SDC-TF/2017/02

Sept. 30, 2017

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

(Rev. 1)

Prepared by:

The Safety Design Criteria Task Force (SDC-TF)

Of the Generation IV International Forum

DISCLAIMER

This report was prepared by the Safety Design Criteria Task Force 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.

Note on Revision History

Initial:	**SDC-TF/2013/01,**	**issued May 1, 2013.**
Revision 1:	**SDC-TF/2017/02,**	**issued Sept. 30, 2017.**

Table of Contents

EXECUTIVE SUMMARY

The Generation-IV International Forum [GIF] Policy Group proposed, at its meeting in October 2010, to develop “Safety Design Criteria [SDC]” for Sodium-cooled Fast Reactors [SFRs]. The terms-of-reference for the establishment of a Task Force to draft these SDC was approved at a Policy Group meeting in May 2011. The first Task Force meeting was held in July 2011, followed by three Task Force meetings and one teleconference to develop/update/modify the SDC, where input, comments and proposals from the Task Force and from other GIF entities were discussed. The result of these discussions is presented in this document.

The objective of the SDC is to present reference criteria for the safety design of structures, systems and components of an SFR system with the aim of achieving the safety goals of a Generation-IV reactor system. The reference criteria are systematically and comprehensively explained in the SDC.

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

I. Chapter 1, *Introduction*, describes the background, objectives and formulation principles and Chapter 2, *Safety Approach to the SFR 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 SFR system.

II. In Chapters 3 to 6, eighty-three 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, 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 SFR concept developers, but also parties interested in the SFR technology in general, including international and national regulatory organisations. The differences between the IAEA SSR 2/1 requirements and the GIF SFR SDC criteria are highlighted in the text and are indicated on a separate page.

III. A Glossary, covering specific terminologies for the SFR system and for Generation-IV reactor systems in general. A number of important terms, defined in e.g. the IAEA safety standards/glossary, are also incorporated for the convenience of the reader.

IV. An Appendix, which includes examples of key items of the SFR system configuration and technical background to understand better the SFR safety characteristics.

Improvements to reactor safety come from continuous efforts to update safety designs, and are enhanced by recently obtained knowledge from operation/hazards experiences. Therefore, the current

SDC will be continuously updated as necessary by, for example, attaching additional guidelines where more detailed explanations/criteria are needed.

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 present in a reactor. This statement is valid for all current nuclear installations and is also guiding the development of the Generation IV type of nuclear reactors. An international forum, 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 utilisation and security expected to be required in the middle of this century.

As the high-level safety standard, the 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”[1] and the GIF Risk & Safety Working Group proposed the “Basis for safety approach for design & assessment of Generation-IV Nuclear Systems”[2], hereinafter referred to as “GRM” and "BSA", respectively. In addition, the SFR System Steering Committee set the design goals for the SFR systems in 2007 in the publication “SFR System Research Plan”[3], hereinafter referred to as “SRP”. It is recognized 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.

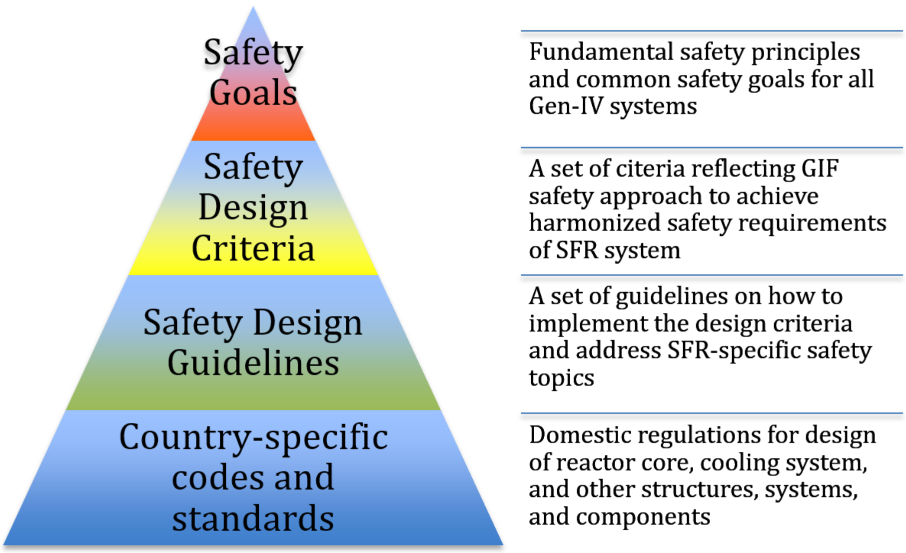


Figure 1 Hierarchy of Safety Standards

The idea to establish “Safety Design Criteria (SDC)” to fill that gap for one of the selected Generation-IV reactor systems was proposed and discussed at a GIF Policy Group meeting in October 2010. It was recognised 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 SDC for this type of reactors. Additional Safety Guides could be subsequently developed to fill the gap with codes and standards.

For light water reactor systems, safety fundamentals (e.g. IAEA SF-1[4]) and safety requirements (e.g. IAEA SSR2/1[5]) have already been established, and are used, in parallel with comparable domestic standards, for the design and regulation of LWRs. Generation-IV reactor systems, on the other hand, are advanced/new systems and the technologies and associated safety issues are, at least in the initial phases of development, likely to be better understood by the developers. For this reason, it is appropriate for developers to propose safety criteria to guide the design.

To date, GIF has developed two fundamental documents, GRM and BSA, for the Generation-IV reactor systems, and one document, SRP, especially for the SFR system. The GRM advocates goals for Generation-IV reactor systems in ‘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. In the SRP, safety design requirements have been established for reactor developers.

The SDC is aimed to fill the gap between high-level GIF safety goals and detailed country-specific codes and standards, and it is intended to be applicable to the design of the structures, systems and components, such as the reactor core, the fuel, the coolant system and the containment. The SDC reflects GIF’s fundamental safety approaches in order to achieve the safety goals of the Generation-IV SFR systems. The primary users of the SDC are expected to be the GIF SFR developers and designers. It is possible that the SDC, developed under GIF, might, in the future, be considered by the regulatory bodies as a reference for developing domestic SFR safety requirements. Hence, the potential users of the SDC may also include SFR developers and designers outside of GIF.

1.2 Principles of the SDC formulation

There are three points to take into account when formulating the SDC as shown in Figure 2. The first is that the safety level for Generation-IV reactor systems should be achieved, the second is that the specific technical features of SFRs should be considered, and the third is that the latest knowledge should be incorporated as it becomes available – for example, 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.

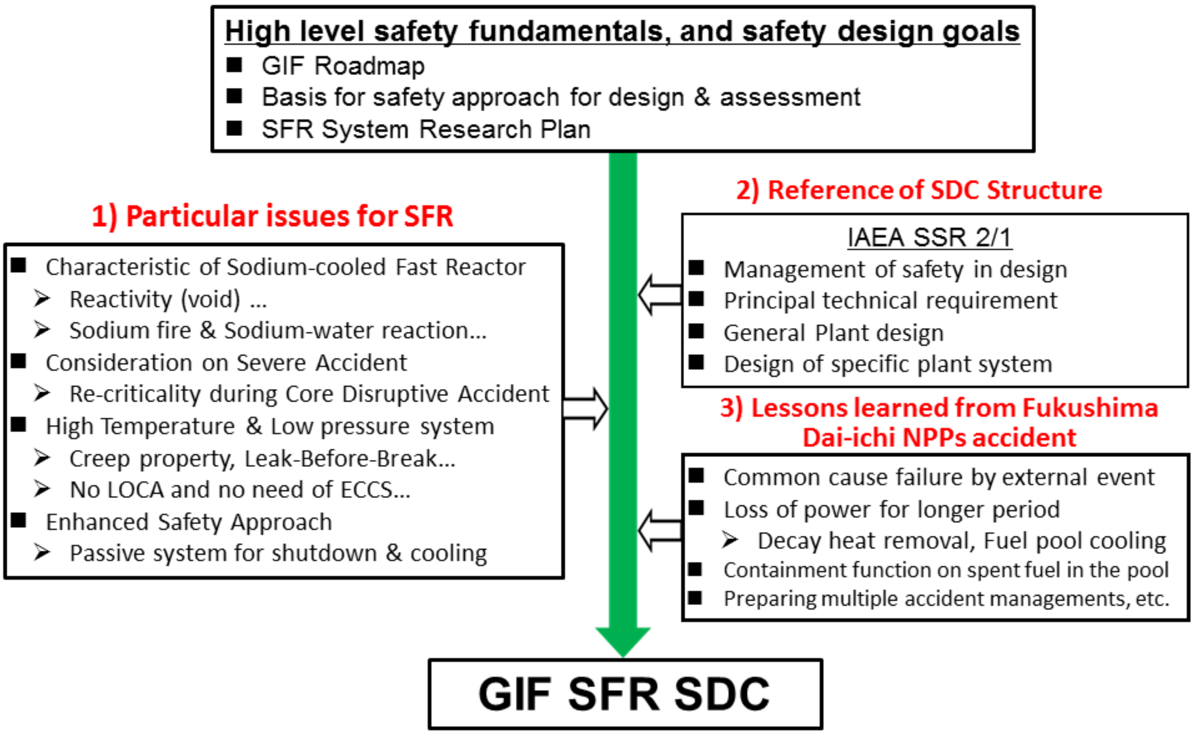


Figure 2 Basic Scheme to outline the SDC

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

1) Policy on goals

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

2) Policy on descriptions

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

3) Policy in definitions and terminology

The IAEA SSR 2/1 is the safety design requirement that was established for Generation-III LWR systems by the IAEA with participation of nuclear regulatory bodies in various countries. When establishing safety design criteria for the Generation-IV SFR systems, SSR 2/1 is considered as a reference document in terms of its basic approach towards safety, comprehensive formulation, as well as terms and definitions. The SDC maintains the basic structure of SSR 2/1 and its original text is preserved as much as possible. The safety-related terms for the SDC are basically the same as the ones defined in the IAEA Safety Glossary [6] (2007), and new definitions are added as needed for terms specific to the Generation-IV SFR systems.

2. SAFETY APPROACH TO THE SFR 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[7], 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 follows the definition in SSR 2/1, which consults INSAG-12[8] for the Defence-in-Depth principle: i.e. the plant states shown in Figure 3 are operational states include normal operation and anticipated operational occurrences; accident conditions include design basis accidents and design extension conditions. 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.

<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="5">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 level and Plant States
based on IAEA INSAG-12 & SSR-2/1

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 Defence-in-Depth Levels 1 - 2 [Operational states].

2) Generation-IV nuclear energy systems will have a very low likelihood and degree of reactor core damage. Reducing frequency of initiating events are 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 safety goals that Generation-IV nuclear energy systems will eliminate the need for off-site emergency response. This means to provide measures for preventing 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. 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 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 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 used 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 interaction.

2.2.2 Relationship among plant states, probabilistic and deterministic approaches

Considering the already ambitious Generation-III safety objectives as the reference, Generation-IV reactor systems will excel in safety, with improved safety design and more robust safety demonstration. In order to realise this, a highly reliable system with very low probability of accidents and with enhanced measures against severe accidents has to be achieved, in addition to improved well-balanced safety throughout the whole range of accident conditions.

The events to be considered for the safety design are internal events, resulting from human errors or plant component failures, and external events. For internal events, anticipated operational occurrences, design basis accidents and design extension conditions will be defined and measures for each of them must be built into the design. As for external events, design conditions will be established in accordance with site conditions in order to protect safety functions, including additional margins to the design conditions as necessary. The approaches for normal operation, anticipated operational occurrences, design basis accidents and design extension conditions are described as follows:

- *Safety for normal operation, anticipated operational occurrences and design basis accidents*

  Feedback on 'operation/accident experience' and 'maintenance/repair experience' is important. High system reliability will be attained by improvements and developments obtained from operational experience with previous and current reactors, by the enhancement of safety margins through the introduction of new technologies, and by the improvement of inspection technology capable of detecting conditions that could lead to failures.

- *Safety for design extension conditions*

  Providing practical measures for managing design extension conditions is important in order to prevent their occurrences (if possible) and/or mitigate their consequences. This will enhance the robustness of the system and will permit reaching the safety level required for Generation-IV reactors. Due consideration of the potential for common cause failures shall be taken into account in the safety design. Due consideration for applying passive design measures, by utilizing/enhancing favourable safety features specific to the Generation-IV SFR system, will also be required for design extension conditions. Feedback from past experience in this field will be used to improve reliability. The reactor should be designed such that accident progresses slow enough to allow time for systems to respond and appropriate actions needed to mitigate the consequences to proceed.

Consideration will be given to the effective functioning of design measures for each Defence-in-Depth level, so that a specific event will not be a dominant factor. The identification/selection of design basis accidents and design extension conditions will be based on the combined use of:

- ✧ “Deterministic approach based on fundamental characteristics of the reactor system supplemented by probabilistic analysis as needed”,
- ✧ “Operation experience” & “External event experience”, and
- ✧ “Licensing experience”.

Although individual design basis accidents and design extension conditions selections depend on the specific plant design, representative event types (categorized groups) are identified based on the fundamental characteristics of the reactor system and on the operation/external-event/licensing experiences, supplemented with Probabilistic Safety Assessment. The application of Probabilistic Safety Assessment from the beginning and throughout the design phases is encouraged to estimate the effectiveness of design measures[9].

2.2.3 Utilisation of passive safety features

Provisions of well-balanced design measures are necessary and can be obtained by using an appropriate combination of active and passive safety systems in order to enhance safety against a number of wide-ranging events, including design basis accidents and design extension conditions. It should be noted that the performance of a passive safety system should not largely rely on its power source, although the possibility to fine control such a system is limited (e.g. coolant temperature overshoot may happen at the start-up of a decay heat removal system.)

For design basis accidents, it is important to well characterize the safety features of structures, systems and components, including inherent characteristics. And the reliability of the safety systems should be preferably enhanced based on proven technologies (safety systems with adequate redundancy and diversity) 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.

2.2.4 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.

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.

2.2.5 Containment function

The containment should be designed so that it can withstand postulated severe accidents with core degradation. Safety provisions required to mitigate consequences of core degradation and to retain the degraded core materials should be built-in.

For radiological confinement, design provisions related to the confinement function should be enhanced, as far as reasonably achievable, and confinement measures must take into account a source term whatever the origin of the radioactive material in the plant (e.g. core, spent fuel storage…)

2.2.6 Provision against hazards

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

One of the main lessons learned from the TEPCO's Fukushima Dai-ichi 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 safety of the plant,
- confirm that consequences of degraded plant situations induced by extreme hazards are acceptable,
- define equipments 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 fundamental safety function shall rely on appropriate diversification and physical separation for enhancing redundancy to ensure the safety function.

2.2.7 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 achievable, 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 terms of the impact on the items important to safety.

2.3 Safety approach of the Generation-IV SFR systems

2.3.1 Target SFR Systems

The target systems for establishing the SDC are SFRs developed under GIF as described in SFR System Research Plan (SRP). SRP provides information about the configuration of the target SFR systems and explains the Generation-IV system safety and reliability goals as developed from the GRM based on qualitative/quantitative design metrics. SFR may use minor actinide bearing fuel.

The specifications of the GIF SFR systems are as follows:

System structure	Loop-type, Pool-type, Small modular
Electric output	50 - 2000 MWe
Coolant system	Primary and secondary [intermediate] coolant system utilizing sodium coolant
Balance of Plant system	Water/Steam cycle Alternative concept: Supercritical CO_2 or other gas cycle
Fuel	MOX, Metal, others

Technical solutions, based on state-of-the-art R&D [10],[11], are used to improve the safety design and enhance reliability and robustness of the SFR. The ongoing efforts to develop new safety-related technologies include industrial partnership and owners/operators as users.

2.3.2 Approach based on basic characteristics of the SFR

- 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 sodium. An important characteristic of an SFR is that the reactor core is not in the most reactive configuration under normal operating conditions and that it is possible to have a positive void reactivity in the centre area of the reactor core. Considering this characteristic, the reactor core should be designed to prevent excessive reactivity insertion.

- Physical and Chemical Properties Sodium Coolant

A positive feature of sodium is that it has a high thermal conductivity. The boiling temperature is 883 ºC at atmospheric pressure, significantly higher than the typical average core outlet temperature of an SFR of 500 – 550ºC. Hence, decay heat removal is possible using natural circulation due to the favourable coolant characteristics in that sodium remains in a liquid phase over that wide temperature range.

Since sodium is chemically active, however, it is necessary to manage sodium leaks (sodium fire on contact with air and reaction with water or concrete) so that it does not affect the safety of the reactor. A secondary coolant system is required for a Generation-IV SFR system to control/manage the consequences of a sodium-working fluid reaction during a heat exchange system tube rupture accidents. Sodium is opaque, making submerged visual monitoring and inspection a challenge. It also freezes at room temperature, having a melting point of 98 ºC. Hence, due consideration of this high melting point of sodium is necessary in the design of the structures, systems and components when addressing capabilities for inspection, maintenance and repairing, i.e. appropriate measures to prevent sodium freezing must be included in the design. As sodium allows the use of low pressure coolant systems, application of the Leak Before Break concept is feasible and would facilitate continuous leakage-monitoring as an inspection method for the coolant boundary. Application of Leak Before Break concept could also help in the determination of design basis leaks.

- Material usage environment

As an SFR operates at a relatively high temperature compared to an LWR (e.g. the coolant temperature range is around 300 - 600 ºC) 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 sodium and the large temperature differences between inlet and outlet of the reactor core, thermal striping is possible and must be accounted for in the design to prevent structural damage.

- ✧ Operation under low pressure condition

    As an SFR is operated under low pressure conditions, close to atmospheric pressure and temperatures far 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, an emergency core cooling systems for coolant injection under high and low pressure conditions, as used in the LWR, is not necessary in an SFR. The only requirements for SFR core cooling are the maintenance of the primary sodium coolant at a level which ensures the flow through the reactor core with sufficient heat removal capability.

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

- ✧ Reactor Core
    - ➢ Fuel elements and assemblies
    - ➢ Reactor core structure and characteristics
    - ➢ Reactor shutdown system
- ✧ Reactor Coolant Systems
    - ➢ Reactor coolant system (Primary coolant system)
    - ➢ Secondary coolant system (Intermediate coolant system)
    - ➢ Decay heat removal system (including final heat sink)
- ✧ Containment System

- ✧ Supporting and Auxiliary Systems, Fuel Handling & Storage
  - ➢ Sodium heating systems
  - ➢ Sodium purification system
  - ➢ Sodium leak detection & Sodium fire suppression
  - ➢ Cover gas system
  - ➢ Fuel storage in sodium

2.3.3 SFR specific safety approach in relation to the plant states

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

Based on the characteristics of the SFR, the design for normal operation, anticipated operational occurrences, and design basis accidents conditions must insure that: 1) the reactor can be reliably shutdown if needed, 2) the core remains covered in the case of a leak in the reactor 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 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 high boiling point of the coolant in an SFR result in single phase conditions in the case of a leak or break in the reactor coolant system. Therefore, injection systems are not required for SFR. Appropriate design measures are needed to prevent/suppress chemical reactions associated with leaks of reactor coolant. Designs should accommodate a loss of reactor coolant event without uncovering the core or interfering with the decay heat removal function. The excellent heat transfer properties of sodium allow efficient decay heat removal from the core, however, decay heat removal systems should be designed to prevent overcooling which might cause freezing of the coolant.

SFR design for design extension conditions

A fast reactor, including an SFR, is characterised 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 (by e.g. sodium boiling or gas bubble in the core), or fuel concentration (by e.g. core compaction by seismic solicitation or molten fuel concentration) 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 be provided and that containment functions be 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. Analysis of the plant response to design extension conditions may 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.

SFR design extension conditions events can be grouped into two categories based on the characteristics of an SFR and Probabilistic Safety Assessment studies. These are: 1) failure to shutdown the reactor following an off-normal initiating event, and 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 shutdown is paired with the three typical SFR 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 following three event categories, if not practically eliminated, can lead to the inability to remove heat from the core:

- loss of coolant flow (flow paths for decay heat removal become disrupted),
- loss of reactor coolant level (core becomes uncovered), and
- long-term loss of heat sink (with scram).

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

For the failure of reactor shutdown events, 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. In order to prevent core damage, the design may make 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 containment function.

For the loss of heat removal events, the design should provide a means to prevent core damage or loss of containment function by maintaining sodium coolant level for core cooling and ensuring decay heat removal even under the conditions with or without core damage. Compared to loss of shutdown events, there is generally more time prior to core damage so that a variety of diverse measures might be provided depending on the circumstances of the event. The degree of core damage may vary depending on the time margin to fuel failure after losing the decay heat removal function. Similar design approaches which address the loss of heat removal events may also be applied for a spent fuel storage pool using sodium, which might be located outside of the containment.

Design extension conditions shall include potential significant sodium chemical reactions (e.g. combustion resulting from leakage, sodium-water reaction resulting from steam generator tube failure, and sodium-concrete interactions resulting from leakage) so as to avoid affecting the safety of the reactor core or loss of containment function.

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. Sodium combustion, sodium concrete reaction, debris-concrete interaction, and combustion of accumulated hydrogen, which have the potential to load or otherwise threaten the integrity of the containment, must be prevented or mitigated.

2.3.4 Lessons Learned from TEPCO's Fukushima Dai-ichi Nuclear Power Plants Accidents

TEPCO's Fukushima Dai-ichi 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 [12], are included in the SDC as far as they have a potential impact on the safety of the GIF SFR systems. The key points are the enhancement of systems that may be needed to decrease the likelihood of a severe accident due to extreme external hazards, the enhancement of response measures against severe accidents, 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 during long term loss of all AC power. Enhancing passive safety functions will 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 accidents, necessary protection measures with adequate margins should be provided. Special attention must be paid to water flooding in buildings with sodium equipment.

The stress tests[13] are one possible method to evaluate the safety margins of nuclear power plants against severe plant conditions and the extreme external hazards. The stress tests may show how large the safety margins are relative to the design basis, whereas the SDC can deal with how robust the prevention and mitigation design features are against severe accidents.

Efforts to update the SDC, by including new lesson learned from the TEPCO’s Fukushima Dai-ichi Nuclear Power Plants accidents, will continue also under/after the initial GIF SDC work is completed.

3. MANAGEMENT OF SAFETY IN DESIGN

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 *research and* 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.

Criterion 2: Management system for *the* plant design [14]

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 *through a corrective action program*.

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 engineering codes, standards *and related supporting research results*, 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. *Any research activity performed to support the safety justification of the plant design shall be subject to quality assurance. Clear links to experimental records and results shall be established and maintained. Design choices made during the design process shall be recorded with adequate tracking.*

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. *The operating organization shall retain responsibility of the quality assurance program.*

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 stor*ag*e and

(iii) confinement of radioactive 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 in design [15]

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 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 to a large radioactive releases have been "practically eliminated" and that there would be no, or only minor, potential radiological consequences for plant states with a significant likelihood of occurrence.

4.4. Acceptable limits for purposes of 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 *contamination of the facility and* the environment *is* 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 is 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 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 effects 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 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;

(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.

(g) Shall consider the benefit of implementing passive safety features for shutdown and cooling.

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.

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.

4.13bis. Management system shall take into account the potential for adverse effects on safety ***or*** *security when designing, and before implementing changes to, the plant configurations, facility conditions, engineering and administrative controls.*

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 [16]

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, erected, *inspected and tested* 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 chemical* 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 chemical* waste generated in operation and provision for managing the radioactive waste that will be generated in the decommissioning of the plant.

(d) The disposal and/or reuse of the sodium 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 core melting.

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.

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, *operating experience* 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 of any initiating event *from the design analysis* 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 in designing the layout of the plant and in determining 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, *and sodium chemical reaction with air, water and other materials, including associated pressure waves, temperature increase and product releases, e.g. hydrogen.* Appropriate features for prevention and mitigation shall be provided to ensure that safety is not compromised.

External hazards [17]

5.17. The design shall include due consideration of those natural and human induced 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 dependent on the availability of off-site services such as electricity supply and fire fighting services. The design shall take *into* account site specific conditions to determine the delay *after* 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 *structures* 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 shall include due consideration of extreme external hazards and their consequences. In addition, specific equipments qualified to withstand these hazards should be provided (e.g. dedicated AC power, instrumentation...) and* 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 *a significant* radioactive relearse 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 *and with relevant research*, 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 *in* all operational states and for all accident conditions.

Criterion 19: Design basis accidents

A set of accidents 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 consequences, on or off the site, and do not necessitate any off-site protective actions.

5.26. The design basis accidents *are preferably* analysed 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, *operating experience,* 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 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. The main technical objective of considering *postulated* design extension conditions is to provide assurance that the design of the plant is such as to prevent accident conditions that are not considered *as* design basis accident conditions, or to mitigate their consequences. This might require additional safety features for design extension conditions, or extension of the capability of safety systems to prevent, or to mitigate the consequence of a severe accident, or to maintain the containment *function*. These additional safety features for design extension conditions, or this extension of the capability of safety systems, shall ensure the capability *of* managing accident conditions in which there is a significant amount of *chemical and* 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, with the result that the possibility of plant states arising that could lead to a significant radioactive releases is “practically eliminated”. 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[1] 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 reliability commensurate with the *safety* 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 by using engineering judgement and input from probabilistic safety assessments.

[1] 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. [From IAEA SSR 2/1 Footnote 9]

5.31. The design shall be such that design extension conditions that could lead to significant radioactive releases are practically eliminated. *Since a fast reactor core is not in its most reactive configuration under normal operating conditions, the following 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 recriticality leading large mechanical energy release during a core degradation progression,

(c) Means for decay heat removal of a degraded core, and

(d) Containment capability of enduring thermal and mechanical loads under severe accident conditions.

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

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 equipments dedicated for severe accident mitigation 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.

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[2].

5.39. Spurious action shall be considered to be one mode of failure when applying the single failure criterion 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.

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.

---

[2] 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 IAEA SSR 2/1 Footnote 10]

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. [18 [SSR-2/2 (Rev.1)]], Req.6 4):

(a) Safety limits;

(b) Limiting settings for safety systems;

(c) Limits and conditions for normal operation;

(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 *relevant* 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 external event, either by test or 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*** **embrittlement and wear-out, and of the potential for age related degradation,** ***due to high operating temperature, the sodium coolant, and the fast neutron irradiation,*** **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 decisions 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. *The design will be capable of performing all functions necessary to bring the plant to a safe state using appropriate allocations of functions to the operator, automation, or a combination of both to minimize errors.*

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 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 releases 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 *or process* 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, *also accounting for the interface of safety with security*.

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 *by detecting, assessing, and delaying the entry*.

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[11]

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 [16], 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 and significant 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;

(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 *inherent capabilities or* automatic actuation of safety systems in combination with prescribed actions of the operator.

(f) Demonstration that the management of design extension conditions is possible by the use of *appropriate* systems and the *reliance on inherent and/or passive* 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 situation 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 of a sodium-cooled fast reactor

The overall plant system shall be designed considering the specific characteristics of a sodium-cooled fast reactor as described below.

- ***(a) The reactor core is not in its most reactive configuration under normal operating conditions. This could lead to a positive reactivity insertion due to an unfavourable change in reactor core geometry.***
- ***(b) The sodium void reactivity may be positive in the central region of the reactor core. This could lead to a positive reactivity insertion due to sodium boiling or gas entrainment.***
- ***(c) The high boiling temperature of sodium at standard atmospheric pressure enables the reactor coolant system to operate at low pressure with a large margin to boiling.***
- ***(d) The high thermal conductivity and heat transfer coefficient of sodium, the large temperature gradient in the reactor core, and the decrease of sodium density with increasing temperature enable decay heat removal by natural circulation of the coolant.***
- ***(e) Sodium is chemically active and opaque, and it is solid below 98 ºC.***
- ***(f) Some mist and vapour of sodium can deposit on the components.***

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, *including fast neutron fluence*, 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; internal pressure *increase* due to *temperature*, fission products and the build-up of helium; irradiation of fuel and other materials in the fuel assembly; variations in temperature resulting from variations in power demand; chemical effects; static and dynamic loading, including flow induced vibrations and mechanical vibrations; and variations in *temperature* 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 *(due to both internal and external events)* other than severe accidents, a geometry that allows for adequate cooling is maintained, *core geometry is preserved to prevent excessive reactivity changes,* and the insertion of control *devices* is not impeded.

For the design extension conditions, provisions shall be included to avoid re-criticality resulting in potentially large mechanical energy release during a core disruptive accident.

6.3bis. The supporting structures shall be designed with due account taken of the creep properties, thermal striping, fast neutron induced changes, other ageing effects, and the material compatibility with sodium and its compounds.

6.3ter. The fuel assemblies and associated core support structure shall be designed to prevent mis-loading of fuel assemblies and any coolant channel blockages.

6.3quater. The assemblies and associated core support structure shall be designed so that the core geometry can be preserved to prevent excessive reactivity effects.

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 *degradation 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, including sodium void worth, 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 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 *and* propagate *result* in *leaks long before the flaws would grow to an* unstable *size*, thereby permitting the timely detection of *coolant leakage*.

6.14bis. Inert gas shall be used as a cover gas in sodium-filled components to prevent chemical reaction at the free surface of sodium, and the boundary of the cover gas shall be designed to be leak tight with isolation valves, except when the lines are equipped with pressure relief valves to protect the reactor vessel from excessive pressure load (over or under pressure). The reactor coolant boundary shall be designed as a barrier against radioactive materials release and be closed by the reactor cover gas boundary.

6.14ter. Provisions shall be made to detect sodium leaks and to mitigate the consequence of sodium chemical reaction in case of postulated sodium leaks from the reactor coolant systems. The *fundamental safety functions shall be maintained under severe sodium leak events considered in the design extension conditions.*

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 striping, fast neutron fluence, and other ageing effects, as well as its compatibility with sodium, and with thermal stress and dynamic load on thin-walled structures used under low pressure and high temperature conditions.

6.15ter. The design shall consider the potential for flow and thermal disturbances, such as flow induced vibrations or thermal striping, and shall reduce or eliminate such effects to maintain the structural integrity of the components of the reactor coolant systems.

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 reactor 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.

6.16bis. Components, which constitute the reactor coolant boundary, shall be designed to maintain the boundary function and to maintain a sufficient sodium inventory in the reactor coolant system in case of anticipated transients without scram.

6.16ter. Chemical reactions between sodium and water/steam or other working fluids shall be considered in the design of the secondary coolant system. Provisions to prevent and/or mitigate such chemical reactions shall be incorporated in the design:

> *(a) Provisions shall be made to detect leaks of working fluids, to control any leak propagation, and to automatically mitigate any leak accident to prevent further damages, such that isolation and relief valves in working fluid system, when a heat exchange system between the sodium and the working fluid is used.*
>
> *(b) A pressure relief system shall be employed in the secondary coolant system to protect the secondary coolant system from consequences resulting from sodium interactions with water/steam in the steam generator or with other working fluids in the heat exchanger.*
>
> *(c) The fundamental safety functions shall be maintained under postulated design extension conditions for severe chemical reactions between the sodium and the working fluid.*

6.16quater. Lines that penetrate the reactor coolant and cover gas boundaries shall be designed in order to prevent air and water ingresses.

6.16quinquies. The design of the reactor coolant system shall be such as to consider implementation of in service inspection of structures and components important to safety contained inside the reactor coolant boundary with dedicated equipments that overcome the sodium opaqueness.

Criterion 48: *Excessive* pressure *load* 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 against *excessive* pressure *load*.

Criterion 49: *Level* of reactor coolant

Provision shall be made for controlling the *level* of the reactor coolant to ensure that specified design limits are not exceeded in operational states *and that the cooling of fuel is maintained in accident conditions*, with tak*ing* due account of volumetric changes *to ensure that the core remains covered.*

Guard vessels and guard pipes shall be designed so as to maintain the sodium surface of the reactor coolant system at a level necessary for decay heat removal in the case of a sodium leak accident in the reactor coolant system. Due considerations shall be taken of a dependent failure and a common cause failure between the reactor vessel and the guard vessel, as well as between main coolant pipes and guard pipes. Provisions shall be made to reduce the amount of sodium that leaks from the reactor coolant system in case of a failure of the reactor coolant boundary.

Criterion 50: Cleanup of reactor coolant

Adequate facilities shall be provided for the removal of radioactive *and chemical* substances *from the reactor coolant*, 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.

6.17bis. Concentration of impurities in the sodium shall be controlled within a limit value in order to prevent excessive corrosion, coolant channel blockage, or other effects resulting from dissolved or particulate impurities in the coolant. A cover gas cleanup system shall be included to ensure purity of the cover gas and to recover any reaction products or contamination, radioactive and chemical.

Criterion 51: *Decay* heat *removal system*

Means shall be provided for the removal of *decay* heat from the reactor core *to an ultimate heat sink after* shutdown of the nuclear power plant *in operational states and in accident conditions*.

6.18. The *decay heat removal systems* for cooling of the reactor core shall be such as to ensure that

(a) The design limits for fuel, the reactor coolant boundary and structures important to safety are not exceeded in the shutdown state of the nuclear power plant,

(b) The cooling of the fuel is restored and maintained under accident conditions even if the integrity of the reactor coolant boundary is not maintained, and

(c) The function to transfer decay heat from items important to safety at the nuclear power plant to an ultimate heat sink shall be carried out with very high levels of reliability for all plant states.

6.19. The decay heat removal system shall be designed as follows:

(a) To provide diversity to the extent practicable and redundancy for reducing common cause failures, including external events.

(b) To prevent freezing of the sodium coolant to avoid blockage of coolant circulation, and

(c) To provide detection and mitigation measures against postulated decay heat fluid leaks.

6.19bis. In design extension conditions, means for decay heat transfer shall be provided, in addition to a decay heat removal system for anticipated operational occurrence and design-basis accidents, with the conditions listed below. Means shall be provided for the capability of core cooling under postulated plant conditions with core degradation.

(a) The cooling of the reactor core is possible even under extreme external hazards and their consequences, such as long-term loss of all AC power supplies,

(b) Passive mechanisms are used to the extent practicable, and

(c) Decay heat removal system has diversity to the extent practicable.

Omitted: Criterion 52: Emergency Cooling of the reactor core

[Included in Criterion 51]

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 radioactive material release 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. *The design basis for the containment shall consider pressure increase and thermal loads due to sodium fire and severe accident*.

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.

Criterion 56: Isolation of the containment

Each line that penetrates the containment at a nuclear power plant as part of the reactor coolant boundary *and the reactor cover gas 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 leaktightness 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 *the reactor cover gas boundary,* and lines that are connected directly to the containment atmosphere shall be fitted with at least two adequate containment isolation valves arranged in series[3], and shall be provided with suitable leak detection systems *for preventing the containment bypass of radioactive materials*. Containment isolation 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*. Each line that penetrates the containment and is neither part of the reactor coolant boundary nor *the reactor cover gas boundary and is not* 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.

6.*24*. Exceptions to the requirements for containment isolation, stated in para*graphs* 6.22, *6.23,* 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*graphs* 6.22, *6.23,* would reduce the reliability of a safety system that includes a penetration of the containment.

[3] 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. [From IAEA SSR 2/1 Footnote 11]

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. *If present,* 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 *it* at acceptably low levels. 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, *e.g. due to temperature and/or pressure increases,* of the containment in all plant states. The use of this provision shall not lead to *a significant* radioactive release.

[6.28B. omitted]

6.29. Design features to control fission products, *sodium*, hydrogen 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) to *prevent or mitigate sodium combustion, sodium-concrete reaction, and debris-concrete interaction and to control the concentration of hydrogen in the containment atmosphere* in accident conditions so as to prevent *thermal,* deflagration or detonation loads that could challenge the integrity of the containment.

[6.30. Omitted]

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 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 releases and amounts of radioactive material that could be released from the locations that are so intended in the design, and for post-accident analysis.

6.31bis. Instrumentation lines, which penetrate or are connected to the boundary of the reactor coolant systems, shall be designed so that sodium leaks and combustions caused by their failure are prevented and/or mitigated.

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.

(d) Shall consist of independent trains such that a single failure would not disable the protective action.

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 shall 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.

6.33bis. Unique trip parameters shall be identified for the representative event sequences of anticipated operational occurrence and design basis accident.

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 the 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 *relevant* 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, *and who are qualified with respect to the environment that the equipment may be subjected to during normal operation, anticipated operational occurrences and accident conditions*;

(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, *decay* 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 para*graphs* 6.39 *and 6.40* 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 withstand 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. In the 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, continuity, *and the environment that the emergency power supply is expected to be subject to during these events*.

6.44. The means to provide emergency power shall have *diversity to the extent practicable and contain redundancy for reducing common cause failure, including external events* (such as *by means of* water, steam or gas turbines, diesel engines or batteries). *The means* shall *also be reliable* and *be of* types 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. omitted]

[6.44B. omitted]

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[4] 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.[25]

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

[4] 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 IAEA SSR 2/1 Footnote 12]

component that they serve at the nuclear power plant *with due consideration of the principle of independence of levels of defence-in-depth*.

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 *and gas* systems

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

(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 gaseous radioactive releases 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. *Water systems used for firefighting shall not be located in the same compartment as sodium circuits and tanks*

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, *including sodium fire*, 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.

6.54bis. Adequate means of protecting the human body from sodium compounds generated by sodium fires shall be provided.

6.54ter. Compartments with sodium components shall be protected from the impacts induces by sodium fire to prevent the fire spread and from water ingress to prevent sodium-water chemical reactions, especially from water used in case of fire fighting in an adjacent compartment.

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: Sodium Heating Systems

Heating systems shall be provided for components as necessary to prevent loss of fundamental safety functions by sodium 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.

Criterion 76ter: Sodium Chemical Reaction Prevention and Mitigation

Due to chemical risk of sodium which burns in air and reacts with water, impact of such chemical reactions to items important to safety must be prevented. Water systems shall be avoided in compartment containing or likely to contain sodium, unless justified with the demonstration that risk of the sodium-water reactions are properly managed.

6.8 Other Power Conversion Systems

Criterion 77: *Power conversion systems, including potential* steam supply systems*,* feedwater system*s* and turbine generators

The design of the *power conversion systems, including potential* steam supply system*s*, feedwater system*s* and turbine generator*s*, 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 *and* 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 of sufficient capacity and shall be 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 *in normal operation and below acceptable limits in accident conditions*.

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 *in normal operation and below acceptable limits in accident conditions*.

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 liquid of radioactive release 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 *including internal and external events*.

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 *and the interruption of the transit*;

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

(g) *To prevent mis-loading*;

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

(i) 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 *and minor actinide bearing 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, *including during long-term loss of all AC power supplies;*

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

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

(d) To prevent the potential *of* damaging the fuel *by dropping* of heavy objects, such as spent fuel casks, cranes or other objects*, onto 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 *a significant* 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. For reactors using a water pool system for fuel storage, the design of the plant shall include the following:

(a) Means for monitoring and controlling the water temperature for operational states and for accident states 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 spend fuel pool;

(d) Means for monitoring and controlling the water chemistry for operational states *(e) Means for removal and inactivation of sodium adhered to the fuel during the transport from a sodium environment to a water pool, in order to prevent fuel damage and for keeping water quality of the water pool.*

(f) Means for providing adequate heat removal from the fuel and for monitoring its status in operational states and in accident conditions, including during long-term loss of all AC power supplies.

6.68bis. For reactors using a sodium tank system for fuel storage, the design shall include the following:

(a) Means for monitoring and controlling the sodium temperature for operational states and for accident states that are of relevance for the fuel storage tank;

(b) Means for monitoring and controlling the sodium level in the fuel storage tank and for detecting leakage for operational states and for accident conditions that are of relevance for the fuel storage tank;

(c)Means for monitoring and controlling the activity in sodium and in cover gas for operational states and means for monitoring the activity in sodium and in cover gas for accident conditions that are of relevance for the fuel storage tank;

(d) Means for monitoring and controlling the water chemistiry for operational states;

(e) Means for preventing the uncovering of fuel assemblies in the tank in the event of a leakage.

(f) Means for providing adequate heat removal from the fuel and for monitoring its status in operational states and in accident conditions, including during long-term loss of all AC power supplies.

(g) Means for preventing sodium freezing to avoid blockage of coolant circulation.

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, *including radioactive sodium coolant,* shall be comprehensively identified and exposures and radiation risks associated with them shall be kept as low as reasonably achievable [15], 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 *radiation* 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 *accident 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 actions 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, and 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] USDOE & GIF "A Technology Roadmap for Generation-IV Nuclear Energy Systems", GIF-002-00 (2002)

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

[3] GIF SFR System Steering Committee, 'System Research Plan' (2007)

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

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

[6] IAEA, "IAEA Safety Glossary, Terminology Used in Nuclear Safety and Radiation Protection, 2007 Edition" (2007)

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

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

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

[10] GIF, "GIF R&D Outlook for Generation IV Nuclear Energy Systems" (2009)

[11] GIF, "GIF 2007 Annual Report" (2008)

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

[13] 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).

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

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

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

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

[18] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna (1999).

INDICATION OF DIFFERENCES BETWEEN IAEA SSR-2/1 Rev.1 (2016) AND GIF SFR SDC Rev.1 (2017)

IAEA SSR 2/1 Rev.1 (2016)		GIF SFR SDC Rev.1 (2017)		Status*
Requirement #	paragraph #	Criterion #	paragraph #	**M/A/D/U**
3. MANAGEMENT OF SAFETY IN DESIGN				
1		1		U
	3.1		3.1	M
2		2		M
	3.2		3.2	M
	3.3		3.3	M
	3.4		3.4	M
3		3		U
	3.5		3.5	M
	3.6		3.6	U
4. PRINCIPAL TECHNICAL CRITERIA				
4		4		M
	4.1-4.2		4.1-4.2	U
5		5		M
	4.3-4.4		4.3-4.4	U
6		6		M
	4.5-4.6		4.5-4.6	U
	4.7		4.7	M
	4.8		4.8	U
7		7		M
	4.9-4.10		4.9-4.10	U
	4.11		4.11	M
	4.12-4.13		4.12-4.13	U
	4.13A		4.13A	U
8		8		U
			4.13bis	A
9		9		U
	4.14-4.16		4.14-4.16	U
10		10		U
	4.17-4.18		4.17-4.18	U
11		11		M
	4.19		4.19	U
12		12		M
	4.20		4.20	M
13		13		U
	5.1		5.1	M
	5.2		5.2	U
5. GENERAL PLANT DESIGN				
DESIGN BASIS				
14		14		U
	5.3		5.3	U
15		15		U
	5.4		5.4	U
16		16		U
	5.5		5.5	M
	5.6-5.8		5.6-5.8	U
	5.9-5.10		5.9-5.10	M
	5.11-5.15		5.11-5.15	U
17		17		U
	5.15A-5.15B		5.15A-5.15B	U
	5.16		5.16	M
	5.17		5.17	M
	[5.18 omit]		5.18	A
	5.19		5.19	M
	5.20		5.20	U
	5.21		5.21	M
	5.21A		5.21A	M
	[5.22 omit]		[5.22 omit]	U
18		18		M
	5.23		5.23	M
19		19		U
	5.24-5.25		5.24-5.25	U
	5.26		5.26	M
20		20		M
	5.27		5.27	M
	5.28		5.28	U
	5.29		5.29	M
	5.30		5.30	U
	5.31-5.32		5.31-5.32	M
21		21		U
	5.33		5.33	U
22		22		U
	5.34		5.34	M
	5.35-5.36		5.35-5.36	U
23		23		U
	5.37-5.38		5.37-5.38	U
24		24		U
25		25		U
	5.39-5.40		5.39-5.40	U
26		26		U
	5.41		5.41	U
27		27		U
	5.42-5.43		5.42-5.43	U
28		28		U
	5.44		5.44	M
DESIGN FOR SAFE OPERATION OVER THE LIFETIME OF THE PLANT				
29		29		U
	5.45-5.47		5.45-5.47	U
30		30		U
	5.48-5.50		5.48-5.50	U
31		31		M
	5.51		5.51	U
	5.52		5.52	M
HUMAN FACTORS				
32		32		U
	5.53-5.58		5.53-5.58	U
	5.59		5.59	M
	5.60-5.62		5.60-5.62	U
OTHER DESIGN CONSIDERATIONS				
33		33		M
	5.63		5.63	U
34		34		U
35		35		M
36		36		U
	5.64-5.65		5.64-5.65	U
37		37		M
	5.66-5.67		5.66-5.67	U
38		38		U
	5.68		5.68	M
39		39		U
40		40		U
	5.69-5.70		5.69-5.70	U
41		41		U
SAFETY ANALYSIS				
42		42		U
	5.71-5.72		5.71-5.72	U
	5.73		5.73	M
	5.74		5.74	U
	5.75-5.76		5.75-5.76	M
6. DESIGN OF SPECIFIC PLANT SYSTEMS				
OVERALL PLANT SYSTEM				
		42bis		A
REACTOR CORE AND ASSOCIATED FEATURES				
43		43		M
	6.1		6.1	M
	6.2-6.3		6.2-6.3	U
44		44		M
			6.3bis	A
			6.3ter	A
			6.3quater	A
45		45		U
	6.4		6.4	M
	6.5		6.5	M
	6.6		6.6	M
			6.6bis	A
46		46		M
	6.7-6.8		6.7-6.8	U
	6.9		6.9	M
	6.10-6.12		6.10-6.12	U
REACTOR COOLANT SYSTEMS				
47		47		U
	6.13		6.13	M
	6.14		6.14	M
			6.14bis	A
			6.14ter	A
	6.15		6.15	M
			6.15bis	A
			6.15ter	A
	6.16		6.16	M
			6.16bis	A
			6.16ter	A
			6.16quater	A
			6.16quinquies	A
48		48		M
49		49		M
50		50		M
	6.17		6.17	M
			6.17bis	A
51		51		M
	6.18		6.18	M
	6.19		6.19	M
			6.19bis	A
52		[52 omit]		D [incl. in #51]
53		53		U
	6.19A		6.19A	U
	6.19A		6.19B	U
CONTAINMENT STRUCTURE AND CONTAINMENT SYSTEM				
54		54		U
55		55		M
	6.20		6.20	M
	6.21		6.21	M
56		56		M
	6.22-6.24		6.22-6.24	M
57		57		U
	6.25-6.26		6.25-6.26	U
58		58		U
	6.27-6.28		6.27-6.28	M
	6.28A		6.28A	M
	6.28B		[6.28B omit]	D
	6.29		6.29	M
	[6.30 omit]		[6.30 omit]	U
59		59		U
	6.31		6.31	M
			6.31bis	A
INSTRUMENTATION AND CONTROL SYSTEMS				
60		60		U
61		61		U
	6.32		6.32	M
	6.33		6.33	U
			6.33bis	A
62		62		U
	6.34-6.36		6.34-6.36	U
63		63		U
	6.37		6.37	M
64		64		U
	6.38		6.38	U
65		65		U
	6.39-6.40		6.39-6.40	U
	6.40A		6.40A	U
66		66		M
	6.41		6.41	M
67		67		U
	6.42		6.42	U
EMERGENCY POWER SUPPLY				
68		68		U
	6.43-6.44		6.43-6.44	M
	6.44A-B		[6.44A-B omit]	D
	6.44C-D		6.44C-D	U
	6.45		6.45	U
	6.45A		6.45A	U
SUPPORTING SYSTEMS AND AUXILIARY SYSTEMS				
69		69		M
70		70		U
	6.46		6.46	U
71		71		U
	6.47		6.47	U
72		72		M
73		73		U
	6.48		6.48	M
	6.49		6.49	U
74		74		M
	6.50		6.50	M
	6.51-6.54		6.51-6.54	U
			6.54bis	A
			6.54ter	A
75		75		U
76		76		U
	6.55		6.55	U
		76bis		A
		76ter		A
OTHER POWER CONVERSION SYSTEMS				
77		77		M
	6.56-6.57		6.56-6.57	M
	6.58		6.58	U
TREATMENT OF RADIOACTIVE EFFLUENTS AND RADIOACTIVE WASTE				
78		78		M
	6.59-6.60		6.59-6.60	U
79		79		M
	6.61		6.61	U
	6.62		6.62	M
	6.63		6.63	U
FUEL HANDLING AND STORAGE SYSTEMS				
80		80		M
	6.64-6.65		6.64-6.65	U
	6.66-6.68		6.66-6.68	M
	6.68A		6.68A	M
			6.68bis	A
RADIATION PROTECTION				
81		81		U
	6.69		6.69	M
	6.70-6.72		6.70-6.72	U
	6.73		6.73	M
	6.74-6.76		6.74-6.76	U
82		82		M
	6.77-6.83		6.77-6.83	U
	6.84		6.84	M

*M: Modified	A: Added	D: Deleted	U: Unchanged

GLOSSARY

#accident conditions

Deviations from normal operation, which are less frequent and more severe than anticipated operational occurrences, and which include design basis accidents and design extension conditions.
[from the DEFINITIONS in the IAEA SSR 2/1]

#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.

An operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions.
[from IAEA Safety Glossary (2007 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]

#confinement function

Prevention or control of releases of radioactive material to the environment in operation or in accidents.
[from the IAEA Safety Glossary]

#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]

#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)]

#design basis accident

Accident causing 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]

#design extension conditions

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 could include severe accident conditions.
[from the DEFINITIONS in the IAEA SSR 2/1]

#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]

#fast reactor

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

#fuel storage in sodium

A sodium tank system (or EVST: Ex-vessel Storage Tank) and/or the reactor vessel (or IVS: In-Vessel Storage) is used for the temporary storage of new fuel before loading to the core and spent fuel from the core. The spent fuel must be stored in this way as the decay of radioactive isotopes cause continuous heat release.
[based on JAEA Monju home page]

#gas entrainment

Cover gas entrainment at the free surface of sodium coolant, which is caused by, for example, surface oscillation due to earthquakes or a standing wave (seiche). An SFR shall be designed to limit the amount of gas entrainment in order to prevent ‘void reactivity insertion’ and ‘decrease in heat removal rate’ due to the entrained gas.

#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 pipe

#guard vessel

Guard pipe is placed outside of the coolant pipe where sodium coolant flows.
Guard vessel is placed outside the reactor vessel containing the sodium coolant.
Both are constructed to maintain sodium coolant level for reactor cooling in case of sodium 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.
[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;
- Those features that are provided to mitigate the consequences of malfunction or failure of structures, systems and components.

[from IAEA Safety Glossary (2007 Edition).]

#leak propagation

Successive tube failures of the steam generator in case of a water-steam leak accident.

#leak tight configuration

Structures to ensure liquid-/gas-tightness of the reactor coolant boundary and the cover gas boundary.

#mis-loading

Loading a fuel assembly into the wrong position in a reactor core. The mis-loading will cause unexpected values of the effective multiplication factors, the neutron flux and power distributions, the coolant velocity, and the temperature distribution.

#normal operation

Operation within specified operational limits and conditions.
[from IAEA Safety Glossary (2007 Edition).]

#operating personnel

Individual workers engaged in the operation of an authorized facility.
[from IAEA Safety Glossary (2007 Edition).]

#operational states

States defined under normal operation and anticipated operational occurrences.
[from IAEA Safety Glossary (2007 Edition).]

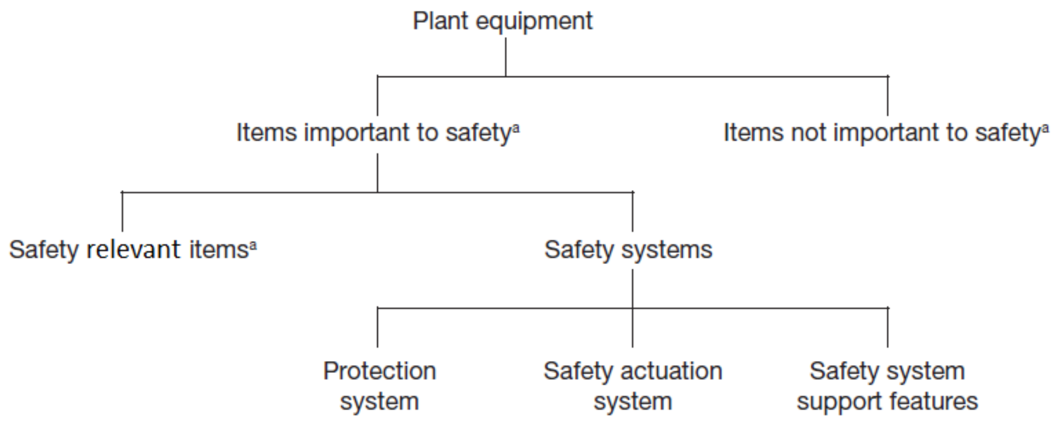
#passive safety feature

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 (2007 Edition) with replacing “Safety related items” by “Safety relevant items”.]

#plant states (considered in design)

Operational states		Accident conditions	
Normal operation	Anticipated operational occurrences	Design basis accidents	Design extension conditions

[from the DEFINITIONS in the IAEA SSR 2/1]

#practically eliminated

The possibility of certain conditions occurring is considered to have been practically eliminated if it is physically impossible for the conditions to occur or if the conditions can be considered with a high level of confidence to be extremely unlikely to arise.
[from FOOTNOTES in the IAEA SSR 2/1]

#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]

#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 (2007 Edition).]

#reactor coolant boundary (or primary coolant boundary)

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

#reactor coolant system (or 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.

#reactor coolant systems

All systems using liquid metal (e.g. sodium, NaK) as coolant; e.g. to remove heat from the reactor core and transfer that heat to the ultimate heat sink. The reactor coolant systems includes: the reactor coolant system, the secondary coolant system, the decay heat removal system, and associated sodium systems (e.g. the cleanup facilities).

#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]

#safety actuation system

The collection of equipment required to accomplish the necessary safety actions when initiated by the protection system.
[from IAEA Safety Glossary (2007 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]

#safety group

The assembly of equipment designated to perform all actions required for a particular postulated 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 (2007 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 (2007 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 (2007 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 (2007 Edition).]

#safety system settings

The 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]

#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 (2007 Edition).]

#secondary coolant system (or intermediate coolant system)

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

#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]

#sodium-concrete reaction

A chemical reaction due to the direct contact between sodium and concrete, which generates hydrogen gas that may cause overpressure in a containment.

#sodium fire

Fire caused by sodium combustion. Sodium spontaneously catches fire when exposed to air at the operating temperature of an SFR.

#sodium water reaction

A chemical reaction caused by the direct contact between sodium and water/steam.

#steam generator

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

APPENDIX

to

the Safety Design Criteria

for Generation-IV Sodium-Cooled Fast Reactors

List of Contents

(A) Definitions of Boundaries of SFR systems

This section is related to the following criteria:

Criterion 47: Design of reactor coolant systems

Criterion 56: Isolation of the containment

The primary boundary

The primary boundary consists of the reactor coolant boundary and the reactor cover gas boundary. The reactor coolant boundary is the boundary that is in contact with the primary sodium. The reactor cover gas boundary is the boundary that is in contact with the primary cover gas. Lines connected to the boundary shall be equipped with isolation valves. (See Figure A-1)

The containment boundary

The containment boundary is the boundary that separates the systems that contain radioactive material from the non-radioactive portions of the plant. Its purpose of this boundary is to contain radioactive materials in case of an accidental release. Lines of the secondary coolant system and of the secondary side of decay heat removal systems penetrating the containment are neither part of the reactor coolant boundary, nor connected directly to the containment atmosphere. Therefore at least one isolation valve shall be installed in each line (according to paragraph 6.23 in criterion 56). Exceptions may be permissible in cases where application of the methods of containment isolation would reduce the reliability of a safety system when the following conditions are met (See Figure A-2):

- The pressure of the secondary side of the boundary is higher than that of the primary side in the operational states, except during maintenance of the containment and the secondary systems.
- The reactor coolant systems are designed so that an adequate inspection of the boundary between the primary and the secondary systems is possible in order to detect a potential boundary failure.
- The reactor coolant systems are designed so that lines of the secondary systems penetrating the containment do not become unacceptable radioactive materials release paths to the environment.

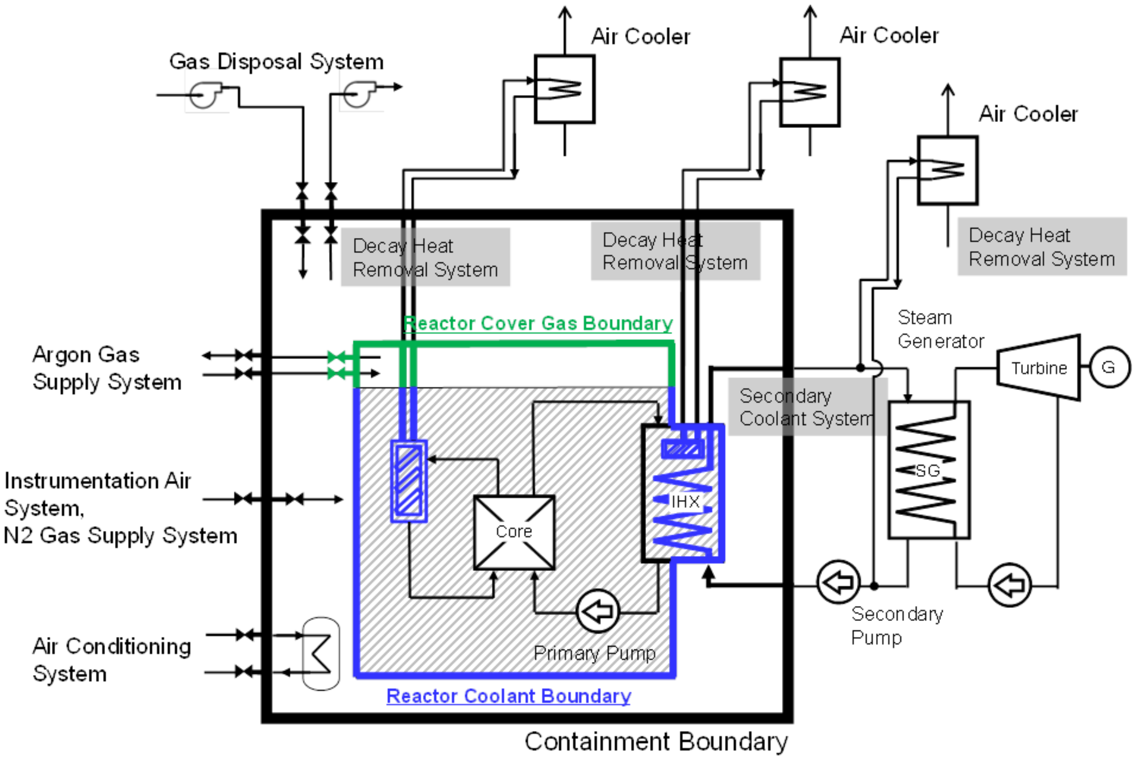


Figure A-1 Concept of the reactor coolant boundary

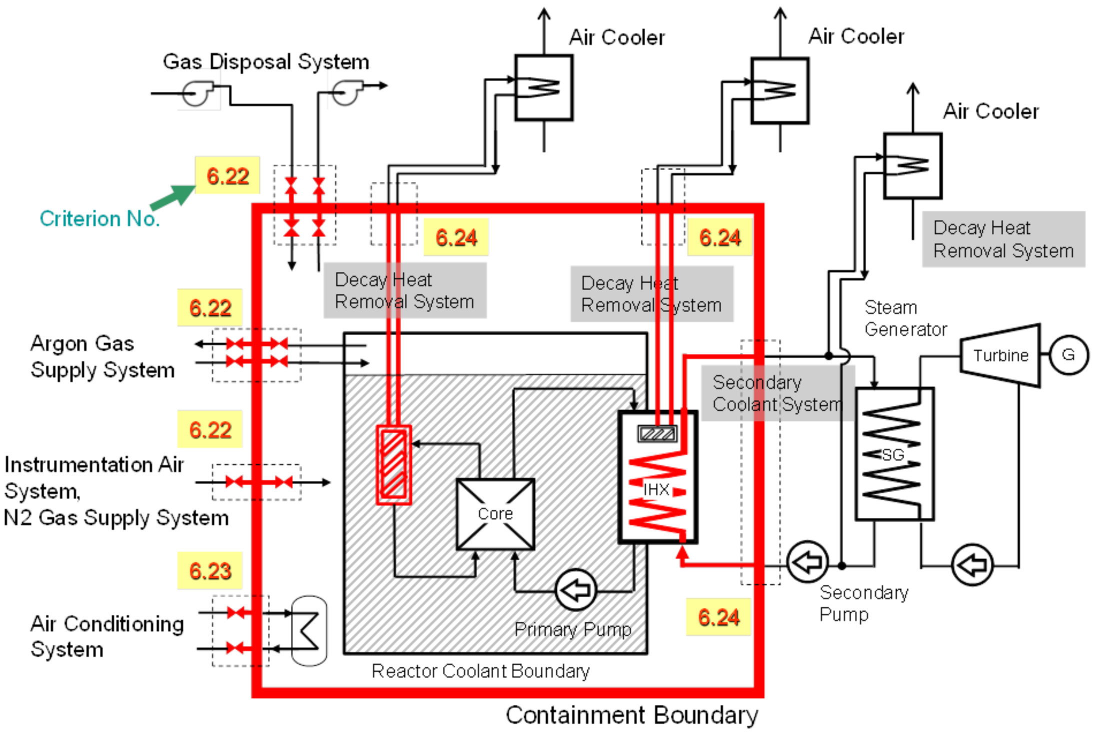


Figure A-2 Concept of the containment boundary

(B) Guide to Utilisation of Passive/Inherent Features

Based on international experience of SFR design and operation, active safety systems, with redundancy and diversity for reactor shutdown and decay heat removal, have been demonstrated to be reliable.

For Generation IV SFRs further enhancement of safety systems are required in order to handle design extension conditions. However, active safety systems already have redundancy and diversity to the extent practicable. Measures with different operation principles are useful to further reduce common cause failure.

Passive or inherent features can provide diversity to active safety systems in terms of the operation principle and dependence upon power source, support system, instrumentation and control systems. Passive or inherent reactor shutdown and passive decay heat removal have been investigated and various design measures are under development worldwide.

Passive or inherent features will provide means of self-termination (self-shutdown and self-cooling) even in cases of failure of active safety systems.

Since the levels of Defence-in-Depth shall be independent as far as practicable (Criterion 7), measures for design basis accidents and design extension conditions shall be somewhat different. Passive or inherent features are suitable for design extension conditions, because they can work as for a complement to active safety systems and become effective mechanisms when considering a wide range of the plant conditions, which exceed design basis accidents. However, utilisation of passive or inherent features should be flexible.

Active measures and accident management measures can also be used for design extension conditions. On the other hand, passive or inherent features can be used for design basis accidents. Although passive or inherent features seem fail-safe, clarification of the range and effect of phenomenological uncertainty and sound demonstration shall be required in order to make them reliable safety features.

(C) Approach to Extreme External Events

This section is related to the following criterion.

Criterion 17: Internal and external hazards

It is required to assure the integrity of the structures, systems and components necessary to prevent large or early radioactive releases into the environment, against extreme external events. This means that a set of vital structures, systems and components shall be identified and designed to have "sufficient margin" or "protection measures" against external design extension conditions, such as beyond design basis earthquakes, external missiles etc. If this requirement is satisfied, the risk of a cliff-edge effect consisting of large or early radioactive releases in the environment is prevented. "Sufficient margin" or "protection measures" against external design extension conditions are different kind of requirements from "Prevention" and "Mitigation". Measures for "Prevention" and "Mitigation" for external design extension conditions are basically the same as those for the internal events, if "sufficient margin" or "protection measures" are properly provided.

External events are for example earthquakes, which give simultaneous stress to the whole plant and potentially lead to common cause failures on many kinds of structures, systems and components, or strong winds or volcanic ash fall, which influence the plant environment or the auxiliary systems. Long term loss of external power supply is anticipated in conditions beyond the design basis.

Basically, it is required to ensure a sufficient seismic margin for the structures, systems and components, since it can affect all of these structures, systems and components. This is an example of the expression "ensure design margin". Design measures for each structure, system and component are required. For instance, for the reactor structure, in addition to preventing the reactor vessel failure due to buckling, prevention of excessive fuel assembly jump-up in terms of their integrity assurance, and prevention of excessive relative offset between core and control rods in terms of prohibition of excessive reactivity insertion, are compulsory.

If the plant is designed so that a design basis tsunami does not influence the performance of structures, systems and components, water proof design at openings of the reactor building is considered for the protection of structures, systems and components against more severe tsunamis postulated as a design extension conditions . This is an example of "protection measures". [Cf. Criterion 17: Internal and external hazards]

In Generation IV SDC, built-in design measures are required to be incorporated for design extension conditions. However, application of possible accident management (AM) measures shall be considered in the plant design in advance, as a supplemental measure. The TEPCO's Fukushima Dai-ichi Nuclear

Power Plants accident showed the importance of AM. For extreme external events, which have a large uncertainty and for which it is difficult to identify representative event scenarios, provision of mobile devices, such as power-supply vehicles for accident management measures, should be considered. In order to effectively use such accident management measures, structures, systems and components, which can withstand severe plant conditions, shall be identified and properly protected.