GEN IV International Forum

Expertise | Collaboration | Excellence

SAFETY DESIGN CRITERIA FOR GENERATION IV LEAD-COOLED FAST REACTOR SYSTEM

March 2021

Safety Design Criteria
for
Generation IV Lead-cooled Fast Reactor System

March 2021

Prepared by:

The LFR provisional System Steering Committee

and endorsed by:

The Risk and Safety Working Group
of the Generation IV International Forum

DISCLAIMER

This report was prepared by the Lead-cooled Fast Reactor provisional System Steering Committee of the Generation IV International Forum (GIF). Neither GIF nor any of its members, nor any GIF member's national government agency or employee thereof, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by GIF or its members, or any agency of a GIF member's national government. The views and opinions of authors expressed therein do not necessarily state or reflect those of GIF or its members, or any agency of a GIF member's national government.

AUTHORS

The Generation IV International Forum Lead-cooled Fast Reactor
provisional System Steering Committee (GIF LFR pSSC)

Alessandro Alemberti (Ansaldo Nucleare, Italy)

Kamil Tuček (European Commission, Joint Research Centre, Netherlands)

Minoru Takahashi (Tokyo Institute of Technology, Japan)

Toru Obara (Tokyo Institute of Technology, Japan)

Masatoshi Kondo (Tokyo Institute of Technology, Japan)

Andrei Moiseev (JSC "NIKIET", Russian Federation)

Lev Tocheny (JSC "NIKIET", Russian Federation)

Craig Smith (Naval Postgraduate School, United States)

Il Soon Hwang (Seoul National University, Republic of Korea)

Yican Wu (Institute of Nuclear Energy Safety Technology [INEST], People's Republic of China)

Ming Jin (Institute of Nuclear Energy Safety Technology [INEST], People's Republic of China)

Tao Zhou (Institute of Nuclear Energy Safety Technology [INEST], People's Republic of China)

Table of Contents

EXECUTIVE SUMMARY

Because of the unique safety characteristics of the Lead-cooled Fast Reactor (LFR), the Generation IV International Forum LFR provisional Steering Committee [GIF LFR pSSC] decided to develop a set of Safety Design Criteria [SDC] that are tailored to the LFR. It was agreed by the pSSC members to start the work on the basis of the previously-developed Sodium Fast Reactor SDC since these two liquid-metal cooled fast GIF Systems share some design solutions, and it was considered to be useful to use the same structure of the already-prepared SFR-SDC report, for the development of the LFR-SDC. The objective of the SDC is to present a set of reference criteria for the safety design of structures, systems and components of LFR systems with the aim of achieving the safety goals of the Generation IV reactor system. A set of eighty-two (82) reference criteria for LFR are systematically and comprehensively explained in the SDC herein.

The contents of the SDC are grouped into the following parts:

I. Chapter 1, *Introduction*, describes the background, objectives and formulation principles; and Chapter 2, *Safety Approach to the LFR as a Generation IV reactor system,* contains GIF's safety goals and basic safety approach, a fundamental orientation on safety, and the safety approach to a Generation IV LFR system.

II. In Chapters 3 to 6, the criteria for the overall safety design and specific structure, system and component design are described in sequence. The structure of this part is the same as that of the IAEA SSR-2/1 (Rev.1)[1] where safety requirements for the current generation light-water reactor power plants are listed. This style is used for the convenience of the users. The potential users of the SDC are not only GIF LFR concept developers, but also parties interested in the LFR technology in general, including international and national regulatory organizations. The differences between the IAEA SSR-2/1 (Rev.1) requirements and the GIF LFR SDC criteria are highlighted in the text in italic characters.

III. A Glossary, covering specific terminologies for the LFR system and for Generation IV reactor systems in general. A number of important terms, defined in documents such as the IAEA safety standards/glossary[2], are also incorporated for the convenience of the reader.

1. INTRODUCTION

1.1 Background and Objectives

Nuclear power plants must always ensure the highest level of safety that can reasonably be achieved in order to protect workers at these plants, the public and the environment from any harmful effects of the ionizing radiation or other hazards present at the installation. This statement is valid for all current nuclear power plants and serves also as guide for the development of the Generation IV nuclear reactors. The Generation IV International Forum (GIF) was established in 2000 to coordinate the R&D of the six nuclear systems that were recognized for having the potential to meet the demands for enhanced safety and reliability, economy, resource utilization, as well as security and proliferation-resistance that are expected to be required by the middle of this century.

As the high-level safety standard, the GIF Policy Group established the safety and reliability goals for Generation IV Nuclear Energy Systems in 2002 in a publication titled "Generation IV Nuclear Energy Systems under the GIF Roadmap (GRM)"[3] and the GIF Risk & Safety Working Group (RSWG) proposed the "Basis for Safety Approach (BSA) for Design & Assessment of Generation IV Nuclear Systems"[4]. In addition, in 2014, the RSWG, with input from the LFR pSSC, published a white paper on the safety of LFR systems[5], which was followed in 2020 by the publication of the LFR System Safety Assessment[6], prepared by the LFR pSSC in collaboration with the RSWG. Finally, an update of the LFR System Research Plan[7], hereinafter referred to as "SRP" is presently under revision by the GIF LFR pSSC.

It is expected that domestic codes and standards will be used when developing the detailed designs of structures, systems and components. However, there is a large gap between the high-level safety fundamentals and the detailed codes and standards, as illustrated in Figure 1.

The idea to establish "Safety Design Criteria (SDC)" to fill that gap, initially for one of the selected Generation IV reactor systems, was proposed and discussed at a GIF Policy Group meeting in October 2010. It was recognized that such SDC would fill the middle level of the safety standard hierarchy and would be essential to achieve the enhanced safety goals of Generation IV reactor systems. It was decided to start with the GIF Sodium Fast Reactor (SFR) systems (reactor and onsite fuel handling and storage systems), and a Task Force was set up to

draft a specific set of SDC for this type of reactor. Additional Safety Guides could be subsequently developed to fill the gap with codes and standards.

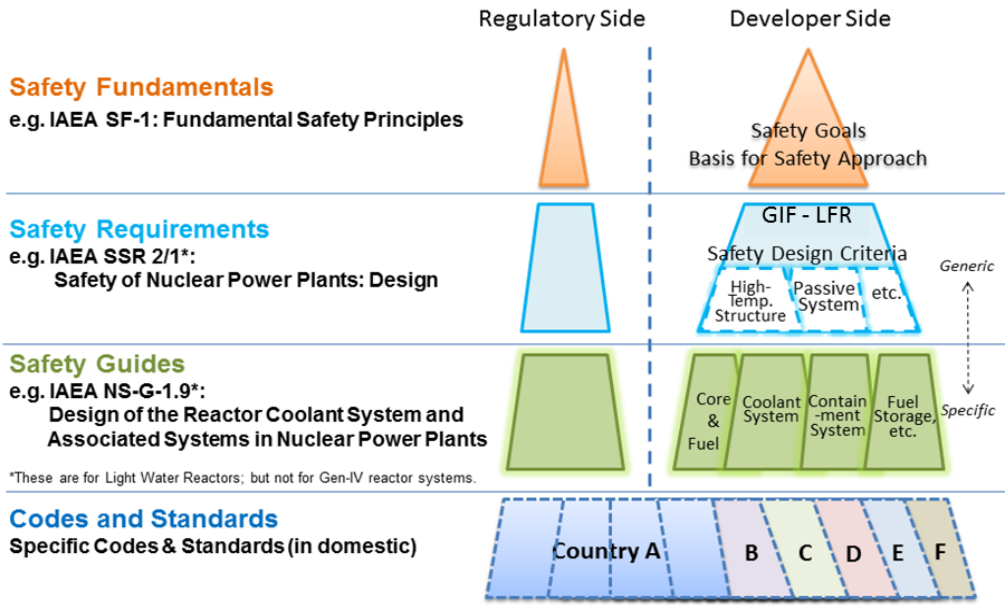


Figure 1. Hierarchy of Safety Standards

Following this first effort, the LFR-pSSC decided that the LFR maturity was sufficient to start the development of an LFR-specific set of SDC. Work started during 2014, and the present report is the result of discussions among members of the LFR pSSC, benefitting greatly from review and consultations with the GIF RSWG, ANL, IRSN and other partners of the Euratom collaborative project ARCADIA[8].

For water-cooled reactor systems, safety fundamentals (e.g., IAEA SF-1[9]) and safety requirements (e.g., IAEA SSR2/1, Rev. 1[1]) have been well established, and are extensively used, in parallel with comparable domestic standards, for the design and regulation of light-water reactors (LWRs) as well as heavy water reactors (HWRs).

Generation IV reactor systems, on the other hand, are advanced/new systems utilizing evolving technologies. Therefore, it is important that their associated safety aspects be taken into account from the initial phases of development, and in this way are likely to be better addressed by the developers.

To date, GIF has developed two fundamental documents, GIF Roadmap (GRM)[3] and Basis for the Safety Approach (BSA) for Design & Assessment of Generation IV Nuclear Systems [4]. System Research Plans (SRP) have also been developed for these systems, including the LFR system[7]. The GRM advocates goals for Generation IV reactor systems in the areas of 'Safety & Reliability'. The BSA provides technology-neutral methods on how to meet the goals for Generation IV reactor systems concerning their design and assessment processes.

As discussed above, the SDC are aimed at filling the gap between high-level GIF safety goals and detailed country-specific codes and standards, and the criteria in the SDC document are intended to be applicable to the design of the structures, systems and components including the reactor core, the fuel, the coolant system, and the containment. The SDC reflect GIF's fundamental safety approaches in order to achieve the safety goals of the Generation IV LFR systems.

The primary users of the SDC are expected to be the GIF LFR developers and designers. It is conceivable that the SDC, developed under GIF, can, in the future, be considered by the regulatory bodies as a reference for developing domestic LFR safety requirements. Hence, the potential users of the SDC may also include LFR developers and designers outside of GIF as well as regulatory bodies.

Note that the primary focus of this document is on heavy liquid metal, more specifically lead, as a reactor coolant, but other lead-based coolant options are also considered, especially lead bismuth eutectic (LBE). Where considerations for LBE coolant differ from those of lead, additional commentary is included in footnotes.

1.2 Principles of the SDC Formulation

There are three points to take into account in formulating the SDC as shown in Figure 2. First, the safety level required for Generation IV reactor systems should be achieved; second, the specific technical features of LFRs should be considered; third, the latest knowledge should be incorporated as it becomes available, such as R&D results for innovative technologies and lessons learned from the accident at the Tokyo Electric Power Company, Inc. (TEPCO) Fukushima Daiichi Nuclear Power Station.

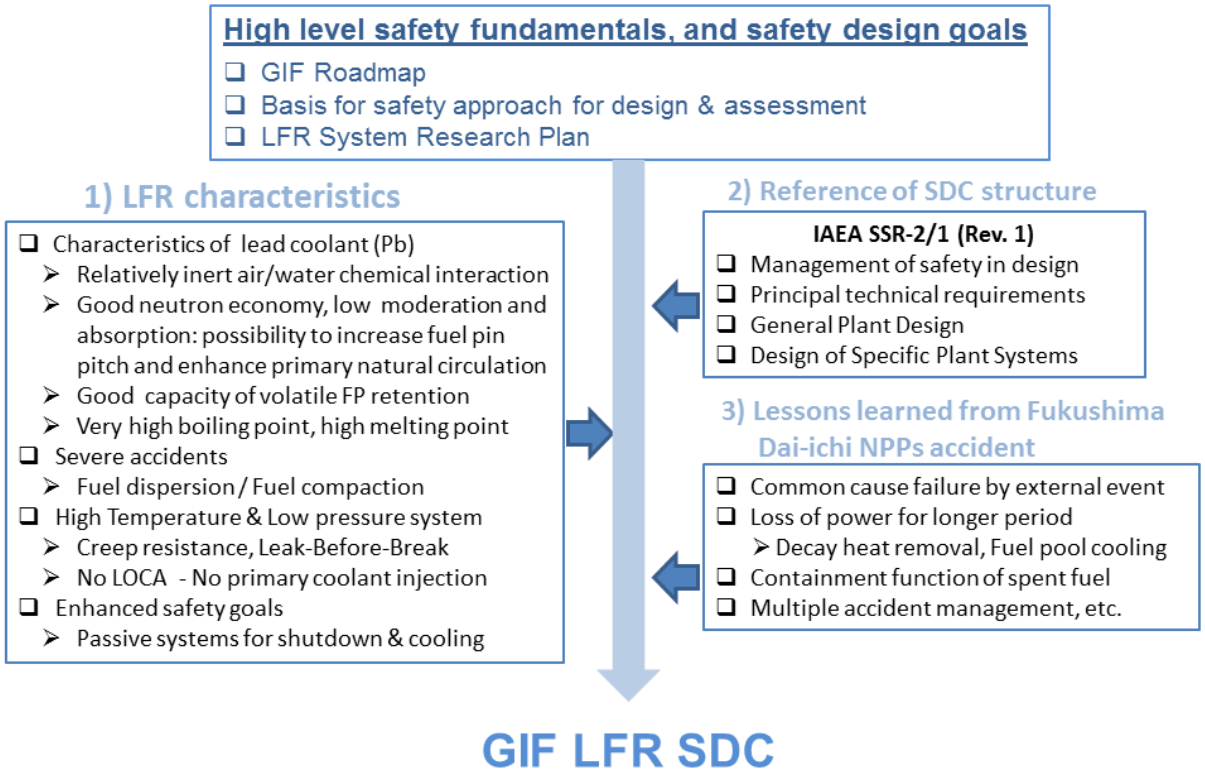


Figure 2. Basic Scheme for development of LFR - SDC

When formulating the SDC, the following three policies have been adopted:

1) Policy on goals

The LFR SDC document developed under the GIF is intended to be a consensus document by the international GIF LFR R&D community, including designers and developers, defining safety performance directions for Generation IV LFRs. In this sense, it can be viewed as the latest international opinion on what LFR safety criteria should be taken into account to serve as a reference for designers. At the same time, it is recognized that the actual LFR design details are the choice of the developers, and therefore it is not the intent of the SDC to define and/or select one specific design.

2) Policy on descriptions

Attention is given to the GIF safety goals and approaches, and the criteria providing performance targets are described in greater depth. The basis of LFR-specific criteria, including the reason and background, are provided for further clarification.

3) Policy in definitions and terminology

The IAEA SSR-2/1 (Rev. 1) is the safety design requirement that was established for Generation-III LWR systems by IAEA with the participation of nuclear regulatory bodies of various countries. When establishing safety design criteria for the Generation IV LFR systems, SSR-2/1 (Rev.1) is considered as a reference document in terms of its basic approach towards safety, comprehensive formulation, as well as terms and definitions. The LFR SDC maintains the basic structure of SSR-2/1 (Rev.1), and its original text is preserved wherever possible. The safety-related terms for the LFR SDC are basically the same as the ones defined in the IAEA Safety Glossary[2] (2018), and new definitions are added as needed for terms specific to the Generation IV LFR systems.

1.3 Practical Elimination of Severe Accident Situations with Large Core Melting

As one of the key design features, GIF LFR designs aim at practical elimination of severe accident situations with large core melting. The approach is based on: (i) utilization of the intrinsic features of lead as a coolant (high boiling point, relative inertness in contact with air and water, natural convection capability, and high thermal inertia); (ii) comprehensive understanding of the fuel degradation phenomena (including phenomena such as fuel dispersion / dissolution / segregation vs. aggregation); as well as (iii) the application of the fundamental principles of redundancy, independence as well as diversity[5]. As an example, in terms of decay heat removal, the latter involves enhanced redundancy, independence as well as diversity in: (i) operational modes (forced/natural convection on both primary and secondary side); (ii) design of the decay heat removal system and related components; and (iii) use of working fluids (lead, water, and air). The categorization and any possible related justifications allowing the “practical elimination” of certain accident sequences shall be further developed in concert with the progress of the specific design of the plant and current state of knowledge acquired through ongoing R&D. Detailed considerations concerning the safety approach for GIF LFR are given in Section 2.

2. SAFETY APPROACH TO THE LFR AS A GENERATION IV REACTOR SYSTEM

2.1 GIF Safety Goals and Basic Safety Approach

In the GIF Roadmap (GRM), three high-level safety and reliability goals for Generation IV reactors were proposed. The GRM also makes note of the essential role that safety has in nuclear energy. In the Basis for Safety Approach (BSA), the following issues are described: 1) the main safety principles (e.g., Defence-in-Depth[10], and risk-informed design); 2) the basic approaches for safety design and safety assessment; and 3) the safety assessment methods and tools. The definition of Defence-in-Depth and plant state generally follows the definition in SSR-2/1 (Rev.1) as shown in Figure 3, which consults INSAG-12[11] for the Defence-in-Depth principle: i.e., operational states include normal operation and anticipated operational occurrences; accident conditions include design basis accidents and design extension conditions.

As discussed in sub-section 1.3, GIF LFR designs aim at practical elimination of severe accident situations with large core melting, in which case the definition of Defence-in-Depth levels and plant states would correspond to Figure 4. In this case, the demonstration of practical elimination of severe accidents with large core melting remains under the responsibility of individual designers. In particular, each sequence possibly leading to a large core damage should be analyzed in detail to demonstrate practical elimination with a high degree of confidence.

<table>
<tr><th colspan="6">Defence-in-Depth Levels</th></tr>
<tr><th>Level 1</th><th>Level 2</th><th>Level 3</th><th colspan="2">Level 4</th><th>Level 5</th></tr>
<tr><td colspan="5">Plant states (considered in design)</td><td rowspan="4">Off-site emergency response (out of the design)</td></tr>
<tr><td colspan="2">Operational States</td><td colspan="3">Accident conditions</td></tr>
<tr><td rowspan="2">Normal operation</td><td rowspan="2">Anticipated operational occurrences</td><td rowspan="2">Design basis accidents</td><td colspan="2">Design extension conditions</td></tr>
<tr><td>Without significant fuel degradation</td><td>With core melting</td></tr>
</table>

Figure 3. Defence-in-Depth levels and Plant States based on IAEA INSAG-12 & SSR-2/1 (Rev. 1). Design extension conditions with core melting encompass severe accident conditions involving significant core degradation.

<table>
<tr><th colspan="6">Defence-in-Depth Levels</th></tr>
<tr><th>Level 1</th><th>Level 2</th><th>Level 3</th><th colspan="2">Level 4</th><th>Level 5</th></tr>
<tr><td colspan="5">Plant states (considered in design)</td><td rowspan="4">Off-site emergency response (out of the design)</td></tr>
<tr><td colspan="2">Operational States</td><td colspan="3">Accident conditions</td></tr>
<tr><td rowspan="2">Normal operation</td><td rowspan="2">Anticipated operational occurrences</td><td rowspan="2">Design basis accidents</td><td colspan="2">Design extension conditions</td></tr>
<tr><td>Without significant fuel degradation</td><td>With limited core damage</td></tr>
</table>

Figure 4. Defence-in-Depth levels and Plant States based on the practical elimination of all Severe Accident Situations with large core melting

The safety and reliability goals, which are proposed in the GRM, are explained in greater detail. The BSA also includes recognition of technology gaps by examining current plant technology and identifying potential safety improvements.

The overall safety and reliability goals are explained in the GRM and the BSA as follows:

1) Generation IV nuclear energy system operations will excel in safety and reliability, as they focus on safety and reliability in the DiD Levels 1-2 [Operational states].

2) Generation IV nuclear energy systems will have a very low likelihood and degree of reactor core damage. Reducing the frequency of initiating events is mentioned, as well as employing design features for controlling the progression of an accident in response to initiating events, and mitigating the consequences of any initiating events without causing core damage. Focus is given to safety design for severe accident prevention in the Defence-in-Depth Levels 1 - 4, and to reliable safety designs with accident management that improve the safety of the nuclear energy system.

   The demonstration of a very low likelihood and degree of reactor core damage will rely on a robust safety demonstration that uses a methodology for its analyses (based on “deterministic” and “probabilistic with associated confidence”) that addresses uncertainties and covers a large spectrum of events.

3) The GIF set a safety goal that Generation IV nuclear energy systems will eliminate the need for off-site emergency response. This indicates that measures must be taken to prevent significant radioactive material release to the environment.

   Although, this does NOT eliminate the need for off-site emergency response in the Defence-in-Depth Level 5, focus is given to the safety designs for severe accident mitigation in the Defence-in-Depth Level 4 (if severe accidents are not practically eliminated). The robustness of the design for design extension condition, as required for a Generation IV reactor, is judged by clarifying the prevention of its occurrence and/or the mitigation of its consequences.

2.2 Fundamental Orientations on Safety

2.2.1 Defence-in-Depth

The LFR SDC follows the Defence-in-Depth philosophy as the most basic safety approach. The safety design based on Defence-in-Depth provides design measures for every plant state, i.e., normal operation, anticipated operational occurrences, design basis accidents and design extension conditions. The design for operational states and the definition of design basis accidents shall be conservative with due account of uncertainties of design conditions and transient phenomena. For design extension conditions, the safety design process employed to prevent significant radioactive material releases to the environment shall be based on best estimate analysis.

In order to ensure the safety of a nuclear power plant facility, the release of radioactive materials must be limited. Beyond normal operation limitations, the appropriate management of radioactive materials and measures to accommodate abnormal events must therefore be provided for the reactor, as well as for the fuel handling and storage systems and for the radioactive waste management facility, and their possible mutual interactions.

Fundamentally, Defence-in-Depth is a rational response to uncertainties associated with the design construction and operation of a nuclear power plant. Defence-in-Depth is judged to be the most appropriate principle for a convincing and irrefutable safety demonstration[4].

One of the main goals of the Defence-in-Depth approach is to assure the so called "Basic safety functions"[11], reported here for completeness:

- Control of the reactivity (reactor power);
- Removal of heat from the core (cooling the fuel);
- Confinement of radioactive materials (within the appropriate barriers) and control of operational discharges, as well as limitation of accidental release.

2.2.2 Barriers and Levels of Defence

The principle of Defence-in-Depth is implemented primarily by means of a series of barriers which would in principle never be jeopardized, and which must be violated in turn before harm can occur to people or the environment[11]. These barriers are physical, providing for the confinement of radioactive material at successive locations.

The barriers may serve operational and safety purposes, or may serve safety purposes only. Power operation is only allowed if this multi-barrier system is not jeopardized and is capable of functioning as designed. The multi-barrier system protects humans and the environment in a wide range of abnormal conditions. Pre-planned countermeasures are provided, as a further component of Defence-in-Depth, against the possibility that radioactive material might still be released from the plant.

The relation between the physical barriers and the levels of defence, together constitute the Defence-in-Depth concept for existing nuclear power plants[11]. The general principle of the Defence-in-Depth concept remains applicable to future newly designed plants (including Generation IV nuclear power plant designs).

2.2.3 Strengthening of Defence-in-Depth for the Next Generation of LFR Plants

The approach for further improvement of Defence-in-Depth is similar for existing and for future (including Generation IV) plants[10]. This includes:

- improving accident prevention, in particular by optimizing the balance between the measures taken at different levels of Defence-in-Depth and by increasing their independence;
- improving the confinement function.

Possible means for strengthening accident prevention are:

- independence and diversity between safety features;
- increased grace periods (e.g., benefiting from large thermal inertia and natural convection);
- optimized human-machine interfaces;
- extended use of information technology;
- reduced complexity;
- improved maintainability;
- expanded use of passive features, in complement to active features;
- a more systematic consideration of the possibilities of multiple failures in the plant design.

The confinement function for advanced reactors should be strengthened by:

- Demonstration, by deterministic and probabilistic means, that hypothetical severe accident sequences that could lead to large radioactive releases due to early containment failure are essentially eliminated with a high degree of confidence;
- Explicit consideration in the design process of severe accidents that could lead to late containment failure (both for prevention and mitigation, if severe accidents are not practically eliminated as discussed in sub-sections 1.3 and 2.1); careful, realistic (best estimate) review of the confinement function and opportunities for improvement;
- Demonstration of no necessity for protective measures (evacuation or sheltering) for people living in the vicinity of a plant in accident situations (without core degradation). Demonstration, by best estimate analysis, that no or only protective measures (limited in scope, in terms of both area and time) are needed for severe accidents considered explicitly in the design (if not practically eliminated as discussed in sub-sections 1.3 and 2.1).

In LFRs, the confinement function is also strengthened by intrinsic characteristics of the coolant.

Meeting the safety objectives set for the next generation of nuclear power plants will necessitate improving the strength and independence of the different levels of defence[10]. The aim is to strengthen the preventive aspect and to consider explicitly the mitigation of the consequences of severe accidents (if not practically eliminated).

INSAG-5[12] recommends that new plant designs, whether derived in an evolutionary manner or by stepwise development on radically different lines, should include the following aims:

- Plant design concept should be extended to include required operating and maintenance procedures;
- Plant design should avoid complexity;
- Plants should be designed to be "user friendly";
- Plant design should further reduce dependence on early operator action;
- The design of systems to ensure confinement of fission products after a postulated accident should take into account the values of pressure and temperature of severe accident analysis;
- Accidents that would be large contributors to risk should be designed out or should be reduced in probability and/or consequences;
- The plant should be protected by design against sabotage and conventional armed attack;
- Design features should reduce the uncertainty in the results of probabilistic safety analysis;
- Consideration should be given to maximize passive safety features.

One of the most difficult questions associated with the safety of any complex technology that has the potential, although very small, for being the source of accidents that might result in significant loss or damage, is always the question of "how safe is safe enough"[4]. As a fundamental tenet, the Risk and Safety Working Group (RSWG) of the Generation IV International Forum believes that safety must be designed into Generation IV technology rather than added onto a basic, mature design through the addition of engineered safety features or backfits intended to reduce vulnerabilities that should have been recognized and eliminated in earlier phases of the design. Potential safety improvements, beyond those already incorporated in the existing nuclear power plants, should simultaneously include consideration of the following elements:

- the concept of "optimal risk reduction" (ALARP – As Low As Reasonably Practicable);
- the consideration of ambitious objectives;
- incorporation of innovative technologies;
- an emphasis on prevention backed up by mitigation;

- the search for robust safety architecture;
- the achievement of extremely reliable plant systems;
- the reduced reliance on human intervention; and finally
- the requirement for the improvement of safety demonstration's robustness.

For LFRs, the strengthening of the Defence-in-Depth aspects (as outlined in sub-sections 2.2.3-2.2.9) shall proceed progressively as designs develop, in a so-called "graded approach". The relevant R&D results, technology developments and qualification programs, as well as the acquired experience feedback with the operation of experimental facilities and reactor prototypes/demonstrators shall be taken into account as well. In this context, dedicated integral facilities and experimental programs to demonstrate the reliability and to qualify full size (or appropriately scaled-down) components are also necessary.

2.2.4 Risk-Informed Design

The second important principle, present already in the Defence-in-Depth concept, and that the RSWG[4] believes must be embodied in Generation IV technology is risk-informed design.

The strategy of Defence-in-Depth ensures that the fundamental safety functions are reliably achieved and with sufficient margins to compensate for equipment failure, human errors and hazards, including the uncertainty associated with estimating such events. This can be done through homogeneous coverage of the risk domain from frequent abnormal events to very low frequency accidents.

This coverage is attained by using the best data from experience feedback (as and when available) for improving the quality of data and analyses, and developing a systematic methodology to identify and manage the risks. Moreover, this methodology has so to merge Defence-in-Depth and probabilistic insights generating a risk-informed approach. The objective of such an approach is to generate safety requirements usable by the designer integrating deterministic success criteria and probabilistic success criteria.

Probabilistic safety assessment has become a highly sophisticated tool to identify potential accident scenarios, quantitatively estimate their probabilities of occurrence in a defined time period, and probabilistically estimate the consequences associated with postulated accidents in terms of a number of consequence parameters. Along with the traditional deterministic

methods, the methodology has come to be widely accepted as one of the bases for ensuring the safety of nuclear power (and increasingly other technologies as well) around the world.

Until recently, Probabilistic Safety Assessment (PSA) was primarily applied after the design was finalized, or even after the plant was built. Applied in this post-facto way, PSA was essentially used as means of measuring the level of risk associated with an operating facility. With the development of current evolutionary plants (Generation III), however, the value of PSA as an important contributor for the design process is recognized. Simultaneously, limitations have to be kept in mind, especially when the PSA techniques are applied to innovative concepts characterized by large uncertainties, lack of reliable data and lack of precise knowledge about provisions, degradation and failure.

Having said that, it is recognized that both safety and economics of Generation IV designs can be positively impacted by formally adopting the use of PSA techniques as a design driver throughout the design process to verify achievement of the whole set of objectives and criteria defined for the safety architecture of Gen IV systems. Ideally these techniques should be applied from the earliest phases of Generation IV plant design[13]. During the more conceptual phases of the design, the associated PSA models will be simple and conceptual as well. These models, however, should be used as a major input to influence the direction of the Generation IV design as it matures and becomes more detailed. As the design evolves, so too, will the PSA model. In this iterative way, the maturing PSA model will both reflect and drive the maturing plant design. Substantial potential exists to use this approach to optimize plant safety and capital costs by focusing safety features where they will do the most benefit, and by eliminating design elements that are unnecessary or marginal to safety.

Nevertheless, as a complement to all these considerations, there is general consensus[4] that, when applied to an innovative design, the PSA is a useful, but not sufficient, tool to assess the achievement of the complementary objectives defined for Defence-in-Depth in future systems. Specific tools, as for example the Objective Provision Tree [OPT][4], and the notion of Line of Protection [LOP][4], have to be implemented (and similar new tools developed) to help assessing their achievement; this will allow the designer to check how the concept fits with the full set of suggested criteria for Defence-in-Depth improvement while preparing the appropriate implementation of the simplified PSA.

The logic of these tools is quite simple: for a given level of Defence-in-Depth, and according to the progress of the approach (Safety functions > Challenges > Mechanisms > Provisions), the full set of provisions needed to address a given mechanism, and so to realize the intended purpose, represents the Line of Protection. The LOP integrates a wide variety of provisions and characterizes them, in a homogeneous way, through their performance, their reliability and the conditions of their mutual independence. The originality of the OPT, with regard to the conventional methods of representation of the safety architecture, lies in the fact that all the provisions are considered independently of their nature; this can represent a valuable precursor to the PSA. The corresponding R&D work to support the development of these tools and the methodology to implement them for the safety analysis, is an important objective within the context of the re-examination of the safety approach definition and content for Gen IV nuclear energy systems.

2.2.5 Simulation, Prototyping and Demonstration

The third important principle that the RSWG[4] believes must be embodied in Generation IV technology is the intelligent use of simulation, prototyping and demonstration capabilities.

Significant research and development that is currently being done around the world has the potential for reducing the duration of the development cycle, reducing both research and capital costs, and improving the safety of Generation IV systems[4].

Making use of sophisticated modelling tools and techniques and advanced computing power, modelling and simulation is increasingly important in the design and evaluation of complex technologies. Prototyping and demonstration systems are expensive and contribute to the long lead time associated with the development of new technologies. Making an increased use of modelling and simulation can provide a means of more thoroughly evaluating a candidate design, thereby reducing uncertainties, and improving safety. By focusing attention to those aspects of the design that are most critical to plant safety, development costs are reduced, and safety is enhanced.

It is obvious, of course, that the use of PSA to guide Generation IV system design is just one of the possible applications. However, similar benefits can be obtained from modelling and simulation applied to reactor physics, thermal hydraulics, fuel performance, materials behavior, and a number of other aspects that are central to reactor design and development.

While modelling and simulation should be used extensively in the development of Generation IV system designs, prototyping and demonstration facilities will also be needed. The overall aim of using modelling and simulation and prototyping is to reduce uncertainties in the design so that resources can be focused where they will be most effective and so the operating plant will be unburdened by unnecessary requirements and regulations. Modelling and simulation can be an effective way to identify those design ideas that are most promising and to eliminate undesirable features.

Ultimately, however, one of the most convincing means of further reducing uncertainties in those concepts that are near actual deployment may be to demonstrate their viability in carefully designed experiments. Some have gone so far as to suggest the idea of "licensing by test." In this approach to licensing, experiments in prototypes would be used to demonstrate to the satisfaction of a licensing authority the ability of a design to cope with an assortment of design basis challenges. Each regulatory body will, of course, define its own protocols. It is the recommendation of the RSWG[4], however, that an effective mix of modelling, simulation, prototyping, and demonstrations can be highly effective in reducing development time, improving safety, reducing uncertainties, and cost saving.

Finally, it is important to point out the fact that separate effects test facilities have to be made available for tools development and qualification. As already discussed, some dedicated integral test facilities will also be needed to achieve the component qualification well as tools validation.

2.2.6 Utilization of Passive Safety Features

Extensive use of passive safety systems is the preferred solution for LFRs in order to enhance safety against a number of wide-ranging events, including design basis accidents and design extension conditions.

For design basis accidents, it is important to well characterize the safety features of structures, systems and components, including inherent characteristics. The reliability of the safety systems could be enhanced based on proven technologies that have been conventionally and widely used.

For design extension conditions, however, it is possible to ensure diversity with different operation principles, without further multiplexing the measures already applied for design basis accidents. Using passive and inherent safety features of the design should allow termination of accidents or mitigation of consequences of a design extension conditions, even in postulated failure of active safety systems.

2.2.7 Prevention of Cliff Edge Effect

Severe accidents that could lead to a significant and sudden radioactive release due to a possible cliff edge effect, not reasonably manageable by design improvement, shall be practically eliminated by appropriate provisions.

The severe accidents that are determined to be practically eliminated should be restricted to those that are not deemed physically impossible as determined by deterministic and probabilistic considerations.

Safety demonstrations of practically eliminated situations shall be robust and based on deterministic and probabilistic analyses that address uncertainties and covers a large spectrum of events.

2.2.8 Provision against Hazards

An exhaustive approach is expected regarding the design basis against hazards, taking into account the type of hazards, combinations of loadings, and design margins.

One of the main lessons learned from the TEPCO's Fukushima Daiichi Nuclear Power Plants accidents is to recommend considering extreme external hazards as considered for the internal events and the possible combination of external and internal hazards in order to:

- improve the robustness of the power plant safety,
- confirm that consequences of degraded plant situations induced by extreme hazards are acceptable,
- define equipment that need to be strengthened to resist extreme natural hazards beyond the reference used for the plant design.

As hazards are a potential common cause failure that can impact several structures, systems and components, each safety function shall rely on appropriate diversification and physical separation for enhancing redundancy to ensure the safety function.

2.2.9 Non-Radiological and Chemical Risks

Non-radiological and chemical risks, introduced by the system features and processes, have to be reduced to as low as reasonably practicable, with the objectives to limit the impact on the outside of the plant area and to protect the health of workers and the public.

Non-radiological and chemical risks must be considered, in order to minimize the risk of nuclear power plant damage and to prevent simultaneous radioactive and toxic chemical releases in the environment, as cumulative consequences of an accident.

2.3 Safety Approach of the Generation IV LFR Systems

2.3.1 Target LFR Systems

The target systems for establishing the SDC are LFRs developed under GIF as described in LFR System Research Plan (SRP)[7], i.e., ELFR (600 MW_e), BREST-OD-300 (300 MW_e) and SSTAR (10-40 MW_e). The LFR SRP provides information about the configuration of the target LFR systems and explains the Generation IV system safety and reliability goals as developed from the GRM based on qualitative/quantitative design metrics. Naturally, the LFR SDC can be applicable as well to other LFRs designs.

The specifications of the GIF LFR systems are as follows:

System structure	Pool-type, Large, Medium size and Small modular
Electric output	10 - 600 MW_e
Coolant system	Primary coolant system utilizing lead coolant
Balance of Plant system	Water/Steam cycle for large and medium size Supercritical CO_2 or other gas cycle for small modular
Fuel	Oxides including Mixed-Oxide (MOX); Nitrides Minor actinide-bearing fuels may be used.

Technical solutions, based on state-of-the-art R&D[14],[15], are used to improve the safety design and to enhance reliability and robustness of the LFR. The ongoing efforts to develop new safety-related technologies include industrial partnerships and owners/operators as users.

2.3.2 Approach Based on the Basic Characteristics of the LFR

Core and Fuel Characteristics

Fuel elements and fuel assemblies are operated in a fast neutron spectrum under the conditions of high-power density, high burn up, and high temperature of lead. An important characteristic of an LFR, as for other fast reactors, is that the reactor core

is not in its most reactive configuration under normal operating conditions, and that it is possible to have a positive void reactivity in the center area of the reactor core. Considering this characteristic, the reactor core should be designed to prevent excessive reactivity insertion. However, the high boiling point of the lead coolant (1749ºC) makes coolant boiling extremely unlikely. On the other hand, gas/voids might appear in the core or its vicinity, for example as a consequence of a fission gas release from failed fuel pins or due to steam generator tube leakages or ruptures.

A positive reactivity effect may also be generated by core compaction. This aspect has to be adequately addressed and the reactor designed accordingly.

Physical, Chemical and Neutronic Properties of Lead Coolant

Neutronic properties – The requirement of a fast neutron spectrum for efficient fertile fuel utilization (conversion/breeding) and actinide waste burning is fulfilled by the use of lead as the coolant which has suitable neutronic characteristics (low moderating power, good diffusion properties, and low neutron absorption).

Density – The high density of lead generates buoyancy forces which should be considered in design of in-vessel structures, especially moveable equipment, like fuel and control rod assemblies. Moreover, challenges to the main vessel and reactor components in terms of seismic response needs to be specifically addressed.

Boiling/Freezing point – The margin to coolant boiling is very high for lead-cooled systems (correlated to the low partial vapor pressure and very high boiling temperature of lead), which makes coolant boiling rather hypothetical since system structures would melt well before the onset of boiling; this allows operating the primary system close to atmospheric pressure. Accident scenarios with boiling lead in the core are therefore considered to be highly unlikely. The freezing temperature[1] of lead is 327°C; coolant solidification has to be therefore prevented. Necessary features for heating of the coolant need to be foreseen to keep lead at the required

[1] Freezing temperature for Lead-Bismuth Eutectic (LBE) is 125°C with advantages in terms of margins to solidification and the possibility to operate at lower temperatures.

temperature in both planned shutdown (including reactor commissioning) and during emergency conditions. Efforts are ongoing to identify systems for freezing prevention and/or increasing of the grace time to freezing during decay heat removal. It is to be noted that lead freezing does not constitute itself a challenge to primary structures. For lead the concern is related to the blockage of circulation flow paths and operational procedures are to be applied for lead re-melting.

Heat transfer – Liquid lead has high thermal conductivity (17 W/m/K at 400°C). The heat transfer coefficients typical for lead coolant ensure efficient heat transfer and limit the temperature difference between outer cladding and bulk coolant. However, surface oxidation should be taken into account in the overall heat transfer evaluations since an additional thermal resistance may be present depending on the thickness of the oxide layer.

Thermal inertia – The volumetric heat capacity of liquid lead is high (roughly 1.54 $J/cm^3/K$). The high volumetric heat capacity combined with the inventory of the coolant present in the primary circuit provides high thermal inertia, which contributes to the slowing of any transient related to loss of forced coolant mass flow or loss of heat sink.

Natural convection capability – Liquid lead coolants have a large volumetric expansion coefficient (1.2×10^{-4} 1/K) and the possibility to operate in a large range of temperatures, typically a few hundred degrees, without boiling or excessive material corrosion-erosion. These characteristics enhance the possibility of core cooling by natural convection, in which pressure losses in the primary circuit are adequately compensated by buoyancy forces. Natural circulation is predicted to be well established in LFR primary systems, due to the simple flow path design and due to neutronic characteristics of lead that allow larger fuel pin pitches and lower coolant velocities, together resulting in low pressure drops.

Pressure – For pool type LFRs, due to the physical characteristics of the coolants, the pressure in the cover gas can be maintained close to atmospheric pressure, while in the pool itself the pressure depends on the hydrostatic level.

Induced radioactivity, coolant activity – Irradiation can, in some materials, lead to the formation of radionuclides that should be confined or their production limited from a radioprotection point of view. These nuclides could complicate inspection and maintenance of the reactor, and its future decommissioning. Pure lead[2] is not exempt from polonium formation; however, the rate of polonium production is very low, typically several orders of magnitude lower with respect to LBE. Additionally, the volatility of polonium is lowered through strong chemical reaction with the lead coolant (e.g., via the formation of lead-polonide), and only a very small fraction, depending on the lead temperature is expected to be vaporized into the Cover Gas System. In addition to its radiotoxic characteristics, heat generation from the decay of ^{210}Po shall be considered for operational as well as shutdown heat removal.

Retention of volatile fission and activation products – Lead provides a relatively good capacity for retention of important volatile fission products as well as activation products. A large body of literature on the chemical and thermo-physical properties of lead and its compounds with cesium, iodine as well as polonium is available and give indications of relatively good retention properties of these nuclides in lead (e.g., volatilized fractions[16] at 700°C for ^{137}Cs, ^{90}Sr, and ^{131}I are 1.1×10^{-6}, 5.1×10^{-14} and 3.7×10^{-6}). Nevertheless, further R&D studies are necessary to assess the corresponding retention capabilities in order to evaluate related occupational hazards and possible accidental source terms.

Corrosion-erosion – Since the beginning of research and development activities on lead coolants, one of the main R&D topics has been related to corrosion-erosion behavior of materials in the lead environment. Historically, corrosion control approaches have centered on oxygen control in the coolant, limitation of coolant temperature, and used of corrosion-resistant materials. More recently, new corrosion prevention approaches have been emerging to further limit corrosion to acceptable levels. Corrosion-erosion is included here for the sake of completeness,

[2] Polonium (^{210}Po) is formed mainly by neutron absorption of ^{209}Bi and the generation is proportional to the bismuth content in the coolant. This issue is significant and shall be addressed especially in the case of Lead-Bismuth Eutectic (LBE), and is considered to be a major difference between lead- and LBE-cooled reactors. The consideration of ^{210}Po shall include both its contribution to coolant radiotoxicity and its decay heat generation.

and the subject is dealt with in detail in the next paragraph dedicated to “operation in lead coolant environment”.

Interaction with oxygen and water – Lead coolants are relatively chemically inert in contact with water or air, which provides conditions for the elimination of the intermediate circuit in comparison with other liquid-metal cooled systems. However, in case of a steam generator tube rupture (SGTR) event, water interaction with lead needs to be considered and adequately prevented and/or mitigated, specifically in view of the potential for over-pressurization of the primary circuit, sloshing and steam/water entrainment, which might result in a positive reactivity insertion (considering the risk of steam/water entrainment in the core and the risk of core compaction) as well as formation of solid PbO possibly causing flow blockages.

Fuel-coolant interaction – In case of cladding failure, fuel and coolant may come into contact resulting in fuel-coolant interaction. Recent work on the topic has not shown formation of specifically troublesome compounds, and the interactions have shown to exhibit low energetics, favoring safety. Further investigations are ongoing to better assess the phenomenology of fuel-coolant interactions.

Coolant-concrete interaction – Based on the present knowledge, the coolant-concrete interaction is expected to be thermal rather than chemical. The penetration of lead into concrete cavities is also expected to be limited due to the high surface tension and high melting point of lead which promotes the formation of a solid layer as the lead coolant encounters temperatures below the freezing point of lead.

Toxicity – Possible releases of chemically toxic lead and its aerosols (lead oxide) need to be considered and properly managed. For example, a strict general annual limit is set for the concentration of lead in ambient air by European Council Directive 1999/30/EC (0.5 $\mu g/m^3$)[17], while occupational exposure limit (OEL), 8-hour time-weighted average, is 150 $\mu g/m^3$[18]. However, due to the low vapor pressure of lead coolants, the lead concentration inside the containment during refueling or in-service inspection operation (with the vessel open) appears to be reasonably low, and the containment mixing itself is expected to reduce this value

to the acceptable limit as stipulated for the external environment (e.g., for lead at 400°C, without considering containment characteristics and assuming a constant atmospheric pressure and temperature for air, the corresponding concentration is conservatively estimated to be about 2 µg/m^3[16]).

Opacity (and high cold state temperature) – Because of the opacity of lead (as well as its high operational temperature) in-service inspection (ISI) presents challenges. As such, certain ISI activities (e.g., visual observation, surface examination, volumetric examination with X-ray or ultrasonic devices) may be performed out of lead (with internal components designed to be readily removable) or alternatively by implementing new ISI methods or approaches for in-situ inspection such as those developed for SFR systems (with its opaque coolant)[19]. In the former case, R&D has been already performed to address the presence of a residual lead layer on structures and components and cleaning/washing techniques have been developed and are routinely used for facilities.

Operation in lead coolant environment

Flowing heavy liquid metals[3] are corrosive and can induce or accelerate a material failure under static (brittle fracture) or time-dependent loading (fatigue and creep).

A preventive measure to limit the corrosion risks is to design LFRs to operate within a relatively low temperature range while maintaining a controlled concentration of dissolved oxygen in the coolant, which must be high enough to support the formation of protective oxide layers on surfaces of structures (containing especially Fe and Cr) and, at the same time, low enough to prevent the formation of large amounts of PbO precipitation, which might lead to the fouling and slagging of the primary system and subsequently coolant blockages. For conventional materials, at temperatures around 500°C the corrosion protection through the oxide barrier seems to fail and the application of functional surface coatings (for example Al_2O_3, SiO_2 or aluminium alloy) or the use of steels with addition of silicon or aluminium is

[3] LBE, in terms of the mechanisms of corrosion, is very similar to lead. HLM corrosion is characterized by dissolution phenomena of structural metals into the coolant. Experimental data shows the solubility of structural metals at the same temperature to be higher in LBE, by about one order of magnitude, in comparison to pure lead.

therefore considered. Fuel cladding, upper core regions and heat exchanger primary coolant inlet regions are particularly sensitive to corrosion, because temperatures are the highest. At any rate, the integrity of the protective layer needs to be ensured during all plant operating conditions, including long-term transients, in order to ensure the integrity of the components. These surface coating techniques are already applied in some conventional plant (non-nuclear) applications, and an experimental program is ongoing to validate the feasibility and reliability of their use for material compatibility in nuclear plants.

To limit the erosion of structural materials as well as protective oxide films, the velocity of lead needs to be limited to a value resulting in negligible erosion (typically less than 2 m/s). When this is not possible, such as at the tip of a pump impeller, where velocities of the order of 10 m/s need to be expected, specific materials or dedicated coatings need to be employed. These materials are currently undergoing evaluation.

Measures for the detection of excessive corrosion do not differ with respect to other technologies and include: component inspection, vessel inspection, and detection of coolant impurities detection.

Mitigation measures, should excessive corrosion occur, are related to modification of the coolant chemistry if any deviation has been detected, recovering the correct oxygen content in the coolant, and may also include substitution of damaged components.

As an LFR operates at a relatively high temperature compared to an LWR (e.g., the coolant temperature range is around 400–600ºC) and in high fast neutron fluence conditions, due consideration of creep and radiation effects on fuel and structural materials is necessary. Because of the good thermal conductivity of lead and the relatively large temperature differences between the inlet and outlet of the reactor core, thermal striping needs to be considered and must be accounted for in the design to prevent structural damage.

Operation under low pressure conditions

As an LFR is operated in low pressure conditions, close to atmospheric pressure, and at temperatures well below the boiling point, coolant leakage or pipe break does not lead to the type of loss of coolant accident experienced in an LWR with depressurization, coolant boiling and the loss of cooling capability. Therefore, emergency core cooling systems for coolant injection under high- and low-pressure conditions, as used in the LWR, are not necessary in an LFR. Nevertheless, LFR core cooling requires the maintaining of the lead coolant level above the steam generator (SG) inlet (or Decay Heat Removal inlet) to provide a normal decay heat removal flow path through SGs or Decay Heat Removal Heat Exchangers.

The LFR SDC are deduced from the safety goals, the basic characteristics of an LFR, available applicable operational experience, experiments on transient and accident phenomena, and the safety approach required for LFR systems. The criteria for structures, systems and components specific to an LFR, as listed below, are reflected in the LFR SDC:

Reactor Core

- Fuel elements and assemblies
- Reactor core structure and characteristics
- Reactor shutdown

Reactor Coolant Systems

- Primary coolant system
- Secondary coolant system (possible intermediate coolant system)
- Decay heat removal system

Containment System

Supporting and Auxiliary Systems, Fuel Handling & Storage

- Leak detection systems
- Lead heating systems
- Lead purification and conditioning system

- Cover gas system
- Fuel storage

2.3.3 LFR Specific Safety Approach in Relation to the Plant States

LFR design for normal operations, anticipated operational occurrences, and design basis accidents

Based on the characteristics of the LFR, the design for normal operations, anticipated operational occurrences, and design basis accident conditions must insure that: 1) the reactor can be reliably shut down if needed, 2) the core remains covered in the case of a leak in the primary coolant boundary, 3) the flow in the core can be maintained such that the decay heat can be removed, 4) an adequate heat sink is available, and 5) the radioactive materials are confined.

Reliable, diverse, independent, and redundant shutdown systems are required in order to assure adequate shutdown in the event of abnormal occurrences. Design of the shutdown system will comply with relevant national or international codes and standards and be based on proven engineering practices. Reliability of the shutdown system is achieved by monitoring, testing, and maintaining of the system throughout the life-time of plant. The shutdown system will be designed to assure that an adequate shutdown margin can be achieved for all operational states and design basis accidents. Separation of control and shutdown functions shall be maintained to assure independence.

The low pressure and the very high boiling point of the coolant (higher than melting point of metal structures) in an LFR result in single phase conditions in the case of a leak or break in the primary coolant system and temperature increase transients. Therefore, primary coolant injection systems are not required for LFRs. Designs should prevent a loss of primary coolant event that would lead to uncovering of the core or to interference with the decay heat removal function. The excellent heat transfer properties of lead allow rapid decay heat removal from the core; however, decay heat removal systems should be designed to prevent overcooling which might lead to freezing of the coolant.

LFR design for design extension conditions

A fast reactor, including an LFR, is characterized by the fact that its core is not in its most reactive configuration under normal operating conditions and thus has a possibility to undergo positive reactivity changes when exposed to various initiators that either reduce neutron capture and moderation (e.g., by gas bubbles in the core) or increased fuel concentration (e.g., by core compaction from seismic excitation) in design extension conditions. In order to manage an excessive insertion of positive reactivity, prevention/mitigation measures for such conditions must be provided in the design. For design extension conditions, it is required that core damage prevention measures are provided and that containment functions are maintained. Plant conditions caused, for example, by an initiating condition combined with multiple failures of safety equipment or severe external events, are postulated as design extension conditions. Analyses of the plant response to design extension conditions will be done using best estimate analysis, and Probabilistic Safety Assessment results will be used to ensure comprehensive coverage of postulated events and to estimate occurrence frequencies and consequences.

LFR design extension conditions events can be grouped into two categories based on the characteristics of an LFR and Probabilistic Safety Assessment studies. These are:

1) failure to shut down the reactor following an off-normal initiating event
2) inability to remove heat from the core following an initiating event. The design of the reactor should assure that such events have a very low frequency of occurrence.

The failure to shut down is combined with the three typical LFR accident sequences resulting in design extension condition events:

- loss of flow with failure to scram,
- overpower transient with failure to scram, and
- loss of main heat removal with failure to scram.

The inability to remove heat from the core can result in other design extension condition events:

- loss of coolant flow (flow paths for decay heat removal become disrupted),
- long-term loss of heat sink (with scram)
- fuel assembly flow blockage (without scram)

This event categorization applies in general to all LFR systems including the GIF LFR systems.

For events involving the failure of reactor shutdown, the design needs to prevent such events from damaging the core and mitigate the consequences of core damage to minimize the load on the containment function. The design measures to prevent core damage should be emphasized, for which the robust demonstration is needed, and may include the use of passive or inherent reactor shutdown capabilities. Restricting generated energy and retaining/cooling of the damaged core will reduce the potential load on the reactor containment function.

Moreover, based on phenomenological analyses and engineering judgment, fuel dispersion (by the buoyancy force) is hypothesized to be favored in LFRs compared to the fuel compaction due to very similar densities of lead and mixed oxide or nitride fuels, mitigating the accident and/or preventing its further progression/aggravation, including re-criticalities. Further R&D is necessary to understand fuel degradation phenomena in LFRs comprehensively (including phenomena such as fuel dispersion / dissolution / segregation vs. aggregation), serving also as a basis for the possible practical elimination of severe accidents or development of severe accident management strategies. These studies may also lead to the establishment of a requirement for specification of a maximum MOX or mixed nitride fuel density for the LFR.

For events involving the loss of heat removal, the design should provide a means to prevent core damage or loss of containment function by maintaining lead coolant level for core cooling, ensuring decay heat removal under the conditions with or without core damage.

Similar design approaches which address the loss of heat removal events may also be applied for a spent fuel storage pool.

The capability of ensuring containment integrity will be required for design extension conditions. Therefore, containment will be required to withstand thermal and mechanical loads generated during the event transient.

Lead-concrete interaction and debris-concrete interaction shall also be adequately prevented or mitigated (the latter if not practically eliminated). As applicable to a design, further R&D is necessary to understand the phenomenology of these interactions comprehensively.

2.3.4 Lessons Learned from TEPCO's Fukushima Daiichi Nuclear Power Plants Accidents

TEPCO's Fukushima Daiichi nuclear power plant accidents, caused by the Great East Japan Earthquake on 11 March 2011, emphasizes the need for ensuring that sufficient design measures against extreme external events and ensuing severe accidents have been implemented in the nuclear plant. Sequence analysis, factorial analysis, and the study of lessons learned are currently being conducted. Key points from the lessons learned, based on the Japanese Government Report[20], IAEA[21] and OECD/NEA[22] reports are included in the LFR SDC as far as they have a potential impact on the safety of the GIF LFR systems. The key points are the enhancement of systems that may be needed to decrease the likelihood of extreme core damage accident due to extreme external hazards, the enhancement of response measures against severe core damage accidents (incl. mitigation measures if severe accidents are not demonstrated to be practically eliminated), and the reinforcement of the safety infrastructure by ensuring independence and diversity of the safety systems.

Provisions for handling external events need to be sufficiently robust in coordination with anticipated conditions at the reactor site. For example, the design must consider ensuring power supply and required safety functions during long-term loss of all AC power, or otherwise rely on systems and approaches that do not require such external or backup power. Extensive use of passive safety functions will strongly reduce the dependency on power supplies, and will also be effective as a measure against power loss. As external events, such as earthquakes, tsunami and flooding, may become initiators of severe core damage accidents, the use of passive safety systems is particularly suited to face efficiently such events.

Stress tests[23] are one possible method to evaluate the safety margins of nuclear power plants against severe plant conditions and extreme external hazards. Stress tests may show how large the safety margins are relative to the design basis, whereas the LFR SDC can deal with how robust the prevention and mitigation[4] design features are against severe core damage accidents.

As already highlighted, the LFR is particularly suited, thanks to the inherent characteristics of the coolant and extended use of passive safety features, to face Fukushima like events.

[4] The mitigation features for accidents with significant degradation of the reactor core need to be considered only if they are not demonstrated to be practically eliminated as discussed in sub-sections 1.3 and 2.1.

Additional engineering provisions are adopted to improve plant response to such extreme events:

Extreme earthquake – LFR concepts are designed to withstand the Design Basis Earthquakes, with margins. However, it shall be demonstrated that the available margins are sufficient to prevent large or early radiological releases for a beyond design basis earthquake. A beyond-design basis earthquake might have an important impact and consequences in terms of fast reactor safety, in particular leading to:

- Core deformation, which might impede the control of reactivity as the control and safety rod function is impaired or deteriorated;
- Core compaction resulting in a positive reactivity insertion and consequent power increase;
- Fuel cladding failures with subsequent risk of fission gas passage into the core (voiding reactivity effect);
- Loss of the integrity of the main and/or safety vessels;
- Loss of the core supporting structures.

Due to the high density of lead, the response of a plant to earthquakes needs to be carefully considered. For example for ELFR, the issue is addressed by the adoption of 2D seismic isolators under the primary building that reduce loads caused by horizontal oscillations. In this respect, the impact of the implementation of seismic isolators on the structures/components/core has been considered in the mechanical design. In other designs different provisions are provided. Generally speaking the problem is normally addressed by adoption of adequate design measures that however may differ depending on designer's solutions.

Extreme flooding – LFR concepts, notably the DHR systems shall be protected from the consequences of a flooding. This is both from a mechanical point of view to prevent the component damage and from a functional point of view since their actuation is to be accomplished by protected energy devices. However, the relative chemical inertness of lead in contact with water permits an extensive use of water cooling.

Total loss of an electric power supply and/or heat sink(s) – The intrinsic characteristics of lead-cooled reactors provide an increased robustness of the plant in response to the total loss of electric power supply and/or heat sink(s) because:

- Liquid lead can maintain an adequate degree of natural convection to accomplish decay heat removal function completely passively;
- The heat sink is usually diverse: water or air.

In case of loss of a normal heat sink, fully passive DHR systems are able to fulfil the safety function. In the very unlikely event of a Fukushima-like scenario leading to the loss of all heat sinks (both secondary and dedicated DHR systems), heat can be possibly extracted by injecting water into the reactor cavity between the reactor and guard (safety) vessels, while in case of a reactor vessel breach, the decay heat can be removed by a dedicated heat removal system that cools the concrete of the reactor cavity walls. As already discussed earlier, such ultimate provisions in a Fukushima-like scenario are possible because lead is relatively chemically inert in contact with air and water.

3. MANAGEMENT OF SAFETY IN DESIGN

In the following sections, criteria are numbered following the same structure and logic of IAEA SSR-2/1 (Rev.1) and the GIF SFR SDC. There are 82 "Requirements" of SSR-2/1 (Rev. 1), which translates to the 82 primary "Criteria" in the following sections. Each of these criteria may have sub-criteria (in the same manner as each requirement of SSR 2/1 usually has several sub-requirements), and they are numbered in accordance with the convention adopted in SSR-2/1 (Rev. 1).

Criterion 1: Responsibilities in the management of safety in plant design

An applicant for a licence to construct and/or operate a nuclear power plant shall be responsible for ensuring that the design submitted to the regulatory body meets all applicable safety requirements.

3.1 All organizations, including the design organizations, engaged in activities important to the safety of the design of a nuclear power plant shall be responsible for ensuring that safety matters are given the highest priority[5].

Criterion 2: Management system for the plant design[24]

The design organization shall establish and implement a management system for ensuring that all safety requirements established for the design of the plant are considered and implemented in all phases of the design process and that they are met in the final design.

3.2. The management system shall include provision for ensuring the quality of the design of each structure, system and component, as well as of the overall design of the nuclear power plant, at all times. This includes the means for identifying and correcting design deficiencies, for checking the adequacy of the design and for controlling design changes.

3.3. The design of the plant, including subsequent changes, modifications or safety improvements, shall be in accordance with established procedures that call on appropriate

[5] The design organization is the organization responsible for preparation of the final detailed design of the plant to be built.

engineering codes and standards and shall incorporate relevant requirements and design bases. Interfaces shall be identified and controlled.

3.4. The adequacy of the plant design, including design tools and design inputs and outputs, shall be verified and validated by individuals or groups separate from those who originally performed the design work. Verification, validation and approval of the plant design shall be completed as soon as is practicable in the design and construction processes, and in any case before operation of the plant is commenced.

Criterion 3: Safety of the plant design throughout the lifetime of the plant

The operating organization shall establish a formal system for ensuring the continuing safety of the plant design throughout the lifetime of the nuclear power plant.

3.5. The formal system for ensuring the continuing safety of the plant design shall include a formally designated entity responsible for the safety of the plant design within the operating organization's management system. Tasks that are assigned to external organizations (referred to as responsible designers) for the design of specific parts of the plant shall be taken into account in the arrangements.

3.6. The formally designated entity shall ensure that the plant design meets the acceptance criteria for safety, reliability and quality in accordance with relevant national and international codes and standards, laws and regulations. A series of tasks and functions shall be established and implemented to ensure the following:

(a) That the plant design is fit for purpose and meets the requirement for the optimization of protection and safety by keeping radiation risks as low as reasonably achievable
(b) That the design verification, definition of engineering codes and standards and requirements, use of proven engineering practices, provision for feedback of information on construction and experience, approval of key engineering documents, conduct of safety assessments and maintaining a safety culture are included in the formal system for ensuring the continuing safety of the plant design;
(c) That the knowledge of the design that is needed for safe operation, maintenance (including adequate intervals for testing) and modification of the plant is available, that this knowledge is maintained up to date by the operating organization, and that due account is taken of past operating experience and validated research findings;

(d) That management of design requirements and configuration control are maintained;
(e) That the necessary interfaces with responsible designers and suppliers engaged in design work are established and controlled;
(f) That the necessary engineering expertise and scientific and technical knowledge are maintained within the operating organization;
(g) That all design changes to the plant are reviewed, verified, documented and approved;
(h) That adequate documentation is maintained to facilitate future decommissioning of the plant.

4. PRINCIPAL TECHNICAL CRITERIA

Criterion 4: Fundamental safety functions

Fulfilment of the following fundamental safety functions for a nuclear power plant shall be ensured for all plant states:

(i) control of reactivity,

(ii) removal of heat from the reactor and from the fuel in any location within the plant,

(iii) confinement of radioactive *and toxic* material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

4.1. A systematic approach shall be taken to identifying those items important to safety that are necessary to fulfil the fundamental safety functions and to identifying the inherent features that are contributing to fulfilling or that are affecting the fundamental safety functions for all plant states.

4.2. Means of monitoring the status of the plant shall be provided for ensuring that the required safety functions are fulfilled.

Criterion 5: Radiation protection[25]

The design of a nuclear power plant shall be such as to ensure that radiation doses to workers at the plant and to members of the public do not exceed the dose limits; that they are kept as low as reasonably achievable in operational states for the entire lifetime of the

plant, and that they remain below acceptable limits and as low as reasonably achievable in and following accident conditions.

4.3. The design shall be such as to ensure that plant states that could lead to high radiation doses or large radioactive releases are practically eliminated and that there are no, or only minor, potential radiological consequences for plant states with a significant likelihood of occurrence.

4.4. Acceptable limits for radiation protection associated with the relevant categories of plant states shall be established, consistent with the regulatory requirements.

Criterion 6: Design for a nuclear power plant

The design for a nuclear power plant shall ensure that the plant and items important to safety have the appropriate characteristics to ensure that safety functions can be performed with the necessary reliability, that the plant can be operated safely within the operational limits and conditions for the full duration of its design life and can be safely decommissioned, and that impacts on the environment are minimized.

4.5. The design for a nuclear power plant shall be such as to ensure that the safety requirements of the operating organization, the requirements of the regulatory body and the requirements of relevant legislation, as well as applicable national and international codes and standards, are all met, and that due account is taken of human capabilities and limitations and of factors that could influence human performance. Adequate information on the design shall be provided for ensuring the safe operation and maintenance of the plant, and to allow subsequent plant modifications to be made. Recommended practices shall be provided for incorporation into the administrative and operational procedures for the plant (i.e., the operational limits and conditions).

4.6. The design shall take due account of relevant available experience that has been gained in the design, construction and operation of other nuclear power plants, and of the results of relevant research programmes.

4.7. The design shall take due account of the results of deterministic safety analyses and probabilistic safety analyses, to ensure that due consideration has been given to the prevention of accidents and to mitigation of the consequences of any accident conditions.

4.8. The design shall be such as to ensure that the generation of radioactive waste and discharges are kept to the minimum practicable in terms of both activity and volume, by means of appropriate design measures and operational and decommissioning practices.

Criterion 7: Application of Defence-in-Depth

The design of a nuclear power plant shall incorporate Defence-in-Depth. The levels of Defence-in-Depth shall be independent as far as is practicable.

The design of a nuclear power plant shall be such that level 4 of the Defence-in-Depth and the associated safety design for prevention and/or mitigation[6] of severe accident conditions shall be incorporated, in order that significant radioactive release can be considered as belonging to the residual risk.

4.9. The Defence-in-Depth concept shall be applied to provide several levels of defence that are aimed at preventing consequences of accidents that could lead to harmful effect on people and the environment and ensuring that appropriate measures are taken for the protection of people and the environment and for the mitigation of consequences in the event that prevention fails.

4.10. The design shall take due account of the fact that the existence of multiple levels of defence is not a basis for continued operation in the absence of one level of defence. All levels of Defence-in-Depth shall be kept available at all times and any relaxations shall be justified for specific modes of operation.

4.11. The design:

(a) Shall provide for multiple physical barriers to the release of radioactive material to the environment;
(b) Shall be conservative, and the construction shall be of high quality, so as to provide assurance that failures and deviations from normal operation are minimized, that

[6] The mitigation features for accidents with significant degradation of the reactor core need to be considered only if they are not demonstrated to be practically eliminated as discussed in sub-sections 1.3 and 2.1.

accidents are prevented as far as is practicable and that a small deviation in a plant parameter does not lead to a cliff edge effect[7];

(c) Shall provide for the control of plant behaviour by means of inherent and engineered features, such that failures and deviations from normal operation requiring actuation of safety systems are minimized or excluded by design to the extent possible;

(d) Shall provide for supplementing the control of the plant by means of automatic actuation of safety systems, such that failures and deviations from normal operation that exceed the capability of control systems can be controlled with a high level of confidence, and the need for operator actions in the early phase of these failures or deviations from normal operation is minimized;

(e) Shall provide for systems, structures and components and procedures to control the course of and as far as practicable, to limit the consequences of failures and deviations from normal operation that exceed the capability of safety systems;

(f) Shall provide multiple means for ensuring that each of the fundamental safety functions is performed, thereby ensuring the effectiveness of the barriers and mitigating the consequences of any failure or deviation from normal operation.

4.12. To ensure that the concept of Defence-in-Depth is maintained, the design shall prevent as far as is practicable:

(a) Challenges to the integrity of physical barriers;

(b) Failure of one or more barriers;

(c) Failure of a barrier as a consequence of the failure of another barrier;

(d) The possibility of harmful consequences of errors in operation and maintenance

4.13. The design shall be such as to ensure, as far as is practicable, that the first, or at most the second, level of defence is capable of preventing an escalation to accident conditions for all failures or deviations from normal operation that are likely to occur over the operating lifetime of the nuclear power plant.

[7] A cliff edge effect, in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.

4.13a. The levels of Defence-in-Depth shall be independent as far as practicable to avoid the failure of one level reducing the effectiveness of other levels. In particular, safety features for design extension conditions (especially features for mitigating the consequences of accidents involving the melting of fuel) shall as far as is practicable be independent of safety systems.

Criterion 8: Interfaces of safety with security and safeguards

Safety measures, nuclear security measures and arrangements for the State system of accounting for, and control of, nuclear material for a nuclear power plant shall be designed and implemented in an integrated manner so that they do not compromise one another.

Criterion 9: Proven engineering practices

Items important to safety for a nuclear power plant shall be designed in accordance with the relevant national and international codes and standards

4.14. Items important to safety for a nuclear power plant shall preferably be of a design that has previously been proven in equivalent applications, and if not shall be items of high quality and of a technology that has been qualified and tested.

4.15. National and international codes and standards that are used as design rules for items important to safety shall be identified and evaluated to determine their applicability, adequacy and sufficiency, and shall be supplemented or modified as necessary to ensure that the quality of the design is commensurate with the associated safety function.

4.16. Where an unproven design or feature is introduced or where there is a departure from an established engineering practice, safety shall be demonstrated by means of appropriate supporting research programmes, performance tests with specific acceptance criteria or the examination of operating experience from other relevant applications. The new design or feature or new practice shall also be adequately tested to the extent practicable before being brought into service, and shall be monitored in service to verify that the behaviour of the plant is as expected.

Criterion 10: Safety assessment[26]

Comprehensive deterministic safety assessments and probabilistic safety assessments shall be carried out throughout the design process for a nuclear power plant to ensure that all safety requirements on the design of the plant are met throughout all stages of the lifetime of the plant, and to confirm that the design as delivered meets requirements for manufacture and for construction, and as built, as operated and as modified.

4.17. The safety assessments shall be commenced at an early point in the design process, with iterations between design activities and confirmatory analytical activities, and shall increase in scope and level of detail as the design programme progresses.

4.18. The safety assessments shall be documented in a form that facilitates independent evaluation.

Criterion 11: Provision for construction

Items important to safety for a nuclear power plant shall be designed so that they can be manufactured, constructed, assembled, installed and erected in accordance with established processes that ensure the achievement of the design specifications and the required level of safety.

4.19. In the provision for construction and operation, due account shall be taken of relevant experience that has been gained in the construction of other similar plants and their associated structures, systems and components. Where best practices from other relevant industries are adopted, such practices shall be shown to be appropriate to the specific nuclear application.

Criterion 12: Features to facilitate waste management and decommissioning

Special consideration shall be given at the design stage of a nuclear power plant to the incorporation of features to facilitate radioactive *and toxic* waste management and the future decommissioning and dismantling of the plant.

4.20. In particular, the design shall take due account of:

(a) The choice of materials, so that amounts of radioactive waste will be minimized to the extent practicable and decontamination will be facilitated;

(b) The access capabilities and the means of handling that might be necessary;
(c) The facilities necessary for the treatment and storage of radioactive *and toxic* waste generated in operation and provision for managing the radioactive *and toxic* waste that will be generated in the decommissioning of the plant.
(d) The disposal and/or reuse of the lead coolant after the reactor final shutdown shall be investigated

5. GENERAL PLANT DESIGN

5.1 Design Basis

Criterion 13: Categories of plant states

Plant states shall be identified and shall be grouped into a limited number of categories primarily on the basis of their frequency of occurrence at the nuclear power plant.

5.1. *On the basis of their frequency,* plant states shall typically cover:

(a) Normal operation;

(b) Anticipated operational occurrences, which are expected to occur over the operating lifetime of the plant;

(c) Design basis accidents;

In addition, despite their low frequency, plant states with potential severe consequences shall be considered:

(d) Design extension conditions including:

- Prevention of core degradation

- Accidents with significant degradation of the reactor core[8].

5.2. Criteria shall be assigned to each plant state such that frequently occurring plant states shall have no, or only minor, radiological consequences and plant states that could give rise to serious consequences shall have a very low frequency of occurrence.

Criterion 14: Design basis for items important to safety

The design basis for items important to safety shall specify the necessary capability, reliability and functionality for the relevant operational states, for accident conditions and for conditions arising from internal and external hazards, to meet the specific acceptance criteria over the lifetime of the nuclear power plant.

[8] The mitigation features for accidents with significant degradation of the reactor core need to be considered only if they are not practically eliminated as discussed in sub-sections 1.3 and 2.1.

5.3. The design basis for each item important to safety shall be systematically justified and documented. The documentation shall provide the necessary information for the operating organization to operate the plant safely.

Criterion 15: Design limits

A set of design limits consistent with the key physical parameters for each item important to safety for the nuclear power plant shall be specified for all operational states and for accident conditions.

5.4. The design limits shall be specified and shall be consistent with relevant national and international standards and codes, as well as with relevant regulatory requirements.

Criterion 16: Postulated initiating events

The design for the nuclear power plant shall apply a systematic approach to identifying a comprehensive set of postulated initiating events such that all foreseeable events with the potential for serious consequences and all foreseeable events with a significant frequency of occurrence are anticipated and are considered in the design.

5.5. The postulated initiating events shall be identified on the basis of engineering judgement and a combination of deterministic assessment and probabilistic assessment. A justification of the extent of usage of deterministic safety analysis and probabilistic safety analysis shall be provided, to show that all foreseeable events have been considered.

5.6. The postulated initiating events shall include all foreseeable failures of structures, systems and components of the plant, as well as operating errors and possible failures arising from internal and external hazards, whether in full power, low power or shutdown states.

5.7. An analysis of the postulated initiating events for the plant shall be made to establish the preventive measures and protective measures that are necessary to ensure that the required safety functions will be performed

5.8. The expected behaviour of the plant in any postulated initiating event shall be such that the following conditions can be achieved, in order of priority:

(1) A postulated initiating event would produce no safety significant effects or would produce only a change towards safe plant conditions by means of inherent characteristics of the plant.
(2) Following a postulated initiating event, the plant would be rendered safe by means of passive safety features or by the action of systems that are operating continuously in the state necessary to control the postulated initiating event;
(3) Following a postulated initiating event, the plant would be rendered safe by the actuation of safety systems that need to be brought into operation in response to the postulated initiating event.
(4) Following a postulated initiating event, the plant would be rendered safe by following specified procedures.

5.9. The postulated initiating events used for developing the performance requirements for the items important to safety in the overall safety assessment and detailed analysis of the plant shall be grouped into a number of representative event sequences that identify bounding cases and that provide the basis for the design and the operational limits for items important to safety.

5.10. A technically supported justification shall be provided for exclusion from the design of any initiating event that is identified in accordance with the comprehensive set of postulated initiating events.

5.11. Where prompt and reliable action would be necessary in response to a postulated initiating event, provision shall be made in the design for automatic safety actions for the necessary actuation of safety systems, to prevent progression to more severe plant conditions.

5.12. Where prompt action in response to a postulated initiating event would not be necessary, it is permissible for reliance to be placed on the manual initiation of systems or on other operator actions. For such cases, the time interval between detection of the abnormal event or accident and the required action shall be sufficiently long, and adequate procedures (such as administrative, operational and emergency procedures) shall be specified to ensure the performance of such actions. An assessment shall be made of the potential for an operator to worsen an event sequence through erroneous operation of equipment or incorrect diagnosis of the necessary recovery process.

5.13. The operator actions that would be necessary to diagnose the state of the plant following a postulated initiating event and to put it into a stable long-term shutdown condition in a timely manner shall be facilitated by the provision of adequate instrumentation to monitor the status of the plant, and adequate controls for the manual operation of equipment.

5.14. The design shall specify the necessary provision of equipment and the procedures necessary to provide the means for keeping control over the plant and for mitigating any harmful consequences of a loss of control.

5.15. Any equipment that is necessary for actions to be taken in manual response and recovery processes shall be placed at the most suitable location to ensure its availability at the time of need and to allow safe access to it under the environmental conditions anticipated.

Criterion 17: Internal and external hazards

All foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety of the nuclear power plant, shall be identified and their effects shall be evaluated. Hazards shall be considered for determination of the postulated initiating events and generated loadings for use in the design of relevant items important to safety for the plant.

5.15a. Items important to safety shall be designed and located, with due consideration of other implications for safety, to withstand the effects of hazards or to be protected, in accordance with their importance to safety, against hazards and against common cause failure mechanisms generated by hazards.

5.15b. For multiple unit plant sites, the design shall take due account of the potential for specific hazards to give rise to impacts on several or even all units on the site simultaneously.

Internal hazards

5.16. The design shall take due account of internal hazards such as fire, explosion, flooding, missile generation, collapse of structures and falling objects, pipe whip, jet impact, release of fluid from failed systems or from other installations on the site. Appropriate features for prevention and mitigation shall be provided to ensure that safety is not compromised.

External hazards[27]

5.17. The design shall include due consideration of those natural and human induced external events (i.e., events of origin external to the plant) that have been identified in the site evaluation process. Causation and likelihood shall be considered in postulating potential hazards. In the short term, the safety of the plant shall not be permitted to be dependent on the availability of off-site services such as electricity supply and firefighting services. The design shall take due account of site-specific conditions to determine the maximum delay time by which off-site services need to be available.

5.18. *For all the postulated initiating events that threaten the supply of power or the heat sinks, due consideration shall be taken of the capability of the plant to reach and maintain a safe state, without external intervention, for a long period after an event. For this purpose, the period of time during which a safety function is ensured in an event without the need of action by personnel should be maximized.*

5.19. Features shall be provided to minimize any interactions between buildings containing items important to safety (including power cabling and control cabling) and any other plant structure as a result of external events considered in the design.

5.20. This paragraph was deleted and its content, with a broader scope, has been transferred to the new paragraph 5.15a.

5.21. The design of the plant shall provide for an adequate margin to protect items important to safety against levels of external hazards to be considered for design, derived from the hazard evaluation for the site, and to avoid cliff edge effects.

5.21a. The design of the plant shall also provide for an adequate margin to protect items ultimately necessary to prevent an early radioactive release or a large radioactive release in the event of levels of natural hazards exceeding those considered for design, derived from the hazard evaluation for the site.

5.22. This paragraph was deleted and its content, with a broader scope, has been transferred to the new paragraph 5.15b.

Criterion 18: Engineering design rules

The engineering design rules for items important to safety at a nuclear power plant shall be specified and shall comply with the relevant national or international codes and standards, with proven engineering practices, with due account taken of their relevance to nuclear power technology.

5.23. Methods to ensure a robust design shall be applied and proven engineering practices shall be adhered to in the design of a nuclear power plant to ensure that the fundamental safety functions are achieved for all operational states and for all accident conditions.

Criterion 19: Design basis accidents

A set of accident conditions that are to be considered in the design shall be derived from postulated initiating events for the purpose of establishing the boundary conditions for the nuclear power plant to withstand, without acceptable limits for radiation protection being exceeded.

5.24. Design basis accidents shall be used to define the design bases, including performance criteria, for safety systems and for other items important to safety that are necessary to control design basis accident conditions, with the objective of returning the plant to a safe state and mitigating the consequences of any accidents.

5.25. The design shall be such that for design basis accident conditions, key plant parameters do not exceed the specified design limits. A primary objective shall be to manage all design basis accidents so that they have no, or only minor, radiological impacts, on or off the site, and do not necessitate any off-site intervention measures.

5.26. The design basis accidents shall be analyzed in a conservative manner. This approach involves postulating certain failures in safety systems, specifying design criteria and using conservative assumptions, models and input parameters in the analysis. *The design basis accidents could also be analysed in a best estimate manner, together with adequately analysed and evaluated uncertainties.*

Criterion 20: Design extension conditions

A set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences.

The design of a nuclear power plant shall be such that the level 4 of the defence in depth and the associated safety design for prevention and/or mitigation[9] of severe core degradation and of serious fuel failures during fuel handling and storage shall be incorporated, in order that significant radioactive release can be considered as belonging to the residual risk.

5.27. An analysis of design extension conditions for the plant shall be performed[10]. The main technical objective of considering design extension conditions is to provide assurance that the design of the plant is such as to prevent accident conditions not considered design basis accident conditions, or to mitigate their consequences, as far as is reasonably practicable. This might require additional safety features for design extension conditions, or extension of the capability of safety systems to maintain the integrity of the containment. These additional safety features for design extension conditions, or this extension of the capability of safety systems, shall be such as to ensure the capability for managing accident conditions in which there is a significant amount of radioactive material in the containment (including radioactive material resulting from severe degradation of the reactor core). The plant shall be designed so that it can be brought into a controlled state and the containment function can be maintained,

[9] The mitigation features for accidents with significant degradation of the reactor core need to be considered only if they are not demonstrated to be practically eliminated as discussed in sub-sections 1.3 and 2.1.

[10] The analysis of design extension conditions for the plant could be performed by means of a best estimate approach (more stringent approaches may be used according to States' requirements).

with the result that significant radioactive releases would be practically eliminated[11]. The effectiveness of provisions to ensure the functionality of the containment could be analysed on the basis of the best estimate approach.

5.28. The design extension conditions shall be used to define the design specifications for safety features and for the design of all other items important to safety that are necessary for preventing such conditions from arising, or, if they do arise, for controlling them and mitigating their consequences.

5.29 The analysis undertaken shall include identification of the features that are designed for use in, or that are capable[12] of preventing or mitigating, events considered in the design extension conditions. These features:

(a) Shall be independent, to the extent practicable, of those used in more frequent accidents;

(b) Shall be capable of performing in the environmental conditions pertaining to these design extension conditions, including design extension conditions in severe accidents, where appropriate;

(c) Shall have a reliability commensurate with the function that they are required to fulfil.

5.30. In particular, the containment and its safety features shall be able to withstand extreme scenarios that include, among other things, melting of the reactor core. These scenarios shall be selected using engineering judgement and input from probabilistic safety assessments.

5.31. The design shall be such that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated'. *The following*

[11] The possibility of certain conditions arising may be considered to have been 'practically eliminated' if it would be physically impossible for the conditions to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise.

[12] For returning the plant to a safe state or for mitigating the consequences of an accident, consideration could be given to the full design capabilities of the plant and to the temporary use of additional systems.

design features for prevention and mitigation of severe accidents in postulated design extension conditions shall be considered:

(a) Additional reactor shutdown measures against failure of active reactor shutdown systems,

(b) Mitigation provision to avoid re-criticality leading to large energy release during a core degradation progression[13]*,*

(c) Means for decay heat removal of a degraded core[13]*, and*

(d) Containment function capability to withstand the thermal and mechanical loads generated by severe accident conditions[13]*.*

5.31a. The design shall be such that for design extension conditions, protective actions that are limited in terms of lengths of time and areas of application shall be sufficient for the protection of the public, and sufficient time shall be available to take such measures.

Combinations of events and failures

5.32. Where the results of engineering judgement, *operating experience,* deterministic safety assessments and probabilistic safety assessments indicate that combinations of events could lead to anticipated operational occurrences or to accident conditions, such combinations of events shall be considered to be design basis accidents or shall be included as part of design extension conditions, depending mainly on their likelihood of occurrence. Certain events might be consequences of other events, such as a flood following an earthquake. Such consequential effects shall be considered to be part of the original postulated initiating event.

Criterion 21: Physical separation and independence of safety systems

Interference between safety systems or between redundant elements of a system shall be prevented by means such as physical separation, electrical isolation, functional independence and independence of communication (data transfer), as appropriate

[13] The mitigation features for accidents with significant degradation of the reactor core need to be considered only if they are not demonstrated to be practically eliminated as discussed in sub-sections 1.3 and 2.1. Nevertheless, these aspects need to be analyzed and, if necessary, dedicated provisions implemented.

5.33. Safety system equipment (including cables and raceways) shall be readily identifiable in the plant for each redundant element of a safety system.

Criterion 22: Safety classification

All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance.

5.34. The method for classifying the safety significance of items important to safety shall be based primarily on deterministic methods complemented where appropriate by probabilistic methods, with due account taken of factors such as:

(a) The safety function(s) to be performed by the item;

(b) The consequences of failure to perform a safety function;

(c) The frequency with which the item will be called upon to perform a safety function; *Even with very low frequencies, the equipment dedicated for severe accident mitigation[14] shall be appropriately classified*.

(d) The time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function.

5.35. The design shall be such as to ensure that any interference between items important to safety will be prevented, and in particular that any failure of items important to safety in a system in a lower safety class will not propagate to a system in a higher safety class.

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

Criterion 23: Reliability of items important to safety

The reliability of items important to safety shall be commensurate with their safety significance.

[14] The mitigation features for accidents with significant degradation of the reactor core need to be considered only if they are not demonstrated to be practically eliminated as discussed in sub-sections 1.3 and 2.1.

5.37. The design of items important to safety shall be such as to ensure that the equipment can be qualified, procured, installed, commissioned, operated and maintained to be capable of withstanding with sufficient reliability and effectiveness all conditions specified in the design basis for the items.

5.38. In the selection of equipment, consideration shall be given to both spurious operation and unsafe failure modes. Preference shall be given in the selection process to equipment that exhibits a predictable and revealed mode of failure and for which the design facilitates repair or replacement.

Criterion 24: Common cause failures

The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.

Criterion 25: Single failure criterion

The single failure criterion shall be applied to each safety group incorporated in the plant design[15].

5.39. Spurious action shall be considered to be one mode of failure when applying the concept to a safety group or safety system.

5.40. The design shall take due account of the failure of a passive component, unless it has been justified in the single failure analysis with a high level of confidence that a failure of that component is very unlikely and that its function would remain unaffected by the postulated initiating event.

[15] A single failure is a failure that results in the loss of capability of a system or component to perform its intended safety function(s) and any consequential failure(s) that result from it. The single failure criterion is a criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure.

Criterion 26: Fail-safe design

The concept of fail-safe design shall be incorporated as appropriate into the design of systems and components important to safety.

5.41 Systems and components important to safety shall be designed for fail-safe behaviour, as appropriate, so that their failure or the failure of a support feature does not prevent the performance of the intended safety function.

Criterion 27: Support service systems

Support service systems that ensure the operability of equipment forming part of a system important to safety shall be classified accordingly.

5.42. The reliability, redundancy, diversity and independence of support service systems and the provision of features for their isolation and for testing their functional capability shall be commensurate with the significance to safety of the system being supported.

5.43. It shall not be permissible for a failure of a support service system to be capable of simultaneously affecting redundant parts of a safety system or a system fulfilling diverse safety functions, and compromising the capability of these systems to fulfil their safety functions.

Criterion 28: Operational limits and conditions for safe operation

The design shall establish a set of operational limits and conditions for safe operation of the nuclear power plant.

5.44. The requirements and operational limits and conditions established in the design for the nuclear power plant shall include (Ref. [11] Req. 6):

(a) Safety limits;

(b) Limiting settings for safety systems;

(c) Operational limits and conditions for operational states;

(d) Control system constraints and procedural constraints on process variables and other important parameters;

(e) Requirements for surveillance, maintenance, testing and inspection of the plant to ensure that structures, systems and components function as intended in the design, to comply with the requirement for optimization by keeping radiation risks as low as reasonably achievable;

(f) Specified operational configurations, including operational restrictions in the event of the unavailability of safety systems or safety related systems;

(g) Action statements, including completion times for actions in response to deviations from the operational limits and conditions.

5.2 Design for Safe Operation over the Lifetime of the Plant

Criterion 29: Calibration, testing, maintenance, repair, replacement, inspection and monitoring of items important to safety

Items important to safety for a nuclear power plant shall be designed to be calibrated, tested, maintained, repaired or replaced, inspected and monitored as required to ensure their capability of performing their functions and to maintain their integrity in all conditions specified in their design basis.

5.45. The plant layout shall be such that activities for calibration, testing, maintenance, repair or replacement, inspection and monitoring are facilitated and can be performed to relevant national and international codes and standards. Such activities shall be commensurate with the importance of the safety functions to be performed, and shall be performed without undue exposure of workers.

5.46. Where items important to safety are planned to be calibrated, tested or maintained during power operation, the respective systems shall be designed for performing such tasks with no significant reduction in the reliability of performance of the safety functions. Provisions for calibration, testing, maintenance, repair, replacement or inspection of items important to safety during shutdown shall be included in the design so that such tasks can be performed with no significant reduction in the reliability of performance of the safety functions.

5.47. If an item important to safety cannot be designed to be capable of being tested, inspected or monitored to the extent desirable, a robust technical justification shall be provided that incorporates the following approach:

(a) Other proven alternative and/or indirect methods such as surveillance testing of reference items or use of verified and validated calculational methods shall be specified;

(b) Conservative safety margins shall be applied or other appropriate precautions shall be taken to compensate for possible unanticipated failures.

Criterion 30: Qualification of items important to safety

A qualification programme for items important to safety shall be implemented to verify that items important to safety at a nuclear power plant are capable of performing their intended functions when necessary, and in the prevailing environmental conditions, throughout their design life, with due account taken of plant conditions during maintenance and testing.

5.48. The environmental conditions considered in the qualification programme for items important to safety at a nuclear power plant shall include the variations in ambient environmental conditions that are anticipated in the design basis for the plant.

5.49. The qualification programme for items important to safety shall include the consideration of ageing effects caused by environmental factors (such as conditions of vibration, irradiation, humidity or temperature) over the expected service life of the items important to safety. When the items important to safety are subject to natural external events and are required to perform a safety function during or following such an event, the qualification programme shall replicate as far as is practicable the conditions imposed on the items important to safety by the natural event, either by test or by analysis or by a combination of both.

5.50. Any environmental conditions that could reasonably be anticipated and that could arise in specific operational states, such as in periodic testing of the containment leak rate, shall be included in the qualification programme.

Criterion 31: Ageing management

The design life of items important to safety at a nuclear power plant shall be determined. Appropriate margins shall be provided in the design to take due account of relevant mechanisms of ageing *such as:* neutron embrittlement*, thermal embrittlement, oxidation, fatigue* and wear out and of the potential for age related degradation, to ensure the capability of items important to safety to perform their necessary safety functions throughout their design life.

5.51. The design for a nuclear power plant shall take due account of ageing and wear-out effects in all operational states for which a component is credited, including testing, maintenance, maintenance outages, plant states during a postulated initiating event and plant states following a postulated initiating event.

5.52. Provision shall be made for monitoring, testing, sampling and inspection to assess ageing mechanisms predicted at the design stage and to help identify unanticipated behaviour of the plant or degradation that might occur in service.

5.3 Human Factors

Criterion 32: Design for optimal operator performance

Systematic consideration of human factors, including the human–machine interface, shall be included at an early stage in the design process for a nuclear power plant and shall be continued throughout the entire design process.

5.53 The design for a nuclear power plant shall specify the minimum number of operating personnel required to perform all the simultaneous operations necessary to bring the plant into a safe state.

5.54. Operating personnel who have gained operating experience in similar plants shall as far as is practicable be actively involved in the design process conducted by the design organization in order to ensure that consideration is given as early as possible in the process to the future operation and maintenance of equipment.

5.55. The design shall support operating personnel in the fulfilment of their responsibilities and in the performance of their tasks, and shall limit the likelihood and the effects of operating errors on safety. The design process shall give due consideration to plant layout and equipment layout, and to procedures, including procedures for maintenance and inspection, to facilitate interaction between the operating personnel and the plant, in all plant states.

5.56. The human–machine interface shall be designed to provide the operators with comprehensive but easily manageable information, in accordance with the necessary decision times and action times. The information necessary for the operator to make a decision to act shall be simply and unambiguously presented.

5.57. The operator shall be provided with the necessary information:

(a) To assess the general state of the plant in any condition;

(b) To operate the plant within the specified limits on parameters associated with plant systems and equipment (operational limits and conditions);

(c) To confirm that safety actions for the actuation of safety systems are automatically initiated when needed and that the relevant systems perform as intended;

(d) To determine both the need for and the time for manual initiation of the specified safety actions.

5.58. The design shall be such as to promote the success of operator actions with due regard for the time available for action, the conditions to be expected and the psychological demands being made on the operator.

5.59. The need for intervention by the operator on a short time-scale shall be kept to a minimum and it shall be demonstrated that the operator has sufficient time to make a decision and sufficient time to act.

5.60. The design shall be such as to ensure that, following an event affecting the plant, environmental conditions in the control room or the supplementary control room and in locations on the access route to the supplementary control room do not compromise the protection and safety of the operating personnel.

5.61. The design of workplaces and the working environment of the operating personnel shall be in accordance with ergonomic concepts.

5.62. Verification and validation, including by the use of simulators, of features relating to human factors shall be included at appropriate stages to confirm that necessary actions by the operator have been identified and can be correctly performed.

5.4 Other Design Considerations

Criterion 33: Safety systems, and safety features for design extension conditions, of units of a multiple unit nuclear power plant.

Each unit of a multiple unit nuclear power plant shall have its own safety systems and shall have its own safety features for design extension conditions.

5.63. To further enhance safety, means allowing interconnections between units of a multiple unit nuclear power plant shall be considered in the design.

Criterion 34: Systems containing fissile material or radioactive material

All systems in a nuclear power plant that could contain fissile material or radioactive material shall be so designed as: to prevent the occurrence of events that could lead to an uncontrolled radioactive release to the environment; to prevent accidental criticality and overheating; to ensure that radioactive *and toxic* releases of material are kept below authorized limits on discharges in normal operation and below acceptable limits in accident conditions, and are kept as low as reasonably achievable; and to facilitate mitigation of radiological consequences of accidents.

Criterion 35: Nuclear power plants used for cogeneration of heat and power, heat generation or desalination

Nuclear power plants coupled with heat utilisation units (such as for district heating) and/or water desalination units shall be designed to prevent processes that transport radionuclides from the nuclear plant to the desalination unit or the district heating unit under conditions of operational states and in accident conditions.

Criterion 36: Escape routes from the plant

A nuclear power plant shall be provided with a sufficient number of escape routes, clearly and durably marked, with reliable emergency lighting, ventilation and other services essential to the safe use of these escape routes.

5.64. Escape routes from the nuclear power plant shall meet the relevant national and international requirements for radiation zoning and fire protection, and the relevant national requirements for industrial safety and plant security.

5.65. At least one escape route shall be available from workplaces and other occupied areas following an internal event or an external event or following combinations of events considered in the design.

Criterion 37: Communication systems at the plant

Effective means of communication shall be provided throughout the nuclear power plant to facilitate safe operation in all modes of normal operation and to be available for use following all postulated initiating events and in accident conditions.

5.66. Suitable alarm systems and means of communication shall be provided so that all persons present at the nuclear power plant and on the site can be given warnings and instructions, in operational states and in accident conditions.

5.67. Suitable and diverse means of communication necessary for safety within the nuclear power plant and in the immediate vicinity, and for communication with relevant off-site agencies, shall be provided.

Criterion 38: Control of access to the plant

The nuclear power plant shall be isolated from its surroundings with a suitable layout of the various structural elements so that access to it can be controlled.

5.68. Provision shall be made in the design of the buildings and the layout of the site for the control of access to the nuclear power plant by operating personnel and/or for equipment,

including emergency response personnel and vehicles, with particular consideration given to guarding against the unauthorized entry of persons and goods to the plant.

Criterion 39: Prevention of unauthorized access to or interference with items important to safety

Unauthorized access to, or interference with, items important to safety, including computer hardware and software, shall be prevented.

Criterion 40: Prevention of harmful interactions of systems important to safety

The potential for harmful interactions of systems important to safety at the nuclear power plant that might be required to operate simultaneously shall be evaluated, and effects of any harmful interactions shall be prevented.

5.69. In the analysis of the potential for harmful interactions of systems important to safety, due account shall be taken of physical interconnections and of the possible effects of one system's operation, maloperation or malfunction on local environmental conditions of other essential systems, to ensure that changes in environmental conditions do not affect the reliability of systems or components in functioning as intended.

5.70. If two fluid systems important to safety are interconnected and are operating at different pressures, either the systems shall both be designed to withstand the higher pressure, or provision shall be made to prevent the design pressure of the system operating at the lower pressure from being exceeded.

Criterion 41: Interactions between the electrical power grid and the plant

The functionality of items important to safety at the nuclear power plant shall not be compromised by disturbances in the electrical power grid, including anticipated variations in the voltage and frequency of the grid supply

5.5 Safety Analysis

Criterion 42: Safety analysis of the plant design

A safety analysis of the design for the nuclear power plant shall be conducted in which methods of both deterministic analysis and probabilistic analysis shall be applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed.

5.71. On the basis of a safety analysis, the design basis for items important to safety and their links to initiating events and event sequences shall be confirmed. It shall be demonstrated that the nuclear power plant as designed is capable of complying with authorized limits on discharges with regard to radioactive releases and with the dose limits in all operational states, and is capable of meeting acceptable limits for accident conditions.

5.72. The safety analysis shall provide assurance that Defence-in-Depth has been implemented in the design of the plant.

5.73. The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects[16] and early radioactive releases or large radioactive releases.

5.74. The applicability of the analytical assumptions, methods and degree of conservatism used in the design of the plant shall be updated and verified for the current or as built design.

Deterministic approach

5.75. The deterministic safety analysis shall mainly provide:

(a) Establishment and confirmation of the design bases for all items important to safety;

(b) Characterization of the postulated initiating events that are appropriate for the site and the design of the plant;

(c) Analysis and evaluation of event sequences that result from postulated initiating events, to confirm the qualification requirements;

[16] A 'cliff edge effect', in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.

(d) Comparison of the results of the analysis with acceptance criteria, design limits, dose limits and acceptable limits for purposes of radiation protection;

(e) Demonstration that the management of anticipated operational occurrences and design basis accidents is possible by safety actions for the automatic actuation of safety systems in combination with prescribed actions by the operator;

(f) Demonstration that the management of design extension conditions is possible by the automatic actuation of safety systems and the use of safety features in combination with expected actions by the operator.

Probabilistic approach

5.76. The design shall take due account of the probabilistic safety analysis of the plant for all modes of operation and for all plant states, including shutdown, with particular reference to:

(a) Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of Defence-in-Depth are independent;

(b) Providing assurance that situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented;

(c) Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.

6. DESIGN OF SPECIFIC PLANT SYSTEMS

6.1 Overall Plant System

Criterion 42bis: Plant system performance

The overall plant system shall be designed considering the specific characteristics of the reactor coolant and, in general, of the fast reactor system. This includes coolant inherent characteristics, such as its freezing and boiling point, density, volumetric heat capacity, degree of opacity, chemical reactivity in contact with air and water, as well as corrosion and

erosion effects, and the reactor neutronic characteristics, such as its susceptibility to reactivity variations due to coolant heat-up and voiding as well as due to the loss of core geometry. Coolant-specific requirements, including the impurity and toxicity limits, need to be considered in the design as well.

6.2 Reactor Core and Associated Features

Criterion 43: Performance of fuel elements and assemblies

Fuel elements and assemblies for the nuclear power plant shall be designed to maintain their structural integrity, and to withstand satisfactorily the anticipated radiation levels and other conditions in the reactor core, in combination with all the processes of deterioration that could occur in operational states.

6.1 The processes of deterioration to be considered shall include those arising from: differential expansion and deformation; external pressure of the coolant; additional internal pressure due to fission products and the buildup of helium in fuel elements; irradiation of fuel and other materials in the fuel assembly; variations in pressure and temperature resulting from variations in power demand; chemical effects; static and dynamic loading, including flow induced vibrations and mechanical vibrations; and variations in performance in relation to heat transfer that could result from distortions or chemical effects. Allowance shall be made for uncertainties in data, in calculations and in manufacture.

6.2. Fuel design limits shall include limits on the permissible leakage of fission products from the fuel in anticipated operational occurrences so that the fuel remains suitable for continued use.

6.3. Fuel elements and fuel assemblies shall be capable of withstanding the loads and stresses associated with fuel handling.

Criterion 44: Structural capability of the reactor core

The fuel elements and fuel assemblies and their supporting structures for the nuclear power plant shall be designed so that, in operational states and in accident conditions other than severe accidents, a geometry that allows for adequate cooling is maintained,

and the insertion of control rods is not impeded.

Criterion 45: Control of the reactor core

Distributions of neutron flux that can arise in any state of the reactor core in the nuclear power plant, including states arising after shutdown and during or after refuelling, and states arising from anticipated operational occurrences and from accident conditions not involving degradation of the reactor core, shall be inherently stable. The demands made on the control system for maintaining the shapes, levels and stability of the neutron flux within specified design limits in all operational states shall be minimized.

6.4. Adequate means of detecting the neutron flux *in* the reactor core and *its* change shall be provided for the purpose of ensuring that there are no regions of the core in which the design limits could be exceeded.

6.5. In the design of reactivity control devices, due account shall be taken of wear-out and of the effects of irradiation, such as burn-up, changes in physical properties and *dimensions, and production of gas during normal operation, anticipated operational occurrences and accident conditions.*

6.6. The maximum degree of positive reactivity and its rate of increase by insertion in operational states and accident conditions not involving degradation of the reactor core shall be limited or compensated for to prevent any resultant failure of the boundary of the reactor coolant systems, to maintain the capability for cooling and to prevent any significant damage of the reactor core.

6.6bis. To avoid significant mechanical energy release during a core disruptive accident, the reactor core shall be designed to have favourable neutronic, thermal, and structural characteristics, considering all reactivity feedbacks to mitigate the consequences of such design extension conditions.

Criterion 46: Reactor shutdown

Means shall be provided to ensure to shut down the reactor of the nuclear power plant in operational states and in accident conditions, and that the shutdown condition can be maintained even for the most reactive conditions of the reactor core.

6.7. The effectiveness, speed of action and shutdown margin of the means of shutdown of the reactor shall be such that the specified design limits for fuel are not exceeded.

6.8. In judging the adequacy of the means of shutdown of the reactor, consideration shall be given to failures arising anywhere in the plant that could render part of the means of shutdown inoperative (such as failure of a control rod to insert) or that could result in a common cause failure.

6.9. The means for shutting down the reactor shall consist of at least two diverse and independent systems. *For design extension conditions, inherent power reduction with complementary shutdown method and/or passive shutdown capabilities (of one of the two diverse and independent systems) shall be provided to prevent severe core degradation and to avoid re-criticality in the long run.*

6.10. At least one of the two different shutdown systems shall be capable, on its own, of maintaining the reactor subcritical by an adequate margin and with high reliability, even for the most reactive conditions of the reactor core.

6.11. The means of shutdown shall be adequate to prevent any foreseeable increase in reactivity leading to unintentional criticality during the shutdown or during refuelling operations or other routine or non-routine operations in the shutdown state.

6.12. Instrumentation shall be provided and tests shall be specified for ensuring that the means of shutdown are always in the state stipulated for a given plant state.

6.3 Reactor Coolant Systems

Criterion 47: Design of reactor coolant systems

The components of the reactor coolant systems for the nuclear power plant shall be designed and constructed so that the risk of faults due to inadequate quality of materials,

inadequate design standards, insufficient capability for inspection or inadequate quality of manufacture is minimized.

6.13. Pipework connected to the *reactor coolant* boundary for the nuclear power plant shall be equipped with adequate isolation devices to limit any loss of radioactive fluid (primary coolant) and to prevent the loss of coolant through interfacing systems so that cooling of the reactor core can be maintained.

6.14. The design of the reactor coolant boundary shall be such that flaws are very unlikely to be initiated, and any flaws that are initiated would propagate in a regime of high resistance to unstable fracture and to rapid crack propagation, thereby permitting the timely detection of flaws.

6.15. The design of the reactor coolant systems shall be such as to ensure that plant states in which components of the reactor coolant boundary could exhibit embrittlement are avoided.

6.15bis. The components of the reactor coolant systems shall be designed with due account taken of creep properties, thermal fatigue, irradiation damage (e.g., fast neutron fluence), coolant-induced environmental effects, and other ageing effects, as well as its compatibility with lead (e.g., in terms of corrosion-erosion), and with thermal stress and dynamic load on structures used under low pressure and high temperature conditions.

6.16. The design of the components contained inside the reactor coolant boundary, such as pump impellers and valve parts, shall be such as to minimize the likelihood of failure and consequential damage to other components of the primary coolant system that are important to safety, in all operational states and in design basis accident conditions, with due allowance made for deterioration that might occur in service.

Criterion 48: Overpressure protection of the reactor coolant boundary

Provision shall be made to ensure that the operation of pressure relief devices will protect the *reactor coolant* boundary of the reactor coolant systems against overpressure and will not lead to the release of radioactive material from the nuclear power plant directly to the environment.

Criterion 49: Inventory of reactor coolant

Provision shall be made for controlling the inventory, temperature and pressure of the reactor coolant to ensure that specified design limits are not exceeded in any operational state of the nuclear power plant, with due account taken of volumetric changes and leakage.

Criterion 50: Cleanup of reactor coolant

Adequate facilities shall be provided at the nuclear power plant for the removal from the reactor coolant of radioactive substances, including activated corrosion products and fission products deriving from the fuel, and non-radioactive substances.

6.17. The capabilities of the necessary plant *cleanup* systems shall be based on the specified design limit on permissible leakage of the fuel, with a conservative margin to ensure that the plant can be operated with a level of circuit activity that is as low as reasonably practicable, and to ensure that the requirements are met for radioactive releases to be as low as reasonably achievable and below the authorized limits on discharges.

Criterion 51: Removal of residual heat from the reactor core

Means shall be provided for the removal of residual heat from the reactor core in the shutdown state of the nuclear power plant such that the design limits for fuel, the reactor *coolant boundary* and structures important to safety are not exceeded.

Criterion 52: Emergency cooling of the reactor core

Means of cooling the reactor core shall be provided to restore and maintain cooling of the fuel under accident conditions at the nuclear power plant even if the integrity of the boundary of the primary coolant system is not maintained.

6.18. The means provided for cooling of the reactor core shall be such as to ensure that:

(a) The limiting parameters for the cladding or for integrity of the fuel (such as temperature) will not be exceeded;

(b) Possible chemical reactions are kept to an acceptable level;

(c) The effectiveness of the means of cooling of the reactor core compensates for possible changes in the fuel and in the internal geometry of the reactor core;

(d) Cooling of the reactor core will be ensured for a sufficient time.

6.19 Design features (such as leak detection systems, appropriate interconnections and capabilities for isolation) and suitable redundancy and diversity shall be provided to fulfil the requirements of para. 6.18 with adequate reliability for each postulated initiating event.

Criterion 53: Heat transfer to an ultimate heat sink

The capability to transfer heat to an ultimate heat sink shall be ensured for all plant states.

6.19A. Systems for transferring heat shall have adequate reliability for the plant states in which they have to fulfil the heat transfer function. This may require the use of a different ultimate heat sink or different access to the ultimate heat sink.

6.19B. The heat transfer function shall be fulfilled for levels of natural hazards more severe than those considered for design, derived from the hazard evaluation for the site.

6.4 Containment Structure and Containment System

Criterion 54: Containment system for the reactor

A containment system shall be provided to ensure or to contribute to the fulfilment of the following safety functions at the nuclear power plant: (i) confinement of radioactive substances in operational states and in accident conditions, (ii) protection of the reactor against natural external events and human induced events and (iii) radiation shielding in operational states and in accident conditions.

Criterion 55: Control of radioactive releases from the containment

The design of the containment shall be such as to ensure that any release of radioactive material from the nuclear power plant to the environment is as low as reasonably

achievable, is below the authorized limits on discharges in operational states and is below acceptable limits in accident conditions.

6.20. The containment structure and the systems and components affecting the leaktightness of the containment system shall be designed and constructed so that the leak rate can be tested after all penetrations through the containment have been installed and, if necessary during the operating lifetime of the plant.

6.21. The number of penetrations through the containment shall be kept to a practical minimum and all penetrations shall meet the same design requirements as the containment structure itself. The penetrations shall be protected against reaction forces caused by pipe movement or accidental loads such as those due to missiles caused by external or internal events, jet forces and pipe whip.

Criterion 56: Isolation of the containment

Each line that penetrates the containment at a nuclear power plant as part of the reactor *coolant boundary* or that is connected directly to the containment atmosphere shall be automatically and reliably sealable in the event of an accident in which the leak-tightness of the containment is essential to preventing radioactive releases to the environment that exceed acceptable limits.

6.22. Lines that penetrate the containment, as part of the reactor *coolant boundary* and, lines that are connected directly to the containment atmosphere shall be fitted with at least two adequate containment isolation valves or check valves arranged in series[17], and shall be provided with suitable leak detection systems. Containment isolation valves or check valves shall be located as close to the containment as is practicable, and each valve shall be capable of reliable and independent actuation and of being periodically tested.

6.23 Exceptions to the requirements for containment isolation stated in para. 6.22 shall be permissible for specific classes of lines such as instrumentation lines, or in cases in which application of the methods of containment isolation specified in para. 6.22 would reduce the reliability of a safety system that includes a penetration of the containment.

[17] In most cases, one containment isolation valve or check valve is outside the containment and the other is inside the containment. Other arrangements might be acceptable, however, depending on the design.

6.24 Each line that penetrates the containment and is neither part of the reactor coolant - boundary nor connected directly to the containment atmosphere shall have at least one adequate containment isolation valve. The containment isolation valves shall be located outside the containment and as close to the containment as is practicable.

Criterion 57: Access to the containment

Access by operating personnel to the containment at a nuclear power plant shall be through airlocks equipped with doors that are interlocked to ensure that at least one of the doors is closed during reactor power operation and in accident conditions.

6.25. Where provision is made for entry of operating personnel for surveillance purposes, provision for ensuring protection and safety for operating personnel shall be specified in the design. Where equipment airlocks are provided, provision for ensuring protection and safety for operating personnel shall be specified in the design.

6.26. Containment openings for the movement of equipment or material through the containment shall be designed to be closed quickly and reliably in the event that isolation of the containment is required.

Criterion 58: Control of containment conditions

Provision shall be made to control the pressure and temperature in the containment at a nuclear power plant and to control any build-up of fission products or other gaseous, liquid or solid substances that might be released inside the containment and that could affect the operation of systems important to safety.

6.27. The design shall provide for sufficient flow routes between separate compartments inside the containment. The cross-sections of openings between compartments shall be of such dimensions as to ensure that the pressure differentials occurring during pressure equalization in accident conditions do not result in unacceptable damage to the pressure bearing structure or to systems that are important in mitigating the effects of accident conditions.

6.28. The capability to remove heat from the containment shall be ensured, in order to reduce the pressure and temperature in the containment, and to maintain them at acceptably low levels after any accidental release of high energy fluids. The systems performing the function of removal of heat from the containment shall have sufficient reliability and redundancy to ensure that this function can be fulfilled.

6.28a. Design provision shall be made to prevent the loss of the structural integrity of the containment in all plant states. The use of this provision shall not lead to an early radioactive release or a large radioactive release.

6.28b. The design shall also include features to enable the safe use of non-permanent equipment[18] for restoring the capability to remove heat from the containment.

6.29. Design features to control fission products, and other substances that might be released into the containment shall be provided as necessary:

(a) To reduce the amounts of fission products that could be released to the environment in accident conditions;
(b) Omitted, not applicable to LFR.

6.30. Coverings, thermal insulations and coatings for components and structures within the containment system shall be carefully selected and methods for their application shall be specified to ensure the fulfilment of their safety functions and to minimize interference with other safety functions in the event of deterioration of the coverings, thermal insulations and coatings.

6.5 Instrumentation and Control Systems

Criterion 59: Provision of instrumentation

Instrumentation shall be provided for determining the values of all the main variables that can affect the fission process, the integrity of the reactor core, the reactor coolant systems and the containment at the nuclear power plant, for obtaining essential

[18] Non-permanent equipment need not necessarily be stored on the site.

information on the plant that is necessary for its safe and reliable operation, for determining the status of the plant in accident conditions, and for making decisions for the purposes of accident management.

6.31. Instrumentation and recording equipment shall be provided to ensure that essential information is available for monitoring the status of essential equipment and the course of accidents; for predicting the locations of release and amount of radioactive material that could be released from the locations that are so intended in the design, and for post-accident analysis.

Criterion 60: Control systems

Appropriate and reliable control systems shall be provided at the nuclear power plant to maintain and limit the relevant process variables within the specified operational ranges.

Criterion 61: Protection system

A protection system shall be provided at the nuclear power plant that has the capability to detect unsafe plant conditions and to initiate safety actions automatically to actuate the safety systems necessary for achieving and maintaining safe plant conditions.

6.32. The protection system shall be designed:

(a) To be capable of overriding unsafe actions of the control system;

(b) With fail-safe characteristics to achieve safe plant conditions in the event of failure of the protection system.

(c) To withstand the environmental conditions that are postulated to exist during normal operation, anticipated operational occurrences and accident conditions

6.33. The design:

(a) Shall prevent operator actions that could compromise the effectiveness of the protection system in operational states and in accident conditions, but not counteract correct operator actions in accident conditions;

(b) Shall automate various safety actions to actuate safety systems so that operator action is not necessary within a justified period of time from the onset of anticipated operational occurrences or accident conditions;

(c) Shall make relevant information available to the operator for monitoring the effects of automatic actions.

Criterion 62: Reliability and testability of instrumentation and control systems

Instrumentation and control systems for items important to safety at the nuclear power plant shall be designed for high functional reliability and periodic testability commensurate with the safety function(s) to be performed.

6.34. Design techniques such as testability, including a self-checking capability where necessary, fail-safe characteristics, functional diversity, and diversity in component design and in concepts of operation shall be used to the extent practicable to prevent loss of a safety function.

6.35. Safety systems shall be designed to permit periodic testing of their functionality when the plant is in operation, including the possibility of testing channels independently for the detection of failures and losses of redundancy. The design shall permit all aspects of functionality testing for the sensor, the input signal, the final actuator and the display.

6.36. When a safety system, or part of a safety system, has to be taken out of service for testing, adequate provision shall be made for the clear indication of any protection system bypasses that are necessary for the duration of the testing or maintenance activities.

Criterion 63: Use of computer-based equipment in systems important to safety

If a system important to safety at the nuclear power plant is dependent upon computer-based equipment, appropriate standards and practices for the development and testing of computer hardware and software shall be established and implemented throughout the service life of the system, and in particular throughout the software development cycle. The entire development shall be subject to a quality management system.

6.37. For computer-based equipment in safety systems or safety related systems:

(a) A high quality of, and best practices for, hardware and software shall be used, in accordance with the importance of the system to safety;

(b) The entire development process, including control, testing and commissioning of design changes, shall be systematically documented and shall be reviewable;

(c) An assessment of the equipment shall be undertaken by experts, who are independent of the design team and the supplier team to provide assurance of its high reliability;

(d) Where safety functions are essential for achieving and maintaining safe conditions, and the necessary high reliability of the equipment cannot be demonstrated with a high level of confidence, diverse means of ensuring the fulfilment of the safety functions shall be provided;

(e) Common cause failures deriving from software shall be taken into consideration;

(f) Protection shall be provided against accidental disruption of, or deliberate interference with, system operation.

Criterion 64: Separation of protection systems and control systems

Interference between protection systems and control systems at the nuclear power plant shall be prevented by means of separation, by avoiding interconnections or by suitable functional independence.

6.38. If signals are used in common by both a protection system and any control system, separation (such as by adequate decoupling) shall be ensured and the signal system shall be classified as part of the protection system.

Criterion 65: Control room

A control room shall be provided at the nuclear power plant from which the plant can be safely operated in all operational states, either automatically or manually, and from which measures can be taken to maintain the plant in a safe state or to bring it back into a safe state after anticipated operational occurrences and accident conditions.

6.39. Appropriate measures shall be taken, including the provision of barriers between the control room at the nuclear power plant and the external environment, and adequate information shall be provided for the protection of occupants of the control room, for a protracted period of time, against hazards such as high radiation levels resulting from accident conditions, releases of radioactive material, fire, or explosive or toxic gases.

6.40. Special attention shall be paid to identifying those events, both internal and external to the control room, that could challenge its continued operation, and the design shall provide for reasonably practicable measures to minimize the consequences of such events.

6.40a. The design of the control room shall provide an adequate margin against levels of natural hazards more severe than those considered for design, derived from the hazard evaluation for the site.

Criterion 66: Supplementary control room

Instrumentation and control equipment shall be kept available, preferably at a single location (a supplementary control room) that is physically, electrically and functionally separate from the control room at the nuclear power plant. The supplementary control room shall be so equipped that the reactor can be placed and maintained in a shutdown state, residual heat can be removed, and essential plant variables can be monitored if there is a loss of ability to perform these essential safety functions in the control room.

6.41. The requirements of paragraph 6.39 for taking appropriate measures and providing adequate information for the protection of occupants against hazards also apply for the supplementary control room at the nuclear power plant.

Criterion 67: Emergency response facilities on the site

The nuclear power plant shall include the necessary emergency response facilities on the site. Their design shall be such that personnel will be able to perform expected tasks for managing an emergency under conditions generated by accidents and hazards.

6.42. Information about important plant parameters and radiological conditions at the nuclear power plant and in its immediate surroundings shall be provided to the relevant emergency response facilities. Each facility shall be provided with means of communication with, as appropriate, the control room, the supplementary control room and other important locations at the plant, and with on-site and off-site emergency response organizations.

6.6 Emergency Power Supply

Criterion 68: Design for withstanding the loss of off-site power

The design of the nuclear power plant shall include an emergency power supply capable of supplying the necessary power in anticipated operational occurrences and design basis accidents, in the event of a loss of off-site power. The design shall include an alternate power source to supply the necessary power in design extension conditions.

6.43. The design specifications for the emergency power supply and for the alternate power source at the nuclear power plant shall include the requirements for capability, availability, duration of the required power supply, capacity and continuity.

6.44. The combined means to provide emergency power (such as water, steam or gas turbines, diesel engines or batteries) shall have a reliability and type that are consistent with all the requirements of the safety systems to be supplied with power, and their functional capability shall be testable.

6.44a. The alternate power source shall be capable of supplying the necessary power to preserve the integrity of the reactor coolant system and to prevent significant damage to the core and to

spent fuel in the event of the loss of off-site power combined with failure of the emergency power supply.

6.44b. Equipment that is necessary to mitigate the consequences of melting of the reactor core shall be capable of being supplied by any of the available power sources.

6.44c. The alternate power source shall be independent of and physically separated from the emergency power supply. The connection time of the alternate power source shall be consistent with the depletion time of the battery.

6.44d. Continuity of power for the monitoring of the key plant parameters and for the completion of short term actions necessary for safety shall be maintained in the event of loss of the AC (alternating current) power sources.

6.45. The design basis for any diesel engine or other prime mover[19] that provides an emergency power supply to items important to safety shall include:

(a) the capability of the associated fuel oil storage and supply systems to satisfy the demand within the specified time period;
(b) the capability of the prime mover to start and to function successfully under all specified conditions and at the required time;
(c) auxiliary systems of the prime mover such as coolant systems.

6.45a. The design shall also include features to enable the safe use of non-permanent equipment to restore the necessary electrical power supply[20].

6.7 Supporting Systems and Auxiliary Systems

Criterion 69: Performance of supporting systems and auxiliary systems.

The design of supporting systems and auxiliary systems shall be such as to ensure that the performance of these systems is consistent with the safety significance of the system or component that they serve at the nuclear power plant.

[19] A prime mover is a component (such as a motor, solenoid operator or pneumatic operator) that converts energy into action when commanded by an actuation device.
[20] Non-permanent equipment need not necessarily be stored on the site.

Criterion 70: Heat transport systems

Auxiliary systems shall be provided as appropriate to remove heat from systems and components at the nuclear power plant that are required to function in operational states and in accident conditions.

6.46. The design of heat transport systems shall be such as to ensure that non-essential parts of the systems can be isolated.

Criterion 71: Process sampling systems and post-accident sampling systems

Process sampling systems and post-accident sampling systems shall be provided for determining, in a timely manner, the concentration of specified radionuclides in fluid process systems, and in gas and liquid samples taken from systems or from the environment, in all operational states and in accident conditions at the nuclear power plant.

6.47. Appropriate means shall be provided at the nuclear power plant for the monitoring of activity in fluid systems that have the potential for significant contamination, and for the collection of process samples.

Criterion 72: Compressed air systems

The design basis for any compressed air system that serves an item important to safety at the nuclear power plant shall specify the quality, flow rate and cleanness of the air to be provided.

Criterion 73: Air conditioning systems and ventilation systems

Systems for air conditioning, air heating, air cooling and ventilation shall be provided as appropriate in auxiliary rooms or other areas at the nuclear power plant to maintain the required environmental conditions for systems and components important to safety in all plant states.

6.48. Systems shall be provided for the ventilation of buildings at the nuclear power plant with appropriate capability for the cleaning of air:

(a) To prevent unacceptable dispersion of airborne radioactive substances within the plant;

(b) To reduce the concentration of airborne radioactive substances to levels compatible with the need for access by personnel to the area;

(c) To keep the levels of airborne radioactive substances in the plant below authorized limits and as low as reasonably achievable;

(d) To ventilate rooms containing inert gases or noxious gases without impairing the capability to control radioactive effluents;

(e) To control releases of gaseous radioactive material to the environment below the authorized limits on discharges and to keep them as low as reasonably achievable.

6.49. Areas of higher contamination at the plant shall be maintained at a negative pressure differential (partial vacuum) with respect to areas of lower contamination and other accessible areas.

Criterion 74: Fire protection systems

Fire protection systems, including fire detection systems and fire extinguishing systems, fire containment barriers and smoke control systems, shall be provided throughout the nuclear power plant, with due account taken of the results of the fire hazard analysis.

6.50. The fire protection systems installed at the nuclear power plant shall be capable of dealing safely with fire events of the various types that are postulated.

6.51. Fire extinguishing systems shall be capable of automatic actuation where appropriate. Fire extinguishing systems shall be designed and located to ensure that their rupture or spurious or inadvertent operation would not significantly impair the capability of items important to safety.

6.52. Fire detection systems shall be designed to provide operating personnel promptly with information on the location and spread of any fires that start.

6.53. Fire detection systems and fire extinguishing systems that are necessary to protect against a possible fire following a postulated initiating event shall be appropriately qualified to resist the effects of the postulated initiating event.

6.54. Non-combustible or fire retardant and heat resistant materials shall be used wherever practicable throughout the plant, in particular in locations such as the containment and the control room.

Criterion 75: Lighting systems

Adequate lighting shall be provided in all operational areas of the nuclear power plant in operational states and in accident conditions.

Criterion 76: Overhead lifting equipment

Overhead lifting equipment shall be provided for lifting and lowering items important to safety at the nuclear power plant, and for lifting and lowering other items in the proximity of items important to safety.

6.55. The overhead lifting equipment shall be designed so that:

(a) Measures are taken to prevent the lifting of excessive loads;

(b) Conservative design measures are applied to prevent any unintentional dropping of loads that could affect items important to safety;

(c) The plant layout permits safe movement of the overhead lifting equipment and of items being transported;

(d) Such equipment can be used only in specified plant states (by means of safety interlocks on the crane);

(e) Such equipment for use in areas where items important to safety are located is seismically qualified.

Criterion 76bis: Coolant Heating Systems

Heating systems shall be provided for primary coolant as necessary to prevent loss of primary coolant circulation by coolant freezing. These heating systems and their controls shall be appropriately designed to assure that the temperature distribution and rate of change of temperature are maintained within the limits.

6.8 Other Power Conversion Systems

Criterion 77: *Power conversion systems*

The design of the *power conversion systems* for the nuclear power plant shall be such as to ensure that the appropriate design limits of the boundary of the reactor coolant systems are not exceeded in operational states or in accident conditions.

6.56. The design of the *power conversion systems* shall provide for appropriately rated and qualified *working fluid* isolation valves capable of closing under the specified conditions in operational states and in accident conditions.

6.57. The *working fluid* supply system shall be sized and designed to prevent anticipated operational occurrences from escalating to accident conditions.

6.58. The turbine generators shall be provided with appropriate protection such as overspeed protection and vibration protection, and measures shall be taken to minimize the possible effects of turbine generated missiles on items important to safety.

6.9 Treatment of Radioactive Effluents and Radioactive Waste

Criterion 78: Systems for treatment and control of waste

Systems shall be provided for treating solid radioactive waste and liquid radioactive waste at the nuclear power plant to keep the amounts and concentrations of radioactive releases below the authorized limits on discharges and as low as reasonably achievable.

6.59. Systems and facilities shall be provided for the management and storage of radioactive waste on the nuclear power plant site for a period of time consistent with the availability of the relevant disposal option.

6.60 The design of the plant shall incorporate appropriate features to facilitate the movement, transport and handling of radioactive waste. Consideration shall be given to the provision of access to facilities and to capabilities for lifting and for packaging.

Criterion 79: Systems for treatment and control of effluents

Systems shall be provided at the nuclear power plant for treating liquid and gaseous radioactive effluents to keep their amounts below the authorized limits on discharges and as low as reasonably achievable.

6.61. Liquid and gaseous radioactive effluents shall be treated at the plant so that exposure of members of the public due to discharges to the environment is as low as reasonably achievable.

6.62. The design of the plant shall incorporate suitable means to keep the release of radioactive liquids to the environment as low as reasonably achievable and to ensure that radioactive releases remain below the authorized limits on discharges.

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

6.10 Fuel Handling and Storage Systems

Criterion 80: Fuel handling and storage systems

Fuel handling and storage systems shall be provided at the nuclear power plant to ensure that the integrity and properties of the fuel are maintained at all times during fuel handling and storage.

6.64. The design of the plant shall incorporate appropriate features to facilitate the lifting, movement and handling of fresh fuel and spent fuel.

6.65. The design of the plant shall be such as to prevent any significant damage to items important to safety during the transfer of fuel or casks, or in the event of fuel or casks being dropped.

6.66. The fuel handling and storage systems for irradiated and non-irradiated fuel shall be designed:

(a) To prevent criticality by a specified margin, by physical means or by means of physical processes, and preferably by the use of geometrically safe configurations, even under conditions of optimum moderation;

(b) To permit inspection of the fuel;

(c) To permit maintenance, periodic inspection and testing of components important to safety;

(d) To prevent damage to the fuel;

(e) To prevent the dropping of fuel in transit;

(f) To provide for the identification of individual fuel assemblies;

(g) To provide proper means for meeting the relevant requirements for radiation protection;

(h) To ensure that adequate operating procedures and a system of accounting for, and control of, nuclear fuel can be implemented to prevent any loss of, or loss of control over, nuclear fuel.

6.67. In addition, the fuel handling and storage systems for irradiated fuel shall be designed:

(a) To permit adequate removal of heat from the fuel *and monitoring its status* in operational states and in accident conditions;

(b) To prevent the dropping of spent fuel in transit;

(c) To prevent causing unacceptable handling stresses on fuel elements or fuel assemblies;

(d) To prevent the potentially damaging dropping on the fuel of heavy objects such as spent fuel casks cranes or other objects, on the fuel;

(e) To permit safe keeping of suspect or damaged fuel elements or fuel assemblies;

(f) To control levels of soluble absorber if this is used for criticality safety;

(g) To facilitate maintenance and future decommissioning of fuel handling and storage facilities;

(h) To facilitate decontamination of fuel handling and storage areas and equipment when necessary;

(i) To accommodate, with adequate margins, all the fuel removed from the reactor in accordance with the strategy for core management that is foreseen and including the entire inventory of fuel in the reactor core;

(j) To facilitate the removal of fuel from storage and its preparation for off-site transport.

6.68. For reactors using a water pool system for fuel storage, the design shall be such as to prevent the uncovering of fuel assemblies in all plant states that are of relevance for the spent fuel pool so that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated' and so as to avoid high radiation fields on the site. The design of the plant:

(a) Shall provide the necessary fuel cooling capabilities;

(b) Shall provide features to prevent the uncovering of fuel assemblies in the event of a leak or a pipe break;

(c) Shall provide a capability to restore the water inventory.

The design shall also include features to enable the safe use of non-permanent equipment to ensure sufficient water inventory for the long term cooling of spent fuel and for providing shielding against radiation.

6.68a. The design shall include the following:

(a) Means for monitoring and controlling the water temperature for operational states and for accident conditions that are of relevance for the spent fuel pool;

(b) Means for monitoring and controlling the water level for operational states and for accident conditions that are of relevance for the spent fuel pool;

(c) Means for monitoring and controlling the activity in water and in air for operational states and means for monitoring the activity in water and in air for accident conditions that are of relevance for the spent fuel pool;

(d) Means for monitoring and controlling the water chemistry for operational states.

6.11 Radiation Protection

Criterion 81: Design for radiation protection

Provision shall be made for ensuring that doses to operating personnel at the nuclear power plant will be maintained below the dose limits and will be kept as low as reasonably achievable, and that the relevant dose constraints will be taken into consideration.

6.69. Radiation sources throughout the plant shall be comprehensively identified, and exposures and radiation risks associated with them shall be kept as low as reasonably achievable [25], the integrity of the fuel cladding shall be maintained, and the generation and transport of corrosion products and activation products shall be controlled.

6.70. Materials used in the manufacture of structures, systems and components shall be selected to minimize activation of the material as far as is reasonably practicable.

6.71. For the purposes of radiation protection, provision shall be made for preventing the release or the dispersion of radioactive substances, radioactive waste and contamination at the plant.

6.72. The plant layout shall be such as to ensure that access of operating personnel to areas with radiation hazards and areas of possible contamination is adequately controlled, and that exposures and contamination are prevented or reduced by this means and by means of ventilation systems.

6.73. The plant shall be divided into zones that are related to their expected occupancy and to radiation levels and contamination levels in operational states (including refuelling, maintenance and inspection) and to potential radiation levels and contamination levels in accident conditions. Shielding shall be provided so that radiation exposure is prevented or reduced.

6.74. The plant layout shall be such that the doses received by operating personnel during normal operation, refuelling, maintenance and inspection can be kept as low as reasonably achievable, and due account shall be taken of the necessity for any special equipment to be provided to meet these requirements.

6.75. Plant equipment subject to frequent maintenance or manual operation shall be located in areas of low dose rate to reduce the exposure of workers.

6.76. Facilities shall be provided for the decontamination of operating personnel and plant equipment.

Criterion 82: Means of radiation monitoring

Equipment shall be provided at the nuclear power plant to ensure that there is adequate radiation monitoring in operational states and design basis accident conditions and, as far as is practicable, in design extension conditions.

6.77. Stationary dose rate meters shall be provided for monitoring local radiation dose rates at plant locations that are routinely accessible by operating personnel and where the changes in radiation levels in operational states could be such that access is allowed only for certain specified periods of time.

6.78. Stationary dose rate meters shall be installed to indicate the general radiation levels at suitable plant locations in accident conditions. The stationary dose rate meters shall provide sufficient information in the control room or in the appropriate control position that operating personnel can initiate corrective action if necessary.

6.79. Stationary monitors shall be provided for measuring the activity of radioactive substances in the atmosphere in those areas routinely occupied by operating personnel and where the levels of activity of airborne radioactive substances might be such as to necessitate protective measures. These systems shall provide an indication in the control room or in other appropriate locations when a high activity concentration of radionuclides is detected. Monitors shall also be provided in areas subject to possible contamination as a result of equipment failure or other unusual circumstances.

6.80. Stationary equipment and laboratory facilities shall be provided for determining, in a timely manner the concentrations of selected radionuclides in fluid process systems, and in gas and liquid samples taken from plant systems or from the environment, in operational states and in accident conditions.

6.81. Stationary equipment shall be provided for monitoring radioactive effluents and effluents with possible contamination prior to or during discharges from the plant to the environment.

6.82. Instruments shall be provided for measuring surface contamination. Stationary monitors (e.g. portal radiation monitors, hand and foot monitors) shall be provided at the main exit points from controlled areas and supervised areas, to facilitate the monitoring of operating personnel and equipment.

6.83. Facilities shall be provided for monitoring for exposure and contamination of operating personnel. Processes shall be put in place for assessing and for recording the cumulative doses to workers over time.

6.84. Arrangements shall be made to assess exposures and other radiological impacts, if any, in the vicinity of the plant by environmental monitoring of dose rates or activity concentrations, with particular reference to:

(a) Exposure pathways to people, including the food-chain;

(b) Radiological impacts, if any, on the local environment;

(c) The possible build-up, and accumulation in the environment, of radioactive substances;

(d) The possibility there being of any unauthorized routes for radioactive releases.

REFERENCES

[1] IAEA, 'Safety of Nuclear Power Plants: Design', SSR-2/1, Rev. 1, (2016)

[2] IAEA, "IAEA Safety Glossary, Terminology Used in Nuclear Safety and Radiation Protection", 2018 Edition (2018)

[3] USDOE & GIF "A Technology Roadmap for Generation IV Nuclear Energy Systems", GIF-002-00 (2002) and Technology Roadmap Update for Generation IV Nuclear Energy Systems, Technical report GIF (2014)

[4] GIF Risk & Safety Working Group, "Basis for safety approach for design & assessment of Generation IV Nuclear Systems", GIF/RSWG/2007/002 (2008)

[5] Alemberti, A., et al., "Lead-cooled Fast Reactor (LFR) Risk and Safety Assessment White Paper", GIF RSWG White Paper (Apr. 2014), https://www.gen-4.org/gif/jcms/c_67650/lead-cooled-fast-reactor-lfr-risk-and-safety-assessment-white-pape

[6] Alemberti, A., et al., "Lead-cooled Fast Reactor (LFR) System Safety Assessment", Generation IV International Forum (June 2020), https://www.gen-4.org/gif/jcms/c_118389/gif-lfr-ssa-june-2020

[7] GIF LFR System Steering Committee, "Draft System Research Plan for Lead Fast Reactor" (2015)

[8] Assessment of Regional CApabilities for new reactors Development through an Integrated Approach (ARCADIA), Euratom 7th Framework Programme Coordination Action Project, https://cordis.europa.eu/project/id/605116

[9] IAEA, "Fundamental Safety Principles", SF-1 (2006)

[10] IAEA, "Defence in Depth in Nuclear Safety", INSAG-10, A report by the International Nuclear Safety Advisory Group, IAEA, Vienna (1996)

[11] IAEA, "Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev.1", INSAG-12 (1999)

[12] IAEA, The Safety of Nuclear Power, 75-INSAG-5, A report by the International Nuclear Safety Advisory Group, Vienna (1992)

[13] GIF Risk & Safety Working Group, "An Integrated Safety Assessment Methodology (ISAM) for Generation IV Nuclear Systems", Report GIF/RSWG/2010/002/Rev. 1 (2008)

[14] GIF, "GIF R&D Outlook for Generation IV Nuclear Energy Systems" (2009) and 2018 Update (2018)

[15] GIF, “GIF 2019 Annual Report” (2020) and “2018 GIF Symposium Proceedings” (2020)

[16] Report on Source Term Assessment for XT-ADS and the lead cooled EFIT, Deliverable no. D1-62/64-2009, EUROTRANS FP6 project (2009)

[17] EU Council Directive 1999/30/EC of 22 April 1999 Relating to limit values for sulphur dioxide, nitrogen dioxide and oxides of nitrogen, particulate matter and lead in ambient air, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1999:163:0041:0060:EN:PDF

[18] EU Council Directive 98/24/EC of 7 April 1998 on the protection of the health and safety of workers from the risks related to chemical agents at work (fourteenth individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:01998L0024-20140325&from=EN

[19] Bowen, J.C., In-service inspection approaches for Lead-cooled Nuclear Reactors, Naval Postgraduate School (2017)

[20] Report of Japanese Government to the IAEA Ministerial Conference on Nuclear Safety, “The Accident at TEPCO's Fukushima Nuclear Power Stations” (2011)

[21] IAEA, The Fukushima Daiichi Accident, Report by the Director General, STI/PUB/1710, Vienna (2015)

[22] OECD/NEA, The Fukushima Daiichi Nuclear Power Plant Accident: OECD/NEA Nuclear Safety Response and Lessons Learnt, Technical report No. 7161, Paris (2013)

[23] COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT on the comprehensive risk and safety assessments ("stress tests") of nuclear power plants in the European Union and related activities, European Commission, COM/2012/571, Brussels (2012)

[24] IAEA, The Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-R-3, IAEA, Vienna (2006)

[25] IAEA, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards (Interim Edition), IAEA Safety Standards Series No. GSR Part 3, Vienna (2011)

[26] IAEA, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR Part 4, Vienna (2009)

[27] IAEA, Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. NS-R-3, Vienna (2003)

[28] Fauske, H.K., et al., Assessment of the FBR Core Disruptive Accident (CDA): The Role and Application of General Behavior Principles (GBPs), Journal of NUCLEAR SCIENCE and TECHNOLOGY, Vol. 39, No. 6, p. 615–627 (June 2002)

GLOSSARY

#accident conditions

Deviations from normal operation that are less frequent and more severe than anticipated operational occurrences. Accident conditions comprise design basis accidents and design extension conditions.
[from the DEFINITIONS in the IAEA SSR-2/1 (Rev.1)]

#add-on / added-on

Mechanism/device, which is additionally incorporated, or action to incorporate, in an existing structure, system and/or component after the nuclear power plant is built in order to reinforce/improve the safety function(s) (and which have not been incorporated in the design concept of the structure, system and component.)
[based on the 'Basis for the safety approach' and 'ISAM' of the GIF Risk & Safety Working Group.]

#anticipated operational occurrence

A deviation of an operational process from normal operation that is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions.
[from IAEA Safety Glossary (2018 Edition).]

#beyond design basis accident

This term is superseded by design extension conditions.

#boundary of the reactor coolant systems

Boundary of the systems, which constitute "reactor coolant systems".

#built-in

Mechanism/device, which is included, or action to include, in the design concept of an structure, system and component and which is forming an integral part of the structure, system and component, in order to reinforce/improve the safety function(s).

[based on the ‘Basis for the safety approach’ and ‘Integrated Safety Assessment Methodology’ of the GIF Risk & Safety Working Group.]

#cliff edge effect

A cliff edge effect, in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.
[from FOOTNOTES in the IAEA SSR-2/1 (Rev.1)]

#controlled state

Plant state, following an anticipated operational occurrence or accident conditions, in which the fundamental safety functions can be ensured and which can be maintained for a time sufficient to implement provisions to reach a safe state.
[from the DEFINITIONS in the IAEA SSR-2/1 (Rev.1)]

#core disruptive accident

A hypothetical severe accident, which occurs under the assumption of loss of control of the balance among heat generation, heat removal, and ineffectiveness of all the plant protective systems.
[based on the paper of Dr. Fauske (2002)[28]]

#design basis accident

A postulated accident leading to accident conditions for which a facility is designed in accordance with established design criteria and conservative methodology, and for which releases of radioactive material are kept within acceptable limits.
[from the DEFINITIONS in the IAEA SSR-2/1 (Rev.1)]

#design extension conditions

Postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process of the plant in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design

extension conditions comprise conditions in events without significant fuel degradation and conditions in events with core melting[21].

[from the DEFINITIONS in the IAEA SSR-2/1 (Rev.1)]

#design organization

The design organization is the organization responsible for preparation of the final detailed design of the plant to be built.
[from FOOTNOTES in the IAEA SSR-2/1 (Rev.1)]

#fast reactor

A nuclear reactor in which the fission chain reaction is sustained by fast neutrons.

#Generation IV Nuclear System

Generation IV nuclear energy systems are future, next-generation technologies that will compete in all markets with the most cost-effective technologies expected to be available for international deployment about the year 2030. Comparative advantages include reduced capital cost, enhanced nuclear safety, minimal generation of nuclear waste, and further reduction of the risk of weapons materials proliferation.
The Generation IV Systems selected by the GIF for further study are Gas-Cooled Fast Reactor (GFR), Lead-Cooled Fast Reactor (LFR), Molten Salt Reactor (MSR), Sodium-Cooled Fast Reactor (SFR), Supercritical Water-Cooled Reactor (SWCR) and Very High Temperature Reactor (VHTR).
[based on the GIF Roadmap and GIF Homepage]

#guard vessel (safety vessel)

Guard (safety) vessel is placed outside the reactor vessel containing the lead coolant.
It is constructed to maintain lead coolant level for reactor cooling in case of lead leakage.

#inherent characteristics

Fundamental property of a design concept that results from the basic choices in the materials used or in other aspects of the design which assures that a particular potential hazard cannot become a safety concern in any way.

[21] If not practically eliminated as discussed in sub-sections 1.3 and 2.1.

[Based on GIF/RSWG/2010/002/Rev.1: “Inherent safety feature”]

#item important to safety

An item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public.
Items important to safety include:

- Those structures, systems and components whose malfunction or failure could lead to undue radiation exposure of site personnel or members of the public;
- Those structures, systems and components that prevent anticipated operational occurrences from leading to accident conditions;
- Safety features (for design extension conditions);
- Those features that are provided to mitigate the consequences of malfunction or failure of structures, systems and components.

[from IAEA Safety Glossary (2018 Edition).]

#normal operation

Operation within specified operational limits and conditions.
[from IAEA Safety Glossary (2018 Edition).]

#operating personnel

Individual workers engaged in the operation of an authorized facility or the conduct of an authorized activity.
[from IAEA Safety Glossary (2018 Edition).]

#operational states

States defined under normal operation and anticipated operational occurrences.
[from IAEA Safety Glossary (2018 Edition).]

#passive safety feature

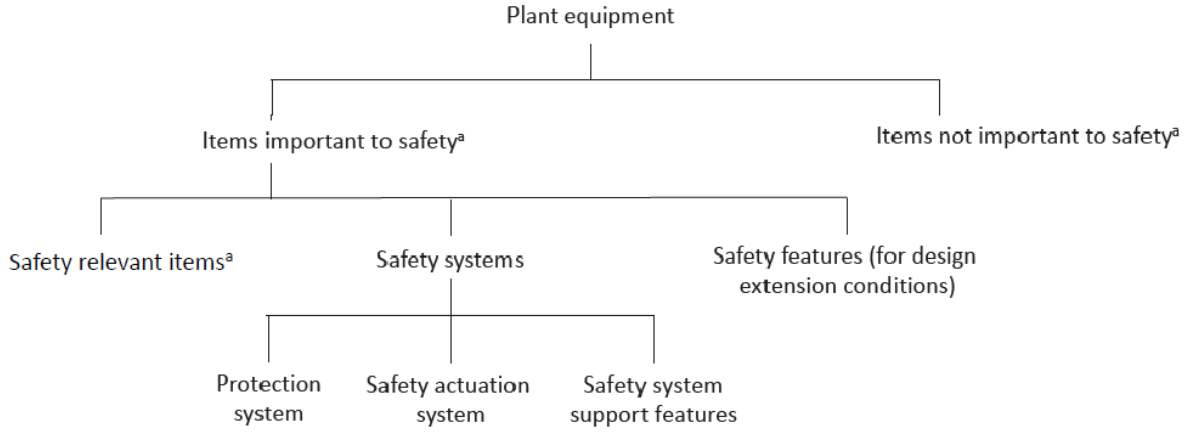
A safety feature that does not depend on an external input such as actuation, mechanical movement or supply of power.
[based on GIF/RSWG/2010/002/Rev.1: “Passive feature”]

#passive safety system

A safety system that uses passive safety feature for its major parts.

A passive safety system for decay heat removal is operated by natural circulation of the coolant and does not depend on safety system support features nor mechanical devices, except for instrumentation and control system, valves or dampers with DC power source.
A passive safety system for reactor shutdown is activated by responding directly to the changes of plant conditions (e.g. coolant temperature and/or pressure) and also operated by natural forces/phenomena (e.g. gravitational drop of absorber materials, enhancement of neutron leakage and/or moderation), which do not depend on protection systems and safety system support features.

#plant equipment

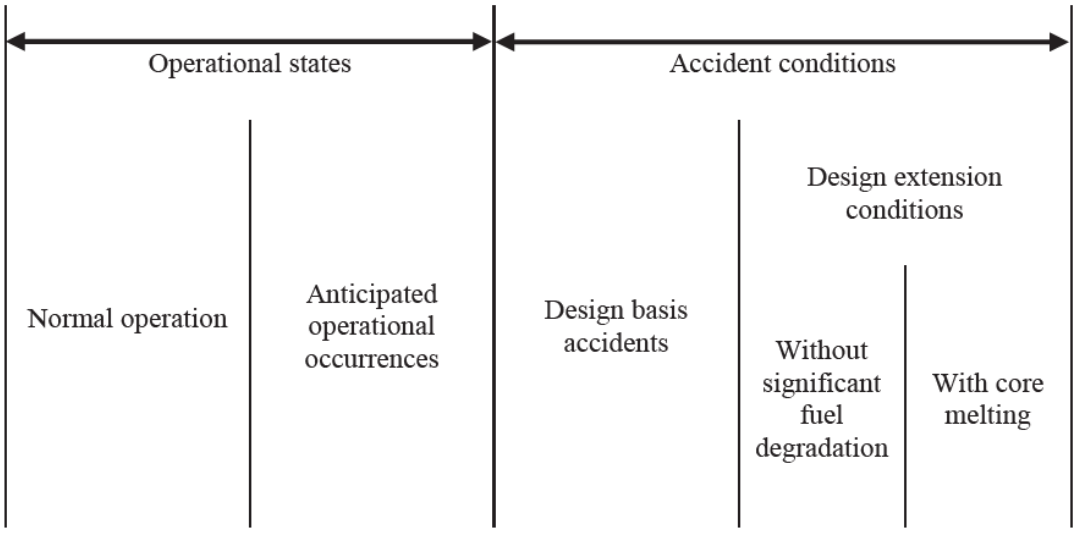


[a] In this context, an 'item' is a structure, system or component.

[Based on IAEA Safety Glossary (2018 Edition) with replacing "Safety related items" by "Safety relevant items".]

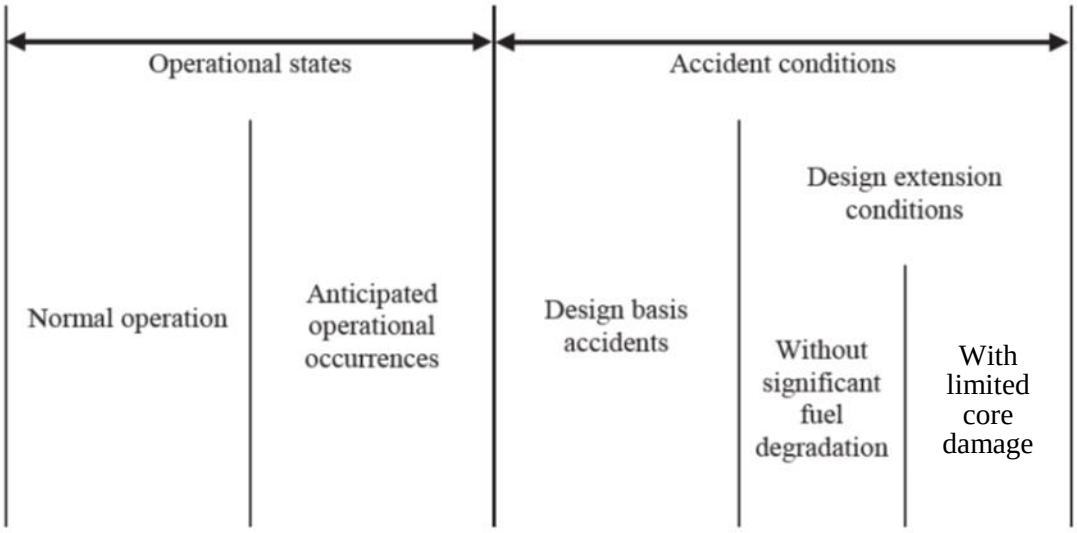
#plant states (considered in design)

In accordance with IAEA SSR-2/1 (Rev. 1)



[from the DEFINITIONS in the IAEA SSR-2/1 (Rev.1)]

In case severe accidents (with large core melting) are demonstrated to be practically eliminated (as discussed in sub-sections 1.3 and 2.1)



#practically eliminated

The possibility of certain conditions arising may be considered to have been practically eliminated if it would be physically impossible for the conditions to arise or if these conditions can be considered with a high level of confidence to be extremely unlikely to arise.
[from FOOTNOTES in the IAEA SSR-2/1 (Rev.1)]

#primary coolant system

The coolant system used to remove heat from the reactor core and to transfer the heat to the coolant in the secondary coolant system.

#prime mover

A prime mover is a component (such as a motor, solenoid operator or pneumatic operator) that converts energy into action when commanded by an actuation device.
[from FOOTNOTES in the IAEA SSR-2/1 (Rev.1)]

#protection system

System that monitors the operation of a reactor and which, on sensing an abnormal condition, automatically initiates actions to prevent an unsafe or potentially unsafe condition.
The system in this case encompasses all electrical and mechanical devices and circuitry, from sensors to actuation device input terminals.
[from IAEA Safety Glossary (2018 Edition).]

#reactor coolant boundary

The reactor coolant boundary is defined as the barrier of components which contains the primary coolant. The breakage of this boundary induces a primary coolant leak. The reactor coolant boundary forms a barrier against radioactive materials release together with the reactor cover gas boundary.

#reactor coolant systems

All systems used to remove heat from the reactor core and transfer that heat to the ultimate heat sink. The reactor coolant systems include: the primary coolant system, the secondary coolant system, the decay heat removal system, the cleanup facilities, and the power conversion system with associated coolant system.

#reactor cover gas boundary

The reactor cover gas boundary is defined as the barrier of components which contains the reactor cover gas. The breakage of this boundary induces a reactor cover gas leak. The reactor cover gas boundary forms a barrier against radioactive materials release together with the reactor coolant boundary.

#safe state

Plant state, following an anticipated operational occurrence or accident condition, in which the reactor is subcritical and the fundamental safety functions can be ensured and stably maintained for a long time.
[from the DEFINITIONS in the IAEA SSR-2/1 (Rev.1)]

#safety actuation system

The collection of equipment required to accomplish the necessary safety actions when initiated by the protection system.
[from IAEA Safety Glossary (2018 Edition).]

#safety feature for design extension conditions

Item designed to perform a safety function or which has a safety function in design extension conditions.
[from the DEFINITIONS in the IAEA SSR-2/1 (Rev.1)]

#safety group

The assembly of equipment designated to perform all actions required for a particular initiating event to ensure that the limits specified in the design basis for anticipated operational occurrences and design basis accidents are not exceeded.
[from IAEA Safety Glossary (2018 Edition).]

#safety relevant item

An item important to safety that is not part of a safety system.
[from “safety related item” in IAEA Safety Glossary (2018 Edition).]

#safety relevant system

A system important to safety that is not part of a safety system.

A safety related instrumentation and control system, for example, is an instrumentation and control system that is important to safety but which is not part of a safety system.
[from “safety related system” in IAEA Safety Glossary (2018 Edition).]

#safety system

A system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents.
Safety systems consist of the protection system, the safety actuation systems and the safety system support features. Components of safety systems may be provided solely to perform safety functions, or may perform safety functions in some plant operational states and non-safety functions in other operational states.
[from IAEA Safety Glossary (2018 Edition).]

#safety system settings

Settings for levels at which safety systems are automatically actuated in the event of anticipated operational occurrences or design basis accidents, to prevent safety limits from being exceeded.
[from the DEFINITIONS in the IAEA SSR-2/1 (Rev.1)]

#safety system support features

The collection of equipment that provides services such as cooling, lubrication and energy supply required by the protection system and the safety actuation systems.
[from IAEA Safety Glossary (2018 Edition).]

#secondary coolant system

The coolant system used to transfer heat from the coolant in the primary coolant system to the working fluid in the turbine system such as a water/steam system via a heat exchanger.

#severe accident

Accident more severe than a design basis accident and involving significant core degradation.
[from IAEA Safety Glossary (2018 Edition).]

#single failure

A single failure is a failure that results in the loss of capability of a system or component to perform its intended safety function(s), and any consequential failure(s) that result from it. The

single failure criterion is a criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure.
[from FOOTNOTES in the IAEA SSR-2/1 (Rev.1)]

#steam generator

A heat exchanger to transfer heat from a lead system to a water/steam system.

A report produced by

GEN IV International Forum

Expertise | Collaboration | Excellence

www.gen-4.org

LFR SSC

LFR provisional System Steering Committee