable.

B. For each postulated initiating event, the feasibility of the manual actions to be performed shall also be verified, taking into account the environmental conditions (radiation levels, temperature, toxic gases, etc.) in those places in which such actions are to take place, along with the availability of the necessary equipment and instrumentation allowing a stable long-term condition to be achieved.

C. Regardless of the classification frequency of the postulated initiating events, the facility shall be designed such that the consequences of these events are reduced to the reasonably achievable minimum level.

In view of the above, the response expected from the facility to any postulated initiating event shall be within one of the options indicated in the following sections (in order of preference):

1) A postulated initiating event does not give rise to any important safety-related effects or only causes the facility to evolve towards a safe situation because of its intrinsic characteristics.

2) Following a postulated initiating event, the facility returns to a safe situation through the actuation of passive safety elements or the actuation of safety systems operating continuously under the conditions in which the postulated initiating event occurs.

3) Following a postulated initiating event, the facility returns to a safe situation through the actuation of safety systems to be placed in service in response to the postulated initiating event.

4) Following a postulated initiating event, the facility returns to a safe situation through feasible manual actions included in procedures.

D. In multiple group sites, each group shall have the capacity to respond independently to initiating events common to all or to initiating events affecting one group and caused by another.

Twelve. *Analysis of results.*

For each design basis event, the corresponding analysis shall contain a detailed description of the relevant phenomena and of the results obtained, a table with a chronological breakdown of important events, the figures and curves necessary to better understand the accidents modelled, the calculated safety variables limit values and the margin obtained between the calculated limit value and the licensing limit.

When the accident analysis contemplates manual safety-related operator actuations, these shall be documented considering the single failure criterion, along with the manipulations implied by the required actuations and the indications and alarms to which credit is given during the accident. If credit is to be given to actuations outside the control room, the feasibility of such actuations shall be documented, with consideration given additionally to the aspects of accessibility, habitability, visibility, communications, protection, tools and equipment.

The time scope of the analysis shall extend to the moment in which a stable state is achieved in the facility, with the basic safety functions recovered.

Thirteen. *Design extension.*

The accident analysis for the facility shall be complemented with a study of the extension of its design.

A. This article addresses the treatment of scenarios belonging to the DEC-A category design extension. DEC-B category scenarios are not part of the subject matter of this Instruction.

B. The facility design extension study shall have the following objectives:

1. Study of the performance of the plant, including interactions between groups in the case of sites with more than one group, or close to other sites, in response to specific accident scenarios whose hypotheses exceed those considered in the design basis of safety-related structures, systems and components.

2. Determination of the possibility of improving the design of existing structures, systems and components, incorporating new structures, systems and components or implementing procedures or other measures, such that these actions contribute to reasonably minimising the risk to the population and the environment of harmful exposures to ionising radiations, and assurance of the existence of a margin with respect to limit situations in which minor variations of parameters give rise to disproportionate changes to the consequences.

3. Identification of reasonable measures allowing severe damage to the fuel to be prevented, such that this be extremely unlikely with a high degree of confidence.

C. Selection of DEC-A category events.

1. The selection of events to be analysed shall be justified on the basis of deterministic and probabilistic arguments and of engineering judgement.

2. The selection process shall take into account all those events or combinations of events that cannot be considered extremely unlikely with a high degree of confidence and that might give rise to accident conditions more severe than those considered in design basis accidents.

This selection process shall contemplate the following:

Any plant operating condition
Its origin in on or off-site risks
Common cause failure modes
The presence of more than one group on the site
Events having an impact on the site groups and on interactions between them or on other nearby groups.

Appendix III includes an illustrative list of events to be considered in the analysis of design extension, excluding those already incorporated in the design basis.

D. Consideration shall be given to the set of credible accident sequences beyond the design basis of the facility and with respect to which it is reasonably feasible to implement prevention or mitigation measures. For the selection of these scenarios, use shall be made of a combination of deterministic methods, probabilistic analysis and engineering judgement.

E. Safety assessment methodology and contents.

1. The methods and hypotheses used shall reflect the foreseeable conditions and evolution in an overall conservative manner, but without this conservatism detracting from the expected evolution of the facility.
2. The methodology and assessment shall take into consideration both the uncertainties and their impact, with special attention to those cases in which use is made of expert judgement.
3. Resources and possibilities for the prevention of damage to the fuel by improving the capacity of the facility to withstand more serious scenarios than those contemplated in the design basis shall be identified.
4. The possible radiological consequences shall be assessed when, given their magnitude, they may exceed the maximum acceptable included in the design basis of the facility.
5. Consideration shall be given in the study to the configuration, location and capacities of the equipment, the conditions expected in each scenario and the feasibility of the actions foreseen for management of the accident.
6. Consideration shall be given in the assessment to the information on the availability of systems obtained from probabilistic safety assessments, allowing the probability of the sequences for analysis to be estimated.
7. A final safe status and mission times shall be defined for the structures, systems and components of which demands are made.
8. The analyses of these accidents shall make use of tools qualified for this purpose.

F. Design extension analysis shall be used to define the design basis of the systems required to prevent the appearance of the conditions postulated in this analysis or, if they occur, to be able to control them and mitigate their consequences.

G. The result of this analysis shall be incorporated in the Safety Assessment as an appendix associated with accident analysis.

Fourteen. *Exemptions.*

The licensees of nuclear power plants subject to this instruction may request that the CSN grant them exemption from compliance with certain of its requirements, justifying and documenting the reasons for such request and incorporating a safety assessment. Likewise, the way in which the alternative or compensatory measures established are met shall be included.

Fifteen. *Infringements and sanctions.*

The present Council Instruction shall be binding, in compliance with the requirements of article 2.a) of Law 15/1980, of April 22nd, creating the Nuclear Safety Council, as a result of which non-compliance will be penalised as set out in Chapter XIV (articles 85 to 93) of the Nuclear Energy Act, Law 25/1964, of April 29th.

Single transitory provision.

The holders of operating permits for nuclear power plants shall have a period of three years as from the publication of this Instruction in which to adapt to its contents. Within one year as from its publication, each licensee shall submit to the CSN an adaptation programme for the correction of whatever deviations might be identified, in order to meet the requirements set out in the present Instruction. This programme shall require approval from the CSN. Adaptation to the contents of this Instruction will not necessarily imply a revision of the methodologies or of the analyses currently in force in the Safety Study, to the extent to which the applicable acceptance criteria and radiological consequences established in this Instruction are verified.

Single derogatory provision.

All provisions of equal or lower rank that oppose what is set out in the present Instruction are hereby repealed.

Single final provision

The present Instruction shall enter into force on the day following its publication in the «Official State Gazette».

Madrid, January 21st 2015.– The President of the Nuclear Safety Council, Fernando Marti Scharfhausen.

APPENDIX I

Illustrative list of postulated initiating events in light water reactors and fuel pools

1. Loss of coolant accidents caused by small, medium-sized and large reactor coolant pressure boundary breaks, including rupture of the largest diameter pipe forming part of this boundary, and effects on containment.
2. Main steam and feedwater system ruptures.
3. Increasing or decreasing reactor coolant flow.
4. Increasing or decreasing feedwater flow.
5. Increasing or decreasing feedwater temperature.
6. Increasing or decreasing main steam flow.
7. Spurious opening of pressuriser relief or safety valves (PWR).
8. Spurious actuation of the emergency core cooling system.
9. Spurious opening of steam generator relief or safety valves (PWR).
10. Spurious opening of main steam system relief/safety valves (BWR).
11. Spurious isolation of main steam lines.
12. Steam generator tube rupture (PWR).
13. Failure of control rod control system.
14. Uncontrolled withdrawal of control rods, rod drop and rod ejection (PWR).
15. Boron dilution accident.
16. Thermohydraulic instability (BWR).

17. Chemical and volume control system failures (PWR).
18. Turbine runback/trip.
19. Uncontrolled load increase.
20. Pipe rupture or heat exchanger tube leakage in systems connected to the reactor coolant circuit and located fully or partially outside containment.
21. Fuel handling accidents during refuelling and fuel inspection and movement activities.
22. Accidents involving erroneous positioning of fuel in the reactor or in the storage racks.
23. Transients originating in disturbances of the off-site electricity grid and loss of this grid.
24. Releases of radioactive material from waste treatment systems or components or storage tanks.
25. Dropping of heavy loads due to failure of hoisting systems.
26. Other criticality accidents.
27. Transients involving the spurious injection of mass and energy in the reactor coolant system during shutdown (PWR).
28. Fuel pool coolant inventory increase or decrease accidents.
29. Fuel pool coolant loss or reduction accidents.

APPENDIX II

Illustrative list of parameters and variables habitually used to establish acceptance criteria in barrier integrity analysis

Fuel

Variable/parameter:

Critical heat flux.
Criticality.
Shutdown margin.
Enrichment.
Depositing of materials on cladding.
Fuel cladding stresses, deformation and fatigue.
Fuel cladding oxidisation and hydriding.
Fuel rod internal gas pressure.
Thermo-mechanical loads and pellet-cladding mechanical interaction (PCMI).
Fuel fragmentation and cladding failure.
Cladding embrittlement.
Rod leak rate and census.
Maximum cladding temperature.
Linear power generation.
Hydrogen generation.
Dynamic loads in handling, normal operation and accidents, including earthquakes and transport.
Attachment loads.
Fuel temperature and meltdown.
Gap and coolant activity.
Burnup.
Source term.

Reactor coolant and secondary systems (PWR)

Variable/parameter:

Design pressure.
Design temperature.
Pressure and temperature limits in vessel.
Coolant activity.
Pressure boundary leak rate.

Containment

Variable/parameter:

Peak containment pressure.
Peak containment temperature.
H_2 concentration.
Drywell/Wetwell differential pressure (BWR).

APPENDIX III

Illustrative list of events to be considered in design extension analysis

1. Anticipated transients without scram.
2. Total loss of alternating current power supply (on and off-site).
3. Loss of ultimate heat sink.
4. Total loss of component-cooling or essential services water system.
5. Loss of coolant accident combined with total loss of an emergency core cooling system.
6. Total loss of feedwater flow in PWR's.
7. Multiple steam generator tube rupture (PWR).
8. Loss of core cooling due to failure of residual heat removal system.
9. Long-term loss of safety systems following a postulated initiating event.
10. Loss of spent fuel pool cooling.
11. Uncontrolled boron dilution in PWR reactors and in fuel pools with credit for dissolved boron.
12. Uncontrolled loss of level in pressurised water reactors during half loop operation or refuelling outages.