SDC-TF/2019/01

August 30, 2019

Safety Design Guidelines

on

Safety Approach and Design Conditions

for

Generation IV Sodium-cooled Fast Reactor Systems

(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 favouring 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/2016/01, issued Mar. 4, 2016.**
Revision 1: **SDC-TF/2019/01, issued Aug. 30, 2019.**

Table of Contents

[This page is intentionally left blank.]

1. INTRODUCTION

1.1. Background and Objectives

Safety Design Criteria (SDC) for Generation-IV (Gen-IV) Sodium-cooled Fast Reactor (SFR) systems [1] have been developed by an SDC Task Force (TF), under the auspices of the GIF Policy Group (PG). Following approval by the PG, the SDC Report was distributed to international organisations and national regulatory bodies for review.

The following needs were identified by the SDC TF members:

- Development of detailed guidelines to support practical applications of SDC.
- Expansion of selected topics, specifically on
  - ✓ practical elimination (PE) of some accidents,
  - ✓ design basis of specific components (e.g. containments).
- Clarification of technical issues such as
  - ✓ prevention and mitigation measures against sodium fire and sodium-water reaction accidents,
  - ✓ implications of the fact that the reactor core is not in its most reactive configuration.

In response, the PG and the GIF Senior Industrial Advisory Panel recommended the TF to:

- develop guidelines for application of the SFR SDC, and
- pursue quantification of key criteria to demonstrate the safety advantages of Gen-IV SFRs over current LWR designs.

The objective of this report is to provide recommendations and guidance on how to comply with the GIF SFR Safety Design Criteria. It presents examples for the measures stated in criteria as the best practices to help the designers achieve high levels of safety. The guidelines are placed below the SDC in the hierarchy of safety standards as depicted in Figure 1 below. Initially, the guidelines will focus on specific safety concerns, such as reactivity characteristics of SFRs and heat removal issues. In the future, the guidelines will be extended by taking into account additional issues, such as fuel handling and storage. These guidelines deal only with safety issues, security considerations are dealt by the Proliferation Resistance and Physical Protection Working Group (PRPPWG) of GIF or by national regulators.

The guidelines, except Chapter 4 “Guidelines for application of safety design criteria”, provide recommendations and guidance on how to comply with the SFR SDC, which are generally applicable for Generation-IV SFR systems. Chapter 4 covers specific issues to be considered in the design of structures, systems and components (SSCs) with examples of design provisions.

The TF expects that these issues and examples will be appropriately considered when applied to specific features of individual designs. Recommendations in this document are expressed as 'should' statements. It is recommended to adopt the stated measures or equivalent alternative measures.

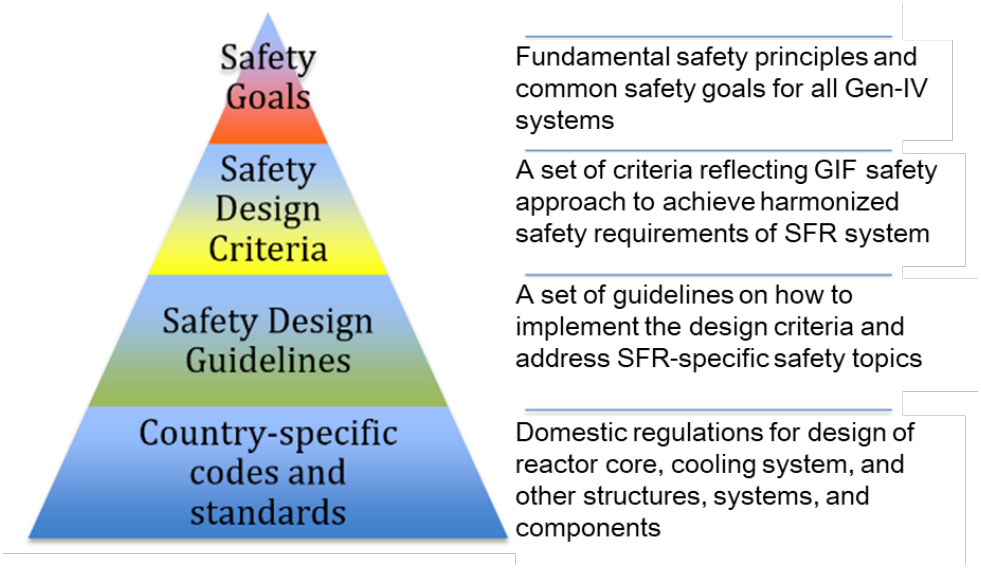


Figure 1 Hierarchy of safety standards and position of Safety Design Criteria (SDC) & Safety Design Guideline (SDG)

[Note: *'Country-specific code and standards'* are not provided by the GIF]

1.2. Scope of the Safety Design Guidelines

The primary focus of this report is to provide Safety Design Guidelines (SDG) for Gen-IV SFR systems as a technical supplement to the SDC report. The enhancement of Gen-IV SFR safety is mainly focused on improving each level of Defence-in-Depth, including the 4th level, with particular attention on the robustness of safety demonstrations (practical elimination demonstrations, independence of lines of defence). The definition of Defence-in-Depth and plant state follows the definition in IAEA SSR 2/1 (2016), which consults INSAG-12 for the Defence-in-Depth principle: i.e. the plant states shown in Figure 2 are operational states include normal operation and anticipated operational occurrences; accident conditions include design basis accidents and design extension conditions.

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

Figure 2 Defence-in-Depth level and Plant States (including Severe Accident) based on IAEA INSAG-12 & SSR-2/1 (Rev.1, 2016)

Like Generation-III Light Water Reactors (LWRs), Gen-IV SFR safety is primarily based on the use of multiple redundant engineered safety features to lower the probability of accidents and to limit the consequences of anticipated operational occurrences and design basis accidents. These safety features include independent and diverse scram systems, multiple coolant pumps and heat transport loops, decay heat removal systems, and multiple barriers against release of radioactive materials. In addition to these features, passive/inherent features for cooling and shutdown / power reduction should also play a significant role in the safety performance of Gen-IV SFRs by improving the diversity of safety systems and reducing reliance on electrical power and external water sources during design extension conditions.

For very low probability Design Extension Conditions (DECs), the following two major groups of accidents merit special attention due to challenges in designing an SFR to successfully respond to these accidents without severe consequences:

1) Failure to reduce power or shut down the reactor following an off-normal initiating event, and
2) inability to remove heat from the core.

To address the potential consequences of such accidents, this report focuses on providing examples of design approaches for “prevention and mitigation of severe accidents” and for “complete loss-of-decay heat removal capability as a situation that needs to be practically eliminated”. The SDG also include:

- Clarification of key points for the design of structures, systems and components (SSCs)
- Identification of sets of design conditions, and
- Listings with examples of “general design choices for SSCs” for Gen-IV SFR systems.

The report covers the following sections:

- Chapter 1 covers “Background and Objective”, as well as “Scope of the SDG”.
- Chapter 2, entitled “Main Characteristics of Gen-IV SFR Systems” presents the systems and fundamental characteristics of four current Gen-IV SFR designs.
- Chapter 3, “General Approach”, explains the general definition of “Plant conditions”. This chapter also contains a “General Approach to Design Extension Conditions”, describing design approaches for prevention and mitigation of accidents, postulated events and conditions, as well as application of SFR safety features. Design considerations for design extension conditions related to reactivity and decay heat removal issues are also described, as are the “Practical Elimination (PE) of accident situations”, comprising identification of the situation, design considerations, and principles of demonstration.
- Chapter 4, “Guidelines for Application of SDC”, describes specific approaches for prevention and mitigation of severe accidents, related to reactivity and decay heat removal issues, with design options, postulated events and design limits, as well as testability and demonstrations.
- Chapter 5 summarises SFR reactor core reactivity characteristics in relation to safety.

2. MAIN CHARACTERISTICS OF GEN-IV SFR SYSTEMS

A Sodium-cooled Fast Reactor (SFR) uses liquid sodium as the reactor coolant, as it can maintain fast neutron spectrum and allows high power density with low coolant volume fraction, at low pressure. While the oxygen-free environment prevents corrosion, sodium reacts chemically with air and water and requires a sealed coolant system. The current plant size options range from small modular reactors, 50 to 300 MWe, to larger plants up to 1,500 MWe. The coolant outlet temperature of primary system is 500 - 550°C, which allows the use of materials developed and proven in prior fast reactor programmes. An SFR closed fuel cycle enables generation of fissile fuel and facilitates the management of minor actinides. Important safety features of SFR systems include core reactivity characteristics such as shorter neutron lifetime, a large margin to coolant boiling during normal operating conditions, a primary system that operates at near atmospheric pressure, and an intermediate coolant loop between the radioactive sodium in the primary circuit and the power conversion system. Water/steam, nitrogen and supercritical carbon-dioxide are among the working fluids considered for the power conversion system to achieve high efficiency, safety and reliability.

Much of the basic technology of the SFR has been established in former fast reactor programmes, and is confirmed by the Phénix end-of-life tests in France, the initial start-up test of Monju in Japan, the lifetime extension of BN-600 and the start-up of BN-800 in Russia, as well as the start-up of the China Experimental Fast Reactor.

A high level of safety can be achieved for an SFR using a combination of engineered active, passive and inherent features, which may also accommodate transients and bounding events with significant safety margins.

An SFR can be arranged in a pool layout or in a compact loop layout. The following three options are considered in the GIF SFR System Research Plan, with examples provided in Figures 3-1 to 3-4 [2]:

- A large size (600 to 1,500 MWe) loop-type reactor with mixed uranium-plutonium oxide fuel and potentially minor actinides, supported by a fuel cycle based on advanced aqueous processing at a central location serving a number of reactors, as shown in Figure 2-1.
- An intermediate-to-large size (300 to 1,500 MWe) pool-type reactor with oxide or metal fuel, as shown in Figures 2-2 and 2-3.

- A small size (50 to 150 MWe) modular pool-type reactor with metal alloy fuel, supported by a fuel cycle based on pyrometallurgical processing in facilities integrated with the reactor, as shown in Figure 2-4.

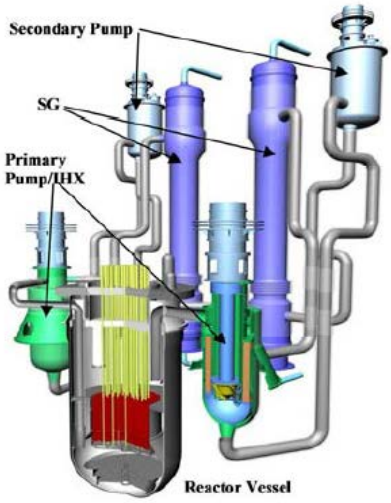


Figure 3-1 JSFR (Loop-configuration)

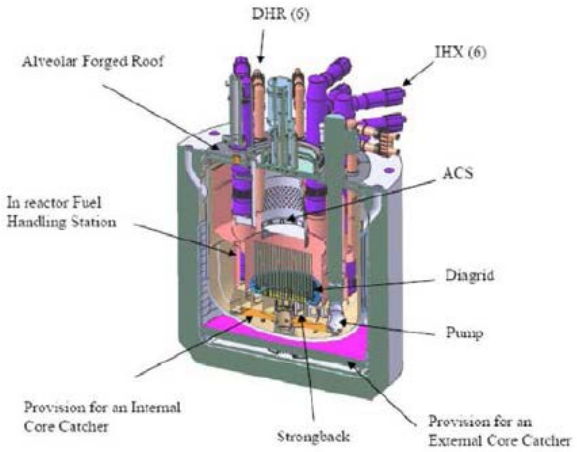


Figure 3-2 ESFR(Pool-configuration)

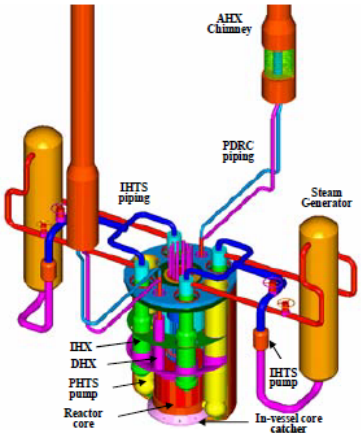


Figure 3-3 KALIMER (Pool-configuration)

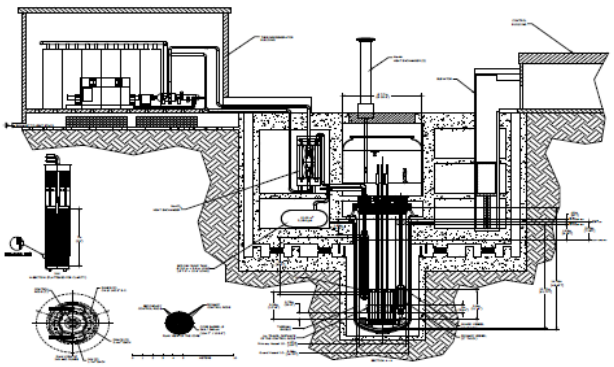


Figure 3-4 SMFR(Small modular-configuration)

3. GENERAL APPROACH

3.1. Design Basis and Residual Risk

In the design of a nuclear power plant, compliance with the fundamental safety objectives[1] [1] should be demonstrated for all initiating events. Initiating events are identified and grouped into a limited number of plant states, primarily on the basis of their frequency of occurrence. Initiating events in the plant states [3], described below, provide the design basis[2] for the safety design of nuclear power plants, while the residual risk is not included in the plant states. Situations to be practically eliminated are considered to be part of the residual risk. An illustration of design basis and residual risk is given in Figure 4.

3.1.1. Plant States for Design Basis

Normal operation – The plant is operating as intended, with all plant parameters (temperature, pressure, etc.) within the design ranges for normal operation, and is considered for the development of design measures for Defence-in-Depth Level 1 [1].

Anticipated Operational Occurrence (AOO) – Includes events, which disrupt plant conditions from their normal state and are expected to occur during the lifetime of a plant, and which are typically caused by a failure or an inadvertent operation of a single SSC, accommodated by the safety systems. When one selects initiating events in each plant state, safety classification of SSCs are taken into account in the relation of its frequency of failure. A failure of an active system manufactured to normal industrial standards would be treated as an AOO. The expected frequency of occurrence of AOOs should be estimated according to component reliability, but it should not be lower than approximately 1×10^{-2} per reactor year because such events may occur during the lifetime of the plant. Plant conditions, expected as a result of an AOO, are considered for the development of design measures for Defence-in-Depth Level 2 [1]. Any significant consequences of an AOO should be prevented (no clad or fuel damage and no significant release of radioactive materials).

Design Basis Accident (DBA) – Includes events, which are typically caused by the failure of a single SSC with consequences of greater severity than those considered for AOOs and which

---

[1] *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. (Criterion 5 in SDC) The dose limits are defined by each national regulatory authority.*

[2] *The range of conditions and events taken explicitly into account in the design of a facility, according to established criteria, such that the facility can withstand them without exceeding authorized limits by the planned operation of safety systems. The authorized limits are defined by each national regulatory authority.*

are not expected to occur during the lifetime of a plant[3]. The expected frequency of occurrence of DBAs is less than 1 x 10^{-2} per reactor year, and as low as approximately 1 x 10^{-5} per reactor year or less, consistent with global probabilistic objectives assigned to core damage frequencies. Plant conditions, expected as a result of a DBA, are considered for the development of safety systems for Defence-in-Depth Level 3 [1]. Reactor and plant systems should respond to prevent any significant core damage or radioactive release exceeding acceptable limits. Although a limited number of fuel pin failures may be acceptable, these should be prevented as far as reasonably practical.

Design Extension Condition (DEC) – Accident conditions that are typically of lower probability than design basis accidents and involve the failure of more than one SSC important to safety or part of a safety system. Design extension conditions should include accident sequences that could lead to severe accident conditions and are considered for design measures to prevent core damage and mitigate core damage as shown in Figure 4. Plant conditions, expected as a result of such events, are considered for the development of design measures for Defence-in-Depth Level 4 [1].

3.1.2. Situations to be practically eliminated situations and Residual Risk

Situations to be practically eliminated situations – Specific situations, whose consequences can lead to early or large radioactive release and which cannot be managed by the design at acceptable conditions, have to be practically eliminated by implemented design measures[4][4]. These situations have to be demonstrated either as physically impossible by design, or as extremely unlikely to arise with a high level of confidence. Situations to be practically eliminated situations are part of the residual risk.

Residual Risk – Accidents with sufficiently low frequency due to the implementation of defence in depth principle and not considered in the design basis.

---

[3] DBAs retained in the safety demonstration are defined as "envelopes" of families of abnormal operating conditions that gather several initiating events of the same type.

[4] WENRA's definition is as follow – "Event sequences that would lead to an early radioactive release or a large radioactive release are required to be "practically eliminated. The possibility of certain conditions arising may be considered to have been "practically eliminated" if it would be physically impossible for the conditions to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise"

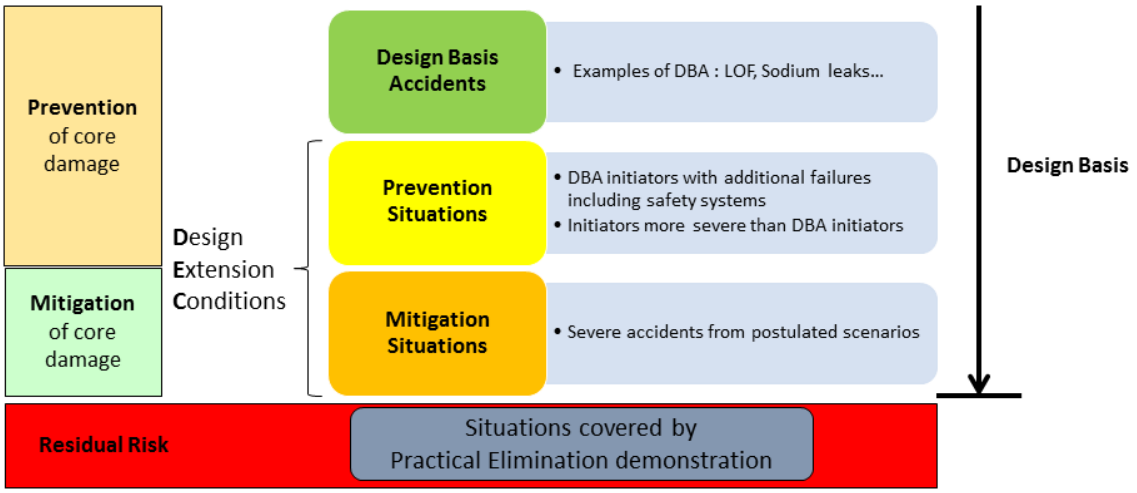


Figure 4 Illustration of design basis and residual risk

3.2. General Approach to Normal Operation, AOOs and DBAs

In the new SFR designs, strong emphasis should be given to the prevention, detection and control of accident sequences [5]. An SFR must be designed to allow for stable normal operation, which requires being able to control reactor temperatures, within a small range set by the designers, possibly also by varying the reactor coolant flow using the coolant pumps, and by keeping the reactor power in balance with the demand for power from the electric grid. Reactor power is regulated using control rods, which are moved in response to the changing demand for power production, such that the steam flow rate and temperature at the turbine can be maintained.

AOOs are expected to be managed to return to a normal operation condition by the plant control provision so that reactor shutdown and decay heat removal systems are not required to operate. While the reactor shutdown and decay heat removal systems should respond to AOOs if needed[5], DBAs are managed by using safety systems to shut down the reactor and remove decay heat. These rapidly responding safety systems can be actuated by using a signal from the plant (i.e. the plant protection system) that detects an off-normal condition of sufficient magnitude (set by

[5] *In general, AOO and DBA for the safety analysis are selected as envelops and representatives of similar kind of events. Therefore most cases of AOOs require activation of safety systems such as automatic reactor shutdown and decay heat removal. Actually AOO domain includes minor troubles, which doesn't require the automatic reactor shutdown. For such cases, measures should be provided to detect and control deviations from normal operation in order to prevent AOOs from escalating to accident conditions. Plant equipment such as normal reactor control system and balance-of-plant is used for that purpose.*

the plant designer). The goal, in cases of AOOs or DBAs, is to ensure the reactor core and system temperatures remain within applicable design limits.

3.3. General Approach to Design Extension Conditions

This document is focused on events that begin with a reactor under normal power operation, as the initial plant condition, excluding accident conditions associated with fuel handling and storage facilities. The following section describes the general approach for the consideration of DECs in the design and involves identifying postulated events to be included in DECs.

3.3.1. Application to Design

Design provisions for DECs are assigned within the fourth level of the Defence-In-Depth (DiD) as shown in Figure 5. This level includes measures for “prevention of core damage” in “prevention situations” and for “mitigation of core damage” in “mitigation situations”.

The goal of design measures in “prevention of core damage” of DiD Level 4 is to provide lines of defence to prevent conditions leading to significant core damage. Design features for “prevention of core damage” in DECs deal with accident sequences that are typically caused by failure of one or more systems related to safety, such as the reactor coolant pumps, followed by failure of other safety systems needed to prevent excessive power and/or temperatures resulting from the off normal conditions of the plant. “Prevention situations” of DECs also include initiating events, more severe than those in DBAs.

Design measures in “mitigation situations” provide design features for mitigation of consequences of postulated accidents where significant core damage occurs, with the objective of maintaining the containment function to limit radioactive release within applicable design limits and practically eliminating a large or early release which would lead to unacceptable off-site consequences.

As described in the following section, design provisions to achieve In-Vessel Retention (IVR) is crucial for addressing “mitigation situations”, since the reactor vessel (RV) can, in this case, serve as the boundary for retention and cooling of core material, limiting any threat to the containment.

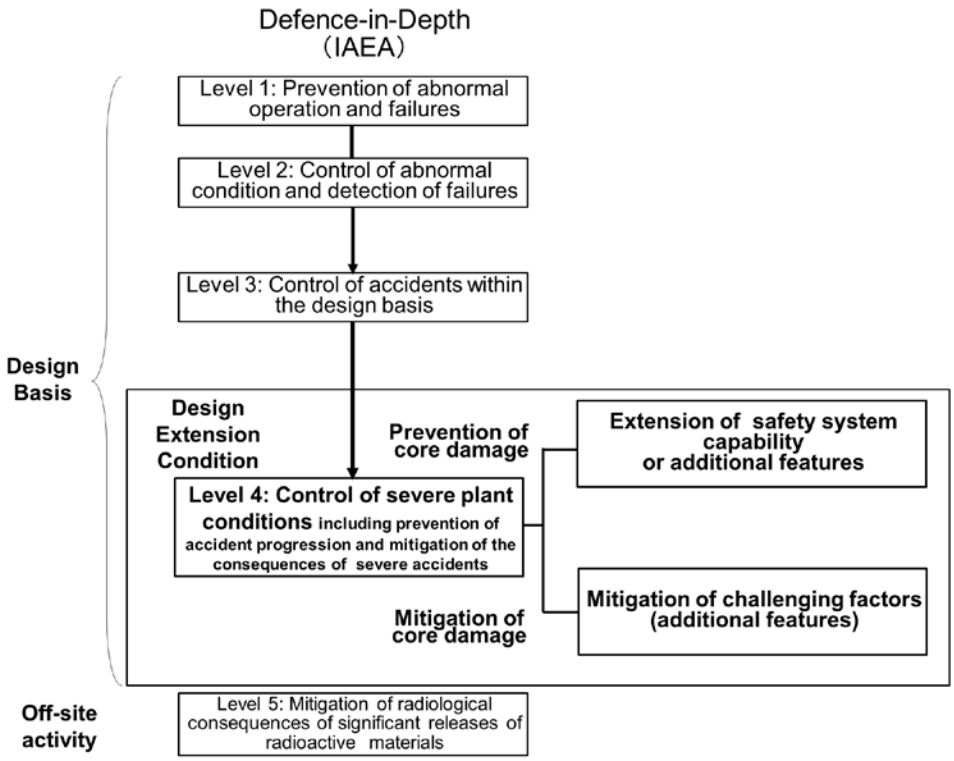


Figure 5 Prevention/mitigation of severe accidents

3.3.2. Initiating Events for DEC

All initiating events for DECs should be considered as long as they are physically realisable and credible, based on SFR design characteristics, as well as deterministic and probabilistic safety assessments (PSA). In particular, Anticipated Transients Without Scram (ATWS), in which failure of an active reactor shutdown system is assumed, are typically considered as DECs. This includes loss of primary flow without scram, loss of main heat sink without scram, and withdrawal of the control rods resulting in a transient overpower without scram. Degradation or loss of safety systems for decay heat removal (DHR) that are not practically eliminated and reactor coolant level reductions are also considered as DECs. Design considerations related to these events are described in section 3.4. The SFR design determines which of these events are to be defined as DECs, where the frequency of occurrence and severity of the consequences are evaluated to ensure that these events are appropriate DECs.

3.3.3. Exploiting SFR Characteristics to Enhance Safety

Inherent and Passive Safety

Inherent reactivity feedback effects are obtained by using intrinsic SFR features to reduce power as the core temperature rises in accident conditions. The large temperature margin to sodium boiling (e.g. from maximum coolant channel temperature in normal operation to about 900°C until boiling) of the reactor coolant provides sufficient room to use reactivity feedback due to thermal expansion of core components, as well as neutron leakage effects due to the change in coolant density. When the change in coolant density may contribute positively to the overall reactivity, it is important that the net reactivity (with contributions from all feedback effects) is negative to foster the potential for inherently safe behaviour in case of a ATWS.

Passive shutdown systems, such as the Self-Actuated Shutdown System (SASS) [6] are also applicable. In SASS, a Curie-point magnetic alloy is utilized for automatic de-latching of control rods under high coolant temperature accident conditions, higher than for normal operating conditions, but still below the coolant boiling point. A Hydraulically Suspended Rod (HSR) [7] system (also called “flow-levitated absorbers”), where the control rods are automatically dropped into the core when the hydraulic force is reduced under accident flow reduction conditions, could also be used. In fast reactors, due to the sensitivity of the core reactivity to neutron leakage, it is also possible to consider using concepts like the Gas-Expansion Module (GEM) [8], where a decrease in core inlet pressure is exploited to increase neutron leakage under a flow reduction condition.

These inherent and passive safety features should contribute to improve the diversity of safety systems and to reduce reliance on electrical power and external water sources.

Decay Heat Removal (DHR)

Since an SFR is operated at nearly atmospheric pressure and at temperatures far below the coolant boiling point, coolant leakage or a pipe break does not lead to the same type of loss-of-coolant accident as postulated in an LWR, which has the potential for depressurisation, coolant boiling and loss of cooling capability. The requirements for core cooling of an SFR comprise keeping the sodium coolant level above the reactor core and the circulation of the liquid coolant to an appropriate heat sink for decay heat removal. As long as these two requirements are satisfied, significant core damage can be prevented. Depending on the plant states, various measures such as the normal heat transport system, a separate sodium-to-air heat exchanger, or any other system that would allow cooling of the sodium can be provided. Natural

circulation of a single phase sodium coolant can be effectively utilised if an adequate difference in height is available between the core and the heat exchanger, due to the fact that sodium has a relatively large density variation with temperature. Such passive Decay Heat Removal Systems (DHRSs) can be placed in different locations, e.g. in the reactor vessel (RV) or in the primary-/secondary-coolant circuits. Alternative emergency cooling can be made available via steam generators and guard vessels (GVs) for enhancing diversity.

In-Vessel Retention (IVR)

For an SFR, in-vessel retention is a safety design strategy aimed at ensuring long-term retention of core materials inside the RV for any accident situation, including those resulting in degradation or loss of core integrity, by providing coolability of the core materials under sub-critical conditions. This is typically accomplished by providing the means to keep the core submerged under the sodium coolant and the decay heat removal paths available. Such an approach can be a key design measure to address “mitigation situations” for DECs.

3.4. Design Considerations for Design Extension Conditions

3.4.1. Anticipated Transient Without Scram (ATWS)

Postulated ATWS events cause an imbalance between generated power (heat) in the reactor core and its removal from the system, either by the normal path through the power production part of the plant, or by specific heat removal systems. If adequate heat removal is not provided, substantial core degradation will occur, which may lead to severe consequences, such as large energy releases. Reliable means of maintaining the balance between heat generation and heat removal must be provided to avoid such consequences. This can be accomplished by ensuring alternate means of shutdown, including the use of inherent and/or passive reactor shutdown, as long as sufficient heat removal capability is also provided. Provisions for retention and cooling of degraded core materials are necessary to mitigate the consequences of a core damage.

Provisions for ATWS can be summarised as follows.

- “Prevention of core damage”

  Means for maintaining an acceptable balance between reactor power and heat removal capabilities should be provided to avoid core damage, given an assumed failure of the active reactor shutdown function in AOOs. These capabilities should include inherent and/or passive means. In order to terminate the accident, means for reactor shutdown should be provided.

Related Criteria in the SDC Report

Criterion 20: Design extension conditions

Criterion 46: Reactor shutdown[6].

- "Mitigation of core damage"

  Provisions for prevention of a large energy release that could threaten the integrity of the containment and provisions for long-term cooling of a degraded core to avoid reactor coolant boundary failure, should be made available for achieving IVR against unprotected transients[7] with core damage.

  Related Criteria in the SDC Report

  Criterion 20: Design extension conditions

  Criterion 44: Structural capability of the reactor core[8]

  Criterion 45: Control of the reactor core[9]

  Criterion 47: Design of reactor coolant systems[10]

  Criterion 51: Decay heat removal system[11]

3.4.2. Loss of Safety Systems for Decay Heat Removal

In a situation of a failed DHRS after the reactor has been shut down and the heat generation has dropped to only a few percent of the nominal power shortly, the temperature of the reactor

---

[6] *Criterion 46: Reactor shutdown*

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

[7] *"unprotected transients" means accident sequences with failure of active reactor shutdown system, which include ATWS.*

[8] *SDC Criterion 44: Structural capability of the reactor core*

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.

[9] *SDC Criterion 45: Control 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 favorable neutronic, thermal, and physical characteristics, considering all reactivity feedbacks, including sodium void worth, to mitigate the consequences of such design extension conditions.

[10] *SDC Criterion 47: Design of reactor coolant systems*

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 primary coolant system in case of anticipated transients without scram.

[11] *SDC Criterion 51: Decay heat removal system*

6.19bis. Means shall be provided for the capability of core cooling under postulated plant conditions with core degradation.

coolant system, including the core, coolant and reactor coolant boundary, increases. The rate at which the temperature increases depends on the overall heat capacity of the system, and it may take a long time before reaching temperatures that would threaten the core or system integrity. It is therefore possible to consider recovery actions for failed DHRSs and/or to implement back up cooling measures, before reaching unacceptable temperatures for SSCs. However, if no heat sink is available the coolant boundary will eventually fail due to creep damage, leading to release of radioactive fission products and sodium vapours into the containment. Such situations should be practically eliminated by design measures for enhanced core cooling capabilities (described in Section 3.5.3). Provisions can be summarized as follows.

- "Prevention of core damage"

  Extension of the DHRS (normally designed for DBAs) capability should be considered, and other alternative cooling provisions should be made available to prevent core damage and reactor coolant boundary failures due to overheating, given the assumed causes of DHRS failures as DECs.

  Related Criterion in the SDC Report

  Criterion 51: Decay heat removal system[12]

3.4.3. Reactor Coolant Level Reduction

If the core is uncovered, following events causing a reduction of the reactor coolant level, it is impossible to avoid core melt. Depending on the course of the accident and under some circumstances, significant radioactive material would be released into the containment atmosphere. Therefore, an uncovered core configuration should be practically eliminated by design measures (described in Section 3.5.3). Provisions can be summarised as follows.

---

[12] *SDC Criterion 51: Decay heat removal system*

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.

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.

- "Prevention of core damage"

  Reactor Vessels (RVs) and Guard Vessels (GVs) should be designed, manufactured, installed, maintained and inspected to have the highest level of reliability in order to prevent double leakage from RVs and GVs. For a loop-type reactor, measures for ensuring a minimal primary coolant level to prevent core damage should be provided against postulated leakage from the primary loop components and piping. If double leakage from RVs and GVs cannot be practically eliminated, the situation has to be considered for implementing design provisions.

  Related Criterion in the SDC Report

  Criterion 49: Level of reactor coolant[13]

3.4.4. Conditions Considered for DEC Design Provisions

When considering design provisions for the prevention of core damage and mitigation of the potential consequences of DECs, the following points need to be taken into account:

- Identification of expected safety functions.
- Identification of accident conditions for the expected safety functions.
- Design to ensure performance under a postulated accident condition and, if necessary, design to ensure performance of any required supporting system, such as plant protection and control systems, and power supplies, under the postulated accident condition.
- Provision of emergency operation manuals for accident diagnosis and management actions, if necessary.
- Performing safety evaluations with validated analytical codes. The evaluations will be based on best estimates to show that design limits are not exceeded.
- Performing reliability analyses to review risk reduction effects against the initiating event; to complement the deterministic analysis as needed.
- Consideration of the independence of the selected design provisions from other safety related SSCs.

[13] *SDC Criterion 49: Level of reactor coolant*

Guard vessels and guard pipes shall be designed so as to maintain the sodium surface of the primary coolant system at a level necessary for decay heat removal in the case of a sodium leak accident in the primary 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 primary coolant system in case of a failure of the reactor coolant boundary.

- Consideration of testability of the abovementioned provisions. Since simulation of severe plant conditions in DECs are generally not possible during normal reactor operations, a best-estimate analysis based on related data, including those obtained during normal reactor operations and their extrapolation, those obtained in experimental installations to faulted conditions as far as possible, will be used to evaluate the effectiveness of the safety functions throughout the life-time of the plant.

Probabilistic Safety Assessments (PSAs) should be implemented at the design stage to support the estimated probability of failures for initiating events, and the adequacy of the design measures for addressing events in DECs. PSA results will also provide the means to evaluate that no particular feature or initiating event makes a disproportionately large or uncertain contribution to the overall risks.

3.5. Practical Elimination of Accident Situations

This section describes the design approach for practical elimination of accident situations, examples of individual situations and considerations for design measures.

One of the high-level GIF safety goals is “elimination of the need for offsite emergency response”. In order to achieve this goal, all scenarios that could lead to early or large release of radioactivity to the environment need to be prevented, mitigated, or practically eliminated. GIF SFR SDC and SDG approach places an emphasis on prevention, and then on mitigation.

Some scenarios for which the mitigation measures may not be sufficient to manage the core damage and subsequent release of radioactivity (or they are too costly to implement) will have to be practically eliminated. These scenarios are usually design-specific, but the selected list included in the SDG report is fairly common set of practically eliminated accidents considered for the Gen-IV SFR design tracks.

3.5.1. Application to Design

- An early or large radioactive release is subject to the practical elimination approach.
- The approach should be applied to any operation state of the plant, including fuel handling and spent fuel storages.
- Situations, which may lead to early or large radioactive release and which cannot be mitigated under acceptable conditions, are identified to be practically eliminated by implementation of design provisions.
- The approach is intended to demonstrate that the identified situation is physically impossible by design, or that the implemented provisions reduce the likelihood to a residual risk with a high degree of confidence.

- Practical elimination can be considered as part of a general approach and as an enhancement of the Defence-in-Depth principle. The design should restrain practical elimination to a very limited list of situations.

  Related description in the SDC Report

  Section 2.2.4 Prevention of cliff edge effect; Severe accidents that could lead to a significant and sudden radioactive release, not reasonably manageable by design improvement, shall be practically eliminated by appropriate design provisions.

3.5.2. Identification of Situations to be Practically Eliminated

All potential situations which might lead to early or large radioactive release should be considered as the situations to be practically eliminated. Some examples of situations to be practically eliminated are as follows:

(1) Severe events with mechanical energy release exceeding the capability of the containment
- Power excursions for intact core situations (during power operation)
  - ✓ Large gas flow through the core
  - ✓ Large-scale core compaction
  - ✓ Collapse of the core support structures

  Note: As far as reasonably possible, severe accidents have to be managed with mitigation means, before implementing a practical elimination demonstration.

(2) Situations leading to failure of the containment with a risk of fuel damage
- Complete loss of the decay heat removal functions, leading to core damage and failure of the reactor coolant boundary
- Core uncovering due to sodium inventory loss

(3) Fuel degradation in the fuel storage or when the containment is not functional due to maintenance (e.g. opening containment for replacement of large equipment)
- Core damage without a functioning containment
- Spent fuel melting in the storage

Table 1 shows the reasons for choosing the specific examples for an SFR. An example of an approach to identify situations to be practically eliminated is provided in Appendix (A).
In practice, situations to be practically eliminated will be determined by giving a concrete shape to the design step by step. Identification of situations to be practically eliminated should be made as the results of tradeoff between practical elimination and mitigation. Robust design provision shall be provided for the demonstration of the practical elimination. Design modification shall be made, if it is not sufficient to the demonstration.

3.5.3. Design Considerations for Situations to be Practically Eliminated

(1) Power excursions for intact core situations

i) Large gas flow through the core

The primary coolant system should be designed to prevent or limit cover gas entrainment from the sodium free surface in the reactor vessel and to limit or prevent gas accumulation in structures and components submerged in sodium. In addition to the gas entrainment from the sodium free surface, any gas generation and release consequences which possibly occur in the reactor coolant system, including fission gas release, should be considered. Gas release paths are necessary where gas accumulation might occur. An evaluation should be made to show that an accidental gas ingress, entrainment and transport through the core does not cause prompt criticality. Such accidental gas ingress might happen in abnormal conditions, e.g. as a consequence of a primary pump over-speed.

Related Criteria in the SDC Report
Criterion 42bis: Plant system performance of a sodium-cooled fast reactor
Criterion 45: Control of the reactor core

ii) Large-scale core compaction

Reactivity insertion, due to motion and deformation of fuel assemblies and other assemblies such as control rod assembly and shielding assembly, should be limited to prevent core damage following any possible causes, including earthquakes. Due consideration should be taken to the fuel assembly design to prevent compaction. Adequate stiffness of the core should be ensured for each plant state, through the suitable design for the core subassemblies, core support plates and the core restraint system, if provided. The gap between the core subassemblies should be adequate taking any core conditions assumed in normal operation, e.g., reactor shutdown state, nominal power operation, and partial power operation into account.

Control rod insertion should be assured with sufficient geometrical clearance margin for a large earthquake. In order to maintain subcritical conditions after control rod insertion, when the control rods disconnected from the drive mechanisms, the upward movement of the inserted control rods should be limited during an earthquake.

Related Criteria in the SDC Report
Criterion 42bis: Plant system performance of a sodium-cooled fast reactor
Criterion 44: Structural capability of the reactor core

iii) Collapse of the core support structure

The core support structure should be designed to ensure a sufficient safety margin, subject to design rules required by the regulator and including the uncertainties against mechanical and thermal loads. In addition, it should, during its lifetime, cope with environmental conditions and aging of core support structure materials. The core support structure shall not undergo high radiation dose. Operation of this structure in brittle domain is forbidden. A minimum material ductility should be preserved until the end of life of the reactor. In normal operation, temperature of the core support structures should remain in the domain of negligible creeping of the stainless steel. Detection of potential core support deformation or failure should be provided, e.g. inspection capability by using ultrasonic detectors and monitoring plant parameters, such as flow rates and temperatures.

Related Criteria in the SDC Report

Criterion 42bis: Plant system performance of a sodium-cooled fast reactor

Criterion 44: Structural capability of the reactor core

(2) Complete loss of the decay heat removal function, leading to core damage and failure of the reactor coolant boundary.

- For DBA, a decay heat removal system should be provided to deal with initiating events typically caused by single failure of an SSC.
- For DEC, design measures should be provided against initiating events, which are more severe than DBAs, or which originate from multiple failures of SSCs.
- Proven technology, based on the design, construction and operation experience of SFRs, should be applied to the basic design of decay heat removal systems.
- Extension of capabilities to deal with DECs, e.g. additional decay heat removal systems, increased capacities of heat removal, and operation with natural as well as forced circulation, should be considered. Application of mobile power sources and manual operations can reinforce the design in case of extreme external hazards of low probability even with their uncertainty of availability.
- Ensuring diversity in systems is essential for improving the overall reliability. Redundancy of systems does not bring the same reliability benefits. It is required to maintain heat removal functions, even under postulated severe external hazards, such as earthquakes, flooding, tsunami and missiles leading to a common cause failure. Physical separation of the diverse or redundant systems can further reduce the potential for common cause failures.

- An SFR should proactively utilise its natural circulation capability to an ultimate heat sink (atmosphere), since this can significantly contribute to improving the reliability of the heat removal capability, even under long-term loss of power supplies. Natural circulation can be used as a measure for DBAs, as well as for DECs.
- Robust demonstrations of practical elimination should consider independence between safety systems for DBAs and decay heat removal capabilities for DECs. If necessary, additional independent decay heat removal systems should be installed.
- It is necessary to clarify all credible factors leading to loss of decay heat removal function and to demonstrate that measures can be implemented to overcome all of them. “Credible factors” are the initiating events concurrent with potential subsequent failures of required safety related systems, structures and components (including common cause failures and dependent failures of redundant systems). Broad range of situations including internal and external events and associated plant states (AOOs, DBAs and DECs) should be comprehensively considered to assess their influence on decay heat removal function.
- Each system, related to decay heat removal, should be able to demonstrate that it can perform its function as expected.

Related Criteria in the SDC Report
Criterion 42bis: Plant system performance of a sodium-cooled fast reactor
Criterion 51: Decay heat removal system

(3) Core uncovering due to sodium inventory loss

- The RVs and GVs should be designed, manufactured, installed, maintained and inspected to have the highest level of reliability.
- Due design considerations should be taken to prevent dependent failures and common cause failures between RVs and GVs, even under postulated severe external hazards, such as earthquakes.
- The reliability of these components may also be challenged by a failure of any adjoining SSCs. The impact of such a failure should be prevented wherever possible by layout optimisation and/or provision of adequate protection by features designed to withstand the global and local loads which may be placed on them.
- In case of a RV leakage, the GV should be designed considering a single failure in the pressure control between the inside and outside RV so that the reactor core remains covered and the decay heat removal paths are maintained.

- In case double failures of RVs and GVs cannot be practically eliminated, provisions should be available to retain the coolant level to keep the reactor core covered until the core can be unloaded.

  Related Criteria in the SDC Report
  Criterion 42bis: Plant system performance of a sodium-cooled fast reactor
  Criterion 49: Level of reactor coolant

3.5.4. Principles for Setting up a Demonstration of Practical Elimination

Demonstrations of situations for practical elimination are made on a case-by-case basis, founded on deterministic methods, and in some cases supplemented with probabilistic studies. A good practical elimination demonstration must be convincing and independent of the methodology.
There are two convincing ways for a demonstration:

- Demonstrate that the situation is physically impossible by design
- Implement devices to make the situation extremely unlikely with a high degree of confidence so that it falls under the residual risk category for which the frequency limit is established in national regulations. For this, uncertainties have to be taken into account in order to reach a sufficient degree of confidence and to reinforce the robustness of the demonstration.

Deterministic demonstrations are organised by the lines of defence based on the following general principles:

- Establishing a complete list of initiating events, including stress and human factors. For each event, provisions to either physically exclude the event or to make it very unlikely, should be established.
- If it is not possible to physically exclude a situation, favouring provisions that enable early detection and corrective actions to avoid degradation or to make the consequences acceptable. The initiators, which may have common mode failures, reducing the effectiveness of the provisions, should be identified and additional provisions taken to avoid their consequences.

In addition, probabilistic studies are performed to ensure the expected very low frequency of occurrence.

Table 1 Examples of Situations to be practically eliminated for an SFR

SFR	
Situations to be practically eliminated	**Reason for choice**
Power excursions from intact core situations (Extreme initiating events)	In case an accident involving uncontrollable reactivity insertion of more than 1$ occurs, it may lead to prompt criticality and a severe power excursion either LWR or SFR. Due to physics of fast neutron spectrum reactors, the SFR cores are not in their most reactive configuration. Therefore, the possible causes of such reactivity insertion in SFR, such as large-scale gas entrainment through the core, large-scale core compaction, and collapse of core support structure, should be practically eliminated because prevention and mitigation measures for them may not be effective to prevent an early or large release of radioactivity.
Complete loss of heat removal function that could lead to core damage and failure of the reactor coolant boundary	If no heat sink is available, a coolant boundary failure will occur, either due to creep damage anywhere in the primary and secondary coolant systems, or from melt-through by degraded core materials.
Core uncovering due to sodium inventory loss	If the core becomes uncovered, it is impossible to avoid a core melt. Depending on the course of the accident and under some circumstances, significant radioactive materials would be released into the containment atmosphere.
Core damage during maintenance, or spent fuel melting in the storage	If a core damage or fuel melting occurs during maintenance (when the containment is not functional), or at the fuel storage outside the containment, significant radioactive release might happen.

This table provides examples not intended to be comprehensive and not implied to be generically applicable to all SFRs. It should be established in the frame of detailed design and safety analysis.

4. GUIDELINES FOR APPLICATION OF SAFETY DESIGN CRITERIA

This chapter contains design guidelines for the application of specific criteria related to the reactivity characteristics of the reactor core, the reactor shutdown system, the containment function, and the decay heat removal system, including important design parameters, postulated events and design limits, as well as testability and safety design demonstrations. These guidelines are intended to be appropriately considered according to the specific features of individual designs and to provide designers with examples of design provisions.

4.1. Reactivity Issues

4.1.1. Prevention of Core Damage

Safety design criteria for reactor shutdown functions are defined in *Criterion 46* in the SDC. The related design guidelines are presented below.

Active Reactor Shutdown

(1) SDC

"The means for shutting down the reactor shall consist of at least two diverse and independent systems."

(2) Design concept

Two diverse and independent active reactor shutdown systems, consisting of control rods, actuation mechanisms, detectors and signal processing systems.

(3) Functional recommendations and Design consideration

(3-1) Reactor shutdown capabilities

- Functional recommendations

  At least one of the two reactor shutdown systems should be able to shut down the reactor and retain it in safe shutdown state[14] in an AOO and a DBA without exceeding the design limits.

  The reactor shutdown system, consisting of control rods, should be designed to have sufficient reactivity worth for a shutdown, even if the control rod with the maximum reactivity worth is not counted (the so-called "one rod stuck margin.").

[14] *Safe shutdown state is defined as the state with the reactivity of the reactor kept to a margin below criticality under a prescribed coolant temperature condition in which interventions such as fuel reloading, periodic inspection and repair works in the reactor can be achievable.*

Control rod insertion should be assured even in case of deformation of core components due to, for instance, irradiation or design basis earthquakes. The reactor shutdown system, which functions as reactor controller under normal operation, e.g. reactor start-up and power regulation, should also be designed so that any failure of the control function, such as control rod position change by motor drive mechanism, shouldn't affect the reactor shutdown function.

Related consideration

The reactor core should be designed to have favourable inherent safety characteristics, e.g. a negative power coefficient, to self-limit any reactor power increase in case of reactivity insertions.

- Design consideration
  - ✓ Duration of signal transmitting and processing to actuate control rod insertion
  - ✓ Duration of control rod insertion
  - ✓ Reactivity worth of control rods
  - ✓ (Reactivity characteristics of reactor core)

(3-2) Diversity and independence

- Functional recommendations

Two shutdown systems should be designed to have independence and diversity to the extent practicable to prevent common cause failures. Examples of design measures are:

- ✓ Different structures/mechanisms for rod insertion, different designs for the control rods and their guide tubes
- ✓ Physical separation of electric distribution boards and cables; isolated arrangements, divided by walls, etc.
- ✓ Electrical isolation of protection system

Detection parameters for the reactor shutdown systems should be diverse to the extent practicable.

At least one of the two reactor shutdown systems should be designed according to a single failure criterion that applies to components of actuation mechanisms, detectors and signal processing systems.

Fail safe features, such as control rod insertion by loss of the holding function in case of electric power supply failure, should be considered.

- Design consideration
  - ✓ Electrical and physical separation

- ✓ Diversification of design (e.g. detection parameters for reactor shutdown, a combination of programmable digital I&C system and diverse system with a different operation principle.)
- ✓ Fail safe measures

(3-3) Consideration for environmental conditions

- ➢ Functional recommendations

  Throughout their life in the reactor including conditions during DBAs, two shutdown systems should be designed to withstand environmental conditions, such as irradiation, temperature, chemical effects, geometrical changes.

- ➢ Design consideration
  - ✓ Temperature, irradiation effects, liquid sodium environmental conditions, cover gas plenum with sodium aerosols.

Reactor Shutdown for DECs

(1) SDC

"For design extension conditions, passive or inherent reactivity reduction capabilities shall be provided to prevent severe core degradation and to avoid re-criticality in the long run."

(2) Design concept

Passive reactivity reduction or feedback capabilities; several different mechanisms, including those responding to coolant temperature increase or coolant hydraulic force change.

Inherent reactivity reduction in balance with heat removal capabilities due to negative reactivity feedback from Doppler effect, axial and radial expansion of core and structure, and even sodium expansion effects, if designed accordingly.

(3) Functional recommendations and Design consideration

(3-1) Capability of passive or inherent reactivity reduction mechanisms

- ➢ Functional recommendations

  Adequate combination of passive reactivity reduction, passive feedback and inherent power reduction capabilities should be provided in case of an AOO with a failure of the active reactor shutdown systems, to avoid exceeding the design limits for DECs.

  1) Passive reactivity reduction or feedback mechanisms should be designed to provide sufficient negative reactivity within an allowable time and to be activated and

operated in direct response to natural phenomena (such as increased coolant temperature or reduced coolant pressure) without any active signals, activation mechanisms or power source. For the passive feedback mechanisms (e.g. HSR, GEM), positive reactivity insertion in response to unintended operation of the reactor component (such as starting primary pump in cold state) should not cause core damage.

2) Inherent reactivity reduction, based on the total power coefficient, isothermal temperature coefficient and power/flow coefficient, should be negative to reduce the core power at elevated temperatures in balance with available heat rejection capacities during an ATWS. Complementary reactor shutdown measures should be provided in order to make the reactor core subcritical in the long term.

- Design consideration

Passive reactivity reduction or feedback mechanisms: Parameter related to the reactor condition to which the passive shutdown mechanisms respond, e.g. coolant temperature at the reactor core outlet, reactor coolant flow etc. Activation point of the parameter, response time, amount of reactivity.

Inherent reactivity reduction: Total power coefficient, isothermal temperature and power/flow coefficients, reactivity feedback mechanisms, such as axial and radial core expansions at elevated temperatures, and thermal expansion of the control rod driveline. Amount and timing of the introduction of favourable feedback should be appropriate to cause power reduction and prevent excessive temperature rise in the reactor.

(3-2) Prevention of common cause failures for passive reactivity reduction mechanisms

- Functional recommendations

Passive reactivity reduction or feedback mechanisms should not be affected by any failures of the active systems. Insertion of control rod type absorbers should be ensured even with static or dynamic core deformation caused by postulated events, such as earthquakes and environmental conditions, including irradiation. Implementation of such devices should not induce additional causes of deviation from normal operation, such as frequent spurious activation.

- Design consideration
  - ✓ Acceptable limits of core deformation for ensuring unforced insertion of absorbers

(3-3) Long term reactor shutdown

- Functional recommendations

Measures to achieve and maintain a safe shutdown state and to monitor the plant conditions should be provided in case of failure of the active shutdown systems.

- Design consideration
  - ✓ Reactivity needed for safe shutdown
  - ✓ Parameters for monitoring the reactor condition after an accident

(3-4) Consideration for environmental conditions

- Functional recommendations

Passive reactivity reduction or feedback mechanisms should be designed to withstand environmental conditions and to maintain insertion function throughout the lifetime of the reactor and DBAs/DECs.

Reactivity effects of inherent reactivity reduction capabilities should be assured throughout the lifetime of the reactor, considering environmental conditions.

- Design consideration
  - ✓ Effects of irradiation and temperature, liquid sodium environmental conditions, and geometrical changes

4.1.2. Mitigation of Core Damage

The mitigation functions of core damage are defined in the Criteria 44, 45, 47 and 51 in the SDC for GIF SFRs. The related design guidelines are presented below. Objectives are to prevent prompt criticality in the course of core degradation and to ensure the coolability of core debris.

Design measures against core damage from unprotected transients should be implemented for the following accident phases, according to the progression of a core damage:

- Initiating phase; accident phase from intact state up to inter-subassembly material motion onset, i.e. subassembly duct failure
- Transition phase; accident phase after initiating phase up to the establishment of stable cooling conditions
- Post accident heat removal; stable cooling condition for a long term

Mitigation in Initiating Phase

(1) SDC

"To avoid significant mechanical energy release during a core disruptive accident, the reactor core shall be designed to have favourable neutronics, thermal, and physical

characteristics, considering all reactivity feedbacks, including sodium void worth, to mitigate the consequences of such design extension conditions."

(2) Design concept

Various core designs with different output power, different fuel material, i.e. oxide, metal and nitride. A common core geometry consists of fuel subassemblies containing the fuel pins in ducts of hexagonal cross-sections, typically referred to as subassembly ducts or hex-cans.

(3) Functional recommendations and Design consideration

(3-1) Limiting the total reactivity during unprotected transients

- Functional recommendations

  Core reactivity characteristics should be designed so as to prevent prompt criticality, i.e. ρ_{net} < 1$ during the initiating phase of unprotected transients. Positive reactivity effects, such as sodium boiling, should be limited so that negative reactivity effects e.g. Doppler effect, fuel expansion and failed fuel dispersion are sufficient to counteract the positive reactivity effects. Design parameters, such as sodium volume fraction, core height and other geometric parameters, should be properly chosen based on the effects of sodium void worth during transients.

- Design consideration
  - ✓ Core reactivity characteristics (sodium void reactivity, Doppler effect, fuel axial expansion, core radial expansion, control-rod driveline expansion, etc.)
  - ✓ Sodium volume fraction and core height and geometry (e.g. heterogeneous arrangements, sodium plenum)

(3-2) Facilitating fuel reactivity effects

- Functional recommendations

  Core design parameters, such as core height, should be properly chosen to obtain effective negative feedback due to failed fuel dispersion. Fuel reactivity feedback is dependent on the choice of fuel type for the reactor. The effects should be appropriately included in transient analysis of an accident.

- Design consideration
  - ✓ Choice of fuel type, core height

Mitigation in Transition Phase

(1) SDC

"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."

(2) Design concept

Various concepts are possible depending on design and fuel characteristics

(3) Functional recommendations and Design consideration

(3-1) Limiting the total reactivity during unprotected transients

- Functional recommendations

In the course of a core degradation during unprotected transients, measures should be provided to prevent prompt criticality, potentially leading to large mechanical energy release. For this purpose, design measures, such as facilitating molten fuel discharge outside the core, neutron absorber added to the core, and core cooling to prevent failure progression, i.e. early termination, should be taken. These measures should include consideration of using favourable inherent phenomena occurring in the course of a core degradation.

The design of a molten fuel discharge path, if present, should:

a) prevent blockage due to freezing of molten relocated cladding and/or fuel,
b) be accessible prior to formation of large amounts of molten fuel, and
c) have enough capacity for timely discharge of molten fuel.

- Design consideration

  - ✓ Choice of fuel type, core geometry, fuel fissile density, fuel mass amount of core, core material properties;
  - ✓ For molten fuel discharge, if present, the required geometry, e.g. diameter, length, and material properties of discharge path.

(3-2) Establishment of a stable cooling condition

- Functional recommendations

Measures should be provided to establish a stable cooling condition of a degraded core. Due consideration should be taken to the coolability of the remaining fuel inside the core region and any relocated molten core materials. Prompt criticality, potentially leading to large mechanical energy release, should be prevented during the relocation process.

- Design consideration
  - ✓ Molten fuel relocation characteristics
  - ✓ Molten fuel relocation path
  - ✓ Coolant flow and re-entry paths to the core.

Prevention of Reactor Coolant Boundary Failures

(1) SDC

"Components, which constitute the reactor coolant boundary, shall be designed to maintain the boundary function and to maintain a sufficient sodium inventory in the primary coolant system in case of a core disruptive accident."

(2) Design concept

Prevention of reactor coolant boundary failures against mechanical load. (Countermeasures depend on the reactor structure design)

(3) Functional recommendations and Design consideration

(3-1) Prevention of reactor coolant boundary failures following mechanical loads

- Functional recommendations

  The reactor coolant boundary should maintain its boundary function following pressure loads, including any loads induced by fuel-coolant interaction (FCI).

- Design consideration
  - ✓ Choice of fuel type, inlet and/or outlet design of core assemblies, plena geometry, structural design of reactor coolant boundary components, material strength.

(3-2) Prevention and mitigation of sodium ejection from a reactor cover gas boundary due to mechanical loads

- Functional recommendations

  Reactor cover gas boundary components should withstand pressure loads to prevent sodium ejection into the containment, including any loads induced by FCI. Design measures, such as strengthened seals of plug structures, including rotating plugs for fuel handling, should be considered.

  Mitigation provisions against sodium ejection should also be implemented as needed.

- Design consideration
  - ✓ Structural design of reactor cover gas boundary components, material strength

(3-3) Prevention of over pressure

- Functional recommendations

  Measures should be provided to cope with temperature and pressure increases due to heat generation and accumulation of fission gases, released from a degraded core.

- Design consideration
  - ✓ Installation of pressure relief devices, such as safety relief valves at the reactor cover gas boundary

Post Accident Heat Removal

(1) SDC

"Means shall be provided for the capability of core cooling under postulated plant conditions with core degradation."

(2) Design concept

Retention and cooling of a degraded core

Depending on reactor core characteristics, perform the retention function with an existing component or structure, or a dedicated structure, e.g. core catcher.

(3) Functional recommendations and Design consideration

(3-1) Retention of a degraded core

- Functional recommendations

  Measures should be provided to retain degraded core materials to facilitate post accident heat removal. Re-criticality of a retained degraded core should be prevented during the post-accident heat removal phase. The retention structure should resist the thermal load from a degraded core, as well as mechanical loads, including any loads from FCIs.

- Design consideration
  - ✓ Design of any structure intended to retain degraded core materials, including the core inlet plenum, core support structure (form, strength), material strength characteristics;
  - ✓ Coolability and re-criticality of degraded core materials;
  - ✓ Fuel retention capacities for such structures;
  - ✓ Characteristics and relocation of degraded core materials.

(3-2) Ensuring a coolant circulation path and heat sink

- Functional recommendations

  A coolant flow path and heat sink should be available for cooling of degraded core materials.

  Natural circulation capability should be incorporated.

  Structures and components that form the flow paths should maintain their functions against adverse effects, such as mechanical loads from FCI and blockage by dispersed fuel debris.

- Design consideration
  - ✓ Reactor cooling system design (coolant flow path, heat sink and natural circulation capability)
  - ✓ Material strength to resist FCI loads

(3-3) Protection of a degraded core retention structure

- Functional recommendations

  For IVR, the reactor structure should facilitate molten fuel dispersion and solidification in the presence of adequate heat removal capability to prevent or mitigate erosion of any structure intended to retain the degraded core materials caused by molten fuel.

  Depending on the characteristics of the degraded core materials, preventive measures against erosion, such as installing protective layers on core retention structures, should be considered.

- Design consideration
  - ✓ For IVR, sodium mass and depth in the lower plenum of the RV above the core catcher or retention place
  - ✓ Material property of protection layers for the core catcher or retention place, if necessary.

4.2. Decay Heat Removal Issues

Decay heat removal functions are defined in *Criteria 49 and 51* in the SDC for GIF SFR. The related design guidelines are presented below.

4.2.1. Prevention of Core Uncovering

(1) SDC

"Guard vessels and guard pipes shall be designed so as to maintain the sodium surface of the primary coolant system at a level necessary for decay heat removal in the case of a sodium leak accident in the primary 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 primary coolant system in case of a failure of the reactor coolant boundary."

(2) Design concept

Guard vessel,

Guard pipes (option for loop type)

(3) Functional recommendations and Design consideration

(3-1) Guard vessel

- Functional recommendations

  A Guard Vessel (GV) should be installed to enclose the Reactor Vessel (RV) so that the reactor sodium level can be maintained in the RV following a sodium leak. The gap volume between the RV and the GV should be limited, so that the sodium surface level inside the RV should, during a safe shutdown state, always be above the design limit level for sodium circulation (EsL; emergency sodium level).

- Design consideration
  - ✓ Gap/volume between the reactor coolant boundary and the GV (guard pipe as loop type option)
  - ✓ EsL in RV

(3-2) Prevention of double failure of the RV and the GV

- Functional recommendations

  In order to substantiate the practical elimination of core uncovering, the conditions for preventing double failure of the RV and the GV are given as follows.

  Ensure the reliability

  The RVs and GVs should be designed, manufactured, installed, maintained and inspected to have the highest level of reliability.

Prevention of GV failure being subordinated to RV failure:

- ✓ The GV should withstand thermal loads due to a sodium leak from the RV.
- ✓ The GV should withstand mechanical loads from all possible causes, such as earthquakes, while retaining leaked sodium for a long time.
- ✓ The GV should withstand any interference with a failed RV (even considering thermal expansion, vibration, dynamic loads from failed RV and/or SSCs, etc.).

Prevention of common cause failure between RV and GV:

- ✓ The design should separate the support structures of the RV and GV to the extent practicable, or prevent failures of common parts of the support structures.
- ✓ The design should prevent common cause defects in manufacturing, e.g., by using different source for the materials, different manufactures.
- ✓ The design should ensure sufficient margins against internal/external hazards, including earthquakes.

In case a double failure of the RV and GV cannot be practically eliminated, provisions should be made to retain the coolant level, i.e. limitation of the free volume in the reactor pit, to mitigate sodium chemical reaction inside the pit and to provide thermal insulation of the reactor building, or for early detection of sodium leakage combined with the ability to rapidly unload fuel assemblies from the reactor before the core is uncovered.

- ➢ Design consideration
  - ✓ Design margin of the RV and GV
  - ✓ Independence of the RV and GV
  - ✓ Inspectability of the RV and GV
  - ✓ Free volume in the reactor pit (In case a double failure of the RV and GV cannot be practically eliminated)

(3-3) Measures against sodium leaks from the primary loops (Note: only required for loop-type designs)

- ➢ Functional recommendations

Measures, such as installing guard pipes and GVs, as well as piping arrangements above the coolant surface level, should be provided for ensuring core cooling and for reducing the effects of sodium leaks from any primary loop pipe or component. Postulated leaks for DBAs should be determined with due consideration taken to the application of the Leak Before Break (LBB) concept.

For DECs, if guard pipes are installed to maintain the coolant level, they should be designed to withstand loads associated with large breaks of the primary pipes. In order to

prevent core damage under severe leak conditions, such as multiple leaks in the primary loops, decay heat removal measures should be provided, e.g. enabling an in-vessel cooler to be operable in case of low sodium levels without coolant circulation in the primary coolant loops.

- Design consideration
  - ✓ Arrangement of the primary coolant system (e.g. vertical position of the horizontal parts of primary pipes), sodium quantity

4.2.2. Decay Heat Removal for DBA

(1) SDC

"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."

(2) Design concept

Various options for system configuration, number of sub-systems (DRACS, PRACS, IRACS, RVACS, SGAHRS etc.) as safety systems. A secondary sodium loop connected to an air cooler is a typical DBA countermeasure.

DRACS; Direct Reactor Auxiliary Cooling System

PRACS; Primary Reactor Auxiliary Cooling System

IRACS; Intermediate Reactor Auxiliary Cooling System

RVACS; Reactor Vessel Auxiliary Cooling System

SGAHRS; Steam Generator Auxiliary Heat Removal System

(3) Functional recommendations and Design consideration

(3-1) Basic capability of a DHRS

- Functional recommendations

A Decay Heat Removal System (DHRS) should be able to cool the reactor core immediately after reactor shutdown and for as long as needed time. The system configuration and heat removal capacity of DHRSs, as well as transient characteristics,

such as flow coastdown of the primary pumps, should be set not to exceed design limits of AOOs and DBAs, as discussed in Section 4.3, assuming a single failure.

- Design consideration
  - ✓ Heat removal capacity of DBA measures
  - ✓ Decay heat characteristics
  - ✓ Pump coastdown
  - ✓ Primary coolant system heat capacity

(3-2) Ensuring reliability of a DHRS

- Functional recommendations

In order to avoid a common cause failure in case of DBAs, including internal and external hazards, redundancy, diversity, physical separation and independence should be adequately provided. DHRSs should be designed to have redundancy and diversity for ensuring sufficient core cooling capacity against AOOs and DBAs, considering loss of off-site power and single failure of components. For instance, three systems at 100% of the capacity required for decay heat removal, or four systems at 50% capacity, would be provided, considering one system failure as an initiating event and a single failure in another system, depending on the design.

Diversity in the system configuration and/or operation mode (forced circulation and natural circulation), as well as physical separation, should be introduced.

- Design consideration
  - ✓ Redundancy (number of subsystems and their heat removal capacity)
  - ✓ Diversity (system level, component level, mechanism level (i.e., forced/natural circulation))
  - ✓ Layout, physical separation and independence (protection against internal and external hazards)
  - ✓ Emergency power supply system, if required (the capacity and the activation time)

(3-3) Prevention of coolant freezing

- Functional recommendations

In order to prevent sodium (or other types of coolant such as NaK) freezing in DHRSs, design measures, such as keeping a minimum flow rate, providing an electric heater, or hot gas blow heating, should be provided. To prevent freezing in the air coolers, design measures should be provided, e.g. keeping sufficient circulation in the sodium circuits and

independent control of subsystems for prevention of common cause failures due to malfunction of the air flow regulators and blowers.

- Design consideration
  - ✓ Operating temperature (standby temperature)
  - ✓ Heat exchange characteristics of air cooler (control characteristics)

(3-4) Measures against sodium leaks

- Functional recommendations

  Design provisions should be made for the prevention and early detection of sodium (or other types of coolant such as NaK) leaks, e.g. aerosol and contact type detectors, and for mitigation of the effects of chemical reactions between sodium and air or water, e.g. guard pipes or enclosures, sodium drain systems.

- Design consideration
  - ✓ Design measures for prevention, detection, control, and mitigation

4.2.3. Decay Heat Removal for DECs

(1) SDC

"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.

(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."

(2) Design concept

Functional extension of the design measures dedicated to AOOs and DBAs to cope with DECs.

Providing alternative cooling measures, in addition to the measures for DBAs.

(3) Functional recommendations and Design consideration

(3-1) Enhancement of decay heat removal capabilities

- Functional recommendations

The design measures, dedicated to AOOs and DBAs, should be supplemented by an adequate combination of additional decay heat removal systems, increased capacities of heat removal, and operation with natural as well as forced circulation, to cope with more severe initiating events than DBAs, taking internal and external hazards, such as missiles, and their probable combinations into account.

Accident management provisions should be made so that recovery operations can be performed in case of failure of the DBA provisions, e.g. manual operation of air cooler dampers.

- Design consideration
  - ✓ Heat removal capacity in DECs
  - ✓ Decay heat characteristics
  - ✓ Primary coolant system heat capacity

(3-2) Alternative cooling measures

- Functional recommendations

The heat removal capacity of alternative decay heat removal measures for DECs should be set so that the reactor systems do not exceed the design limits for DECs, as discussed in Section 4.3. The measures should be independent from those for AOOs and DBAs. Start-up and operation procedures should be established in line with diagnostic processes, even under severe plant conditions, such as after failure of DBA provisions.

- Design consideration
  - ✓ Heat removal capacity
  - ✓ Decay heat characteristics
  - ✓ Primary coolant system heat capacity
  - ✓ Diversity and independence to the AOO and DBA measures

(3-3) Natural circulation capability

- Functional recommendations

In order to enhance the reliability of the decay heat removal function and to maintain the function under long-term loss of all AC power, natural circulation capability should be properly incorporated into the whole decay heat removal system, which consists of systems dedicated to AOOs and DBAs, and alternative ones for DECs. The reactor cooling system should be designed to have an adequate height difference between core and heat exchangers, and an adequate pressure drop for enhancing natural circulation

capabilities of the coolant. Use of active devices, as well as instrumentation and control, should be limited, and should have sufficient grace time in both automatic and manual operation modes.

- Design consideration
  - ✓ Height difference between core and heat exchanger to ultimate heat sink
  - ✓ Pressure drop
  - ✓ Natural circulation start-up characteristics

(3-4) Enhancement of the reliability of the decay heat removal function

- Functional recommendations

In order to avoid a common cause failure in case of DECs, in addition to AOOs and DBAs or as a consequence of internal hazards, external hazards, or their probable combinations, diversity of and physical separation and independence of the decay heat removal measures should be adequately assured for both AOOs/DBAs and DECs. Examples of potential common cause failures are earthquakes, aircraft crashes, flooding, sodium freezing in air coolers, sodium fires on the reactor roof, and loss of all AC power. Diversity in system configurations, components, working fluids (sodium, gas), operational principles (forced circulation and natural circulation) and independence (including optimising the layout against internal hazards, external hazards and/or physical separation) should be adequately provided.

- Design consideration
  - ✓ Diversity and independence (including provision of suitable physical separation as appropriate) of decay heat removal measures

4.3. Initiating Events and Design Limits

4.3.1. AOO and DBA

(1) Typical initiating events

Initiating events under AOOs and DBAs include those that challenge the fundamental safety functions of the reactor, such as reactivity control, core heat removal, and the containment of radioactive materials. Examples of initiating events for AOOs and DBAs for an SFR are provided in Appendix (B).

(2) Design limits

Multiple barriers against the release of radioactivity consist of fuel elements, fuel cladding, reactor coolant and cover gas boundaries, guard vessels (and pipes in a loop configuration), and containments. These functions need to be maintained for AOOs. For DBAs, the reactor core geometry is preserved and should be coolable, and the reactor coolant boundary, cover gas boundary, and containment should uphold their barrier functions.

Typical indices for design limits of the reactor core are the maximum temperatures of the fuel, cladding, and coolant. Coolant boiling should be prevented to maintain the cooling of the reactor core, and to limit its contribution to the net reactivity.

Cladding failure during normal operation and AOOs should be avoided and specified acceptable fuel design limits are not exceeded. Cladding time-at-temperature during AOOs and DBAs, cladding stress and strain due to internal pressure are used (e.g. to evaluate the cladding cumulative damage).

The integrity of the reactor coolant boundary should be maintained during a postulated accident. Typical indices are the maximum coolant temperature and the duration of the accident when the reactor coolant boundary is exposed to elevated temperature.

Typical indices for the containment are the containment temperature and internal pressure.

Concerning release of radioactive materials, the potential public radiation exposure dose should be limited according to the criteria for operational states and accident conditions.

4.3.2. DEC

Core damage prevention under DECs

(1) Typical initiating events

Typical initiating events include ATWS that require other means of controlling or reducing the reactor power, such as passive shutdown or provisions for favourable inherent reactivity feedback. Postulated ATWSs, i.e., AOOs associated with failures of active reactor shutdown systems, comprise: Loss of Flow (LOF), e.g. loss of power in all the primary pumps, Transient Over Power (TOP), e.g. uncontrolled withdrawal of a control rod, and Loss of Heat Sink (LOHS), e.g. loss of main heat removal system typically via the secondary coolant system or the water-steam system.

Typical events, challenging the “reactor core heat removal” safety function, are: multiple failures in the coolant system or multiple failures of the decay heat removal function, which might result in a reduction of the reactor coolant level or loss of the safety systems for decay heat removal. For these events, core degradation, due to core uncovering or complete loss of decay heat removal capabilities, should be practically eliminated by design measures.

(2) Design limits

As for the reactor core, core coolable geometry should be maintained by averting or limiting possible causes of cooling deficiencies due to coolant boiling, cladding failure or deformation (e.g. ballooning). Fuel melting should be averted or limited to prevent propagation of fuel failures.

As for the coolant boundary, creep failure caused by a temperature increase should be prevented. Hence, temperature increase and duration of the events should be adequately limited.

Containment failures should be avoided, i.e. temperature and pressure limits should not be exceeded.

Any release of radioactive materials from the containment should be limited and should not exceed acceptable regulatory dose limits to achieve “elimination of the need for off-site emergency response” for these events [9]. It should be noted that an off-site emergency plan is still envisioned for Gen-IV SFRs, even if the goal is elimination of the need for off-site emergency response.

Mitigation of consequences of core damage under DECs

(1) Typical initiating events

Unprotected transients resulting in core degradation, are representative of DECs with core melt. If inherent power reduction capabilities are insufficient, core degradation can occur, and analyses should include considering the uncertainty of individual reactivity feedback effects.

The potential for propagation of damage from local fuel failures should be considered as a core degradation mode and different from that of core damage from unprotected transients.

Provisions for achieving IVR should mitigate challenges to the containment structure from either type of core degradation modes.

For most SFRs, the containment design basis include a fire from sodium leakage and combustion. The containment function should be able to withstand pressures, temperatures, chemical reactions, aerosol deposition etc. which arise as a result of such a sodium fire.

(2) Design limits

Severe mechanical energy release, resulting in a reactor coolant boundary failure, should be prevented for unprotected transients that may lead to core degradation. Possible indices are:

the limitation of the fuel temperature or the prevention of prompt criticality, i.e. maximum net reactivity should be less than 1$.

To prevent coolant boundary failures, the strain on the RV should be limited so that the failure won't occur during a dynamic load. In addition, creep damage, due to thermal stress at an elevated temperature, should be prevented.

Containment failures should be avoided, i.e. the temperature and pressure should not exceed specified limits, and dynamic effects should not challenge the containment boundary. Hydrogen generation should be prevented as far as possible, and its concentration should be limited to avoid reaching deflagration and detonation limits.

Release of radioactive materials should not exceed the regulatory limits for the public radiation exposure dose that initiates off-site response.

4.4. Testability

The safety functions of SSCs mentioned in 4.1 and 4.2 should regularly be inspected and tested throughout the plant's lifetime according to their safety classifications. Examples of tests and inspections to be performed during the plant's lifetime are given below.

Particular attention should be paid to the following aspects:

- integrity of the barriers between radioactive materials and the environment (such as fuel cladding, the reactor coolant boundary and the containment);
- availability of safety systems, such as protection systems, safety actuation systems and safety system support features;
- availability of items, whose failure could adversely affect safety;
- accessibility and operability for monitoring and inspection of components under submerged in sodium coolant.

(1) Reactivity feedback

- Measurement of reactivity feedback during start-up to verify both sign and magnitude for normal operation and accidents

(2) Reactor shutdown

- Functional tests of reactor shutdown systems e.g. control rod positions and insertion times to ensure that the tested system or component is capable of performing its design function

(3) Decay heat removal

- Functional tests of active components, such as pumps and blowers

- Confirmation of natural circulation heat removal capabilities, for instance, by checking temperature and flow rate changes from a safe shutdown state in case of termination of forced convection. This could be done as a performance test in the commissioning stage or pre-start-up phase in service.

4.5. Demonstration

The effectiveness of the safety functions of SSCs, mentioned in 4.1 and 4.2, should be demonstrated according to their safety classification before starting any power operation of a nuclear power plant. Examples of information required for the safety demonstration are given in this section.

For DBAs and DECs without core damage, experiments, using scale models of the actual SSCs or actual reactor tests during commissioning stage, can be possible and useful for the safety demonstration.

For DECs with core damage, direct performance demonstration on the actual reactor is impossible. Thus, numerical simulations have an important role. In addition, experiments should be set up to validate the analytical tools and to understand the basic phenomena having a bearing on the accident analysis.

(1) Passive shutdown mechanism (example for SASS)

- Material tests: understanding physical properties of sensing alloys (Curie point temperature, thermal aging and irradiation effect), productivity.
- Component tests: control rod insertion performance by model tests, transient response tests, thermal hydraulic tests at the reactor outlet by scale models.
- Reactor tests: stability of the in-vessel holding force, operability and material tests.
- Development of analytical methods for design and evaluation.
- Validation of analytical methods based on above-mentioned experiments.
- Evaluation of the core damage frequency from reactor shutdown failures using PSA.

(2) Decay heat removal by natural circulation

- Validation of analytical models by water and sodium tests and applying the results to the evaluation of the reactor case.
- The performance of the actual plant should be confirmed during the performance test phase.
- Evaluation of the core damage frequency from loss of heat removal using PSA.

(3) Mitigation of core damage

- Development of analytical models, combining fuel pin failures and relocations with reactivity feedback; In-pile experiments for fuel pin failures and relocation behaviours.

5. CONSIDERATIONS FOR SFR REACTIVITY CHARACTERISTICS

In the course of the international reviews of the “SDC Phase 1 Report”, a request was made for a technical clarification of the “sodium void reactivity in the fast reactor core reactivity characteristics” to be included in the SDG. In general, the idea and design concept of a so-called “negative sodium void reactivity reactor core” has been proposed and examined from many angles during the some half-century long SFR development history.

This chapter summarises the general reactivity characteristics of an SFR and contains concluding remarks on the sodium void reactivity in relation to SFR safety, emphasising that it is the overall reactivity feedback that is important and not any single part, such as sodium void. In addition, integrated transient analysis is required to determine if the sodium void of the design is acceptable or not since the entire core typically does not void during a postulated transient, but sodium voiding is usually predicted to initially occur locally with a much lower reactivity effect. The core reactivity can be dominated by reactivity change induced by motion of molten core materials such as fuel and steel in a CDA (Core Disruptive Accident). Positive sodium void reactivity should be appropriately limited but the sodium void is not necessarily negative.

General view

Regardless of the LWR or the fast reactor including the SFR, the reactor core should have the inherent reactivity feedback characteristics so as to achieve stable control in operational states and terminate an abnormal event in an accident condition without resulting in core damage. In addition to the inherent reactivity feedback characteristics, the nuclear facility should have an instrumentation and control system that ensures stable control of the reactor in operational states, and safety systems such as a reactor shutdown system against a DBA to prevent the events from exceeding the design limits. Furthermore, the facility should utilise the inherent reactivity feedback, and also a passive mechanism complementary to the function of the feedback if needed, as a preventive measure against core damage under a DEC.

A fast reactor core has a critical geometry for which moderation of fast neutrons generated by nuclear fission is not required in principle. The core reactivity is affected by the change in temperature of or in distribution of coolant and structural materials, which have the capability to moderate neutron, and fuel itself. Therefore, the safety design should prevent excessive power increase caused by re-criticality in a CDA.

The core of a commercial power-generating fast reactor generally has regions of positive void reactivity (interior) and negative void reactivity (the periphery); sodium voiding hardens the neutron spectrum, leading to positive void reactivity in the interior, while it facilitates neutron leakage, leading to negative void reactivity in the periphery. In a fast reactor core except very

small one, it is impossible to make local void reactivity of coolant negative in all core regions regardless of the type of coolant in principle. The overall sodium void reactivity can be positive for large cores, and can be reduced to zero or become negative for small cores because of larger neutron leakage. Fast reactor cores with a certain level of power can be designed to have zero or negative sodium void reactivity in total in sodium voiding by installing an upper sodium plenum or improving heterogeneousness of the core. In this case, however, local sodium void reactivity is still positive in some region in the core. With such reactivity characteristics taken into account, the core and safety measures should be carefully designed to ensure safety under any operational states and accident conditions.

Operational states and DBAs

Various reactivity coefficients, such as the Doppler coefficient, sodium coolant temperature coefficient and cladding temperature coefficient, exist for the respective core constituents in relation to changes in temperature and geometry. The core characteristics are commonly represented by an integral effect from these reactivity coefficients, e.g. the total power coefficient, the isothermal temperature coefficient and the power/flow coefficient. For operational states, these integral coefficients are required to have certain characteristics, such as a negative power coefficient, to allow stable operation and reliable control of the reactor.

In an SFR, its power is increased generally by withdrawing control rods in normal start-up operation. To achieve the stable control of power increased by positive reactivity insertion by the withdrawal, the total power coefficient should be negative under normal operation. In AOOs for which emergency reactor shutdown is not required, various factors can cause abnormal core conditions such as mismatch between the core output power and the coolant flow rate. In this case too, the inherent reactivity feedback should be worked to correct the mismatch.

Safety systems, such as a reactor protection system and a reactor shutdown system, have a major role to shut down the reactor in events beyond the range, in other words, within AOO and DBA domains for which emergency reactor shutdown is required. In this case, the core condition can be so remarkably changed that inherent reactivity feedback hardly corrects it.

To address these events, the safety design should be implemented to avoid exceeding the design limits set for each plant state, e.g., AOO, DBA, by using an appropriate combination of core and plant characteristics including core reactivity feedback and functions of safety systems. Therefore, quantitative requirements on each reactivity feedback characteristic or reactivity coefficient cannot be necessarily set, although the core should have inherent reactivity feedback characteristics as mentioned earlier.

The coolant temperature coefficient is defined as the rate of reactivity change due to the coolant density change with temperature. It is also related to the sodium void reactivity, as the liquid

phase turns into vapour phase at elevated temperatures (in excess of around 900C for a sodium coolant). In general, a core with a large sodium void reactivity in total has also a large coolant temperature coefficient. It is therefore important to take measures to rapidly shut down the core against an event involving rapid increase in coolant temperature so as to avoid exceeding the design limits such as the maximum temperature of coolant.

For the DBAs that cause increase in coolant temperature in the whole core, design limits should be set so that the maximum temperature of coolant does not reach its boiling point with an enough margin, and the safety design should meet the requirement. Other DBAs include an event that potentially involves local coolant voiding in the core. Such events should be identified and thoroughly examined so that the safety measures will be able to terminate them without core damage resulting from insertion of excessive positive reactivity or without propagating an abnormality from one fuel assembly to an unacceptable level. For example, a fuel pin of an SFR has a gas plenum to collect FP gas released from fuel pellets in normal operation. If a cladding tube incidentally fails in normal operation, the collected FP gas can be discharged into coolant channels. For such cases, the safety design should consider the effects of reactivity and the decrease of the coolability caused by the gas discharge.

Core damage prevention under DECs

As long as boiling of the sodium coolant is prevented, any effect of sodium void reactivity is not relevant. It is therefore important for an SFR to be designed to prevent the maximum coolant temperature from exceeding the boiling point so as to prevent core damage under a DEC. Although increase in coolant temperature can cause the reactivity to be positive, the importance of various reactivity coefficients comes into play during an ATWS event. To prevent coolant boiling and terminate an ATWS event by using inherent reactivity feedback of the core, the total power coefficient, isothermal temperature coefficient, and power/flow coefficient should all be sufficiently negative, and should respond in a timely manner to quickly achieve a sub-criticality during the event.

In a loss-of-flow transient, with failure of the reactor protection system (i.e. without scram), increase in coolant temperature can cause the reactivity to be quite positive. Therefore, the coolant temperature coefficient should be limited within a range where other reactivity feedback effects (such as thermal expansion of control rod drive shaft, core expansion) can compensate. If the effects of inherent reactivity feedback are not enough, a passive reactivity reduction mechanism or reactivity feedback mechanism should be installed to prevent coolant boiling in an ATWS.

Mitigation of consequences of core damage under DECs

A coolant phase change and a material relocation of a degraded core under a core damage condition can have significant reactivity consequences, both favourable and unfavourable, depending on design choices. When a core damage and material relocation occur, prompt criticality should be avoided in order to prevent large mechanical energy release. In particular, the maximum net reactivity during an initiating phase involving coolant boiling in the early stage of core damage should be limited below 1$. Positive reactivity effects, such as sodium boiling, should be limited considering e.g. spatial and temporal incoherence of the sodium voiding during the transient so that other negative reactivity components from the Doppler effect, fuel expansion and failed fuel dispersion can overcome them during the entire phase of the transient. As long as the maximum net reactivity below 1$, there are several design options with positive, zero or negative sodium void reactivity in total of the whole core under normal operation.

After an initiating phase, it is considered that the original core geometry will be lost, and the larger reactivity effects of molten fuel and cladding motions will dominate the overall reactivity. The molten fuel discharge from the degraded core has significant effect to provide strong negative reactivity. Design measures for that by using steel duct structures in the core are under investigation. In this context, the importance of having zero or negative sodium void reactivity is less certain. The situation of sodium in the core depends on the design and a postulated core damage condition. Evaluation of reactivity change in a process of core damage should also consider the reactivity change caused by boiling of sodium remained in the core.

REFERENCE

[1] GIF, SDC Phase 1 Report: “Safety Design Criteria for Generation IV Sodium-cooled Fast Reactor System (Rev.1)”, GIF SDC-TF/2017/01, Sep 30 (2017)

[2] GIF, GIF Annual Reports 2013 (2014)

[3] IAEA, “Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No.SSR-2/1 (Rev.1)”, IAEA, Vienna (2016)

[4] IAEA, “Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants”, TECDOC 1791 (2016)

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

[6] M. Ichimiya, T. Mizuno and S. Kotake, “A Next Generation Sodium-Cooled Fast Reactor Concept and its R&D Program”, Nuclear Engineering and Technology, Vol.39 No.3, pp.171-186 (2007)

[7] IAEA, “Absorber materials, control rods and designs of shutdown systems for advanced liquid metal fast reactors”, IAEA-TECDOC-884, Proceeding of a Technical Committee meeting held in Obninsk, Russian Federation, 3-7 July 1995, IAEA (1996)

[8] Burke, T.M., “Summary of FY 1997 related to JAPC-U.S.DOE contract study on improvement of core safety -- study on GEM (III)”, HNF-2195-VA, Prepared for USDOE by Fluor Daniel Hanford, Inc. (1998)

[9] OECD/NEA and Generation IV International Forum, “Technology Roadmap Update for Generation IV Nuclear Energy Systems”, January (2014)

GLOSSARY

#accident conditions

Deviations from normal operation that are less frequent and more severe than anticipated operational occurrences. Accident conditions comprise design basis accidents and design extension conditions.
[from the DEFINITIONS in the IAEA SSR 2/1 (Rev.1, 2016)]

#anticipated operational occurrence

A deviation of an operational process from normal operation that is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions.
[from IAEA Safety Glossary (2016 Edition)]

#beyond design basis accident

Postulated accident with accident conditions more severe than those of a design basis accident.
[from IAEA Safety Glossary (2016)]

#cliff edge effect

In a nuclear power plant, a cliff edge effect 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 IAEA Safety Glossary (2016)]

#confinement function

Prevention or control of releases of radioactive material to the environment in operation or in accidents.
[from IAEA Safety Glossary (2016)]

#design basis accident

A postulated accident leading to accident conditions for which a facility is designed in accordance with established design criteria and conservative methodology, and for which releases of radioactive material are kept within acceptable limits.
[from IAEA Safety Glossary (2016)]

#design extension conditions

Postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions comprise conditions in events without significant fuel degradation and conditions in events with melting of the reactor core.
[from IAEA Safety Glossary (2016)]

#diversity

The presence of two or more independent (redundant) systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure.

Examples of such attributes are: different operating conditions, different working principles or different design teams (which provide functional diversity), and different sizes of equipment, different manufacturers, and types of equipment (which provide diversity of equipment) that use different physical methods (which provide physical diversity).

functional diversity. Application of diversity at the level of functions in applications in process engineering (e.g. for the actuation of a trip on both a pressure limit and a temperature limit).

[from IAEA Safety Glossary (2016)]

#fast reactor

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

#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.

#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 pipe is placed outside of the coolant pipe where sodium coolant flows.
It is constructed to maintain sodium coolant level for reactor cooling in case of sodium leakage for the loop-type SFR.

#guard vessel

Guard vessel is placed outside the reactor vessel containing the sodium coolant.
It is 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 operating 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 (2016)]

#normal operation

Operation within specified operational limits and conditions. For a nuclear power plant, this includes start up, power operation, shutting down, shutdown, maintenance, testing and refuelling.
[from IAEA Safety Glossary (2016)]

#site personnel

All persons working in the site area of an authorized facility, either permanently or temporarily.
[from IAEA Safety Glossary (2016)]

#operational states

States defined under normal operation and anticipated operational occurrences.
[from IAEA Safety Glossary (2016)]

#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”]

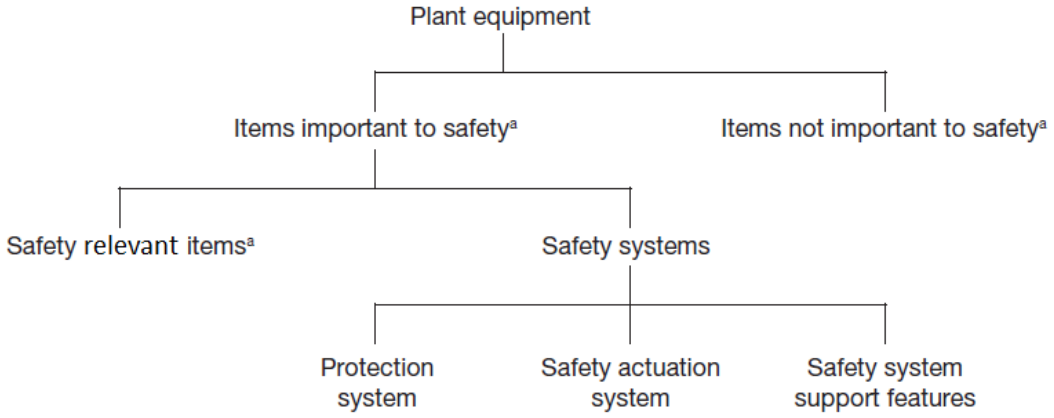
#passive safety system

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.

#physical separation

Separation by geometry (distance, orientation, etc.), by appropriate barriers, or by a combination thereof.
[from IAEA Safety Glossary (2016)]

#plant equipment



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

[Based on IAEA Safety Glossary (2016) with replacing "Safety related items" by "Safety relevant items"]

#plant states (considered in design)

Operational States		Accident conditions		
			Design extension conditions	
Normal operation	Anticipated operational occurrences	Design basis accidents	Without significant fuel degradation	With core melting

[from the DEFINITIONS in IAEA SSR 2/1 (Rev.1) (2016)]

#practically eliminated

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

[from FOOTNOTES in IAEA SSR 2/1 (2016)]

#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.

#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 (2016)]

#reactor coolant boundary

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

#reactor coolant systems

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

#reactor cover gas boundary

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

#redundancy

Provision of alternative (identical or diverse) structures, systems and components, so that any single structure, system or component can perform the required function regardless of the state of operation or failure of any other.
[from IAEA Safety Glossary (2016)]

#safe state

Plant state, following an anticipated operational occurrence or accident condition, in which the reactor is subcritical and the main safety functions can be ensured and maintained stable for a long time.
[from IAEA Safety Glossary (2016)]

#safety actuation system

The collection of equipment required to accomplish the necessary safety actions when initiated by the protection system.
[from IAEA Safety Glossary (2016)]

#safety feature for design extension conditions

Item that is designed to perform a safety function for or that has a safety function for design extension conditions.
[from IAEA Safety Glossary (2016)]

#safety group

The assembly of equipment designated to perform all actions required for a particular initiating event to ensure that the limits specified in the design basis for anticipated operational occurrences and design basis accidents are not exceeded.
[from IAEA Safety Glossary (2016)]

#safety relevant item

An item important to safety that is not part of a safety system.
[from “safety related item” in IAEA Safety Glossary (2016)]

#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 (2016)]

#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 (2016)]

#safety system settings

Setting for 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 IAEA Safety Glossary (2016)]

#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 (2016)]

#secondary coolant system (or intermediate coolant system)

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

#single failure

A failure which results in the loss of capability of a single system or component to perform its intended safety function(s), and any consequential failure(s) which 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 Safety Glossary (2016)]

#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

(A) Illustration of an Approach to Identify Situations to be Practically Eliminated Situations by using Objective Provision Trees (OPTs)

(B) Examples of Initiating Events for AOOs and DBAs

(C) Members of Safety Design Criteria Task Force (Phase II)

Appendix (A): Illustration of an Approach to Identify Situations to be Practically Eliminated by using Objective Provision Trees (OPTs)

An approach to identify candidates for situations to be practically eliminated is the use of Objective Provision Trees (OPTs) [A-1]. This involves analysing failure modes of the containment, challenging phenomena and their causes. Examples of OPTs for the JSFR containment, which is a steel-plate reinforced concrete containment vessel (SCCV) containing the primary coolant system, guard vessels and guard pipes [A-2], are shown in Figures A-1 to A-5.

Implementing measures for each individual situation will be required. Situations, which cannot be managed by the design at acceptable conditions, are considered as candidates for situations to be practically eliminated. Design modification should be considered to cope with them. All initiators that could lead to situations that need to be practically eliminated need to be identified and proper design measures should be provided to prevent such situations to arise. Mitigation of consequences of core damage is included in DEC “mitigation of core damage”, hence the mitigation situations, for which such measures should be reasonably implemented, are not considered for practical elimination.

Challenging Phenomena Generating Mechanical Loads

Challenging phenomena and their causes in the “mechanical loads” domain are shown in Figures A-2 and A-5 for JSFR. These situations might cause containment failures due to direct heating of the containment atmosphere by dispersed molten fuel, large sodium spray fire, deflagration or detonation of hydrogen, and molten fuel-coolant interaction (vapour explosion). Energetic fuel dispersion should be prevented. Thus, design measures to prevent the causes of severe reactivity insertions, e.g., energetic core damage due to unprotected transients, should be provided. Although mitigation measures for the unprotected transients are provided as DEC “mitigation of core damage”, severe reactivity insertion due to extreme initiating events, such as large gas flow through the core, large-scale core compaction and collapse of the core support structures, needs to be practically eliminated. Inerting of the containment atmosphere is a possible design measure to prevent or mitigate pressure loads from a large sodium spray fire or hydrogen explosions. In order to avert hydrogen generation, design measures for prevention of a reactor vessel (RV) melt-through or failure, and prevention of sodium and concrete contact, are required.

Challenging Phenomena Generating Thermal Loads

Challenging phenomena and their causes in the “thermal loads” domain are shown in Figures A-3 and A-5 for JSFR. These situations might cause a containment failure due to heating of the containment by a sodium pool fire, sodium vapour and gaseous fission products, due to floor concrete erosion from sodium-concrete reaction, and due to debris-concrete interaction or containment wall heating by a connecting sodium pool. Significant loads, which are caused by a RV melt-through due to complete loss of heat removal and core uncovering, and which cannot be reasonably managed by original design, should be practically eliminated by design modifications. It should be possible to design the containment to withstand other loads, i.e. those generated by a sodium pool fire and gaseous fission products.

Containment Bypass

Challenging phenomena and their causes in the “bypass” domain are shown in Figure A-4 for JSFR. These situations might cause a containment boundary failure due to thermal loads or a primary/secondary boundary failure due to mechanical loads.

Summary

Based on the above, the following candidates for situations to be practically eliminated in JSFR are identified:

A) Abnormal reactivity insertion leading to prompt criticality (large gas flow through the core, large-scale core compaction and collapse of the core support structures).
B) Complete loss of heat removal
C) Core uncovering

REFERENCE

[A-1] An Integrated Safety Assessment Methodology (ISAM) for Generation IV Nuclear Systems, June 2011

[A-2] H. Hara, et. al., “Conceptual Design Study of JSFR (4) – Reactor Building Layout –“, FR09, 08-13P, 2009

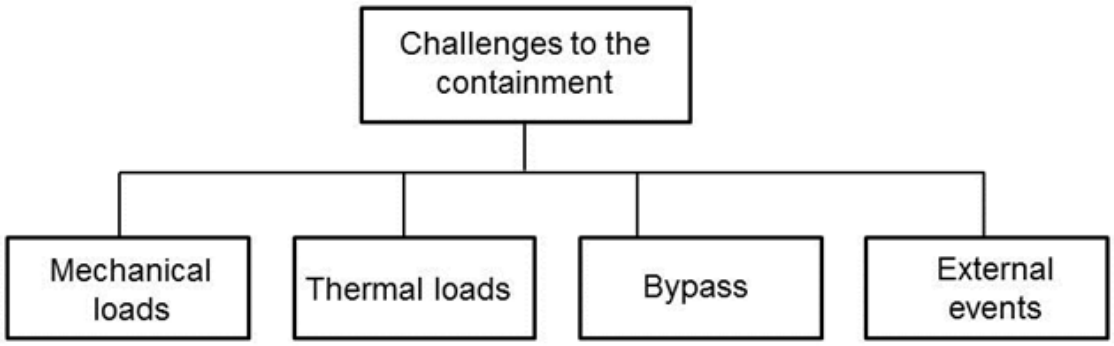


Figure A-1 OPT for consideration of situations practically eliminated
(Example for JSFR)

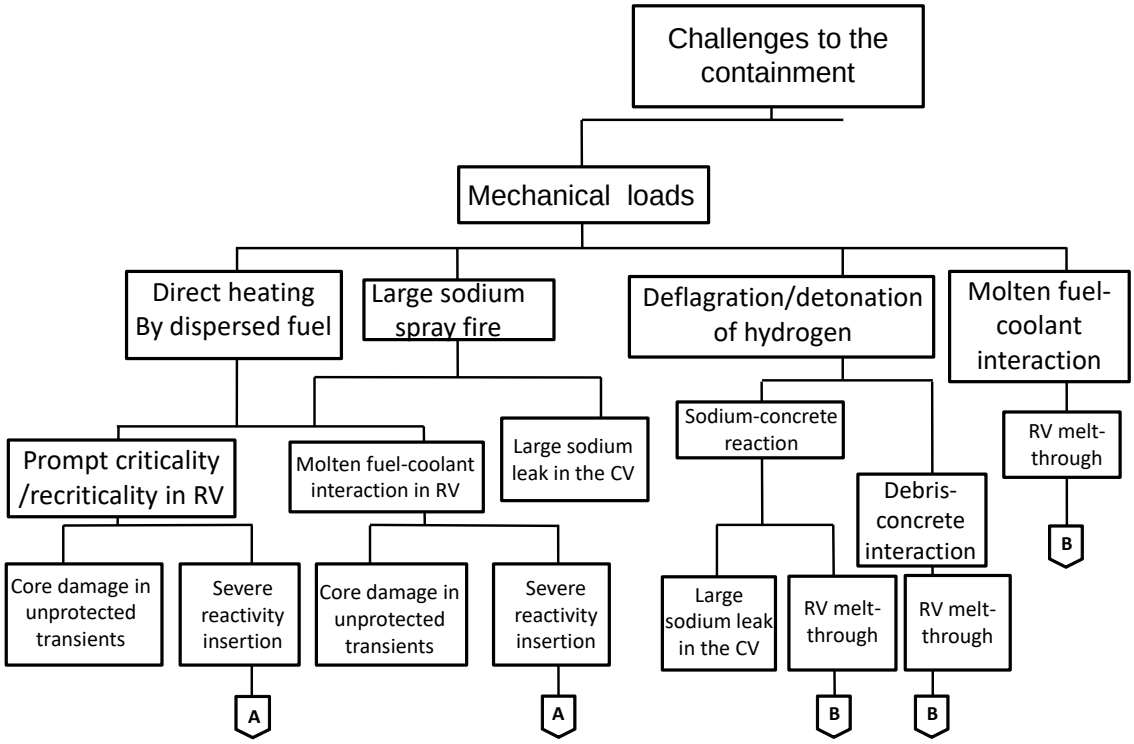


Figure A-2 OPT for consideration of situations that need to be practically eliminated by the design
(Example for JSFR)

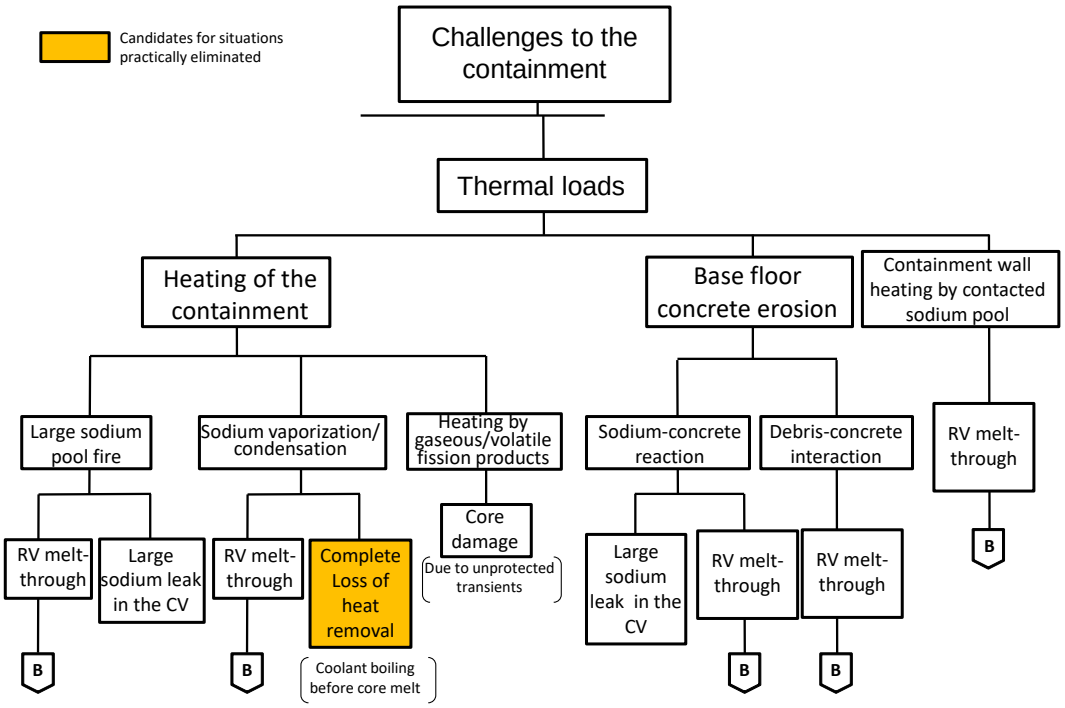


Figure A-3 OPT for consideration of situations that need to be practically eliminated by the design

(Example for JSFR)

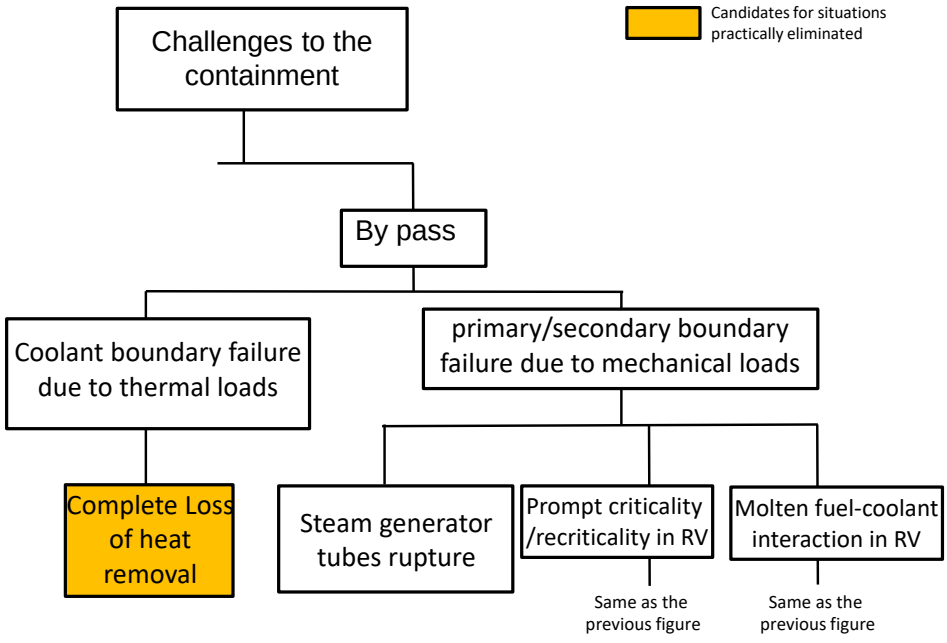


Figure A-4 OPT for consideration of situations that need to be practically eliminated by the design

(Example for JSFR)

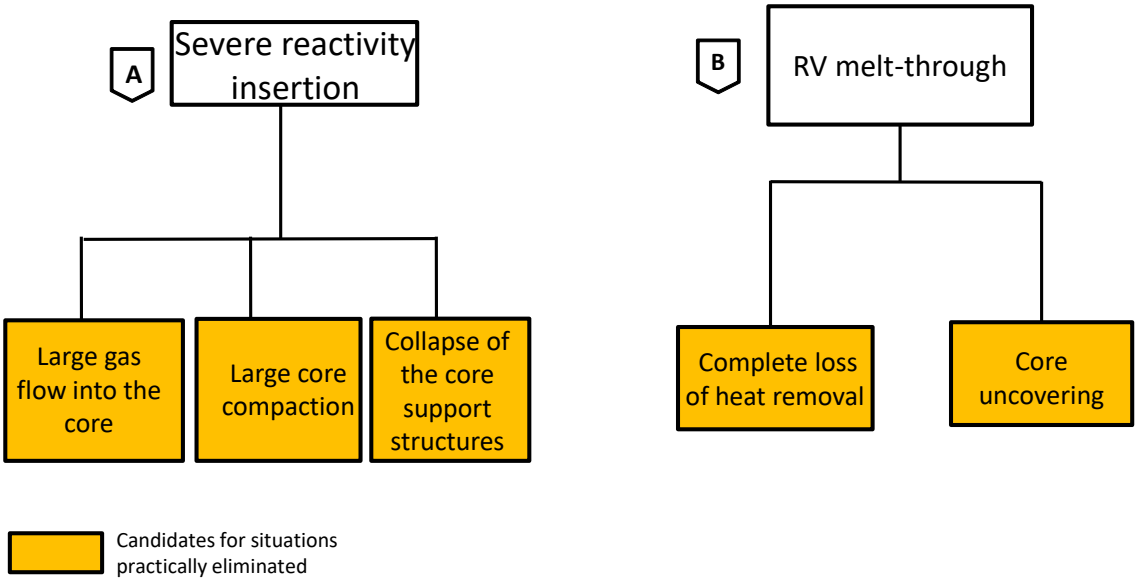


Figure A-5 OPT for consideration of situations that need to be practically eliminated by the design

(Example for JSFR)

Appendix (B): Examples of Initiating Events for AOOs and DBAs

Using the Objective Provision Tree (OPT) method, presented in the Integrated Safety Assessment Methodology (ISAM) [B-1] and proposed by the GIF Risk Safety Working Group (RSWG), the challenges and mechanisms[B1] for preventing core degradation and securing the containment function are identified for a typical Sodium-cooled Fast Reactor (SFR) design. Consequently, typical initiating events and design limits for AOOs and DBAs (limited to the reactor; fuel handling and waste treatment facilities are not considered) are identified as shown in Table B-1.

REFERENCE

[B-1] An Integrated Safety Assessment Methodology (ISAM) for Generation IV Nuclear Systems, June 2011

[B1] *Challenges: generalized mechanisms, processes or circumstances (conditions) that may have an impact on the intended performance of safety functions. Challenges are caused by a set of mechanisms having consequences that are similar in nature.*
Mechanisms: specific reasons, processes or situations whose consequences might create challenges to the performance of safety functions.

Table B-1　Example of objective provision tree for AOO and DBA

Objective	Safety function	Criteria	Challenge	Mechanism	Typical initiating events	
					AOO	DBA
”Control of abnormal operation and detection of failures” / “Control of accidents related to AOO and DBA”	Reactivity control	Shut down reactor, maintain core cooling to ensure barriers. For AOO, fuel cladding tube, reactor coolant and cover gas boundary should be kept their barrier function. For DBA, core should be coolable. Reactor coolant and cover gas boundary should be kept their barrier function. [Typical index] ・max. fuel temp. ・max. cladding temp. ・max. coolant temp. ・max. coolant boundary temp.	Imbalance of core power and cooling	Core power increase	Erroneous withdrawal of control rod (normal speed), control rod drop, control rod withdrawal due to erroneous pump operation during fuel handling	Erroneous rapid withdrawal of control rod, gas bubble passage
				Primary coolant flow decrease	Loss of external power, primary pump trip	One primary pump seizure, primary coolant pipe failure (In-vessel pipe for pool type)
				Abnormality in heat sink	Secondary pump trip, feedwater pump trip, loss of load, small leak of steam generator heat exchanger tube	One secondary pump seizure, secondary coolant pipe breach, main feedwater/ steam generator pipe rupture, heat exchanger pipe rupture on steam generator
				Local abnormality in subassembly	Stochastic fuel pin failure	Sub channel blockage
	Core heat removal		Abnormality in reactor coolant level	Reactor coolant boundary failure	Leakage of the intermediate heat exchanger	Primary coolant pipe failure (loop type)
			Abnormality in decay heat removal	Abnormality in coolant flow path	—	Primary coolant pipe failure (loop type)
				Abnormality in DHRS coolant flow	—	DHRS secondary sodium leak
				Abnormality in air flow	Air flow regulator failure (single failure of active component	

Objective	Safety function	Criteria	Challenge	Mechanism	Typical initiating events	
					AOO	DBA
”Control of abnormal operation and detection of failures” / “Control of accidents related to AOO and DBA”	Containment of radioactive materials	Maintain containment function [Typical index] ・Containment ambient temp. ・Containment ambient pressure Limit off-site radioactive consequence should be under the acceptable limit [Typical index] ・Public radiation exposure dose	Radioactive material release into containment	Primary coolant leak	—	Primary coolant pipe failure (loop type)
				Primary argon gas leak	—	Pipe failure of primary cover gas system.
			Mechanical loads on the containment	Sodium combustion (large spray fire)	—	Primary coolant pipe failure (loop type), secondary coolant pipe failure (inside the containment).
			Thermal loads on the containment	Sodium combustion (pool fire/ small spray fire)	—	Primary coolant pipe failure (loop type), secondary coolant pipe failure (inside the containment).
			Containment bypass	Primary/secondary boundary failure	—	Sodium-water reaction in steam generator

*This table provides examples not intended to be comprehensive and not implied to be generically applicable to all SFRs. It should be established in the frame of detailed design and safety analysis.

Appendix (C): Members of Safety Design Criteria Task Force (Phase II)

The contributors of this report (members of SDC-TF Phase II, including the past members) were:

Haileyesus Tsige Tamirat	JRC, EURATOM	
Luca Ammirabile	JRC, EURATOM	
Javier Yllera	IAEA	
Hongtao Qian	CIAE, China	
Yizhe Liu	CIAE, China	
Paul Gauthe	CEA, France	
Philippe Dufour	CEA, France	
Shigenobu Kubo	JAEA, Japan	(Chair, from 2018)
Ryodai Nakai	JAEA, Japan	(Chair, until 2018)
Yasushi Okano	JAEA, Japan	
Dohee Hahn	KAERI, Republic of KOREA	
Jinwook Chang	KAERI, Republic of KOREA	
Taeho Lee	KAERI, Republic of KOREA	
Iurii Ashurko	IPPE, Russian Federation	
George Flanagan	ORNL, United States of America	
Roald Wigeland	INL, United States of America	
Tanju Sofu	ANL, United States of America	(Co-chair)