TECHNICAL GUIDELINES FOR THE DESIGN AND CONSTRUCTION OF THE NEXT GENERATION OF NUCLEAR POWER PLANTS WITH PRESSURIZED WATER REACTORS

Adopted during the GPR/German experts
plenary meetings held on October 19th and 26th 2000

Contents

INTRODUCTION AND SCOPE OF APPLICATION

These technical guidelines present the opinion of the French Groupe Permanent chargé des Réacteurs nucléaires (GPR) concerning the safety philosophy and approach as well as the general safety requirements to be applied for the design and construction of the next generation of nuclear power plants of the PWR (pressurized water reactor) type, assuming the construction of the first units of this generation would start at the beginning of the 21st century. These technical guidelines are based on common work of the French Institut de Protection et de Sûreté Nucléaire (IPSN) and of the German Gesellschaft für Anlagen- und Reaktorsicherheit (GRS). Moreover, these technical guidelines were extensively discussed with members of the German Reaktor Sicherheitskommission (RSK) until the end of 1998 and further with German experts.

The context of these technical guidelines must be clearly understood. Faced with the current situation of nuclear energy in the world, the various nuclear steam supply system designers are developing new products, all of them claiming their intention of obtaining a higher safety level, by various ways. GPR believes that, for the operation of a new series of nuclear power plants at the beginning of the next century, the adequate way is to derive the design of these plants in an "evolutionary" way from the design of existing plants, taking into account the operating experience and the in-depth studies conducted for such plants. Nevertheless, introduction of innovative features must also be considered in the frame of the design of the new generation of plants, especially in preventing and mitigating severe accidents.

GPR underlines here that a significant improvement of the safety of the next generation of nuclear power plants at the design stage is necessary, compared to existing plants. If the search for improvement is a permanent concern in the field of safety, the necessity of a significant step at the design stage clearly derives from better consideration of the problems related to severe accidents, not only in the short term but also in the long term, due to the potential contamination of large areas by long life radionuclides like caesium ; for existing plants, improvements are implemented on a pragmatic basis within the limits of their actual design and within the current process of periodic safety reassessments of the plants.

GPR believes that a significant step at the design stage is possible in the "evolutionary" way if due consideration is given to the lessons learned from operating experience and from probabilistic studies performed for existing plants as well as to results of safety research, notably on severe accidents, with the view to obtaining reduction of the calculated probabilities of occurrence and of the calculated accidental releases of radioactive materials. Research and development work performed during the design stage (and subsequently during operation) will also contribute to the improvement of safety or to the validation of system and plant behaviour.

A - PRINCIPLES OF THE SAFETY CONCEPT

A.1 - General safety approach

The significant improvement of the safety of the next generation of nuclear power plants, compared to existing plants, is specified by the following objectives.

A.1.1 - General safety objectives

a) For normal operation and abnormal occurrences, one objective is the reduction of individual and collective doses for the workers, which are largely linked to maintenance and in-service inspection activities. Reduction of the occupational exposures shall be aimed at by an optimization process taking into account the data obtained from operating experience. Consideration must also be given to the limitation of radioactive releases within the corresponding dose constraints, and to the reduction of quantities and activities of radioactive wastes.

b) Another objective is to reduce the number of significant incidents, which involves seeking improvements of the equipment and systems used in normal operation, with a view to reducing the frequencies of transients and incidents and hence to limiting the possibilities of accident situations developing from such events.

c) A significant reduction of the global core melt frequency must be achieved for the nuclear power plants of the next generation. Implementation of improvements in the "defence-in-depth" of such plants should lead to the achievement of a global frequency of core melt of less that 10^{-5} per plant operating year, uncertainties and all types of failures and hazards being taken into account.

d) Moreover, an important objective is to achieve a significant reduction of potential radioactive releases due to all conceivable accidents, including core melt accidents.

For accident situations without core melt, there shall be no necessity of protective measures for people living in the vicinity of the damaged plant (no evacuation, no sheltering).

Accident situations with core melt which would lead to large early releases have to be "practically eliminated" : if they cannot be considered as physically impossible, design provisions have to be taken to design them out. This objective applies notably to high pressure core melt sequences.

Low pressure core melt sequences have to be dealt with so that the associated maximum conceivable releases would necessitate only very limited protective measures in area and in time for the public. This would be expressed by no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no long term restrictions in consumption of food.

A.1.2 - The "defence-in-depth" principle

The "defence-in-depth" principle remains the fundamental principle of safety for the nuclear power plants of the next generation, with the implementation of several levels of protection including successive barriers against the release of radioactive substances to the environment.

This principle has to be used to demonstrate that the three basic safety functions - reactivity control, cooling the fuel and confining radioactive substances - are correctly ensured. The aim is to ensure protection of the public and of the workers. This includes accident prevention as well as accident mitigation.

For the next generation of nuclear power plants, the general safety objectives set in section **A.1.1** imply to reinforce the "defence-in-depth" of these plants compared to existing plants ; these objectives notably call for a more extensive consideration of the possibilities of multiple failures and the use of diversified means to fulfill the three basic safety functions mentioned above ; they also call for a substantial improvement of the containment function, considering in particular the different possible failures of this function for core melt situations. Results of operating experience as well as results of in-depth studies like probabilistic safety assessments conducted for pressurized water reactors and the progress in knowledge of the physical phenomena which may occur during the development of accident situations, particularly core melt situations, have to be taken into account.

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

In particular, special attention at the design stage has to be given to shutdown states with particular allowance for the specific operating modes required by the actions performed during shutdown periods.

It is also underlined that the quality of design, manufacturing, construction and operation is essential for safety in the frame of the first level of "defence-in-depth". Quality must be obtained and demonstrated notably by an adequate set of requirements for design, manufacturing, construction, commissioning and operation, as well as by quality assurance.

Moreover, due consideration must be given at the design stage to inspectability and testability of equipment as well as to the possibility of replacement of some equipment, considering that maintenance and testing activities are essential to maintain the safety of the plant throughout operation.

A.1.3 - General strategy related to severe accidents

The general objectives set in section **A.1.1** have the following general implications concerning severe accidents.

a) "Practical elimination" of accident situations which would lead to large early releases

- Accident sequences involving containment bypassing (via the steam generators or via circuits connected to the primary system which exit the containment) have to be "practically eliminated" by design provisions (such as adequate piping design pressure) and operating provisions, aimed at ensuring reliable isolation and also preventing failures.
- Special attention shall be given to shutdown states and open containment building.
- Reactivity accidents resulting from fast introduction of cold or deborated water must be prevented by design provisions so that they can be "excluded".
- Overpressurization of the primary circuit must also be prevented as far as necessary by design provisions and operating procedures so as to contribute in particular to the "exclusion" of the reactor pressure vessel rupture.
- High pressure core melt situations must be prevented by design provisions (such as diversity and automatic actuation) for the secondary side safety systems and if necessary for the reactivity control and primary feed and bleed systems. It must be a design objective to transfer high pressure core melt to low pressure core melt sequences with a high reliability[1] so that high pressure core melt situations can be "excluded". The depressurization must be such that loads from ejected melt into the containment atmosphere ("direct containment heating") and loads on the reactor pressure vessel support and cavity structures can be coped with.
- Global hydrogen detonations and in-vessel and ex-vessel steam explosions threatening the containment integrity must be "practically eliminated".

b) Mitigation of low pressure core melt accident situations

- As regards containment leaks, there shall be no path of direct leakage from the containment building to the outside. Pipes liable to carry radioactive substances outside the containment building shall lead to peripheral buildings providing adequate confining capabilities. Improvements must be sought for the permanent surveillance of the containment building leaktightness. Penetrations through the pressure boundary of the containment have to cope with loads from core melt sequences.

- Due consideration must be paid to the different aspects of a spray system inside the containment building for severe accident situations. This system allows lowering both the pressure and the radioactive aerosols concentrations in the containment building ; however a spray system reduces the inerting influence of steam and increases the flame velocity of hydrogen combustion.

[1] As an orientation, the equipment used to depressurize the primary circuit has to be as reliable as the relief valve system used to prevent an overpressurization.

- The residual heat must be removed from the containment building without venting device ; for this function, a last-resort heat removal system must be installed.

- Concerning the possible formation of combustible gas mixtures, the containment building must be designed to withstand the global deflagration of the maximum amount of hydrogen which could be contained in this building in the course of core melt accidents and also to withstand a representative fast local deflagration. Besides, provisions must be taken with respect to local detonations and to possibilities of deflagration to detonation transition (DDT) sequences which might jeopardize this building and its internal structures. Limitation of the concentrations of combustible gases by design of internal structures and the use of catalytic devices have notably to be considered.

- The penetration of the basemat of the containment building by a "corium" must be avoided, as this phenomenon could imply significant releases and durable contamination of underground waters and of the sub-soil. Moreover, adequate provisions have to be implemented to prevent leakage of contaminated water and gases to the sub-soil via cracks in the basemat.

A.1.4 - Safety demonstration

The safety demonstration for the nuclear power plants of the next generation has to be achieved in a deterministic way, supplemented by probabilistic methods and appropriate research and development work.

In this demonstration, single initiating events have to be "excluded" or "dealt with" -that is to say that their consequences are examined in a deterministic way. Single initiating events can be "excluded" only if sufficient design and operation provisions are taken so that it can be clearly demonstrated that it is possible to "practically eliminate" this type of accident situations ; for example, the reactor pressure vessel rupture and other large components (as steam generator secondary side or pressurizer) rupture can be examined in that way.

Other single initiating events can be grouped so as to define a limited number of reference transients, incidents and accidents ; these reference transients, incidents and accidents can be categorized according to the estimated frequencies of the corresponding groups of events. For the different reference transients, incidents and accidents, appropriate technical criteria have to be respected, with conservative assumptions including aggravating failures. It has to be verified that, for the different reference transients, incidents and accidents with radiological significance, assuming the corresponding technical criteria are respected, radiological consequences are tolerable and consistent with the general safety objectives mentioned in section **A.1.1** for accident situations without core melt. Higher radiological consequences can be deemed tolerable for categories of lower estimated frequency.

Complementary to the single initiating events, the safety demonstration has to analyse multiple failure situations as well as internal and external hazards. The safety demonstration with respect to these situations and hazards can be supported by probabilistic assessments. Possible links between internal and external hazards and single initiating events have also to be considered.

A probabilistic safety assessment must be conducted, beginning at the design stage, including at least internal events ; this probabilistic safety assessment would indicate the frequencies of core melt sequences with a view on the possible consequences of the different types of core melt situations on the containment function.

However, the "practical elimination" of accident situations which could lead to large early releases is a matter of judgement and each type of sequences has to be assessed separately. Their "practical elimination" can be demonstrated by deterministic and/or probabilistic considerations, taking into account the uncertainties due to the limited knowledge on some physical phenomena. It is stressed that the "practical elimination" cannot be demonstrated by the compliance with a general "cut-off" probabilistic value.

As for low pressure core melt accidents, due to the wide range of potential accidental conditions in severe accident situations, the achievement of the general safety objectives set in section **A.1.1** has to be demonstrated by the calculation of the radiological consequences of different representative sequences which have to be precisely defined, depending on the design of the plant. For the assessment of the results, the intervention levels proposed by ICRP 63 (for evacuation and relocation) and the EU limits (for food commercialization) can be used as references.

It is underlined that, generally speaking, for incident and accident situations, including core melt situations, radiological consequences calculations must deal with short term and long term consequences, considering the different ways of transferring radioactive materials to the environment (air, surface water, underground water) and to men (irradiation -cloudshine and groundshine-, radionuclides intake by ingestion or inhalation). Notably, atmospheric dispersion and deposition on vegetation, soil and other surfaces have to be determined. The assessment of radiation exposures of critical groups shall take into account realistic assumptions and parameters in particular for living habits, exposure conditions, integration times, meteorological conditions and transfer of radionuclides in the environment.

A.2 - General safety principles

A.2.1 - Plant transient behaviour

Generally speaking, the plant design shall be such that the inherent reactor behaviour is stable (e.g. negative moderator feedback).

Improvements can be achieved by making the plant behaviour less sensitive to operator errors and failures in operational systems, e.g. by proper automatic control and by the provision of sufficiently large coolant capacity in the primary and the secondary systems and in the primary and secondary feed systems. Adequate grace periods have to be obtained for necessary operator actions.

More precisely, prevention of and lower sensitivity to human errors has to be sought by increase of design basis margins, by use of passive systems or systems using more passive features, by simplification of the design and by limitation of interactions between systems, while taking care not to overlook the possible advantages of functional redundancy, by more extensive automation of safety systems for specific situations and by improvements of the man-machine interface so as to provide the operators with additional reaction time and reliable information to diagnose the actual plant behaviour.

To the extent possible, unnecessary safety system actuation shall be avoided. To avoid such actions, the introduction of appropriate limitation functions may be advisable, that are additional control functions which act when the operational control systems are not capable of keeping controlled variables within specified limits for normal operation. Sufficient margins shall be provided with respect to the safety limits, taking into account both measurement uncertainties and abnormal plant behaviour due to minor disturbances or operator errors.

A.2.2 - Redundancy and diversity in the safety systems

For events which are not controlled by the operational systems and/or limitation functions, protection and safeguard systems are required to bring and to maintain the plant in a safe state with respect to subcriticality, core cooling and confinement of radioactive materials. The reliability of these systems must be consistent with the general objective of reducing the frequencies of occurrence of accidents, taking into account the estimated frequencies of initiating events and the durations of the corresponding actions of the systems.

This reliability has to be achieved through an adequate combination of redundancy and diversity. Due attention has to be paid to the fact that possible common cause failures limit the potential to reduce the unavailability by adding identical trains (on this point, it is underlined that the unavailability of a redundant safety system consisting of identical trains probably cannot be demonstrated to be less that 10^{-4} per demand), as well as to the fact that diversity can imply more complex systems and maintenance difficulties ; moreover, due consideration has to be paid to the support systems when assessing the benefits from diversified systems or equipment.

Particular attention has to be given to minimizing the possibilities of common cause failures. Physical and spatial separation shall be applied as far as possible. Support functions (energy, control, cooling, etc.) shall be also independent to the largest possible degree. Special emphasis has to be placed on the redundancy and diversity of electrical power supplies. In addition, provisions (including hardware and software diversity) have to be implemented at the level ot the overall instrumentation and control architecture to limit software-induced common cause failures.

A.2.3 - Man-machine interface

Due consideration has to be given to human factors throughout the design stage, taking into account aspects of operation, testing and maintenance, with special emphasis on operating experience.

The general aim is to take advantage of the human abilities, while minimizing the possibilities for human errors and making the plant less sensitive to these errors (see section **A.2.1**). Appropriate consideration has to be given to simplify operation, to minimize human actions necessary to ensure safety functions, to provide for good maintainability, testability and reliable monitoring of the availability of the safety systems.

A comprehensive human factors engineering program has to be implemented. This program must cover also maintenance and testing activities in order to ensure consistency and tracking of human factors issues and design choices in a well-structured and state-of-the-art human factors approach. This human factors engineering program should be implemented by a special program management team which includes human factors experts.

Developing adequate man-machine interfaces shall be applied in all the locations where men interact with technical equipment, taking into consideration teams organization. Besides operation in the control room, this includes testing, repair and maintenance.

Minimizing operator errors and making the plant less sensitive to those errors can be achieved by applying appropriate ergonomic design principles and by providing sufficiently long grace periods for the response. The necessary length depends on the complexity of the situation to be diagnosed and on the actions to be taken.

Sufficient and appropriate information shall be made available to the operators for a clear understanding of the actual status of the plant, including severe accident conditions, and for the clear assessment of the effects of their interventions.

A.2.4 - Protection against internal hazards

Internal hazards can be defined as events originated in the plant with the potential of causing adverse conditions or damages to equipment necessary for the fulfilment of the three basic safety functions mentioned in section **A.1.2**. They include notably failures of pipes, vessels, tanks, pumps, valves as well as floodings, fires, explosions, missiles and load drops.

The "defence-in-depth" principle has to be applied to the protection against internal hazards so as to limit the likelihood and the consequences of such hazards by the implementation of prevention, control and mitigation provisions, consistently with provisions for internal events.

In connection with the definition of the three basic safety functions, not only the buildings containing systems necessary to reach and maintain a safe shutdown state, but also the buildings with systems containing radioactive material have to be considered.

It is stressed that the occurrence of internal hazards during shutdown states has to be considered precisely, taking into account the specific configurations of safety systems and equipment which could be needed during these states.

For the design verification and the safety demonstration relative to the internal hazards, particular attention has to be devoted to assess the completeness of the potential causes of such hazards, including for example erroneous alignment or electromagnetic interference, as well as the possibilities of internal hazards resulting from other plant internal or external events or having the potential to affect the three basic safety functions in more than one of the successive defence-in-depth levels.

A.2.5 - Protection against external hazards

External hazards can be defined as natural or man-induced events originated outside the plant with the potential of adversely affecting the safety of the plant. They include notably earthquakes, airplane crashes and explosions.

External hazards can affect consecutively or simultaneously different lines of defence of the plants and they are site-dependent. In that way, due consideration must be paid to the choice of the sites with a view to not enforce excessive requirements on the design of the corresponding plants. Generally speaking, design provisions must be taken with respect to external hazards, consistently with provisions for internal events and internal hazards ; that is to say, external hazards must not constitute a large part of the risk associated to nuclear power plants of the next generation.

The general objective of the design provisions is to ensure that the safety functions of the systems and components which are required to bring the plant in a safe shutdown state and to prevent and limit radioactive releases are not inadmissibly affected by any external hazard. However, as external hazards are site-dependent, it is not necessary to take into account all these hazards in a standardized design ; such external hazards like external flooding, drought, ice formation and toxic, corrosive or burnable gases, can be dealt with only for a specific plant, depending on the site.

Equipment which is required to function during external events has to be qualified for the range of parameters assumed to occur during such events.

A.2.6 - Use of probabilistic safety assessment

As already stated in section **A.1.4,** a probabilistic safety assessment has to be performed with the following objectives at the design stage : supporting the choice of design options, including redundancy and diversity in the safety systems, well-balanced safety concept and valuation of deviations from present safety practices, appreciation of the improved safety level compared to existing plants.

Evaluation of the results of a probabilistic safety assessment against quantitative probabilistic targets can provide useful guidance. But, generally speaking, quantitative probabilistic targets are not to be seen as requirements ; they are essentially meant to be orientation values for checking and evaluating the design.

Concerning the general methodology, the probabilistic safety assessment can be carried out in two or more steps : a simplified assessment at the conceptual stage, and more complete studies during the engineering phases, when more precise information on the design becomes available.

The simplified assessment, including at least internal events, has to present a preliminary evaluation of the core damage frequency and the corresponding sequences ; furthermore, the designer has to distinguish between the different types of core melt sequences according to their consequences related to containment behaviour.

Moreover, at the conceptual stage, different design alternatives have to be analysed, and sensitivity studies have to be performed. However, the application of a probabilistic safety assessment at an early stage of the design has to be handled cautiously because the final results will be dependent on the real choice of components, system techniques and operational procedures.

It is nevertheless underlined that, even for the first assessment at the conceptual stage, the designer has to consider a list as complete as possible of initiating events. It is stressed that the treatment of common cause failures is essential for the assessment of some design options. Another special concern is the treatment of human interventions, including diagnosis and maintenance. The use of qualified data is also essential.

In the frame of more complete studies, internal and external hazards should be considered along with the development of appropriate methodologies ; moreover, the need and feasibility of a level 2 PSA study might be considered.

A.2.7 - Radiation protection of workers and of the public

A.2.7.1 - Occupational exposures

As stated in section **A.1.1**, reduction of the occupational exposures shall be aimed at by an optimization process taking into account the data obtained from operating experience notably in France and in Germany.

It is underlined that the identification of the relevant radiation protection options is the first step of an ALARA approach which has to be complemented by a comparison assessment of the efficiency of these options. Collective doses as well as individual doses targets shall be defined.

The operating experience shows that possible improvements in individual and collective doses can result from design provisions, e.g. the choice of materials in connection with an adequate water chemistry to avoid corrosion products, shielding devices, better reliability of components, robotics and easy serviceability. In particular, the designer has to consider easy access to the work places, environmental working conditions, development of specific tools and robotics in order to reduce dose rates and/or durations of interventions.

The designer has to consider also, to the extent possible and reasonable, the performance of unscheduled activities such as repair and replacement.

A.2.7.2 - Radioactive releases and wastes

The plant shall be designed to limit, following the optimization principle, the radiation exposure of the public resulting from the discharge of radioactive materials to air or water. The corresponding radiation exposure will be determined for a reference person (member of the critical group) at the most unfavorable receiving point considering all relevant exposure pathways and taking into account discharges from other installations.

In setting release limits for a plant in the licensing process, the specific site conditions will be considered ; due consideration will also be given to allow for further potential man-made contributions to the exposure at the site.

Design provisions have to be made to further reduce the activity and volume of radioactive materials to be removed from the plant as wastes. Taking those materials as a basis, the efforts taken to reduce the releases have to be balanced against the amount of wastes produced by these efforts. Regarding radiation protection, the doses to the public from the releases, the exposures of the personnel and the doses caused by the wastes have to be considered in the optimization process.

B - CONCEPTUAL SAFETY FEATURES

B.1 - Design of barriers

B.1.1 - Fuel cladding and core design

The design of the fuel assemblies for nuclear power plants of the next generation can be based on present reference designs such as 17 x 17 fuel assemblies with UO_2 or UO_2-PuO_2 pellets, the excess of reactivity in fresh fuel assemblies being compensated as far as necessary by burnable poisons (such as UO_2 mixed with Gd_2O_3).

Further improvements in the knowledge of the behaviour of fuel assemblies materials under normal and accident conditions as well as the objective of higher burn-ups than for existing plants could lead the designer to propose evolutions in the design of the fuel. Evolutions in the fuel designs and burn-ups have to be introduced cautiously. The designer has to demonstrate that fuel design evolutions do not affect adversely the global behaviour of the fuel assemblies during their irradiation, notably with regard to the bowing and deformation phenomena, and to justify the criteria proposed for normal and accident conditions. Any application concerning a modification of the fuel design or of its burn-up has to be supported by adequate research and development results, including the results of demonstration fuel assemblies with the same or higher burn-up, and due qualification of the computer codes (notably for slow power ramps, loss of coolant accidents and reactivity induced accidents).

For example, it would be advisable to eliminate by the design of the fuel the risk of clad ruptures resulting from pellet-clad interactions during reference transients, without restriction on reactor operation (grid following, extended reduced power operation). It is stressed that the corresponding demonstration has to be supported by experimental justifications.

For the neutronic and thermal-hydraulic aspects, the considerations developed in the second paragraph of this section about the design of the fuel apply in particular to the residual heat curve, and to the treatment of the uncertainties related to the critical heat flux correlation for the calculation of the departure from nucleate boiling (DNB) ratio.

Concerning the reactivity coefficients, as already stated in section **A.2.1,** the plant design shall be such that the reactor inherent behaviour is stable (e.g. negative moderator feedback). In principle, the moderator temperature coefficient must be kept negative from hot zero power to nominal conditions with all the control rods out of the core[2] ; the coolant void coefficient has to be negative for all conditions.

The monitoring of the power distribution in the core can be ensured by fixed in-core neutronic instrumentation, an aeroball movable system and ex-core neutronic instrumentation.

[2] However, *s*ome fuel managements could lead to high boron concentrations at the very beginning of life of the core and, consequently, to a positive moderator temperature coefficient.

B.1.2 - Primary circuit

B.1.2.1 - General requirements

The integrity of the primary coolant system boundary is an issue which requires special attention. High quality levels have to be achieved for its components, through the choice of materials, of manufacturing processes and associated inspections, of calculation rules with appropriate assumptions in systems and accident analyses, of measures taken at the design stage to simplify maintenance and monitoring during operation and of proper operating procedures and through surveillance during operation, including in-service inspections.

B.1.2.2 - Break postulates

Break postulates of the primary coolant system boundary are part of the events to be dealt with in the safety demonstration.

Because of phenomena like vibrations and corrosion, the break of small pipes cannot be excluded. On the other hand, the complete guillotine rupture of a large pipe correctly designed, manufactured and inspected is very unlikely ; so, when adequate design, manufacturing and inspection provisions are implemented, the complete guillotine break of a main coolant line can be "excluded" (with the meaning of section **A.1.4**). The accessibility and the inspectability of each point of these lines are of course prerequisites ; the designer has notably to implement provisions to allow access for a 100 % volumetric inspection of all the welds of the main coolant lines and of the parts of the large connecting pipes with a potential of degrading effects and to allow the use of two volumetric inspection methods for the dissimilar welds. Moreover an appropriate combination of available methods shall be implemented to monitor primary leaks[3].

B.1.2.3 - Consequences on the safety demonstration

The loads to be considered for the design of the internal structures of the reactor vessel and for the design of the structures in the containment building are then limited to those resulting from a break equivalent to the complete guillotine rupture of the largest pipe connected to a main coolant line (surge line).

In practice, the designer has to assume that any pipe connected to a main coolant line might separate from its connecting nozzle. In these conditions, the flow area through which the primary water might escape once the broken pipe has moved away, is equal to the internal cross section of the nozzle ; no flow limiter can be taken into account in the corresponding calculations (mass flow, pressure wave, ...).

[3] Additional provisions can be implemented locally to detect small leak rates.

Moreover, the mass flow equivalent to a 2A-opening of a main coolant line has to be assumed for the design of the emergency core cooling function (using realistic assumptions and models and appropriate criteria to be proposed by the designer) and of the containment pressure boundary, so as to implement safety margins concerning the cooling of the core to prevent core melt and concerning the containment function ; the 2A-opening is also to be assumed for the supports of the components and for the qualification of equipment.

B.1.3 - Requirements related to the main secondary lines

Regarding the secondary circuit, breaks on the main steam lines between the steam generators and the first isolation devices located outside the reactor building or the first following fixed points and on the main feedwater lines between the steam generators and the reactor building penetrations could be "excluded" under the following requirements :

- generally speaking, regulatory requirements and construction codes aiming at high quality must be applied ; moreover, design requirements shall be more stringent than general rules for class 1[4] piping ;
- fluid induced significant dynamic effects shall be prevented ;
- the fixed points shall be as close as possible to the containment penetrations ;
- the materials shall be in the ductile upper shelf for the lowest temperatures which could be encountered during reference transients, incidents and accidents ;
- pipes and elbows shall be seamless. Geometrical singularities and stress concentrations shall be avoided ; this applies notably to the welds for the supports, attachments or fixtures. Temporary welds or fixtures shall be prohibited ;
- the water chemistry shall be monitored with high reliability ;
- the layout of the lines shall enable easy access to the entire outer surfaces of the pipes ; in-service inspection of the welded zones shall be possible, using efficient methods.

Moreover, the possibilities of common cause failures on the main steam and main feedwater pipes must be minimised by an adequate separation of the lines.

Anyhow, the designer has to assume that any pipe connected to the main secondary lines might separate from its connecting nozzle.

It has also to be underlined that the designer has to specify the load cases he will consider for the mechanical design of the steam generators supports and internal structures, for the supports of the main steam lines and of the main feedwater lines inside the reactor building.

[4] In the meaning of the technical codes related to mechanical equipment.

B.1.4 - Confinement function

As already stated in section **A.1.2**, the general objectives set for nuclear power plants of the next generation call for a substantial improvement of the containment function ; the general strategy related to severe accidents defined in section **A.1.3** presents more precisely technical objectives concerning this function.

B.1.4.1 - Design requirements for the containment building and the peripheral buildings

These objectives can be achieved through the use of a double wall containment concept including an inner wall in prestressed concrete, an outer wall in reinforced concrete, with the annulus between the inner and the outer walls being maintained at a subatmospheric pressure in order to collect all possible leaks through the inner wall and to filter them before release to the environment via the stack.

The design pressure and design temperature of the containment inner wall must be such to allow a grace period of at least 12 hours without containment heat removal after a severe accident and to ensure its integrity and leaktightness even after the global deflagration of the maximum amount of hydrogen which could be contained in the containment building in the course of low pressure core melt accidents (see section **A.1.3**). It can be assumed that this amount of hydrogen is generated and released to the containment not instantly, but as a function of time dependent on representative sequences of severe accidents ; catalytic recombiners can be used to reduce substantially the amount of hydrogen in the containment and the time dependent concentrations of hydrogen. So, the amount of hydrogen to be considered for the design of the containment inner wall depends notably on parameters like the characteristics of the core, the time dependent release of hydrogen into the containment, the efficiency of the catalytic recombiners.

Moreover, the containment volume and the mitigation means must be such as to prevent the possibility of a global hydrogen detonation. The possibilities of high level hydrogen concentrations must be prevented as far as achievable by the design of the internal structures of the containment ; besides, specific provisions, such as reinforced walls of the compartments and of the containment, have to be implemented as far as necessary to deal with such phenomena as fast local deflagrations or deflagration to detonation transition sequences (see paragraph **E.2.2.4**).

Concerning the basemat, the objectives set in section **A.1.3** related to low pressure core melt situations can be achieved by the implementation a large "corium" spreading compartment adequately cooled.

A low leak rate of the inner wall of the containment is essential[5]. In view of the existing experience, it is advisable to use, for this containment inner wall, high-performance concrete with low deferred strain

[5] Calculations of radiological consequences show that, for a double wall containment concept as described in this section, assuming a leak rate of the containment atmosphere to the annulus of 1 % per day or less and no direct leak of the containment to the outside atmosphere, the radiological consequences of a medium size loss of coolant accident followed by a low pressure core melt are consistent with the objectives set in section **A.1.1**.

properties. Injection products should be used systematically, notably at each concrete construction joint and each penetration sleeve concrete interface. Specific attention has also to be paid to design measures to obtain an adequate leaktightness of the prestressed concrete for all the singular zones such as the basemat, the gusset, the area between the polar crane bracket and the ring beam, the vicinity of the equipment hatch and the dome. Anyhow, the implementation of a liner on the inner wall of the containment building appears necessary locally on all the singular zones[6].

Periodic leak tests of the containment building shall be possible at the design pressure of this building. In principle, an air test at the design pressure of the containment shall be done before the inner wall liner application, so as to detect any major construction defect which could be hidden by the liner leaktightness. Provisions have also to be implemented to check and to restore if necessary the adequate leaktightness of the outer wall of the containment building.

Specific devices have to be implemented for the collection of possible leakages associated with the different types of penetrations[7] as well as provisions to ensure adequate confining possibilities for the peripheral buildings.

Detailed information has to be provided by the designer concerning the system in charge of containment leakage collection and of containment leaktightness monitoring : design and operational criteria (leaktightness, periodic tests,..), qualification of the valves to the corresponding ambient conditions, protection against hazards (as defined in sections **A.2.4** and **A.2.5**) which could damage equipment of the system,…

Concerning the peripheral buildings, a leaktightness value has to be defined for each of the peripheral buildings with a confinement function, including the nuclear auxiliary building, the safeguard building and the fuel building. Furthermore, adequate means have to be considered to restore the leaktightness of the safeguard building following a break of the safety injection/residual heat removal system outside the containment building.

Provisions have also to be implemented to maintain as far as necessary a negative pressure in the containment and in the peripheral buildings during shutdown states, taking into account the location of the fuel during these states.

B.1.4.2 - Prevention of containment bypass

As stated in section **A.1.3**, core melt sequences involving containment bypassing (via the steam generators or via circuits connected to the primary system which exit the containment) have to be "practically eliminated".

[6] As far as the efficiency and robustness of the hydrogen risk mitigation concept will be clearly demonstrated, the implementation of a liner on the whole inner surface of the containment building is not necessary.

[7] These devices would include a leakage exhaust system for the equipment hatch, the personnel and emergency air locks, the fuel transfer tube as well as some mechanical penetrations communicating with ventilated rooms.

This implies a systematic review of all potential bypass sequences, with a deterministic analysis of the corresponding lines of defense, complemented by the results of probabilistic safety assessments. The following concerns can be mentioned :

a/ the list of potential containment bypass sequences shall include leaks of the containment heat removal system, containment bypass via the leakage exhaust system, liquid effluents crossing through the annulus building,

b/ generally speaking, with respect to leaks or breaks in circuits connected to the reactor coolant system, design provisions have to be implemented to avoid overpressurization of low pressure parts in connected systems or to ensure an adequate design of those parts with respect to overpressurization. The corresponding provisions have to be specified (design pressure and design temperature as well as associated criteria). Moreover, stringent requirements have to be applied to the means implemented to detect and to mitigate primary leakages in peripheral buildings. Exceptions have to be justified on a case by case basis ; this applies to the leakage detection means in the nuclear auxiliary building.

For the circuits connected to the primary system, the designer has to investigate the use of diversified isolation means, the possibilities of failures of these means and the associated monitoring devices, as well as the use of pipes designed to cope with the primary pressure under the corresponding situations. Moreover, the risk of containment bypass through lines equipped with only manual valves has to be assessed by the designer.

As regards the large borated water tank inside the reactor building used for the safety injection, the suction lines outside the containment building up to the first valve shall be equipped with guard pipes designed to withstand accident conditions in the containment not only at the beginning of the accident but also during the long term of the accident ; the guard pipes must be designed so as to allow periodical inspections of the inner suction pipes. Moreover, the consequences of a leak of an internal pipe have to be assessed.

Accident sequences including core melt with a significant leak of the steam generator tubes (up to multiple steam generator tube rupture) have to be "practically eliminated". On this subject, the designer has to investigate the situations mentioned in paragraph **E.2.2.5**.

As regards core melt accident sequences which could occur during shutdown states with open containment building, which will be allowed only for some phases (see paragraph **E.2.2.5**), the designer has to show that, for representative accident sequences, the containment building will be reliably closed before significant radioactive releases could occur inside the containment ; this requirement concerns notably the containment hatch, taking into account the time available before water boiling in the reactor core and the ambient conditions in the reactor building as well as the need for support systems, if any.

B.2 - Safety functions and systems

B.2.1 - Classification of the safety functions, barriers, structures and systems

A safety function[8] can be defined as the combined action of a set of technical features to perform a certain task in a certain plant condition. A safety function can be performed by one or several systems.

The implementation of the "defence-in-depth" principle can be supported by the introduction of a classification for the safety functions and systems. The aim of this classification is to define general requirements applicable to safety functions and systems with a hierarchisation of the requirements depending on the safety importance of the functions and systems.

A possible way to define an appropriate classification is to assess the different reference transients, incidents and accidents, according to their estimated frequencies, with consideration of two physical states :

a) in the controlled state, the core is subcritical (short term recriticality before operator actions with only low neutron power could be accepted for a few events on a case by case basis), the heat removal is ensured in the short term e.g. by the steam generators, the core coolant inventory is stable, the activity releases remain tolerable [9];

b) in the safe shutdown state, the core is subcritical, the decay heat is removed durably[10], the activity releases remain tolerable[9].

For the multiple failures conditions, a final state can be defined : the core is subcritical, the decay heat is removed by primary or secondary systems, the activity releases remain tolerable[9].

With these definitions :

- safety functions needed to reach the controlled state after a reference transient, incident or accident are classified F1A ;
- safety functions needed beyond the achievement of the controlled state to reach the safe shutdown state and to maintain it after a reference transient, incident or accident are classified F1B ;
- safety functions needed to reach the final state for multiple failures conditions are classified F2. Moreover, safety functions needed to cope with internal hazards and external hazards are also classified F2[11]. At last, instrumentation and control functions which contribute to maintain the initial conditions of the plant within the limits taken into account in the safety demonstration as well as the limitation functions implemented to avoid unnecessary actuation of protection actions are classified F2.

[8] To be distinguished from the basic safety functions mentioned in section **A.1.2**.

[9] In consistency with the objectives stated in section **A.1.4**.

[10] The cooling chains are able to transfer durably the heat to the ultimate heat sink.

[11] When studied in an event approach.

The classification of safety systems (including in principle support systems) can be derived from the classification of safety functions :

- if for a single reference transient, incident or accident, a given system has to handle a F1A function, this system is classified F1A ; however, the support systems of a F1A function can be classified F1B if they are in operation, with no change of state when the event occurs, and if they are not impaired by the event ;
- if for a single reference transient, incident or accident, a given system has to handle a F1B function, this system is classified at least F1B ;
- if for the prevention or the mitigation of a multiple failures condition, a given system is important to reduce significantly the core melt frequency, this system is classified at least F2.

General requirements for a F1A system are : implementation of the single failure criterion[12] (at the system level), physical separation of redundant trains, emergency power supply by the main emergency diesel generators, periodic testing, quality assurance, seismic design and, for the corresponding components, use of accepted design codes and qualification to accident conditions.

General requirements for a F1B system are : implementation of the single failure criterion (at the function level), physical separation of the redundant trains (at the function level), emergency power supply by the main emergency diesel generators, periodic testing, quality assurance, seismic design and, for the corresponding components, use of accepted design codes and qualification to accident conditions.

General requirements for a F2 system are : periodic testing, quality assurance and use of accepted design codes for the corresponding components ; physical separation is implemented when a F2 system is used as a backup for a F1A or F1B system ; requirements concerning the emergency power supply, the seismic design and the qualification to accident conditions of the corresponding components are defined on a case by case basis.

In addition, the classification concept has to take into account the barriers in connection with the prevention, control and mitigation of radioactive releases. This implies that the classification of the barriers related to different radioactive sources complements the classification derived from studies related to reference transients, incidents and accidents and to multiple failures conditions ; a system, component or structure can then be classified for a barrier function as well as for a barrier protection function.

All barrier classified components have to be classified at least F2 for the functional classification and mechanical components have to be designed according at least to the appropriate technical codes. In addition, precise functional (e.g. leaktightness) and operational (e.g. maintenance, periodic tests) requirements have to be defined for barrier classified systems and buildings with confinement function, for all parts of the plant. These requirements must also take into account the assessment of internal and external hazards ; so, due attention has to be paid to the components with high energy damage potential.

[12] The definition of the single failure criterion and its combination with scheduled maintenance are given in section **C.2.1**.

Specific attention has to be paid to the barrier classification and the associated requirements for the containment isolation valves, for the penetration of the leakage exhaust system and for the transfer tube as well as for the spent fuel pool active and passive components, structures and other containment related devices.

B.2.2 - Requirements on safety equipment

B.2.2.1 - Qualification of safety equipment

Equipment needed to achieve the safety demonstration has to be qualified for the conditions in which it is required.

Qualification includes both function and reliability, considering environmental conditions which materials and equipment would be exposed to in the plant, including severe accident conditions. The qualification process, especially for new materials or equipment, shall be completed before plant start-up.

The designer has to specify his overall approach of classified equipment qualification ; this approach must be applied to all kinds of equipment (mechanical, electrical, ...) inside and outside the reactor building and take into account internal and external accident conditions as well as ageing.

For this approach, the methods of qualification and the standards covering ambient conditions for reference as well as for severe accident situations have to be defined and their representativeness has to be justified (notably for ageing).

As regards electrical equipment, qualification can be obtained by testing one or several samples of this equipment against a sequence of conventional representative tests or by a clear demonstration of the capacity of the equipment to operate under defined conditions, for example by analogy with another equipment ; a combination of both methods can also be used. Consideration can also be given to experience feedback. In principle, test sequences for seismic qualification include ageing before seismic tests and test sequences for loss of coolant accident (LOCA) qualification include ageing and test for seismic qualification before LOCA tests. For these LOCA tests, profiles corresponding to envelope thermodynamical, chemical and irradiation conditions in the containment shall be defined with adequate margins.

In order to prevent any degradation of the emergency core cooling function, the debris generation during accident conditions, in particular from insulation materials, has to be taken into account in the qualification approach.

B.2.2.2 - Computerized safety systems

To obtain the necessary high reliability for instrumentation and control systems, when using computerized systems, the designer has to implement specific safety requirements concerning the qualification of such computerized systems of each safety class, including design rules for software.

The three main principles for designing computers for safety systems are fault avoidance, fault removal and fault tolerance.-
Fault avoidance can be implemented in a constructive approach by stringent rules and guidelines applicable during the entire life cycle of a system, including system specification (hardware, software and integration), production (design, coding of software and implementation of hardware, tests), operation and maintenance.-
Fault avoidance has to be complemented by an analytical approach for fault removal. This includes non formal procedures like inspections, walkthroughs, audits, reviews as well as formal procedures like proofs of correctness, static analysis and various integration tests.
To cope with residual faults remaining in spite of the measures taken towards fault avoidance and removal, fault tolerance is to be introduced in the design. For hardware, this can be achieved by redundancy and diversity. Diversity has to be examined to achieve software fault tolerance.

B.2.3 - Requirements on specific safety functions

B.2.3.1 - Reactivity control function

The reactivity control function can be achieved by control rods and borated water injection systems, including an extra borating system with two trains, each of them being able to transfer the plant from the controlled state to the safe shutdown state for any reference transient, incident or accident other than a loss of coolant accident without challenging the opening of the pressurizer safety valves. This system has to be classified F1B for this safety function and can be manually activated. Moreover, this system has to be automatically activated for anticipated transients without scram ; the corresponding instrumentation and control function has to be classified F2.

Concerning inadvertent openings of secondary valves as well as secondary line breaks, the designer has to specify if the plant can become critical after reactor scram in the course of such transients, incidents and accidents ; instrumentation and control equipment has to be classified accordingly.

Concerning homogeneous boron dilutions, the designer has to investigate the implementation of an automatic actuation of a reactor scram or of a boration system at least for homogeneous boron dilution reference transients.

Anyhow, the reliability of the reactor scram function has to be high enough to contribute to "practically eliminate" high pressure core melt sequences. Notwithstanding the role of the extra borating system, adequate means have to be implemented to deal with this objective, such as diversification for the main components of the reactor scram system (physical measurements, signals and associated processing, reactor scram breakers).

As stated in section **A.1.3**, reactivity accidents resulting from fast introduction of cold or deborated water must be prevented by design provisions so that they can be "excluded". Among these design provisions, automatic features to avoid inadvertent diluted water slug formation, leak detection devices, supervision of the boron concentration in systems have to be considered to the appropriate extent.

B.2.3.2 - Residual heat removal function

The residual heat removal function must be ensured with a high reliability. Generally speaking, a four trains system designed to achieve the residual heat removal function as well as the low head safety injection function can be convenient as far as adequate provisions are implemented for the parts of the residual heat removal system which are outside the reactor building, in order to "practically eliminate" severe accident sequences with containment bypassing.

The residual heat shall be transported from the combined residual heat removal and low head safety injection system to the ultimate heat sink through an intermediate component cooling water system.

However, a detailed demonstration has to be provided by the designer concerning the achievement of the safe shutdown state for the various accident situations to be considered in the different plant states. Specific attention has to be paid to event sequences for which a switch-over of trains of the combined low head safety injection and residual heat removal system from one mode of operation to the other is necessary and to the corresponding delays ; besides, the diversification and the adequacy of the automatic water injection signals as well as the sufficiency of the make-up flow rate shall be justified ; at last, the adequacy of the manual water make-up foreseen to cope with a failure of the automatic means has to be demonstrated.

Experience feedback has shown that special attention has to be paid on the potential loss of an adequate water level during shutdown states when the core is inside the reactor vessel. Design provisions have to be implemented to reduce the need for mid-loop operation when the core is inside the reactor vessel[13] and to cope with the loss of the normal residual heat removal system. Moreover, the design features of the water level measurement in the loops need a particular attention ; diverse measurement means should be implemented. The assumptions related to the recovery of the residual heat removal system pumps after a water level drop have to be clearly justified.

At last, the situations which need a primary circuit water level lowering during shutdown states have to be specified and justified by the designer, as well as the provisions - including design margins, instrumentation and adequate procedures - implemented to cope with the associated risks.

B.2.3.3 - Emergency core cooling function

Break postulates to be considered for the emergency core cooling function are defined in section **B.1.2** ; other assumptions related to the design of the corresponding systems are provided in part **D.2**.

The emergency core cooling function can be provided through an optimized concept comprising a cold leg medium head safety injection with an operating pressure below the opening setpoint of the steam generator safety valves, a cold leg accumulator injection and a cold leg low head safety injection, with switching to a combined cold leg and hot leg injection after a time period of a few hours, relying on a large water storage tank inside the containment building.

[13] It would be advisable that, during standard refuelling outages, steam generators maintenance or in-service inspections will be undertaken only after the total core unloading.

The arrangement of a large borated water storage tank inside the reactor building provides significant benefits for coping with loss of coolant accidents. Nevertheless, due consideration has to be paid to the mixing of the tank content and to the water temperature increase (subcooling should be maintained) during the course of such accidents (in connection with the volume of the tank), as well as to the quality of water for the design of the emergency core cooling system pumps.

The function of the emergency core cooling system to "practically eliminate" high pressure core melt situations must also be considered.

B.2.3.4 - Secondary side heat removal function

The secondary side heat removal function deserves special attention. It must have the capability to remove the heat from the reactor core via the steam generators in conjunction with the steam generator relief valves and the emergency feedwater supply during reference transients, incidents and accidents. After shutdown, the transition of the primary side from hot subcritical conditions to intermediate conditions must be assured by this function to enable further shutdown to cold subcritical conditions by the primary side heat removal function.

For specific events (small primary break and steam generator tube rupture), the secondary side heat removal function must have the capability for ensuring reliably cooldown of the primary side to enable operation of the emergency core cooling system[14] (reliability of the start-up and shutdown system, reliability of the main steam bypass, …).

To obtain the "practical elimination" of high pressure core melt sequences linked to the loss of normal and emergency feedwater systems, the designer has to implement and justify an adequate combination of means, including an independent start-up and shutdown system, an increased water reserve in each steam generator as compared to existing plants, the use of secondary feed and bleed as well as primary feed and bleed (automatically or manually activated).

B.2.3.5 - Containment heat removal function

The containment heat removal function in low pressure core melt conditions can be performed by a system achieving containment spray and corium cooling, subdivided in two trains, one train being sufficient after 15 days to maintain the containment pressure below the design pressure. These trains would be cooled by a dedicated chain as a diverse system to the component cooling water system used for the systems related to core melt prevention. The two trains of this dedicated cooling chain would be power supplied by small diesel generators as described in paragraph **B.2.4.1.**

It is stressed that a containment heat removal system with a radioactive fluid recirculation outside of the containment implies to deal with the possible failures of the corresponding pipes and the associated radiological consequences.

[14] The opening of the pressurizer valves could be not sufficient to make the safety injection efficient.

B.2.3.6 - Primary circuit overpressurization protection and depressurization functions

Adequate overpressurization protection of the primary circuit has to be provided for the different reference transients, incidents and accidents as well as for anticipated transients without scram. Overpressurization protection has also to be provided for circuits connected to the primary circuit (as the system designed to achieve the residual heat removal function and the low head safety injection function, when connected to the primary circuit).

As regards cold overpressurization, an adequate protection of this system and of the reactor coolant system during cold shutdown states can be provided by the pressurizer safety valves, with their opening actuated by a dedicated order elaborated by a pressure signal derived from a pressure threshold.

On another side, the primary circuit depressurization system must be designed to contribute to core melt prevention by the primary feed and bleed function.

The depressurization function to transfer high pressure core melt sequences to low pressure core melt sequences (see section **A.1.3**) can be ensured by adding to the depressurization function of the pressurizer valves, a dedicated bleed valve with an isolation valve, designed so that the opening of these specific valves can be guaranteed even for hot gas temperatures. This discharge function must be available in case of loss of off-site power and unavailability of all diesel generators. Once open, the bleed path should stay open with high reliability through the progression of the accident.

B.2.3.7 - Secondary side overpressure protection function

The secondary side overpressure protection function can be provided by a combination of isolable steam relief trains and steam safety valves located between the containment building and the main steam isolation valves. The adequacy of this combination of relief trains and safety valves has to be verified considering also the decay heat removal, the limitation of radioactive releases and the prevention of excessive cooling of the core.

For the overpressure protection function, the reactor scram can be taken into account as a pressure reducing measure, which allows to reduce the overall discharge capacity, provided the reliability and diversity of the provisions related to the reactor scram are similar to those of the protection of the core. This approach can be used for the reference transients, incidents and accidents. For transients, short overshoots of the steam pipes design pressure can be tolerated as far as the steam safety valves are not actuated. Besides, anticipated transients without scram have to be coped with ; the most penalizing transients with respect to pressure increase on the primary side and on the secondary side have to be assessed, taking into account the durations of the transients and the influence of these durations on the secondary valves reliability.

The relief valves and safety valves have to be qualified for fluid conditions which could occur during their use.

More precisely, from the safety point of view, the secondary side overpressure protection function could be ensured by two steam safety valves, each with a 25 % discharge capacity, in addition to one steam relief train (one steam relief isolation valve and one steam relief control valve) with a 50 % discharge capacity, for each steam generator. The setpoint for the reactor trip would be set to a value below or equal to the steam generators design pressure. The setpoints and opening characteristics of the safety valves and of the relief valves would be chosen so that no safety valve actuation would occur in the case of a steam generator tube rupture. This concept implies the classification of the steam relief trains as F1A systems ; moreover, an adequate reliability of the corresponding valves has to be clearly demonstrated.

B.2.4 - Requirements on support safety systems

B.2.4.1 - Electrical power supplies

Electrical power supplies are essential as support systems for the reduction of core melt frequency and for the "practical elimination" of high pressure core melt sequences.

Considering a general layout of the plant with four trains for safety systems, an adequate reliability of the electrical power supplies could be achieved through the implementation of four main identical diesel generators, supplemented by two small diesel generators able to backup particularly two of the emergency feedwater pumps and necessary support systems.

The small diesel generators have to be diversified from the four main diesel generators for eliminating as far as possible common cause failures between the two kinds of diesel generators, taking into account experience feedback of such generators, and connected to busbars with different voltage.

The independence between the main and the small diesel generators has to be completely justified by an assessment of the failure modes of the diesel generators. Notably, the failure probabilities of the main and of the small diesel generators have to take into account the risk of failure of their batteries, with due consideration to the related experience feedback.

Due consideration has also to be paid to the electrical switchboards and the possibility of common cause failures in these switchboards.

B.2.4.2 - Component cooling water system and essential service water system

The component cooling water system and the essential service water system are important support systems to transfer to the ultimate heat sink the residual heat from the system designed to achieve the residual heat removal and the low head safety injection functions.

Potential common cause failures of the component cooling water system and of the essential service water system have to be fully investigated.

Moreover, the designer has to show that the heat removal capacity of each heat exchanger between the component cooling water system and the essential service water system is adequate for all normal operating conditions, including shutdown conditions, as well as for all reference transients, incidents and accidents. The reliability of the isolating devices for those users the heat loads of which are not taken into account has to be thoroughly assessed.

C - ACCIDENT PREVENTION AND PLANT SAFETY CHARACTERISTICS

C.1 - Reduction of the frequencies of initiating events

The aim of reducing the frequencies of initiating events - as called for in section **A.1.2** - implies to evaluate operating experience to increase, as far as possible, the reliability of operational systems and components (e.g. main feedwater system) and to eliminate to the largest possible extent the occurrence of phenomena liable to challenge the integrity of mechanical equipment like vibrations, corrosion, cavitation, ...

Experience feedback shows notably that adequate provisions have to be implemented to cope with thermal fatigue phenomena linked to mixing between cold and hot fluids. Their appropriateness has to be justified.

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

Quality of design, manufacturing, construction, operation and maintenance has to guarantee that those malfunctions leading to the actuation of safety system functions are unlikely.

C.2 - Redundancy and diversity

C.2.1 - Single failure criterion and preventive maintenance

A system is designed according to the single failure criterion if it is able to fulfil its function in spite of a single failure being independent of the event the control of which necessitates the system operation. The postulated single failure can be active in the short and long term or passive in the long term (after 24 hours).

An active single failure is defined as a failure or a mispositioning sufficient to prevent the safety relevant function of a component. Such a fault can have the following characteristics :

a) malfunction of a mechanical or electrical component which relies on mechanical movement to complete its intended function upon demand (e.g. operation of a relay, starting of a pump, failure of a valve to open or to close, etc …),
b) malfunction of an instrumentation and control component.

The consequences of spurious actuations of components due to single failures in the instrumentation an control systems have notably to be assessed in order to identify weak points, if any, in the separation of redundant equipment and in instrumentation and control systems (as detailed in part **G.3**).

Some active single failures can be excluded when implementing the single failure criterion for the design of systems ; such exclusions have to be clearly justified by appropriate methods in connection with precise design and operation provisions, taking into account operational experience. Justifications should include an analysis of the consequences of the failure, using realistic assumptions.

Such exceptions could include :

a) the failure to open of the accumulator check valves,
b) the failure to close of a main steam isolation valve in case of a single or multiple steam generator tube rupture (the behaviour of the main steam line filled with water and the amount of primary coolant lost have to be specified as well as the possible radiological consequences).

A passive single failure is defined as a failure which occurs in a component which does not need a change of state in order to carry out its function. A passive failure can be :

- a leak of the pressure boundary of a fluid system ; such a leak, if not detected and isolated, is assumed to escalate to the flow corresponding to a full rupture ;
- another mechanical failure impairing the normal process flow line of a fluid system.

The consideration of passive failures only in the long term (after 24 h) of operation of safety systems, with a leak rate conventionally postulated of 200 liters per minute up to the isolation of the leak, is acceptable in principle. However, for each F1 system, sensitivity studies must be performed to show that the postulation of a passive single failure in the short term (before 24 h) as well as the postulation of leak rates larger than 200 l/min (up to the rupture of a connected pipe with an inner diameter of 50 mm) is covered by the consideration of active single failures or do not lead to cliff edge effects regarding the effectiveness of the system as well as radiological consequences. Moreover, possible leaks in the short term have to be considered for all passive headers.

Anyhow, the designer has to indicate precisely the preventive and mitigative measures he will implement to cope with passive failures, including provisions for the detection and isolation of leaks, as well as for water exhaust[15]. F1 requirements (except possibly the redundancy) must be applied to the corresponding detection and isolation devices.

Preventive maintenance is defined as taking equipment out of operation for servicing at defined times independently of failure occurrences. During its periods of preventive maintenance, the equipment is considered to be unavailable for its design function. If the nature of the preventive maintenance is such that the system can be restored to an operational state in due time which enables the necessary safety function in case of demand mode, the part of the system shall be considered to be available.

If preventive maintenance is done during periods of time when a F1 system is in the demand mode or in stand-by, this maintenance must be combined with the implementation of the single failure criterion (at the system level for F1A systems, at the function level for F1B systems), taking into account the required capacity of the corresponding safety function during the corresponding situation. For each

[15] The designer should develop a pragmatic approach of the leak rates associated to passive failures (including the possible failures of small pipes), based on the investigation of sensitive locations, and taking into account the existing experience feedback.

safety system for which periodic tests in one train will be performed during preventive maintenance in another train, appropriate measures have to be taken to avoid the unavailability of a safety system train during testing.

Cross connections between AC power supply trains should be allowed only for maintenance and only between two of the four trains (trains 1 and 2 on one hand, trains 3 and 4 on the other hand) During power operation, maintenance should not be carried out on more than one train at the same time.

C.2.2 - Probabilistic safety assessment and diversity

Common cause failure possibilities must be eliminated as far as possible by suitable design and equipment installation rules, including for instance selecting diversified equipment. It is to be noted that, for frequent initiating events, the reliability requirement on a safety function is such that two diverse systems or equipment might be necessary.

For determining the adequate combination of redundancy and diversity in safety systems, the designer can, as stated in section **A.2.6**, use probabilistic targets as orientation values ; in that case, orientation values of 10^{-6} per year for the probabilities of core melt due to internal events respectively for power states and for shutdown states could be used, having in mind the necessity to consider associated uncertainties.

For the performance of the probabilistic safety assessment, the list of initiating events has to be as complete as possible, even for the first assessment at the conceptual stage ; it must be at least representative of all sequences already analysed in French probabilistic safety assessments, including events during shutdown, even with very rough estimations of their frequencies in a first step.

The use of simplified models and generic data as well as the limitation of calculations to a duration of 24 hours can be sufficient to provide valuable insights as a first step about the design of nuclear power plants of the next generation. Nevertheless, even at the conceptual stage, it would be appropriate to investigate specific events which could occur after 24 hours (e.g. refilling of a tank) in order to show the absence of cliff-edge effect. In particular, due attention has to be paid to external hazards which would require long mission times for some systems.

Concerning common cause failures, the designer has to consider this type of failures for component parts within a system and to investigate possibilities of common cause failures across system boundaries.

It would not be appropriate to exclude a priori common cause failures for components continuously in operation and in the same operational state prior to the accident and during the accident, or for components belonging to a large population of identical components operated under similar conditions. Such exclusions have to be dealt with on a case by case basis. In particular, common cause failures to run during the mission time, between identical pumps belonging to the same system and fulfllling the same function in the same conditions, have to be considered.

Unavailability due to maintenance has already to be investigated from the beginning of the design phase, especially if maintenance operations are foreseen during power operation. The potential influence of human errors during maintenance and tests has to be investigated in the design phase. Preventive maintenance has to be considered in a realistic way ; the unavailabilities due to preventive maintenance should not induce a large part of the global core melt frequency.

On another side, it is stressed that maximum repair times before plant shutdown have to be specified for the components of safety systems ; for that purpose, probabilistic studies can also be used, taking into account the orientation values defined above, with due consideration for the associated uncertainties. Maximum repair times must also be consistent with the "practical elimination" of accident situations which would lead to large early releases.

Human reliability is particularly difficult to deal with at the design stage, since human factors depend strongly on plant specific characteristics of operation which are not defined at this stage (procedures, organisation, ...). The first estimation can only be very rough. It has to be pointed out that it is not possible to assess the benefits due to the improvement of man-machine interface, without some experimental results. A program for data collection has to be defined as soon as possible.

Assumptions, criteria, and data have to be justified. Reliability data have to be updated and extended, considering in particular French and German operating experience ; in this frame, particular attention has to be devoted to common mode failures as well as to instrumentation and control systems (hardware and software). The uncertainties concerning reliability data, common cause failures and human reliability have to be dealt with at the design stage using sensitivity studies.

The designer has also to carefully assess the frequencies of sequences leading to core melt with containment heat removal system unavailability and the corresponding consequences, taking into account possible operator actions. Sequences with initial leakages of the containment have to be investigated too.

C.3 - Human factors

As stated in section **A.2.3**, a comprehensive human factor engineering program has to be implemented. The following issues should be dealt with by this program, in an iterative way as far as necessary :

a) task description and analysis : this would cover systematically interactions between men and equipment as well as interactions between men, for all the operation, maintenance, repair and testing activities. In a first step, data would be preferably collected by direct observation of these activities in existing plants, complemented by interviews and later by trials on mockups and simulators ;

b) allocation of functions to equipment and to men : this would notably result in a justified list of tasks to be automated, not automated or shared in a human-machine cooperation ;

c) design of the interfaces : this would cover the definition of information to be presented and its organization and layout, notably in the main control room where an overall vision of the actual state of the plant is necessary, the alarm system, the communication means for the different types of activities, the working environment and the control means to be provided to the operators ; particular attention would be devoted to the remote shutdown station defined in part **G.3** as well as to other workplaces outside the main control room ;

d) staffing : this would cover the definition of the required number and competences of personnel, to derive selection criteria and training programs, as well as the organization of the teams with a clear allocation of responsibilities ;

e) operator guidance development, including adequate documentation and procedures ; computerized procedures should be developed in a coherent and integrated way with other interfaces used by the operators ;

f) verification and validation : depending on the results of the verification and validation process taking into account assessments of human reliability in all design phases, adjustments would have to be implemented.

A specific concern is related to the alarm system for which the designer has to consider the maintenance, repair and testing situations and to define criteria for alarm prioritization at an early stage of the design. Such prioritization must not impair the possibility to conduct consistency tests of incoming alarms.

C.4 - Radiation protection of workers and of the public

C.4.1 - Radiation protection in normal operation

For the implementation of the ALARA approach for nuclear power plants of the next generation (as called for in paragraph **A.2.7.1**), a detailed assessment of the existing experience feedback is needed. This assessment would concern notably :

- dose rates near the reactor coolant system during outages, with the respective contributions of corrosion products deposits (^{58}Co, ^{60}Co, ^{124}Sb) ;
- shieldings in the reactor building and in the auxiliary buildings.

Concerning the choice of materials; it would be advisable for nuclear power plants of the next generation to reduce as far as possible the use of stellites and antimony and to select materials with low cobalt impurities content. The choice of the steam generator tubes alloy has also to be justified by the designer, taking into account experience feedback concerning the corresponding activity levels in the reactor coolant system as well as the prevention of corrosion on the primary and secondary sides.

Concerning shieldings, it would be appropriate to take into account design activities for fission products and corrosion products in the reactor coolant system more realistically than for existing plants, with due consideration of experience feedback. These activities, with the corresponding spectra, must be specified by the designer ; all relevant sources of irradiation have to be taken into account (neutron and gamma radiations around the reactor pressure vessel, ^{16}N around the reactor coolant system, ...).

The following topics have also to be specified by the designer :

- the purification rate of the primary coolant in normal operation and in cold shutdown state,
- the design arrangements provided for avoiding or limiting as far as possible the areas where corrosion products deposits could accumulate,
- the surface treatments (such as electrolytic polishing) applied for parts of the primary circuit or of the reactor pool,
- the provisions considered to facilitate decontamination operations,
- the design provisions for use of robotics,
- the design provisions to facilitate work in the containment building, by shortened work durations and increased distances between the radioactive sources and the workers.

Moreover, the radiological impact of the tasks performed in the reactor building during power operation has to be precisely investigated by the designer.

C.4.2 - Radioactive releases, waste reduction and dismantling

C.4.2.1 - Waste reduction and dismantling

The designer has to specify how he will take into account the objective related to the reduction of radioactive releases and waste stated in paragraph **A.2.7.2** in the frame of an optimisation process**.** This implies a detailed assessment of the existing experience feedback. The following topics have notably to be dealt with :

- material specifications for components which are in contact with the reactor coolant ;
- reactor coolant chemistry (advantages and drawbacks of possible modifications of this chemistry) ;
- provisions to minimize deposition of corrosion products which are or can be activated when passing through the reactor core ; this applies in particular to deposition on the fuel assemblies and on the structures surrounding the reactor core ;
- treatment processes for liquid and gaseous radioactive effluents, as well as for radioactive solid waste according to the characteristics of the different types of effluents and waste, taking into account plausible situations such as clad failures.

Some choices of materials already called for in section **C.4.1** for radiation protection purposes (such as the reduction as far as possible of the use of stellites and antimony and the selection of materials with low cobalt impurities content) would also present benefits concerning radioactive waste management. Another concern related to the choice of materials is the production of long lived radionuclides which has to be considered in connection with waste disposal.

It is also essential to make a clear distinction at the design stage between conventional waste areas within which waste produced is not liable to be contaminated or activated and nuclear waste areas within which waste produced is liable to be contaminated or activated ; the extent of the nuclear waste areas should be minimized by suitable design.

Concerning dismantling, adequate provisions have to be implemented at the design stage to facilitate the corresponding works. Notably, it would be advisable to install the large components so that they can be removed and transported for subsequent treatment ; care has to be taken to the necessary handling devices, evacuation arrangements and biological shielding. Moreover, provisions for cleaning and decontamination in situ should be considered in the design and layout of systems and vessels.

C.4.2.2 - Effluent treatment system

In connection with the objective stated in paragraph **A.2.7.2** and recalled in the previous section**,** the designer has to specify the following topics related to the effluent treatment systems :

- the management policy of radioactive gaseous and liquid effluents in the plant ;
- the methodology and database used to determine the source terms to be considered (including C14) for the design of the effluent treatment systems. These source terms shall cover all transients considered in the design of the plant (normal operation, including outages and load following, other reference transients). The management of effluents which could result from incident and accident conditions has also to be taken into account ;
- the demonstration of the identification of all potential radioactive and chemical releases and of the adequacy of their monitoring.

D - CONTROL OF REFERENCE TRANSIENTS, INCIDENTS AND ACCIDENTS

D.1 - List of reference transients, incidents and accidents

As stated in section **A.1.4**, reference transients, incidents and accidents within the plant have to be considered to demonstrate the safety of the plant.

The definition of the reference transients, incidents and accidents to be assessed comprises several steps :

- identification of possible initiating events which could result in a release of radioactive materials inside or outside the plant ;
- exclusion of single initiating events sufficiently prevented by design and operation provisions ;
- grouping of all other identified events so as to define a limited number of reference transients, incidents and accidents in such a way that the consequences of each reference event cover those of the corresponding group of events.

Due emphasis has to be laid on reference transients, incidents and accidents starting from shutdown conditions, taking into account the associated specific operating conditions, notably the possible non-availability of some of the barriers and some of the safety systems. Specific attention has also to be laid on initiating events which could result in a bypass of the containment barrier, including isolation failures in systems connected to the primary circuit and penetrating the containment as well as steam generator tube ruptures.

It is appropriate to categorise the reference transients, incidents and accidents according to the estimated frequencies of the groups of initiating events they cover ; this implies the definition of four plant conditions categories from normal operation and transients to incidents and accidents. For each category of plant conditions, the list of initiating events, the associated assumptions, rules and criteria have to be specified by the designer.

For the definition of the internal initiating events to be dealt with concerning the plant unit, it can be convenient to distinguish different reactor states :

- State A power state as well as hot or intermediate shutdown state with all the automatic reactor protection functions available ; some functions can be deactivated at low pressure ;
- State B intermediate shutdown above 120°C, residual heat removal system not connected ; some automatic reactor protection functions might be deactivated ;
- State C intermediate and cold shutdown, with the residual heat removal system in operation and the primary coolant system closed or that can be rapidly reclosed ;
- State D cold shutdown with the primary coolant system open ;
- State E cold shutdown with the reactor cavity flooded ;
- State F cold shutdown with the reactor core totally unloaded.

The list of the reference plant conditions to be dealt with in the safety demonstration of nuclear power plants of the next generation can be largely derived from the experience of existing plants, adapted to the more detailed concept deemed acceptable in the present technical guidelines. In the preliminary list presented hereafter, when no reactor state is mentioned, it is assumed that the respective plant condition has to be assessed in state A for the most demanding power level.

Normal operation : Plant Conditions Category 1 (PCC 1)

Normal operating conditions include the situations which are coped with operational systems, such as plant heat up and cooldown, step load change, ramp load change, ... For these situations, the plant is kept within the limits specified by its technical specifications (regarding in particular the availability of systems and the number of occurrences).

Reference transients: Plant Conditions Category 2 (PCC 2)

- reactor trip (spurious),
- feedwater system malfunction causing a reduction in feedwater temperature,
- feedwater system malfunction causing an increase in feedwater flow,
- excessive increase in secondary steam flow,
- turbine trip,
- inadvertent closure of one main steam isolation valve,
- loss of condenser vacuum,
- short term loss of offsite power (≤ 2 hours) (states A, C, D),
- loss of normal feedwater flow (loss of all the main feedwater pumps and of the startup and shutdown pump),
- loss of one reactor coolant pump without partial trip,
- uncontrolled rod cluster control assembly bank withdrawal (state A),
- rod cluster control assembly misalignment up to rod drop, without limitation,
- startup of an inactive reactor coolant loop at an incorrect temperature,
- malfunction of the chemical and volume control system that results in a decrease in boron concentration in the reactor coolant (states A to E),
- malfunction of the chemical and volume control system causing an increase or decrease in the reactor coolant inventory,
- primary side pressure transient (spurious pressurizer spraying, spurious pressurizer heating),
- uncontrolled reactor coolant system level drop during mid-loop operation (state C or D),
- loss of one cooling train of the residual heat removal during mid-loop operation (state C or D).

Reference incidents: Plant Conditions Category 3 (PCC 3)

- small steam or feedwater system piping failure,
- long term loss of offsite power (> 2 hours) (state A),
- inadvertent opening of a pressurizer safety valve,

- inadvertent opening of a steam generator relief train or of a steam generator safety valve (state A),
- small break loss of coolant accident (states A, B),
- steam generator tube rupture (one tube),
- inadvertent closure of all the main steam isolation valves,
- inadvertent loading and operation of a fuel assembly in an improper position,
- forced decrease of the reactor coolant flow (4 pumps),
- failures in liquid or gazeous waste systems,
- uncontrolled rod cluster control assembly bank withdrawal (states B to D),
- uncontrolled single control rod withdrawal,
- rupture of a line carrying primary coolant outside of the containment (e.g. sampling line).

Reference accidents : Plant Conditions Category 4 (PCC 4)

- long term loss of offsite power (> 2 hours) (state C),
- steam system pipe break (states A, B),
- feedwater system pipe break (states A, B),
- inadvertent opening of a steam generator relief or safety valve (state B),
- rod cluster control assembly ejection (states A, B)
- intermediate break and large break loss of coolant accident (up to the surge line break[16] in states A and B)
- small break loss of coolant accident (up to 50 mm diameter in states C and D),
- residual heat removal system break outside the containment (up to 250 mm diameter in states C and D),
- reactor coolant pump seizure (locked rotor),
- reactor coolant pump shaft break,
- rupture of two steam generator tubes in one steam generator,
- fuel handling accident,
- boron dilution due to a non isolable rupture of a heat exchanger tube (states A to E).

The definitive list has to be completed and justified by the designer, taking into account the following remarks :

- if one plant condition considered in PCCn at power state is shifted to PCCn+1 at shutdown states, this shift has to be justified case by case on the basis of the estimated frequency of the initiating event at shutdown states ;
- the categories of some plant conditions such as "inadvertent opening of a steam generator safety valve (state A)" or "boron dilution due to a non isolable rupture of a heat exchanger tube (states A to E)" will have to be precisely justified on the basis of the detailed design of the corresponding components ;

[16] Without taking into account the influence of a flow limiter.

- the inadvertent opening of the dedicated depressurization device (described in paragraph **B.2.3.6**) has to be introduced in the list of plant conditions, unless a precise justification can be presented ;
- the break areas of the small break loss of coolant accidents in PCC 3 have to be specified and justified ;
- the specific case of a small break loss of coolant accident in the most unfavourable position with respect to the extra borating system injection, together with a single aggravating failure in the non-affected train of this system, has to be assessed ;
- the rod cluster control assembly ejection has to be considered in state C, unless the designer provides adequate justifications ;
- the approach for internal initiating events outside the reactor building, notably in the spent fuel pool, has to be specified and justified (see part **G.1**) ;
- concerning the auxiliary buildings which contain systems with radioactive material, accidents studies have to be included in the plant conditions categories and assessed with the corresponding rules. As far as the layout of systems in these buildings is such that high energy lines are separated from those which carry radioactivity, the failure of radioactivity containing equipment must in principle be assessed only as a possible initiating event ;
- concerning homogeneous boron dilutions of the primary coolant, the scenarios retained for accident studies, as well as their classification in the plant conditions categories, have to be justified, based on an exhaustive identification of possible dilution initiating events, with the corresponding flowrates, and an assessment of their respective likelihoods ;
- the exclusion of intermediate break loss of coolant accidents in state B2 when the accumulators are isolated has also to be precisely justified ;
- an application for operation with only three main coolant pumps would necessitate the assessment of the corresponding accident studies.

The probabilistic safety studies done at the design stage will have also to be used to check and adjust the list presented above.

D.2 - Safety analysis rules and acceptance criteria

For the different reference transients, incidents and accidents, safety demonstration rules have to be applied and appropriate decoupling technical criteria have to be respected with conservative assumptions. For some of these reference transients, incidents and accidents, the designer has to present accident studies covering all foreseen fuel managements.

It has to be verified that, for the different reference transients, incidents and accidents with radiological significance, assuming the corresponding technical criteria are respected, radiological consequences are tolerable and consistent with the general safety objectives defined in section **A.1.1** for accident situations without core melt.

D.2.1 - Safety analysis rules

The safety demonstration related to the plant conditions categories has to take into account the following rules :

- in principle, only F1 systems can be used for the safety demonstration in order to reach and to maintain the safe shutdown state (as defined in section **B.2.1**) ; non F1 equipment is considered only if it is not beneficial for the transient. However, very limited exceptions for non F1 equipment beneficial for the transient could be accepted if adequate requirements are applied to this equipment. The designer has to provide a complete list of the corresponding equipment, with the associated requirements, and a verification of the absence of cliff edge effect when this equipment is not taken into account in the safety demonstration ;

- the most penalizing aggravating failure must be taken into account. It is a single failure applied to an equipment used to achieve the safety demonstration, including non F1 equipment if any as defined here above. In particular :

a) a stuck rod has to be considered as a possible aggravating failure for reference transients, incidents and accidents. As far as adequate provisions are implemented to prevent any blockage of a control rod, with due attention to existing experience feedback, it is not necessary to consider the superposition of a stuck rod and of another aggravating failure ;

b) the failure to close of a main steam relief valve has to be assumed as a possible aggravating failure for reference transients such as homogeneous dilution and rod cluster control assembly withdrawal ;

- preventive maintenance must be combined with the implementation of the most penalizing aggravating failure, with the conditions stated in section **C.2.1** ;

- manual action from the main control room can be assumed to take place, at the earliest, 30 minutes after the first significant information is given to the operator. For a local manual action, outside the main control room, the earliest time to be taken into account is 1 hour.

In addition, reference transients, incidents and accidents (except those initiated by human action), have to be studied with a loss of off site power at the most penalizing time ; only seismic classified equipment can be used for the safety demonstration. The technical decoupling criteria to be complied with are similar to those of the reference accidents.

D.2.2 - Acceptance criteria

The technical decoupling criteria to be respected in the safety demonstration are notably the following.

For reference transients (PCC 2), the integrity of the fuel cladding has to be maintained. This implies to define a limit for the departure from nucleate boiling ratio, to be specified by the designer, and, possibly, a criterion concerning pellet-cladding interaction.

The appreciation of the consequences of reactivity accidents like control rod withdrawal on the fuel behaviour necessitates detailed investigations taking into account the precise characteristics of the fuel and the associated burn-up.

For the surge line break in reactor state A (PCC 4), the peak cladding temperature must remain lower than 1200°C, the maximum cladding oxidation must remain lower than 17 % of the cladding thickness, the maximum hydrogen generation must remain lower than 1 % of the amount that would be generated if all the active part of the cladding were to react. It is also necessary to prevent long duration of deteriorated core cooling conditions which could lead to extended fuel damage.

Other decoupling technical criteria have to be proposed and justified by the designer, to deal with :

- the maximum energy release inside the fuel during fast transients such as a rod cluster control assembly ejection (PCC 4),
- the long term coolability of the reactor core after a loss of coolant accident,
- the maximum numbers of fuel rods which could experience departure from nucleate boiling in plant conditions of categories 3 and 4,
- the maximum peak cladding temperature for fast transients to avoid cladding embrittlement,
- the maximum fuel melting in plant conditions of categories 3 and 4.

In addition, the safety assessment of reference transients, incidents and accidents according to the associated rules has to include an assessment of the overpressure protection of the primary and of the secondary circuits with adequate specific criteria.

More generally, it has to be checked that the design rules applied to the classified equipment used in the safety demonstration are covering with adequate margins the conditions (notably sollicitations for mechanical components) resulting from reference transients, incidents and accidents.

The safety assessment of reference transients, incidents and accidents has also to include a precise justification of the volume of the emergency feedwater system tanks, with due account to an aggravating failure and to the preventive maintenance strategy.

Moreover, the subcriticality requirements related to the shutdown states have to be specified with regard to the accident conditions which might occur during these states.

D.2.3 - Use of computer codes

For each of the computer codes used to justify the design, the designer has to specify its experimental validation and qualification and how the remaining uncertainties are taken into account (e.g. sensitivity studies). This applies to computer codes used for neutronic and thermalhydraulic calculations related to reference transients, incidents and accidents, and notably to computer codes of the new generation (3 D neutronic and thermalhydraulic coupled computer codes), in order to demonstrate that the envelope values determined by the results are actually conservative for the whole set of PCC studies. This applies also to the computer codes used to determine the residual decay heat evolution for plant conditions studies.

Realistic assumptions and models can be used for the safety demonstration related to the surge line break (PCC 4) in reactor state A; but the compliance of the results with acceptance criteria must be proven at a high confidence level -this implies the use of a frozen version of the computer code which has to be qualified and verified and an explicit evaluation of the associated uncertainties, combining the elementary uncertainties (code models, scaling effects, initial and boundary conditions, user effects, ...). An alternative approach could be the use of models and criteria already applied to existing plants in a conservative way.

Additional tests or a reevaluation of previous tests could be necessary for design features differing from existing ones in order to reduce uncertainties ; this has to be considered in connection with the use of best estimate analyses.

D.2.4 - Radiological consequences

The potential radiological consequences shall be calculated as indicated in section **A.1.4**. The realistic hypotheses used for the calculations have to be justified by the designer ; this applies to the nuclide spectrum considered for the calculation of doses and to the fission products activity in the primary coolant (which has to be assessed taking into account operational technical specifications) as well as the iodine carry over considered for steam generator tubes ruptures.

Radiological consequences must notably be calculated for accident situations during shutdown states, including a guillotine break of the residual heat removal system outside the containment building as well as for accident situations with long term circulation of contaminated fluids outside the containment building.

The final results of the assessment of reference transients, incidents and accidents with radiological significance shall include effective doses of members of critical groups as well as potential contaminations of food. It is notably underlined that thyroïd dose equivalents for adults and for children are important indicators of the radiological consequences of some accident situations. Doses resulting from contaminated foodstuff ingestion and from deposited radioactive substances have to be presented for different distances and different time frames.

For a first approach, the following assumptions can be made for the largest loss of coolant accident inside the containment :

- fuel cladding failure rate : 10% (this value necessitates justifications, taking into account the composition and the burn up of the fuel),
- primary containment building leak rate : 1% per day of the free volume of the internal containment (with no direct leak to the outside),
- annulus filters efficiency : 1000 for molecular iodine and for aerosols, 100 for organic iodine.

Moreover, generally speaking, a sensitivity study concerning the radiological consequences of accident situations leading to releases in the reactor building has to be performed, assuming a small leakage from the atmosphere of the reactor building to a peripheral building, taking into account the leaktightness and the retention capacity of this peripheral building.

E - CONTROL OF MULTIPLE FAILURES CONDITIONS AND CORE MELT ACCIDENTS

E.1 - Multiple failures conditions

E.1.1 - Consideration in the safety demonstration

In addition to reference transients, incidents and accidents, multiple failures conditions have to be considered in the safety demonstration.

A list of multiple failures conditions, called RRC[17]-A, to be assessed deterministically in order to design additional measures, is presented in paragraph **E.1.2.1**. The results of the probabilistic safety studies done at the design stage will have to be used to check and adjust the preliminary list of multiple failures conditions and to check the appropriateness of the foreseen additional measures.

E.1.2 - Deterministic assessment of RRC-A conditions

E.1.2.1 - List of RRC-A

The following list of multiple failure conditions to be dealt with in the safety demonstration of nuclear power plants of the next generation is derived from the experience of existing plants, adapted to the more detailed concept deemed acceptable in the present technical guidelines.

When no reactor state is mentioned, it is assumed that the respective plant condition has to be assessed in state A for the most demanding power level.

Multiple failures conditions: Risk Reduction Category A (RRC-A)

- station blackout: loss of offsite power cumulated with the failure of the four main diesel generators (state A and mid-loop operation in state C or D),
- loss of the component cooling water system/essential service water system cooling chains (state A and mid-loop operation in state C or D),
- total loss of feedwater (loss of the main feedwater, startup and shutdown, emergency feedwater systems),
- small break loss of coolant accident (up to 50 mm diameter) and loss of the medium head safety injection trains (loss of the pumps or loss of partial secondary cooldown) (states A and C),
- small break loss of coolant accident (up to 50 mm diameter) and loss of the low head safety injection system (states A and C),
- small break loss of coolant accident and simultaneous loss of the component cooling water system/essential service water,
- anticipated transients without scram,

[17] Risk Reduction Category.

- rupture of several steam generator tubes (up to 10 tubes in one steam generator),
- steam line break and simultaneous steam generator tube rupture (up to one tube in the affected steam generator),
- steam generator tube rupture (one tube) with a main steam relief train stuck open at the affected steam generator,
- total loss of the spent fuel pool cooling system.

E.1.2.2 - Investigation of specific sequences

1/ Concerning anticipated transients without scram, the situations considered in the safety demonstration will have to be precisely justified , in connection with the results of probabilistic safety studies. The designer has to justify the conservatism of the reactivity coefficients used in the corresponding studies.

2/ Detailed investigations are particularly needed concerning :

- the steam generator tube rupture combined with a main steam relief train stuck open (consideration of the hot stand-by case, location of the tube rupture) ;
- the small break loss of coolant accident combined with the loss of the low head safety injection system (subcriticality at cold shutdown, formation of plugs of deborated water, clogging, long term heat removal from the inner refuelling water storage tank) ;
- the small break loss of coolant accident with the loss of the medium head safety injection system (calculations related to core subcriticality, impact of the fast secondary cooldown on the structures of the primary and secondary circuits) ;
- the total loss of the spent fuel cooling system, for which ambient conditions in the corresponding building and their impact on the structures and systems located in this building, as well as the possibilities to provide a water make-up or to repair the faulted components have to be completely assessed. Additional measures have to be implemented as far as necessary notably regarding support systems.

E.1.2.3 - Accident analysis rules and acceptance criteria

For the assessment of multiple failures conditions, all systems can be deemed available, except those which are assumed to have failed in the multiple failures combination. No additional failure and no unavailability due to maintenance have to be deterministically postulated in the systems needed to reach the final state defined in section **B.2.1**.

Moreover, for the multiple failures conditions, the technical decoupling criteria related to reference accidents can be used to demonstrate the integrity of the barriers.

In particular, the safety assessment of RRC-A conditions according to the associated rules has to include an assessment of the overpressure protection of the primary and of the secondary circuits with adequate specific criteria.

For anticipated transients without scram, the maximum pressure of the primary circuit must not exceed 1.3 times its design pressure for any core configuration.

It is stressed that, for RRC-A conditions, including those with containment bypass, the calculated radiological consequences must be consistent with the general objective set in section **A.1.1** for accident situations without core melt. The methodology to be applied to the determination of potential radiological consequences of RRC-A conditions is similar to that applied to reference incidents and accidents as described in section **D.2.4**. Radiological consequences must notably be calculated for the total loss of the fuel pool cooling system.

E.1.3 - Probabilistic assessment of multiple failures conditions

As support systems are essential contributors to the global core melt frequency, particular attention has to be paid to these systems. This concerns notably :

1. the sequences of the probabilistic safety assessment associated to a loss of offsite power :

- the possibilities of a long loss of offsite power (which can be site dependent) have to be investigated precisely. If a maximum duration of 24 hours is convenient at the conceptual stage, at a later stage, the designer would have to identify clearly the initiating events which could lead to a loss of offsite power with long duration ;
- due to the uncertainties related to the delay for core uncovering in the case of a loss of offsite power in state D, the situation of a loss of off-site power in state D followed by the failure of the four main diesel generators has to be investigated precisely taking into account the provisions implemented to cope with this situation ;
- the expected reliability parameters for the diesel generators and the independence between the two types of diesel generators have to be justified ;
- the provisions taken for maintaining the integrity of the primary pumps seals in the long term have to be justified ;
- the autonomy of the emergency feedwater system tanks has to be carefully checked for all the failure chronologies ; a failure probability of refilling should be introduced in the corresponding sequences.

2. the sequences of the probabilistic safety assessment associated to a loss of the cooling chains :

- the possibilities of long loss of ultimate heat sink durations (which can be site dependent) have to be assessed ;
- due to the uncertainties related to the recovery of the ultimate heat sink before the containment and the inner refuelling water storage tank conditions could reach too high values in state D, the loss of heat sink situation (taking into account the corresponding provisions which may be site-dependent) has to be investigated precisely ;
- the efficiency of the diversification of the cooling of two pumps of the low head safety injection system by chillers of the instrumentation and control systems has to be justified.

Due attention has also to be paid to :

- the frequency and consequences of a total loss of the fuel pool cooling system, with specific attention paid to situations with unloaded core, taking into account the means which could be used to cope with such a failure as well as specific measures to be implemented during maintenance of one train ;
- all the possible causes of an inadvertent water level drop in the reactor cooling system during shutdown states, taking into account the detailed design of the plant and the foreseen operational practices ;
- concerning the total loss of feedwater, all the possible dependencies between the start-up and shutdown system and the main feedwater system.

E.2 - Protection measures against core melt accidents

E.2.1 - Safety objectives

As stated in section **A.1.1,** accident situations with core melt which would lead to large early releases have to be practically eliminated. Low pressure core melt sequences have to be dealt with so that the associated maximum conceivable releases would necessitate only very limited protective measures in area and in time for the public.

-

Due to the fact that, up to now, there is only limited experience related to the consideration of severe accidents in the design of pressurised water reactors, the following guidelines are more detailed than those related to reference transients, incidents and accidents and multiple failures conditions.

E.2.2 - Practical elimination of sequences with large early releases

E.2.2.1 - Prevention of core melt under high pressure and direct containment heating

As stated in section **A.1.3**, a design objective is to transfer high pressure core melt sequences to low pressure sequences with a high reliability so that high pressure core melt situations can be "excluded".-

This objective implies to limit the pressure in the reactor coolant system in the range of 15 to 20 bar, at the moment of the reactor pressure vessel rupture. This objective can be ensured by adding, to the depressurization function of the pressurizer valves, a dedicated bleed valve with an isolation valve as described in paragraph **B.2.3.6**.

The discharge capacity of the dedicated valve has to be determined considering the following situations, with realistic assumptions :

- loss of off-site power with unavailability of all diesel generators,
- loss of off-site power with unavailability of all diesel generators but with recovery of water supply during core melting,
- total loss of feedwater combined with the failure of the primary feed and bleed[18].

However, sensitivity studies regarding the discharge capacity, the hot gas temperatures and the opening criteria have to be performed by the designer considering delayed bleeding and late reflooding as well as the uncertainties of the code models related to the late core degradation phase or reflooding. These sensitivity studies will also assist in determining the way of actuation of the dedicated valve (manual or automatic), considering the possibility of human errors during the course of the accident.

The dedicated valve and its isolation valve must be qualified under representative conditions. Experimental justifications may be necessary, especially for those conditions that deviate considerably from normal operating conditions.

On another hand, design provisions have to be taken to cope with the mechanical loads which would result from the reactor pressure vessel failure at 20 bar so as to limit the vertical upward movement of the reactor pressure vessel.

Moreover, design measures have to be taken to limit the dispersal of corium into the containment atmosphere in the event of a reactor pressure vessel meltthrough, to prevent "direct containment heating". These design measures are related to the reactor pit and its ventilation as well as to the excore neutron measurements, so as to ensure that large quantities of corium released from the reactor pressure vessel cannot be carried out of the reactor pit.

E.2.2.2 - Prevention of fast reactivity accidents

The "practical elimination" of fast reactivity accidents implies a detailed assessment of each heterogeneous dilution scenario, considering the whole set of lines of defence for this scenario.

The analysis could proceed with the three following steps :

- a maximum volume size for deborated water slugs is defined on the basis of thermalhydraulic and neutronic considerations with respect to core subcriticality, independently of real dilution scenarios ;
- this maximum volume is used to define deterministic means to ensure that this volume is not overpassed for each real dilution scenario ;
- a probabilistic assessment is used to check that, for each real dilution scenario, the overall implemented provisions provide adequate defence in depth to "practically eliminate" the corresponding reactivity accidents.

[18] It is supposed that the pressurizer valves are not available ; the dedicated valve and its isolation valve remain available.

Concerning the first step, calculations concerning mixing phenomena would have to be done with different codes, including validation calculations using preferably hydraulic experiments in large scale test facilities.

Concerning the second step, all dilution scenarios have to be precisely investigated, including those resulting from operator errors, auxiliary systems malfunctioning, leakages of steam generator tubes as well as those concerning borated water tanks.

It is underlined that the implementation of an automatic F1A switch-over of the chemical and volume control system (CVCS) charging pumps suction to the inner refuelling water storage tank to mitigate dilutions coming from the CVCS lines actuated on detection of diluted flow through a single F1A boronmeter, composed of a neutron source and four flux detectors would be a positive design measure[19]. However, the capability of the boronmeter to be classified F1A has to be established.

Adequate means has to be defined by the designer for the "practical elimination" of heterogeneous boron dilution scenarios through component cooling water system cooled heat exchangers. In particular, requirements from the corresponding studies could be provided to pump designers in order to avoid inadmissible heterogeneous diluted water plug formation in connected auxiliary systems through seal cooling means of their pumps.

Moreover, it is emphasized that, in the case of a station blackout, when the residual heat removal is ensured by the steam generators in the reflux-condenser mode, low borated water could accumulate in the primary circuit ; this situation has also to be carefully assessed by the designer.

It is also underlined that high boron concentrations at the beginning of life of the core would reinforce the attention to be paid to "practically eliminating" reactivity accidents resulting from fast introduction of cold or deborated water. These boron dilution accidents have to be seen in connection with the reactivity margins in the shutdown systems.

At last, as inherent dilution mechanisms occur during some accident situations (e.g. boiling-condensing heat transfer mode inside steam generators during loss of coolant accidents, reverse flow in case of steam generator tubes ruptures, ...), these mechanisms and the corresponding codes have to be fully assessed, considering the mixing phenomena which can mitigate the plugs of deborated water. Some configurations need special attention : simultaneous insertion of two plugs into the reactor pressure vessel, restart of natural circulation in a loop without safety injection, low density plugs entering the reactor pressure vessel. In particular, design measures such as appropriate automatic interlocks have to be implemented for all relevant PCC and RRC-A conditions to exclude the restart of reactor coolant pumps after a significant inherent heterogeneous dilution.

[19] Furthermore, the designer has to investigate the possible use of the F1A boronmeter designed for heterogeneous dilutions to prevent recriticality due to homogeneous boron dilution.

E.2.2.3 - Prevention of steam explosions

In-vessel phenomena

A high mechanical energy release would be necessary to threaten the reactor pressure vessel and the containment ; nevertheless, the designer has to assess the potential for in-vessel steam explosions linked to core melt. Due attention has to be paid to :

- the justification of the maximum mixed mass, taking into account the specific design of the lower core support plate and uncertainties related to core relocation and behaviour in the vessel lower head ; in this frame, reflooding scenarios have to be precisely assessed ;
- the transposition of the experimental results[20] to the specific design of the nuclear power plants of the next generation;
- the range of the vessel upper internal structures and head temperature rises during core melt sequences and their consequences ;
- the behaviour of the reactor coolant system (including the steam generators) in the case of an energetic water slug through the downcomer resulting from an in-vessel energetic melt water interaction.

Ex-vessel phenomena

The amount of water which could be present in the reactor pit and in the spreading compartment at the time of the reactor vessel meltthrough has to be limited by the design. The possibility of a large steam explosion during corium flooding must be prevented and loads resulting from melt-water interaction must be taken into account in the design**.**

E.2.2.4 - Prevention of hydrogen detonation

As stated in paragraph **B.1.4.1**, the possibilities of local high level hydrogen concentrations must be prevented as far as achievable by the design of the internal structures of the containment. When it is not possible to demonstrate that the hydrogen local concentration remains below 10%, specific criteria[21] could be used, as far as they are fully justified and validated, to demonstrate the prevention of deflagration to detonation transitions and of fast deflagrations ; otherwise, adequate provisions have to be implemented such as reinforced walls of corresponding compartments and of the containment.

A systematic and deterministic approach regarding the selection of relevant scenarios in terms of hydrogen release rates has to be performed by the designer, taking into account the mitigation means and it has to be proved that the selected scenarios are bounding.

[20] Including results from the BERDA facility.

[21] Such as the 7 λ criterion or the σ criterion.

Concerning the mitigation means, a concept with only recombiners and no igniters implementation including a direct discharge of the primary circuit into the containment via a large pressurizer relief tank with two discharge pipes equipped with rupture disks, the discharges being directed to two reactor coolant pump compartments, is acceptable in principle and has the potential to fulfill the safety objectives mentioned above. But it has to be optimized and the methodology as well as the tools used for the demonstration have to be fully justified and validated.

It is however underlined that significant uncertainties exist concerning the production of hydrogen during severe accident sequences; these uncertainties are essentially linked to such phenomena as late flooding of a partially damaged core at high temperature, slumping of molten core material into residual water in the lower head of the reactor pressure vessel and interactions between corium and sacrificial materials. These uncertainties call for investigations with various codes and models.

Notably, scenarios with passive or active reflooding as well as scenarios characterized by multiple release locations have to be addressed in the demonstration of the effectiveness and of the robustness of the hydrogen risk mitigation concept.

It is emphasized that the consequences on the mixture inflammability of the steam partial pressure decrease following actuation of the containment heat removal system has to be precisely assessed by the designer, considering various start up times.

E.2.2.5 - Prevention of containment bypass

As stated in section **A.1.3**, "accident sequences (with core melt) involving containment bypassing ... have to be "practically eliminated" by design provisions ... aimed at assuring reliable isolation and also preventing failures".

Concerning the low head safety injection/residual heat removal system (LHSI/RHR), the continuous monitoring of the pressure and of the temperature in the pipe sections between the first and second reactor coolant system isolation check valves which are kept under the accumulator pressure would provide for an effective surveillance of the leaktightness of these check valves. Nevertheless, in order to "practically eliminate" core melt with containment bypass due to a realistic significant leak through the two isolation check valves, the designer has to justify the capability of the motor operated isolation valves located outside the containment on the safety injection lines to stop a reverse flow (that might be a two phase flow). In any case, the pipe sections of the LHSI/RHR system outside the containment up to and including the motor-operated isolation valves have to be designed so that their integrity would be maintained under primary coolant conditions.

The safety importance during residual heat removal operation of the leaktightness of the check-valve located on the LHSI/RHR suction line from the inner refuelling water storage tank as well as of the check-valve on the medium head safety injection line inside the containment must also be underlined. Specific attention shall be devoted to the closure of these check-valves subsequently to a switch-over sequence from safety injection to residual heat removal mode, taking into account the possible presence of particles in the flow going through each of these check-valves during safety injection. In any case, adequate provisions have to be implemented to guarantee the integrity of the concerned parts of the safety injection system outside the containment in case of leakage through these check-valves.

Stringent design requirements have to be implemented to the parts of the residual heat removal system outside the containment so as to prevent large breaks in these parts of the system. Besides, the capability of the isolating valves for closing has to be proven for all break sizes (up to a guillotine break), including two phase flow[22].

Concerning the possible breaks inside the reactor coolant pump thermal barriers and inside the chemical and volume control system high pressure cooler, the designer has to justify the maximum break size taken into account as well as the provisions implemented for the detection and isolation of such a break, even for two phase flow conditions.

Concerning the possible breaks inside the LHSI/RHR system heat exchangers, the designer has also to justify the maximum break size taken into account and to evaluate the consequences of such breaks on the component cooling water system circuits with respect to the pressure and temperature build-up.

As regards core melt accident sequences which could occur during shutdown states with open containment building, the designer has to specify the different phases of shutdown states for which an open containment is permitted. It would be advisable that the containment would be maintained in a closed position with the annulus ventilation system in operation at least for states A, B and C (with a coolant temperature higher than 70℃) as well as within state D before the refueling phase. The secondary side of the steam generators would also be closed and the containment isolation devices would be operational during the same phases of states A, B, C (with a coolant temperature higher than 70℃) and D before the refueling phase. Anyhow, the designer has to show that, for representative accident sequences, the containment building would be reliably closed before significant radioactive releases could occur inside the containment ; as stated in paragraph **B.1.4.2**, this requirement concerns notably the containment hatch.

As regards core melt accident situations with a significant leak of the steam generator tubes (up to multiple steam generator tube rupture), the following situations have to be investigated : single or multiple steam generator tube rupture with the loss of systems necessary to cope with this rupture, single or multiple steam generator tube rupture with the failure to close of the corresponding main steam isolation valve, steam pipe rupture with associated steam generator tube leaks, spurious opening of a secondary safety valve with associated steam generator tube leaks.

As core melt sequences with consequential steam generator tube failures have to be "practically eliminated", scenarios leading to natural circulation flow through the primary loops and the steam generators have also to be precisely investigated with adequate validated codes.

[22] It is recalled that the guillotine break of the largest pipe is a reference accident (PCC 4).

E.2.2.6 - Prevention of fuel melt in fuel pool

As far as the fuel pool is not situated in the containment building, it has to be demonstrated that spent fuel melt conditions in the pool are "practically eliminated". This demonstration has to take into consideration the case of earthquake.

E.2.3 - Mitigation of low pressure core melt scenarios

E.2.3.1 - Ex-vessel molten core coolability

Regarding the basemat of the containment building, the objectives stated in section **A.1.3** for low pressure core melt situations can be achieved as mentioned in paragraph **B.1.4.1** by the implementation of a large "dead-end" spreading compartment and the cooling of the corium when it is spread on this large area. This large spreading compartment would be spatially separated from the reactor pit and protected from the thermo-mechanical loads consecutive to the reactor pressure vessel failure. Design provisions would prevent the flow of condensate from any part of the containment into this compartment. Moreover, a steel gate would physically separate the reactor pit from the spreading compartment.

In this concept, sacrificial concrete layers would be implemented in the reactor pit and in the spreading compartment to obtain adequate characteristics of the melt. The basemat penetration would be prevented by a protective refractory layer covered by a steel layer. The cooling of the melt would be ensured by melt flooding from above by water coming from the inner refuelling water storage tank. Thermal loads on the basemat would be limited by a thick steel plate under a protective layer (refractory $ZrO2$), with cooling channels linked to the containment heat removal system.

Up to now, no validated code system can describe reliably the phenomena for severe accident sequences. So, the design of the reactor pressure vessel cavity and of the large spreading compartment, including the corium cooling, have to be justified by the designer on the basis of experimental results and associated calculations relative to a large spectrum of potential scenarios.

Experiments are necessary to investigate the different spreading conditions which might occur (rapid outpouring, slow outpouring, successive outpourings, local frozen corium formation, crust formation, ..) and the possibilities of highly energetic corium-water interactions as well as the erosion of sacrificial materials and its influence on the melt composition in the spreading compartment. In particular, there is a need for separate effects experiments in order to assess the physicochemical and thermodynamical properties of corium and mixtures. Spreading tests should also be performed with corium-like materials up to a representative scale, taking into account the actual concept of the spreading compartment, notably the implementation of sacrificial materials.

The robustness of the concept described above will have to be checked for various scenarios, including late reflooding and low residual power scenarios; specific attention has to be paid to the gate opening (notably the possibility of an early or partial failure of the steel gate) as well as to the optimization of the reactor pit design, in terms of composition and masses of the sacrificial concrete layers and of the transfer channel between the reactor pit and the spreading compartment. The refractory layer behaviour has also to be validated taking into account the capacities of the cooling systems (notably the critical heat flux) and the possibilities of thermochemical attacks by iron oxides or corium oxides. Specific attention has also to be paid to the long term liquid melt conditions in the spreading compartment and the stability of the layered system under these conditions.

E.2.3.2 - Containment heat removal without venting

The containment heat removal function in low pressure core melt conditions can be performed by a system achieving containment spray and corium cooling subdivided in two trains as described in paragraph **B.2.3.5**, with a dedicated cooling chain as a diverse system to the component cooling water system used for the systems related to core melt prevention. The pressurization of the dedicated cooling chain over the operating pressure of the containment heat removal system would ensure the absence of leaks from this system to the dedicated cooling chain.

Due attention has to be paid to the following topics :

a) the potential leaks of the system, notably :

- the design of the guard pipe on the non-isolable part of the suction line of the containment heat removal system as well as the surveillance of these line and guard pipe, taking into account possible corrosion effects ;
- the design of the parts of the containment heat removal system which are installed outside the containment and of the corresponding dedicated rooms, in connection with the reliability of the leak detection devices and of the isolation of a defective train ;
- the consequences of a leak in the containment heat removal system compartments (pressure, temperature, relative humidity, irradiation,…) with the classification of the corresponding equipment.

b) the possibilities of common cause failures of the containment heat removal system and of systems needed for core melt prevention, notably :

- the loss of common support systems : as the reliability of the heat removal function could be limited by the reliability of the support systems, including power supplies and ultimate heat sink, the designer has to investigate improvements as far as necessary in the frame of site specific studies
- clogging of the inner refuelling water storage tank filters : detailed information has to be provided by the designer : flow characteristics, volume and behaviour of the debris, …

c) the long term reliability of the corium cooling in the spreading compartment.

E.2.3.3 - Instrumentation

It is stressed that, for severe accident conditions, relevant information is needed not only by the operators but also by the crisis teams. A detailed proposal has to be presented by the designer with adequate justifications.

E.2.3.4 - Qualification under severe accident conditions

As stated in paragraph **B.2.2.1**, equipment needed in case of severe accidents has to be qualified for the conditions in which it is required. Notably, the behaviour of the penetrations and of the internal liner has to be investigated as far as necessary, taking into account the various phenomena which could occur in the course of severe accidents, notably hydrogen combustions ; the designer has to specify the corresponding qualification program.

E.2.4 - Safety demonstration

Severe accident conditions have to be assessed in the safety demonstration of nuclear power plants of the next generation. Examples of such conditions are :

- loss of offsite power with unavailability of all the diesel generators, i.e. station blackout as in RRC-A conditions combined with the unavailability of the small diesels,
- total loss of feedwater (as in RRC-A conditions) combined with the failure of the primary feed and bleed[19],
- small break loss of coolant accident with the complete failure of the safety injection system,
- loss of coolant accident (up to the surge line break) with the complete failure of the safety injection system.

However, the uncertainties related to some of the phenomena which could occur during severe accidents sequences call for the consideration of various scenarios and the performance of sensitivity studies.

For each of the computer codes used to justify the design, the designer has to specify its experimental validation and qualification and how the remaining uncertainties are taken into account (e.g. sensitivity studies).

Concerning the loads resulting from hydrogen combustion, with the hydrogen risk mitigation concept described in paragraph **E.2.2.4**, local dynamic effects due to such phenomena as fast deflagration or deflagration to detonation transition sequences are only expected on internal structures of the containment building ; provisions such as reinforced walls of corresponding compartments have to be implemented as far as necessary.

For the internal wall of the containment, it has also to be demonstrated that, taking into account the mitigation means and whatever the selected scenario, the pressure load resulting from an adiabatic, isochoric and complete hydrogen combustion does not exceed the containment design pressure at any time.

To demonstrate the achievement of the safety objective for low pressure core melt sequences described in section **A.1.1**, calculations of potential radiological consequences shall take into account realistic assumptions and parameters.

As a sensitivity study, the case of a small leakage from the reactor building to a peripheral building has to be assessed in detail, considering the leaktightness and retention behaviour of the concerned building.

F - PROTECTION AGAINST HAZARDS

F.1 - Protection against internal hazards

F.1.1 - General requirements

As stated in section **A.2.4**, the internal hazards to be considered in the safety demonstration include :

- failures of pressure retaining components ;
- internal floodings ;
- fires ;
- internal explosions ;
- internal missiles ;
- load drops.

The possibilities of common mode failures due to internal hazards can be minimized by the installation of the parts of the safety systems trains which are located outside the containment building in divisional areas designed so that even the complete loss of one divisional area due to a specific internal hazard would not prevent the fulfilment of the three basic safety functions, assuming the application of a single failure consistently with the safety demonstration rules applied for the reference transients, incidents and accidents. Installation provisions for redundant equipment of safety systems not separated by the divisional arrangement have to be specified by the designer.

Moreover, the safety demonstration has to be done for each internal hazard with the assumption that all the affected non-protected equipment is lost and with the consideration of an aggravating single failure and of first operator actions with the same rules as for the reference transients, incidents and accidents. In principle, internal hazards which do not result from such transients, incidents and accidents should not induce a plant condition which would be categorized as incident or accident. Otherwise, the designer has to show that this plant condition is covered, regarding its probability and consequences, by the assessment of the reference incidents, accidents and multiple failures conditions.

Links between internal hazards (such as floodings resulting from pipe breaks or fires resulting from explosions) have to be considered in the safety demonstration as well as internal hazards which could result from external hazards or severe accidents (see paragraph **F.2.2.1** for earthquakes).

F.1.2 - Requirements for the design of protection measures against internal hazards

F.1.2.1 - Failures of pipes, vessels, tanks, pumps and valves

The design and layout of pipes, vessels, tanks, pumps and valves shall be based as far as possible on the principle of physical or spatial separation in order to prevent the worsening of an initial event, assuming notably an aggravating failure consistently with the rules applied for the reference transients, incidents and accidents, and to avoid common cause failures in systems necessary to reach and maintain a safe shutdown state. In this respect :

a) the primary piping layout should be such that a failure in one loop would not induce a failure in another loop,

b) the primary and secondary piping layout should be such that a failure of the primary circuit would not induce a failure in the secondary circuit and vice versa,

c) a secondary pipe failure[23] should not lead to the simultaneous depressurization of two steam generators),

d) the depressurization of a steam generator from steam and water sides simultaneously should be avoided,

e) the first isolation valves on the branch connections should be located close to the main coolant lines.

Non-conformances with these rules have to be justified.

Regarding the effects of failures of pipes, vessels, tanks, pumps and valves, for high energy components (components of water and steam carrying systems with a pressure of more than 2,0 MPa or a temperature of more than 100℃ during normal operation, gas carrying components operated above the atmospheric pressure), the local effects to be considered include effects internal to the systems (pressure wave forces and increased flow forces) and effects on the neighbourhood of the components (jet impingement forces, reaction forces, pipe whips). Moreover, in every case, the global effects to be considered include flooding, increased ambient conditions and differential pressure forces for building structures**.**

In addition to the "exclusion" of the guillotine breaks of a main coolant line and of a main secondary line as stated in sections **B.1.2** and **B.1.3,** breaks could be "excluded" from the safety demonstration for vessels, tanks, pumps and valves designed, realized and operated with high quality requirements ; however this approach has to be clearly justified by the designer on a case by case basis, taking into account the operating experience of existing plants ; with these justifications, only leaks would have to be assessed. Other "exclusions" of breaks could be discussed for pipes of internal diameter of more than about 50 mm designed, realized and operated with high quality and surveillance requirements when these pipes are operated at high energy less than 2 % of the reactor life ; when these "exclusions" of breaks would be justified, only leaks would have to be assumed.

The locations of postulated pipe breaks or leaks to be considered have to be chosen considering not only the calculated stresses in the pipes but also the potential consequences of the high energy or low energy pipes failures in every compartment containing such pipes; this has notably to be applied to the containment penetration lines.

Moreover, appropriate assumptions have to be proposed and justified by the designer concerning the size of initial leaks through pipe wall cracks and from flanges and penetrations of pumps and valves as well as concerning the size of consequential leaks for pipes or other equipment aggressed by whipping effects of a broken pipe.

[23] See in section **B.1.3** the breaks to be postulated.

F.1.2.2 - Internal floodings

As regards floodings, complementary to the breaks and leaks of pipes, vessels, tanks, pumps and valves defined in paragraph **F.1.2.1**, potential intiators of floodings such as erroneous alignment, water ingress from neighbouring buildings, misoperation of a fire fighting system, overfilling of a tank, opening of safety valves, failure or spurious actuation of isolating devices, ..., have to be dealt with in the safety demonstration.

All relevant effects of potential floodings have to be considered, including those of an increase of the water level for active and passive components in the affected area, of a rise of pressure, temperature, humidity or radioactive ambient conditions for equipment in the affected area, of spraying for electrical components, of releases of boric acid, as well as resulting loads on the building structures, including doors and hatches. The delays assumed for necessary operator interventions have to be justified by the designer, taking into account the different sources of flooding which could occur simultaneously and the environmental conditions on the access routes.

In addition, avoiding underground water contamination must be a design objective ; the corresponding provisions have to be specified and justified by the designer even for the case of internal flooding of an auxiliary building.

F.1.2.3 - Fires

According to the "defence-in-depth" principle, fire protection includes fire prevention, fire detection and extinguishing (fire controlling) and mitigation of fire effects (fire containing). Priority is given to measures aimed at the limitation and encapsulation of fire loads, at the limitation of the formation of smoke as well as at avoiding ignition sources in the vicinity of combustible materials ; it means choosing uninflammable or hardly inflammable equipment and fluids as far as possible and appropriate; potential ignition sources have to be clearly identified and assessed.

Notwithstanding the preventive measures, the fire protection has to be based on the assumptions that a fire may break out anywhere in the plant and under any normal operating condition of the plant ; one fire at a time has to be considered. Particular attention has to be devoted to the fire protection provisions for shutdown situations, including maintenance activities. Moreover, the protection against fires which might break out during an abnormal status of the plant, in particular during post-accidental shutdown conditions, has to be specified by the designer.

Concerning the mitigation of fire effects, priority has to be given, firstly to physical protection by fire compartments, secondly to spatial separation by fire cells. Keeping safety related fire barriers in an open position during shutdown states must be exceptional and submitted to a case by case analysis with the definition of appropriate compensatory measures. This requirement has to be taken into account from the design stage.

The safety assessment of fire effects has to clearly identify common mode failures possibilities (including internal flooding risks linked to the use of fire fighting systems) which could result from incomplete separation of redundant equipment necessary to reach and maintain a safe shutdown state; in these cases, additional provisions have to be implemented as far as necessary. More generally, the functional failure of all equipment, except those with an adequately justified protection, has to be postulated within the fire compartment or the fire cell where the fire breaks out.

Moreover, the following points need to be underlined :

- the fire resistance rating of the fire barriers has to be specified by the designer, taking into account evolutions in knowledge ;
- the pressure effects due to a fire have to be evaluated ; if necessary, adequate qualification has to be provided for fire resistant closures of openings, in particular for those located at the boundary of a fire compartment ;
- the monitoring of fire spreading has to be considered as an aim in the design of the fire detection systems ;
- those countermeasures that are needed in case of fire to protect safety classified systems (fire barriers, fire detection and fire fighting systems) have to be seismically designed.

F.1.2.4 - Internal explosions

Priority has to be given to the prevention of internal explosions notably by the strict limitation of the use of explosive gases and fluids. The corresponding means as well as the links between internal explosions and other hazards have to be specified by the designer.

F.1.2.5 - Internal missiles

Internal missiles can originate from the failure of rotating equipment or from the failure of high energy components. These failures have to be prevented as far as possible by quality and surveillance requirements ; the corresponding measures have to be specified by the designer, notably the implementation of devices to prevent overspeeding of rotating equipment.

Nevertheless, studies have to be performed to assess the potential consequences of representative internally generated missiles, notably a low pressure turbine missile ; considering the results of these studies, additional provisions have to be implemented as far as necessary.

F.1.2.6 - Load drops

In principle, load drops on the safety related equipment shall be prevented according to the severity of the resulting consequences. The levels of defence against the load drops hazards (prevention, control and mitigation provisions to be implemented) have to be specified by the designer.

F.2 - Protection against external hazards

F.2.1 - Events to be considered

The external hazards to be considered in the safety demonstration and for which design provisions are asked for in section **A.2.5** include :

- earthquake,
- airplane crash,
- external explosion,
- lightning and electromagnetic interference,
- groundwater,
- extreme meteorological conditions (temperature, wind, snow, rain, ...)
- external flooding,
- drought,
- ice formation,
- toxic, corrosive or burnable gases.

Generally speaking, a good way to determine provisions to be implemented against external hazards is to define load cases. An appropriate methodology has to be defined for each external hazard to determine the loads as well as the structures, systems and components which have to be resistant against these loads ; moreover, for some external hazards, this approach has to be complemented by an event approach including, if necessary, functional analysis, to assess dependencies between external hazards and internal hazards or events.

F.2.2 - Requirements for the design of protection measures against specific external hazards

F.2.2.1 - Earthquakes

There exist two possibilities for the seismic design of a plant : to design with site specific spectra and acceleration values or to design using standardized spectra. In the latter case, an intensity of VIII in the MSK scale could be retained, for instance for the design of non site specific buildings and equipment ; this implies that, for some sites, adaptations could be necessary, on a case-by-case basis.

Considering the European seismotectonic context, the three spectra presented in figure **F.1** appear well adapted and sufficiently conservative for a standard design. Before any decision about the construction of a plant on a specific site, the designer has to prove that this standard protection is adequate in view of the actual features of the site.

The safety classified buildings must be designed with regard to earthquakes, using suitable criteria according to their functional requirements. Moreover, the safety functions must be fulfilled for the design basis earthquake, assuming damages to non-seismic equipment ; this implies a detailed verification of the behaviour of the installations, with due allowance for the precise layout of the equipment.

An "inspection earthquake" with a maximal horizontal acceleration of 0.05 g in the free field is convenient ; after the occurrence of an earthquake up to this level, no verification and inspection of the components important to safety would be needed prior to return or to maintain the plant to normal operation. However, adequate provisions have to be implemented at the design stage to allow inspections and tests which would appear necessary in case of exceedance of this acceleration level.

For the design of components and structures of nuclear power plants of the next generation, the combination of the design basis earthquake with the reference loss of coolant accident has to be taken into account. For the design of the internal structures of the reactor vessel, this requirement could be dealt with by considering a load case combining the design basis earthquake and the rupture of the largest pipe connected to a main coolant line. Moreover, concerning the design and the leaktightness of the containment, the designer has to specify his position about the combination of a steam line failure with the design earthquake. Systems necessary to cope with reference transients, incidents and accidents have to be designed or qualified for the combination of loads resulting from the corresponding transients, incidents or accidents and the design earthquake.

An event approach has to be applied to identify exhaustively equipment the failure of which could induce the failure of seismically designed equipment necessary for the fulfilment of safety functions ; this approach has to be complemented during the construction phase by a plant walkdown. Complementary design measures have to be implemented as far as practicable to suppress identified difficulties. Moreover, simultaneous failures of non seismically designed equipment have to be considered with an appropriate methodology.

The designer has also to specify how he intends to prove the existence of sufficient design margins consistently with the general safety objectives stated in section **A.1.1**. The margin assessment has to be achieved with the aim to demonstrate that no cliff-edge effect in terms of radiological consequences would occur for acceleration values postulated beyond the site specific acceleration values ; the corresponding methodology has to take into account the actual behaviour of representative equipment and the possibilities of simultaneous failures of equipment.

To cope with the potential long-term loss of off-site electrical power, all the emergency power supplies have to be seismically designed and qualified.

F.2.2.2 - Aircraft crashes

As regards aircraft crashes, provisions must be taken to ensure an adequate protection of safety related buildings with due consideration to the general and military aircraft traffics near the site and anticipating as far as possible their evolution during the lifetime of the plant.

Protection of the safety systems has to be considered with regard to the direct impact (penetration) as well as to the indirect impact by induced vibrations.

These objectives can be dealt with by the design of the reactor building, of the spent fuel building and of some auxiliary buildings (so as to ensure without redundancy the protection of equipment needed to shutdown the reactor and to prevent core melt)[24] using the load-time diagrams C1 and C2, presented in figure **F.2**, applied to a circular area of 7 m^2 in the following way :

1. Load-time diagram C1 has to be used for the design of the inner structures of these buildings against induced vibrations, assuming a linear elastic material behaviour and impact in the center of each outer protecting wall. To avoid extreme excitations, decoupling of the inner structures from the outer shells shall be used. As far as possible, fixing of systems and components at the outer walls should be avoided. The corresponding response spectra to be considered for equipment design have to be computed for the main structural elements of the buildings only.
2. Regarding protection against penetration, load-time diagram C1 has to be used for the design of the outer shells of the same buildings against the direct impact loads, so as to ensure that no penetration nor scabbing will occur and that deformation (rebars, concrete) would be limited.
3. In addition, the load-time diagram C2 has to be used for the design to the ultimate limit state (according to Eurocode 2, part 1)[25] of :
   a) the reactor building so as to ensure that perforation is prevented and scabbing which could occur would not jeopardize the shutdown of the reactor and the prevention of core melt,
   b) the spent fuel building so as to ensure that there is no uncovering of the spent fuel.

The dynamic analysis of induced vibrations can be carried out using a modal analysis superposition technique with the combination of modal responses according to "the square root of the sum of the squares" methodology.

It is underlined that, with an adequate layout ensuring a geographical separation of non-protected redundant equipment, it is not necessary to complement the corresponding load case approach by an event approach. However, it is pointed out that in connection to the fact that the steam lines are implemented by pairs and not protected against airplane crashes, the simultaneous emptying of two steam generators should be studied with adequate rules.

F.2.2.3 - Explosions

Concerning external explosions, it is necessary to take into account, for the design of nuclear power plants of the next generation, as a standard load-time function, a steep front triangular pressure wave with a maximum overpressure of 100 mbar and a duration of 300 ms. That is to say, the load-time function at the building walls, taking into account possible reflections from building walls and roofs, will result in a maximum overpressure at plane walls of 200 mbar.

[24] This paragraph implies that some auxiliary buildings can be designed without any protection relative to aircraft crashes as far as the equipment inside the protected buildings are sufficient for the shutdown of the reactor and the prevention of core melt without redundancy.

[25] The definition of ultimate limit state in Eurocode 2, part 1, is "associated with collapse or with other forms of structural failure which may endanger the safety of people". So the safety demonstration relative to this paragraph can take into account protecting walls other than the outer shells of the reactor building and the spent fuel building.

For an adequate protection of nuclear power plants of the next generation, the reactor building, the fuel building, the safeguard buildings and the diesel buildings must be protected as well as site specific structures and ducts related to the service water supply. In addition, the protection of the nuclear auxiliary building has to be considered with regard to the risk of radioactive releases.

Before any decision about the construction of the plant on a specific site is made, the designer has to prove that the standard protection relative to explosions is adequate taking into account the actual and planned industrial development around the site. Otherwise administrative measures must be taken or additional protection has to be provided.

Figure F.1 - SEISMIC SPECTRA

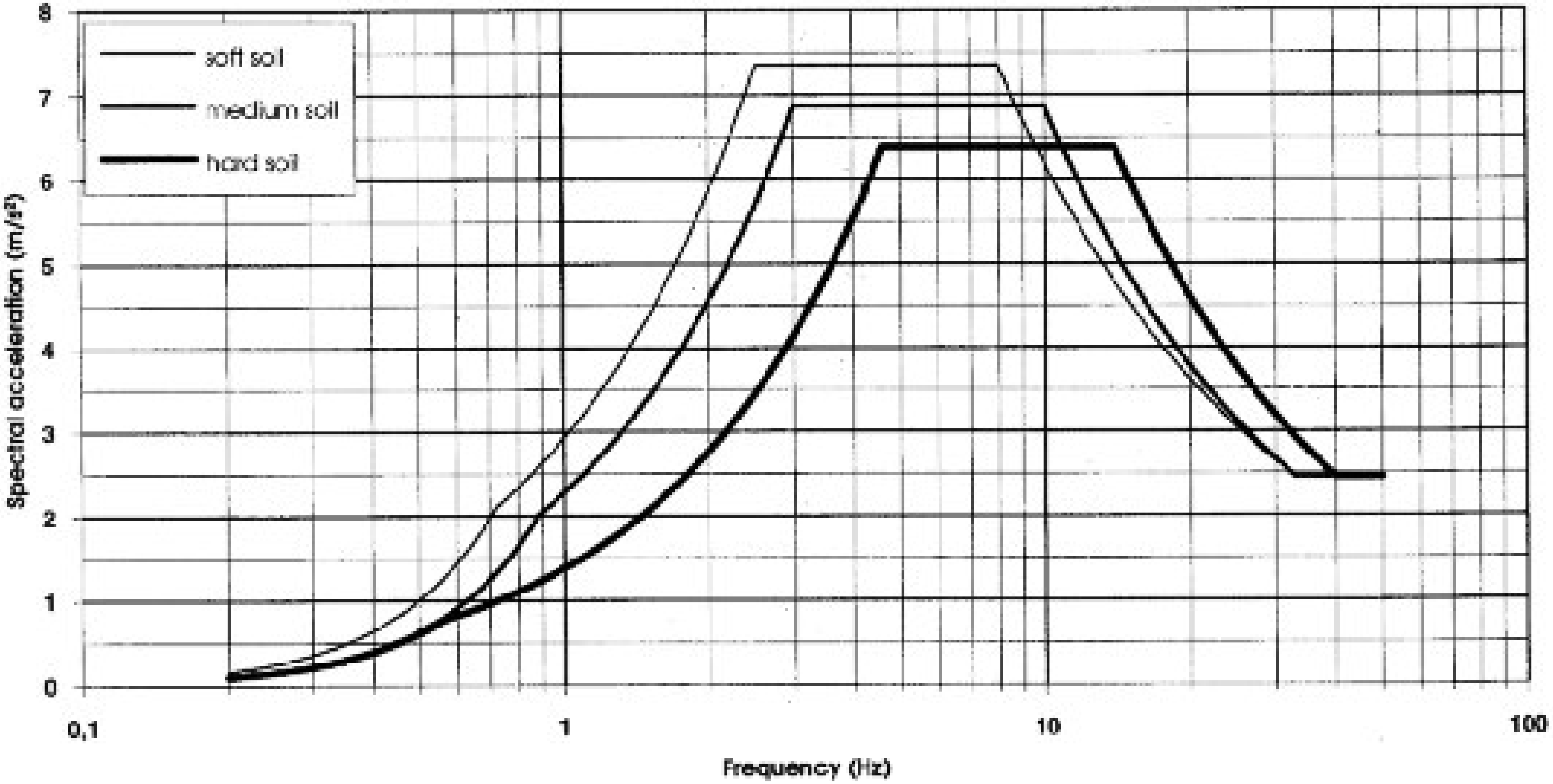
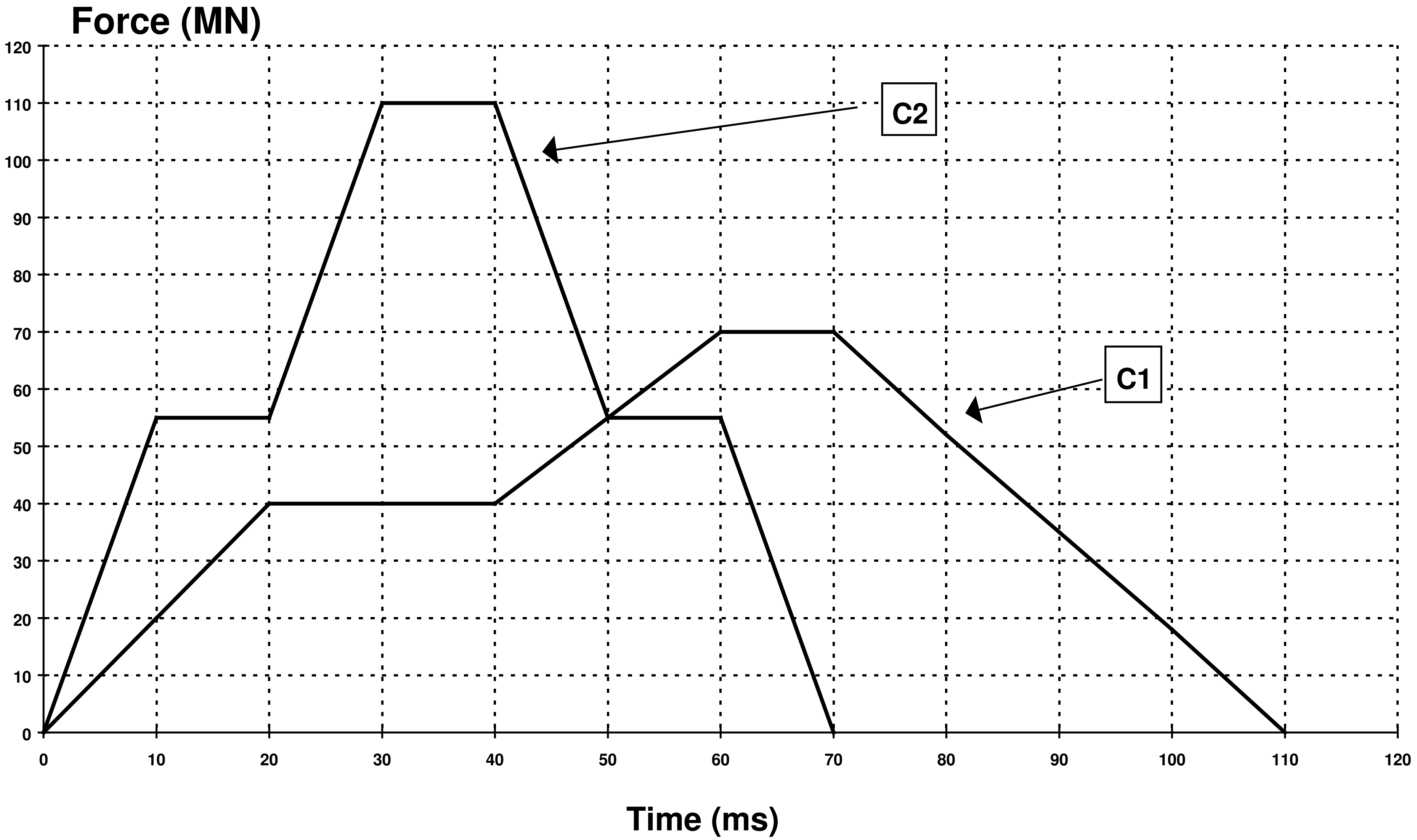


Figure F.2 - LOAD-TIME DIAGRAMS



G - SYSTEM DESIGN REQUIREMENTS AND EFFECTIVENESS OF THE SAFETY FUNCTIONS

G.1- Design of the fuel pool cooling system

The fuel pool cooling system could consist of two identical independent trains, each train with two pumps and one heat exchanger cooled by the component cooling water system.

The following requirements would be applied to the fuel pool cooling system :

- the design of the fuel pool and the arrangement of the suction and outlet nozzles of the fuel pool cooling system would be such as to prevent direct recirculation between outlet and suction of the cooling system ;
- the fuel pool temperature would be kept to less than 50°C during normal plant operation (power and shutdown states up to the beginning of core unloading in state E with one pump on one train in operation ;
- the fuel pool temperature would be kept to less than 50°C during shutdown states E and F with two trains in operation and one operating pump on each train ;
- the system and the fuel pool would have to withstand a temperature of 100°C. Restart and operation of the system have to be possible when the fuel pool is at 100°C.

Such a design allows the availability of one pump following the loss of one train with the assumption of an active single failure on the other train, recognizing that the "exclusion" of the passive single failure on this other train could be tolerated if stringent requirements are applied at the design and construction stages as well as for in-service inspection of the fuel pool cooling system and of the component cooling water system headers.

However, the approach relative to initiating events in the spent fuel pool cooling system and the associated support systems, has to be specified by the designer, with the classification of these events in the plant conditions or risk reduction categories and the corresponding assessment rules. The spent fuel pool cooling system design requirements must reflect the importance of the decay heat removal function. For reference transients, incidents and accidents, more stringent requirements should be applied to more frequent plant conditions. Notably, adequate limitations of the spent fuel pool temperature have to be defined for reference transients, assuming the failure of one train of the system, even during foreseen preventive maintenance[26] and periodic testing ; these limitations have to take into account requirements applied to the pool liner as well as to the concrete structures and to be consistent with the protection of other safety systems.

It is also stressed that the designer has to foresee provisions allowing the control of the total loss of the fuel pool cooling system while maintaining the confinement function ; otherwise, the likelihood of water boiling in the fuel pool has to be reduced by adequate improvements, notably regarding support systems of the fuel pool cooling system. Moreover, as stated in paragraph **E.2.2.6**, fuel melting in the pool has to be "practically eliminated" ; the designer has to provide justifications of this "practical elimination", including the results of probabilistic safety studies.

[26] The time necessary to restore the function in case of maintenance can be taken into account.

G.2 - Effectiveness of the leaktightness of the containment

As stated in paragraph **B.1.4.1**, a low leak rate of the inner wall of the containment is essential.

Due attention has to be paid to the following topics :

- the high performance concrete needs to be specified in detail ; acceptance criteria and adequate tests concerning parameters such as porosity, permeability, workability, shrinkage and creep have to be defined independently of the choice of a site. After the choice of a site, these tests will have to be implemented ;
- in addition to the investigations achieved by calculations in a first step, the validity of the construction tolerances and construction processes for a combined use of a high performance concrete and 55T15 tendons has to be experimentally verified at least by laboratory tests with the specified composition of the concrete ;
- the qualification process of the liner material and of the injection products has to be specified ; the choice of these components will be based on the results of the corresponding tests ;
- the inner wall of the containment building will have to be equipped with adequate instrumentation to accurately monitor the loss of prestress in the singular zones over time ; provisions need to be taken to replace or to supplement the corresponding devices if necessary.

Information has also to be provided by the designer concerning the provisions implemented to prevent non collected leaks from the containment during the whole lifetime of the plant. Anyway, this validity has to be proven by adequate testing.

Concerning the design of the annulus ventilation system, detailed information has also to be provided by the designer about :

- the assumptions related to steam condensation in the concrete of the inner wall of the containment have to be defined after due assessment of the available experimental results[27] ; the annulus ventilation system has to be designed accordingly,
- the time duration during which the annulus would be maintained at a negative pressure after the stop of the annulus ventilation system has to be specified and justified,
- the annulus ventilation system design has also to take due account of possible leaks or ruptures of components implemented on the outer wall of the containment building,
- the absence of electrical back-up of the annulus ventilation fans by the small diesels has to be justified,
- the interest of a permanent and recorded measurement of iodine and aerosols in the annulus ventilation ducts downstream the filters has to be assessed,
- detailed information has also to be provided concerning the confinement means associated to the annulus ventilation systems rooms, with the classification of the corresponding equipment.

[27] Including results from the MAEVA facility.

G.3 - Design of Instrumentation and Control

1. The requirements on safety related instrumentation and control (I&C) have to be described by the designer in a specification ; consistency of these requirements with the safety demonstration related to reference transients, incidents and accidents as well as to multiple failures conditions has to be justified.

2. Instrumentation and control functions can be categorized F1A, F1B or F2 according to the general safety function classification (see section **B.2.1**). The efficiency of the automated actions in these classes must ensure the defined grace periods for manual countermeasures in case of incidents.

3. To achieve these functions, the implementation of I&C systems architecture could be as follows :

a) process interface (instrumentation, switchgears and actuators) ;
b) system automation (monitoring and actuation of the plant in all normal operating conditions, core control, limitation functions, protection functions, support and post-accident functions, actuators control and prioritization of commands from classified functions) ;
c) plant supervision and control with man-machine interface.

4. The physical structure of I&C systems and equipment has to be designed in such a way that an adequate independence between functions in different levels of defence-in-depth can be demonstrated. This applies notably to boundaries between systems of different safety classes. Likewise, independence has to be demonstrated for redundant equipment provided to meet the single failure criterion as well as maintenance and separation (for protection against internal hazards) requirements ; F1 functions should be able of complying with the single failure criterion during maintenance or periodic test conditions. Independence must be justified by provisions such as segregation, isolation, autonomy, diversification ; in particular, provisions (including hardware and software diversity) have to be implemented to limit software common cause failures, as stated in section **A.2.2**.

5. In principle, the safety demonstration should be achieved considering the means normally used by the operators in the main control room. However, implementing a F1B classified conventional man-machine interface in the main control room in order to be able to achieve the safety demonstration with equipment classified F1 whereas the operator would use a computerized man-machine interface classified F2, could be accepted as far as :

a) the hardware and architecture of the computerized man-machine interface comply with requirements applicable to F1B systems,
b) the corresponding software complies with detailed qualification requirements to be proposed by the designer,
c) the means implemented for the detection and the signalling of the failure of essential F2 functions and equipment of the computerized man-machine interface comply with requirements applicable to F1B functions and equipment.

6. In addition to the main control room, a remote shutdown station has to be implemented for the case of unavailability of the main control room. The designer has to specify the situations for which the main control room would be unavailable, the consequences of such situations and consequently the tasks to be performed in the remote shutdown station and the associated means.

7. I&C failures have to be considered in a systematic way for the design and the safety demonstration of nuclear power plants of the next generation. Notably, the designer has to consider all reasonable possibilities for generation of initiating events by inappropriate actions of the I&C systems and to check if these initiating events are covered by the assessment of the reference transients, incidents, accidents and multiple failures conditions.
On another side, such inappropriate actions of the I&C systems have also to be considered in the assessment of the reference transients, incidents, accidents as aggravating failures. Only spurious actions (single or multiple) which can be the result of a single failure in I&C subsystems or support systems have to be considered.
Anyhow, suitable techniques have to be applied to reduce the possibilities of inappropriate actions when designing control computer hardware, software and functional applications. Specific attention should be given at the design stage to simultaneous control actions susceptible to design or operator error.

8. As stated in parts **A.1**, **F.1** and **F.2**, the safety demonstration of nuclear power plants of the next generation has to deal with internal and external hazards. This includes the consequences of such hazards on I&C systems. The possibilities of hazards originating in I&C equipment have also to be considered.

G.4 - Use of technical codes

As stated in section **A.1.2**, the quality of design, manufacturing, construction and operation is essential for safety in the frame of the first level of "defence-in-depth". Quality must be obtained and demonstrated notably by an adequate set of requirements for design, manufacturing, construction and operation, as well as by quality assurance. These requirements can be grouped in technical codes.

Concerning instrumentation and control equipment for nuclear power plants of the next generation, the following points are underlined :

- black box components (hardware and software) need to have a validated component specification based on specific tests and possibly on relevant experience feedback ;
- in principle, for instrumentation and control systems achieving F1A functions, software parts that are not used (i.e. unused code) shall be avoided ; exceptions shall be justified. Any unused code shall be identified. The unused code shall be specified, coded, verified and validated with the rest of the code of the concerned systems.

Concerning civil works for nuclear power plants of the next generation :

- the consistency of applicable rules has to be demonstrated, taking into account additions and modifications compared to existing technical codes ;
- an average residual compression criterion in the current part of the inner wall of the containment building is not sufficient to guarantee an adequate leaktightness of this inner wall including the singular zones under accident conditions ; supplementary criteria as adequate limitation of crack widths should be considered ;
- provisions shall be implemented to ensure the leaktightness of the inner wall of the containment building and of its penetrations for the combination of the surge line loss of coolant accident and of the design earthquake ; as far as they are justified, the corresponding criteria could be less severe than those applied for leaktightness under severe accident conditions ;
- measures taken to satisfy the design lifetime objective have to be specified and justified, taking into account the uncertainties related to the parameters that affect containment ageing ;
- adequate rules have to be defined to satisfy functional requirements related, on one side to other buildings than the reactor building, on another side to metallic structures (penetrations of the reactor building, spent fuel pool liner, ...).

Concerning heating, ventilation and air conditioning systems of nuclear power plants of the next generation :

- the design of the static and dynamic confinement devices of peripheral buildings including the nuclear auxiliary building, has to be consistent with the fulfilment of the safety objectives set in section **A.1.1** ; for severe accidents, sensitivity studies concerning the availability of ventilation systems and the leak rates in these buildings have to be presented ;
- the precise list of iodine risk rooms, including rooms where active liquid is routing during accident situations shall be specified by the designer, as well as adequate criteria for the confinement function of these rooms under the various accident situations, taking into account the suction effects of winds on buildings ;
- methodology has to be presented concerning the definition of basic atmospheric and extreme conditions (temperature, humidity, duration, ..) as well as the requirements to be applied, notably to ventilation systems, to cope with these conditions ;
- the design provisions taken to ensure the habitability of the main control room have to be detailed.