

# Applicability of Design Safety Requirements to Small Modular Reactor Technologies Intended for Near Term Deployment

*Light Water Reactors*

*High Temperature Gas Cooled Reactors*



**IAEA**

International Atomic Energy Agency

# IAEA SAFETY STANDARDS AND RELATED PUBLICATIONS

## IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish or adopt standards of safety for protection of health and minimization of danger to life and property, and to provide for the application of these standards.

The publications by means of which the IAEA establishes standards are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety. The publication categories in the series are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides**.

Information on the IAEA's safety standards programme is available on the IAEA Internet site

<http://www-ns.iaea.org/standards/>

The site provides the texts in English of published and draft safety standards. The texts of safety standards issued in Arabic, Chinese, French, Russian and Spanish, the IAEA Safety Glossary and a status report for safety standards under development are also available. For further information, please contact the IAEA at: Vienna International Centre, PO Box 100, 1400 Vienna, Austria.

All users of IAEA safety standards are invited to inform the IAEA of experience in their use (e.g. as a basis for national regulations, for safety reviews and for training courses) for the purpose of ensuring that they continue to meet users' needs. Information may be provided via the IAEA Internet site or by post, as above, or by email to [Official.Mail@iaea.org](mailto:Official.Mail@iaea.org).

## RELATED PUBLICATIONS

The IAEA provides for the application of the standards and, under the terms of Articles III and VIII.C of its Statute, makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety in nuclear activities are issued as **Safety Reports**, which provide practical examples and detailed methods that can be used in support of the safety standards.

Other safety related IAEA publications are issued as **Emergency Preparedness and Response** publications, **Radiological Assessment Reports**, the International Nuclear Safety Group's **INSAG Reports**, **Technical Reports** and **TECDOCs**. The IAEA also issues reports on radiological accidents, training manuals and practical manuals, and other special safety related publications.

Security related publications are issued in the **IAEA Nuclear Security Series**.

The **IAEA Nuclear Energy Series** comprises informational publications to encourage and assist research on, and the development and practical application of, nuclear energy for peaceful purposes. It includes reports and guides on the status of and advances in technology, and on experience, good practices and practical examples in the areas of nuclear power, the nuclear fuel cycle, radioactive waste management and decommissioning.

APPLICABILITY OF DESIGN SAFETY  
REQUIREMENTS TO SMALL MODULAR  
REACTOR TECHNOLOGIES INTENDED  
FOR NEAR TERM DEPLOYMENT

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN	GEORGIA	OMAN
ALBANIA	GERMANY	PAKISTAN
ALGERIA	GHANA	PALAU
ANGOLA	GREECE	PANAMA
ANTIGUA AND BARBUDA	GRENADA	PAPUA NEW GUINEA
ARGENTINA	GUATEMALA	PARAGUAY
ARMENIA	GUYANA	PERU
AUSTRALIA	HAITI	PHILIPPINES
AUSTRIA	HOLY SEE	POLAND
AZERBAIJAN	HONDURAS	PORTUGAL
BAHAMAS	HUNGARY	QATAR
BAHRAIN	ICELAND	REPUBLIC OF MOLDOVA
BANGLADESH	INDIA	ROMANIA
BARBADOS	INDONESIA	RUSSIAN FEDERATION
BELARUS	IRAN, ISLAMIC REPUBLIC OF	RWANDA
BELGIUM	IRAQ	SAINT LUCIA
BELIZE	IRELAND	SAINT VINCENT AND THE GRENADINES
BENIN	ISRAEL	SAN MARINO
BOLIVIA, PLURINATIONAL STATE OF	ITALY	SAUDI ARABIA
BOSNIA AND HERZEGOVINA	JAMAICA	SENEGAL
BOTSWANA	JAPAN	SERBIA
BRAZIL	JORDAN	SEYCHELLES
BRUNEI DARUSSALAM	KAZAKHSTAN	SIERRA LEONE
BULGARIA	KENYA	SINGAPORE
BURKINA FASO	KOREA, REPUBLIC OF	SLOVAKIA
BURUNDI	KUWAIT	SLOVENIA
CAMBODIA	KYRGYZSTAN	SOUTH AFRICA
CAMEROON	LAO PEOPLE'S DEMOCRATIC REPUBLIC	SPAIN
CANADA	LATVIA	SRI LANKA
CENTRAL AFRICAN REPUBLIC	LEBANON	SUDAN
CHAD	LESOTHO	SWEDEN
CHILE	LIBERIA	SWITZERLAND
CHINA	LIBYA	SYRIAN ARAB REPUBLIC
COLOMBIA	LIECHTENSTEIN	TAJIKISTAN
COMOROS	LITHUANIA	THAILAND
CONGO	LUXEMBOURG	TOGO
COSTA RICA	MADAGASCAR	TRINIDAD AND TOBAGO
CÔTE D'IVOIRE	MALAWI	TUNISIA
CROATIA	MALAYSIA	TURKEY
CUBA	MALI	TURKMENISTAN
CYPRUS	MALTA	UGANDA
CZECH REPUBLIC	MARSHALL ISLANDS	UKRAINE
DEMOCRATIC REPUBLIC OF THE CONGO	MAURITANIA	UNITED ARAB EMIRATES
DENMARK	MAURITIUS	UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
DJIBOUTI	MEXICO	UNITED REPUBLIC OF TANZANIA
DOMINICA	MONACO	UNITED STATES OF AMERICA
DOMINICAN REPUBLIC	MONGOLIA	URUGUAY
ECUADOR	MONTENEGRO	UZBEKISTAN
EGYPT	MOROCCO	VANUATU
EL SALVADOR	MOZAMBIQUE	VENEZUELA, BOLIVARIAN REPUBLIC OF
ERITREA	MYANMAR	VIET NAM
ESTONIA	NAMIBIA	YEMEN
ESWATINI	NEPAL	ZAMBIA
ETHIOPIA	NETHERLANDS	ZIMBABWE
FIJI	NEW ZEALAND	
FINLAND	NICARAGUA	
FRANCE	NIGER	
GABON	NIGERIA	
	NORTH MACEDONIA	
	NORWAY	

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world".

IAEA-TECDOC-1936

APPLICABILITY OF DESIGN SAFETY  
REQUIREMENTS TO SMALL MODULAR  
REACTOR TECHNOLOGIES INTENDED  
FOR NEAR TERM DEPLOYMENT

LIGHT WATER REACTORS  
HIGH TEMPERATURE GAS COOLED REACTORS

INTERNATIONAL ATOMIC ENERGY AGENCY  
VIENNA, 2020

## COPYRIGHT NOTICE

All IAEA scientific and technical publications are protected by the terms of the Universal Copyright Convention as adopted in 1952 (Berne) and as revised in 1972 (Paris). The copyright has since been extended by the World Intellectual Property Organization (Geneva) to include electronic and virtual intellectual property. Permission to use whole or parts of texts contained in IAEA publications in printed or electronic form must be obtained and is usually subject to royalty agreements. Proposals for non-commercial reproductions and translations are welcomed and considered on a case-by-case basis. Enquiries should be addressed to the IAEA Publishing Section at:

Marketing and Sales Unit, Publishing Section  
International Atomic Energy Agency  
Vienna International Centre  
PO Box 100  
1400 Vienna, Austria  
fax: +43 1 26007 22529  
tel.: +43 1 2600 22417  
email: [sales.publications@iaea.org](mailto:sales.publications@iaea.org)  
[www.iaea.org/publications](http://www.iaea.org/publications)

For further information on this publication, please contact:

Safety Assessment Section  
International Atomic Energy Agency  
Vienna International Centre  
PO Box 100  
1400 Vienna, Austria  
Email: [Official.Mail@iaea.org](mailto:Official.Mail@iaea.org)

© IAEA, 2020  
Printed by the IAEA in Austria  
December 2020

### IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.  
Title: Applicability of design safety requirements to small modular reactor technologies intended for near term deployment / International Atomic Energy Agency.  
Description: Vienna : International Atomic Energy Agency, 2020. | Series: IAEA TECDOC series, ISSN 1011-4289 ; no. 1936 | Includes bibliographical references.  
Identifiers: IAEAL 20-01375 | ISBN 978-92-0-130820-7 (paperback : alk. paper) | ISBN 978-92-0-130920-4 (pdf)  
Subjects: LCSH: Nuclear power plants — Safety measures. | Nuclear reactors — Safety measures. | Nuclear reactors — Design and construction. | Design. | Nuclear reactors.

## FOREWORD

Over the past several years, IAEA Member States have expressed an interest in small and medium sized or modular reactors (SMRs). Many types of SMR designs are being developed in several Member States based on a range of reactor technologies, including light water reactors, high temperature gas cooled reactors, fast neutron reactors and molten salt reactors. In most cases, these new designs are in the initial stages, and only some are at an advanced stage or are under construction.

Among the SMR designs using light water reactor technology, some are intended for land based deployment and others for marine propulsion (e.g. icebreakers) or for floating nuclear power plants. This publication relates only to SMR designs to be deployed as land based stationary nuclear power plants.

The IAEA safety requirements on the design of nuclear power plants are applicable primarily to land based stationary plants with water cooled reactors designed for electricity generation or for applications such as district heating or desalination. The applicability of these requirements to other reactor technologies and design characteristics, such as SMRs, needs consideration of all factors unique to the specific design. Taking into account the relevant activities being implemented worldwide regarding SMRs, IAEA Member States requested additional information on the applicability of the IAEA safety standards on design safety and safety assessment to SMR technologies intended for near term deployment.

In this publication, the applicability to SMRs of the requirements for nuclear power plants established in IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design, is considered. Given the status of development of the different SMR designs, this publication covers those SMR technologies currently intended for near term deployment, namely light water SMRs and high temperature gas cooled SMRs.

The IAEA would like to thank all the experts who contributed to the identification, review and enhancement of the insights included in this publication, in particular to those who attended the consultancy meetings organized for its drafting and review. The IAEA officer responsible for this publication was P. Villalibre of the Division of Nuclear Installation Safety.

#### *EDITORIAL NOTE*

*This publication has been prepared from the original material as submitted by the contributors and has not been edited by the editorial staff of the IAEA. The views expressed remain the responsibility of the contributors and do not necessarily represent the views of the IAEA or its Member States.*

*Neither the IAEA nor its Member States assume any responsibility for consequences which may arise from the use of this publication. This publication does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.*

*The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.*

*The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.*

*The authors are responsible for having obtained the necessary permission for the IAEA to reproduce, translate or use material from sources already protected by copyrights.*

*The IAEA has no responsibility for the persistence or accuracy of URLs for external or third party Internet web sites referred to in this publication and does not guarantee that any content on such web sites is, or will remain, accurate or appropriate.*

## CONTENTS

1.	INTRODUCTION .....	1
1.1.	BACKGROUND .....	1
1.2.	OBJECTIVE .....	2
1.3.	SCOPE.....	2
1.4.	STRUCTURE .....	2
2.	DESIGN CHARACTERISTICS AND FUNDAMENTAL TECHNICAL BASIS FOR THE CONSIDERATIONS ON APPLICABILITY.....	3
2.1.	GENERAL CONSIDERATIONS .....	3
2.2.	DESIGN CHARACTERISTICS AND SAFETY CONSIDERATIONS FOR LW-SMRS .....	4
2.3.	DESIGN CHARACTERISTICS AND SAFETY CONSIDERATIONS FOR HTG-SMRS .....	6
3.	APPROACH TO DETERMINE THE APPLICABILITY OF THE DESIGN SAFETY REQUIREMENTS .....	9
4.	SUMMARY RESULTS AND CONCLUSION .....	10
APPENDIX I.	APPLICABILITY OF DESIGN SAFETY REQUIREMENTS TO LW-SMRS .....	19
APPENDIX II.	APPLICABILITY OF DESIGN SAFETY REQUIREMENTS TO HTG-SMRS .....	65
REFERENCES.....		133
ANNEX I.	APPLICABILITY OF DESIGN SAFETY REQUIREMENTS RELATED TO THE REACTOR CONTAINMENT TO HTG-SMRS.....	135
CONTRIBUTORS TO DRAFTING AND REVIEW .....		143



# 1. INTRODUCTION

## 1.1. BACKGROUND

Over the past several years an increasing number of IAEA Member States has expressed relevant interest in small and medium sized or modular reactors (SMRs). In accordance with the IAEA booklet *Advances in Small Modular Reactor Technology Developments*, a Supplement to IAEA Advanced Reactors Information System (ARIS) [1], at present, there are at least 50 SMR designs for which research and development work has been and continues to be undertaken. SMRs are new generation reactors designed to generate electric power up to 300 MW. Components and systems of SMRs can be factory fabricated and then transported as modules to the sites for installation as demand arises. Some SMRs are in advanced stages of construction – including the CAREM (a 30 MW(e) integral pressurized light water reactor in Argentina) and the HTR-PM (a 211 MW(e) high temperature gas cooled reactor undergoing commissioning in China) – while others are either subject to regulatory assessments, such as the NuScale in the United States of America and Canada, or are in the various stages of development, including the GTHTR300 in Japan, the SMART in the Republic of Korea and the ACP100 in China.

The technological characteristics of the different SMR designs represent significant changes compared to the large nuclear power plants (NPPs) currently deployed. Consequently, Member States are establishing new specific design safety requirements or applying their current design safety requirements to the SMR designs.

The IAEA safety requirements on the design of NPPs are primarily applicable to land based stationary NPPs with water cooled reactors designed for electricity generation or for other heat production applications (such as district heating or desalination), and the applicability of these requirements to the different SMR technologies, and particularly to specific types of SMR designs, necessitates expert judgement. Taking into account the SMR licensing processes that are being implemented in several Member States, the IAEA facilitated discussions about the applicability of the design safety requirements (IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), *Safety of Nuclear Power Plants: Design*) [2], to SMR technologies intended for near-term deployment, i.e. light water reactors (LW-SMRs) and high temperature gas cooled reactors (HTG-SMRs).

A study on current views of SMR designer organizations about the applicability of the requirements established in SSR-2/1 (Rev. 1) [2] to SMR technologies intended for near-term deployment was organized by the IAEA, and a team of international experts participated in the study. The output of the study was used as a starting point for the discussions made by the contributors to this TECDOC, that included representatives from regulatory bodies, technical and scientific support organizations, SMR design organizations and operating organizations.

The results of the discussions are provided in this TECDOC as considerations for the applicability of the requirements of SSR-2/1 (Rev. 1). These results represent the views of the contributors and cannot be considered as IAEA guidance or recommendations. Regarding the design safety requirements analysed in the present publication, it has to be noted that the establishment of safety requirements at the IAEA is implemented through a formal process that includes several reviews by representatives from Member States and by specialists in IAEA safety standards. Such a review and approval process is not applied to the preparation of TECDOCs and, therefore, was not applied to the present publication.

## 1.2. OBJECTIVE

The main objective of this publication is to provide practical information on the applicability of the requirements established in SSR-2/1 (Rev. 1) [2] to SMR technologies having reactor designs intended for near-term deployment, i.e. LW-SMRs and HTG-SMRs.

The publication is intended for use by organizations involved in SMR activities such as design, safety assessment, manufacturing, construction, operation and decommissioning, as well as by regulatory bodies and technical and scientific support organizations.

## 1.3. SCOPE

This publication focuses on the applicability of the IAEA design safety requirements established in SSR-2/1 (Rev. 1) [2] to the SMR reactor technologies intended for land-based stationary deployment in the near-term, i. e. LW-SMRs and HTG-SMRs.

The assessment of the applicability of the safety requirements has been conducted based on their significance for safety and by applying engineering judgement, taking into account the state of the art knowledge, expertise and feedback from current practices in IAEA Member States. The specific characteristics of each of the SMR technologies considered in this publication, representing differences compared to the designs of the large reactors that currently are under construction, have been used as basis for the assessment. Examples of these characteristics are the way how the fundamental safety function on confinement of radioactive material is fulfilled in HTG-SMRs and the use of multi-module units.

The assessment identifies requirements established in SSR-2/1 (Rev. 1) [2] for which modifications of the existing wording or different interpretations are necessary for SMRs, together with the corresponding justifications. The assessment also includes suggestions for the introduction of new requirements applicable to SMRs, as necessary.

## 1.4. STRUCTURE

This publication comprises four sections, two appendices and one annex. Section 2 describes the main design characteristics of each of the SMR technologies considered in this publication and the fundamental technical basis that was taken into account in the considerations for the applicability of the design safety requirements established in SSR-2/1 (Rev. 1) [2] relating to each SMR technology. Section 3 summarizes the approach used to determine the applicability of the design safety requirements and the format used to present the results. A summary of the considerations on applicability is provided in Section 4, together with a conclusion on the suggested use of the results.

A copy of SSR-2/1 (Rev. 1) [2] is used in Appendix I to incorporate considerations on the applicability of the safety requirements to LW-SMRs. The same approach is used in Appendix II to incorporate considerations on the applicability of the safety requirements to HTG-SMRs. A table including relevant aspects of an approach used to determine the applicability of the design safety requirements related to containment system and containment structure to high temperature gas cooled SMRs is provided in the Annex.

## 2. DESIGN CHARACTERISTICS AND FUNDAMENTAL TECHNICAL BASIS FOR THE CONSIDERATIONS ON APPLICABILITY

### 2.1. GENERAL CONSIDERATIONS

Most SMRs designs evolved from those used in existing NPPs. Most of the design safety requirements of SSR-2/1 (Rev.1) [2] can be applied without modifications or interpretations to different types of SMR reactor design, in particular to those covered by this publication, whereas other requirements require expert engineering judgement. Design safety requirements that can be directly applied include those related to management of safety in design, some of the principal technical requirements (e.g. those regarding fundamental safety functions, radiation protection in design, application of defence in depth and proven engineering practices) and some of the general requirements on plant design (e.g. engineering design rules and single failure criterion).

Common areas that need specific attention in the considerations on applicability of the design safety requirements to both LW-SMRs and HTG-SMRs are discussed in the sections that follow. Corresponding insights are intended to be consistent with the justifications of the changes or interpretations to the requirements suggested in the text boxes provided in Appendix I and Appendix II, as applicable.

#### *a) Modular design*

LW-SMRs and HTG-SMRs can be deployed in units that consist of multiple reactor modules (referred to as ‘multi-module units’); see ‘Definitions’ in the appendices. In some of the designs available, multiple reactor modules share some safety systems, safety features for design extension conditions, or supporting services. The potential for design approaches using multiple modules introduces new safety considerations in areas such as common-cause failures, internal hazards and human factors (e.g. shared control room design). For multi-module units, it is important to ensure that the safety of the NPP is not negatively impacted by the adoption of a modular design, and this provides the driving force for the formulation of changes to the safety requirements established in SSR-2/1 (Rev. 1).

#### *b) Use of passive safety features*

In general terms, both LW-SMR and HTG-SMR designs use passive safety features to a greater extent than large reactors, which do not need external energy or driving forces and are based on natural phenomena, such as gravity-driven and natural circulation (i.e. buoyancy force). Relatively small core size and power are favourable features which enable introduction of passive systems, such as buoyancy driven cooling or gravity driven injection. The introduction of passive safety features in the design has potential benefits for safety, for availability and for reliability of performing the safety functions assigned to the systems. These benefits may increase the ‘grace period’ for operator actions and slow down the progression of accidents. Passive safety features may also simplify the design and operation of the facility. However, the effectiveness of these features needs to be adequately demonstrated. Common issues in this regard include:

- Application of design principles, such as redundancy, diversity and single failure criterion;
- Reliability assessment;

- Relatively small driving forces, which result in more complex phenomena and higher uncertainties in experiment and analysis;
- Use of sophisticated safety analysis tools;
- Use of extensive research to confirm the full range of operation;
- Need for use of active systems for initiation, actuation or logic sensing.

*c) Low thermal power and source terms*

The power of both LW-SMRs and HTG-SMRs is typically considered to be limited to 300 MW(e) per module. Adopting a lower power output may improve the ability of the NPP to rely on passive safety features (as described in 2.1 b). The potential radiological source term that could be released in accident conditions is also reduced.

*d) Coupling with heat utilization facilities*

SMRs are normally designed with the flexibility to allow coupling to a heat utilization facility instead of, or in addition to electricity generation, to a greater extent than traditional large NPPs. In this case, the heat utilization facility may be located off the licensed site of the NPP, and as such the treatment of hazards and transients initiated by the heat utilization facility will require careful consideration during the design development of the SMR. Therefore, enhancements in the wording of the safety requirements related to coupled facilities may be needed to ensure that these aspects are adequately addressed.

## 2.2. DESIGN CHARACTERISTICS AND SAFETY CONSIDERATIONS FOR LW-SMRs

LW-SMRs may incorporate advanced and innovative features, including the following:

*a) Design Simplification and compactness*

The integral configuration results in a lighter in weight and more compact reactor. This integration yields substantial reduction in the size of the nuclear steam supply system. Some integral pressurized water reactor (iPWR) designs adopt natural circulation for the primary heat removal from the core. The need for reactor coolant primary pumps can then be eliminated; hence, the event of loss of primary coolant flow due to pump failure can also be eliminated. Natural circulation also reduces mechanical complexity. Other iPWR designs adopt conventional forced convection either using horizontally or vertically mounted primary pumps directly connected to the reactor vessel through nozzles. In-vessel steam generators are adopted for all iPWR designs, such as the once-through helical coil steam generator that offers a larger heat transfer area in a compact geometry.

*b) Enhanced safety*

The integral design of the nuclear steam supply module eliminates external coolant loop piping, which can in turn eliminate the large-break loss of coolant accidents (LOCA). In addition, small-break LOCAs might not significantly challenge the safety of the plant. The passive engineered safety features might reduce the need for external electrical power supply under accident conditions. The core damage frequency for internal events is typically claimed to be of the order of  $10^{-6}$  to  $10^{-8}$  per year; however, this needs to be confirmed by further detailed probabilistic safety analysis as the designs evolve.

Many LW-SMR designs adopt the iPWR concept, for which the components within the primary reactor coolant system (e.g. steam generators and pressurizer) are installed within the reactor vessel together with the core. This integration of the primary reactor coolant system is an approach mainly used to enable modular deployment and is possible when the reactor power is lower than 1000 MW(t). From the point of view of safety, large and medium break loss of coolant accidents, such as hot and/or cold leg breaks, pressurizer surge line breaks and primary pump suction and/or discharge line breaks, are event sequences which might not need to be postulated as initiating events in these design approaches.

Below are some specific claims related to the design characteristics of the LW-SMRs that have been taken into account in the considerations provided in Appendix I, where appropriate:

*Compact design (integral design) and therefore:*

- Reduction of length of connecting pipes, hence reduction of pipe break events;
- Reduction of the impact of small-break LOCAs;
- Elimination of large-break LOCAs when obviating the need for external piping between reactor vessel and steam generators;
- Positioning of the core vessel penetrations at higher levels, reducing the potential for core uncover.

*Significant reduction of overall power, hence:*

- Lower source term owing to lower fuel inventory in the core;
- Low core power density;
- Larger amount of coolant per reactor, as compared to the large reactors (this might slowdown transient development);
- Generally low fuel burn-up.

*Extensive use of inherent and passive safety features in comparison to larger reactors, such as:*

- Use of steam generators integrated with the core allowing for sufficient elevation differences that permit natural circulation;
- Passive safety systems reducing the reliance on features actuations and human actions, as well as reducing the need of supporting power supply (thus having potential for improving the overall risks from the reactor).

*Multiple modules design approach:*

- Potential for interactions among the reactor modules;
- Potential for sharing safety systems and features;
- In case of ultimate heat sinks of limited capacity, shared ultimate heat sink offering an overall significantly larger cooling capability in comparison to several individual ultimate heat sinks for each module.

*Modularity regarding construction and decommissioning:*

- Built-in factory of entire parts to be assembled on-site: enables improved quality control and in-series construction due to manufacture and tests of integral parts (several systems assembled in factory);
- Transportability: entire parts and even an entire module (without fuel) can be transported for initial construction and also for off-site maintenance or outage;
- Separate construction and/or deployment of modules or part of the unit, having corresponding impact in safety considerations;
- Potential to optimize the decommissioning via a process to decommission integral parts (after fuel removal).

So far, no major differences have been highlighted in terms of fuel handling during refuelling and spent fuel management in comparison to larger reactors.

### 2.3. DESIGN CHARACTERISTICS AND SAFETY CONSIDERATIONS FOR HTG-SMRS

The main design characteristics differentiating HTG-SMRs from LW-SMRs are the use of helium as coolant, the introduction of graphite as moderating material and the use of all-ceramic coated particles fuel [3–5]. Two main technological variants of HTG-SMRs have been developed, one incorporates prismatic type graphite fuel blocks (graphite block type reactor) and the other spherical fuel elements (pebble bed type reactor). A demonstration plant of the pebble bed type reactor is under construction in China.

The innovative features and safety characteristics intended to allow HTG-SMRs to provide safe, reliable and affordable energy and corresponding utilization are the following:

#### *a) Fuel*

The HTG-SMRs deploy tri-structural isotropic (TRISO) coated fuel particles that represent one of the fundamental characteristics of this reactor technology from the point of view of safety [3–5]. These fuel particles are incorporated to prismatic blocks (prismatic core) or to fuel elements having spherical form (pebble bed core).

- *Fuel particles*

The TRISO coated fuel particles have an overall diameter in the range of 500 to 1000  $\mu\text{m}$ . Each particle contains a spherical fuel kernel of fissile or fertile fuel materials, usually in the form of  $\text{UO}_2$ ,  $\text{PuO}_2$ , or  $\text{UCO}$ , the enrichment of the fissile part ( $^{235}\text{U}$  wt%) ranging between 8 and 20. The fuel kernels are coated with layers of low density pyro carbon (PyC), inner high density PyC, silicon carbide (SiC) and outer high density PyC.

TRISO coated fuel particles are designed to minimize fission product release rates during operational states and accident conditions as long as the maximum temperature of the fuel particle is kept below acceptable values (in the order of 1600°C).

- *Fuel elements*

In a prismatic HTG-SMR design, the fuel element is a hexagonal block. The TRISO coated fuel particles are imbedded within a graphite matrix to form cylindrical compacts.

These compacts are then inserted into the hexagonal graphite block. Some HTG-SMR designs may assemble the compacts into the fuel rods and these fuel rods are then inserted into the hexagonal graphite block.

In a pebble bed HTG-SMR design, the fuel element is a spherical pebble with about 60 mm diameter. The fuelled portion of the fuel element is about 50 mm diameter and contains TRISO coated fuel particles imbedded into the graphite matrix.

*b) Inherent safety characteristics*

The safety characteristics of HTG-SMRs are mainly defined by the quality of the ceramic coated particle fuel that is expected to contain the vast majority of fission products to a very high temperature and for sufficiently long time. The coated particle fuel together with the core design features aims to prevent unacceptable releases of radioactive materials from the fuel. A low power density and the use of passive means of decay heat removal aim to make the forced flow not necessary to ensure that the maximum fuel temperatures do not reach unacceptable levels under any credible event, including total loss of the coolant.

Due to the large heat capacity and relatively low power density of the reactor core, the evolution of certain transients and postulated accidents is expected to be very slow.

*c) Containment system*

Confinement function: Among the radionuclide retention barriers of a traditional LWR (fuel pellets, fuel cladding, reactor coolant pressure boundary and containment), the containment building is regarded as the final and most significant confinement barrier to retain the radioactive products in some postulated accidents when the integrity of other barriers is lost or degraded and is especially important when core melt is assumed. However, for the HTG-SMR, the TRISO fuel is claimed as the dominant contributor to the confinement function for being the first and most reliable among all the barriers (the SiC layer of a fuel particle can be considered as a kind of ‘micro-containment’). The degree of importance of an HTG-SMR containment in terms of fulfilling the confinement function is therefore not expected to be as high as that of an LWR containment.

*d) Design Extension Conditions*

Regarding the safety features to be incorporated to the design for design extension conditions, there are significant differences between light water reactor technologies and high temperature gas cooled reactor technologies. In the latter, during plant operations, the only potential mechanism for common mode failure of TRISO fuel currently identified is associated with exceeding the safety limit on fuel temperature [3–4]. Studies for HTG-SMRs have demonstrated that this safety limit will not be exceeded in operational states and postulated accident scenarios [6]. Studies have also shown that when this safety limit is exceeded, the release rate of radioactive materials from fuel particles increases gradually with a relatively large temperature margin, without reaching a cliff edge in terms of consequences [7–8]. Common mode failures of the TRISO fuel could be originated by reasons other than operation, such as manufacturing defects or internal and external hazards (e.g. air ingress or water intake) and consequently specific requirements in this regard have to be provided.

e) *Shutdown means*

Generally, there are two independent and diverse reactor shutdown means for an HTG-SMR and each of these is used to scram the reactor in the case of an accident. Some HTG-SMR designs propose to rely upon the means of the combination of full range negative temperature coefficient of reactivity and large margin of temperature increase under accident conditions to introduce large negative reactivity, leading to automatic shutdown due to negative temperature feedback even when the other reactor shutdown means fail.

f) *Decay heat removal*

The power density of an HTG-SMR core is typically chosen in such a way that for all operational states and accident conditions, decay heat removal by radiation, conduction and natural convection to the environment may be claimed, in accordance with design calculations, without exceeding limits for fuel temperatures in respect of fission product releases. Specifically, the decay heat transfer inside the reactor depends only upon thermal properties of solid materials in case of scenarios such as a loss of coolant, or a loss of flow. No active cooling measures and off-site power are claimed to be necessary.

g) *Used and spent fuel storage*

As the power density of the fuel is low and a large temperature margin in the fuel in regard to reaching its design limit is claimed, spent or used fuel could potentially be stored in casks or tanks that can be cooled by air and shielded by a concrete structure. It is also claimed that no water is needed for either cooling or radiation shielding, and that no active cooling system is needed.

h) *Modularity*

In order to achieve the desired inherent safety characteristics, the HTG-SMR module power level and the power density are limited. In addition, in case of higher levels of power, the use of helium coolant would lead to large reactor vessels for which transport by road might represent challenges. The term ‘modular HTGR’ was already used in the 1980’s and rather refers to the multiple units that can be deployed to fulfil the specific needs, contrary to the more modern term used for factory construction and road transportability.

i) *Utilization*

In addition to contributing to an increased efficiency for electricity generation, the high coolant outlet temperatures of the HTG-SMRs (~700–950°C) also facilitate the reactor’s utilization for high temperature process heat applications, such as providing heat for industrial applications, gas reforming and hydrogen production.

The main technical bases for inherent safety claims of HTG-SMRs are the TRISO coated particle fuel, the graphite as the core structure and the helium coolant; in addition to these, the dedicated core layout and lower power density facilitate passive decay heat by natural means. These features are claimed to keep the maximum fuel temperature below the safety limits in accident conditions so as to efficiently contain fission products inside the fuel. Therefore, the possibility of fuel melting is not postulated, and consequently early radioactive releases and large radioactive releases are claimed as not being credible.

There are scenarios in which chemical attack on the graphite might occur, such as those involving a water or air ingress [3, 5], having an impact on radioactive releases. However, it has been reported [7, 8] that such an impact on the fuel integrity is very limited since the process is very slow (long time margin allowed to take mitigation actions) and the amount of ingress is limited. Therefore, the integrity of most of the fuel elements is expected to be maintained, hence efficiently containing fission products.

### 3. APPROACH TO DETERMINE THE APPLICABILITY OF THE DESIGN SAFETY REQUIREMENTS

The considerations provided in this publication have taken into account the output of a study performed with representatives of design organizations and operating organizations of the two technologies covered, LW-SMRs and HTG-SMRs. The group of contributors to this TECDOC is provided at the end of the publication.

The contributors had experience in reactor design, regulatory guidance, design and safety review and applicability of design safety requirements to both large NPPs of classical design, using water cooled reactors, and the two SMR technologies covered in this publication. Current practices applied at the national level and corresponding feedback experience have been taken into account in developing this publication.

Aspects of the expert engineering judgement, such as the rationale behind each safety requirement, its contribution to defence in depth and whether the safety requirement is technology-neutral or technology-dependent, taking also into account the fulfilment of the fundamental safety functions, were kept in mind in developing the considerations on applicability. An example of the implementation of these aspects is provided in the Annex, regarding the safety requirements related to the containment structure and containment function (see Annex).

The result of the considerations on applicability of each of the safety requirements, including its title, the overarching requirements and the associated requirements, is provided in Appendix I for LW-SMRs and in Appendix II for HTG-SMRs. The Annex includes the approach used by the contributors to determine the applicability of the design safety requirements related to containment to HTG-SMRs.

The following scheme is used in this publication to present the results of the considerations:

- In each appendix (Appendix I and Appendix II), the Sections 1 to 6 from SSR-2/1 (Rev.1) [2], including the 82 design safety requirements, the references and the definitions are copied.
- In both appendices, no observations are provided to the paragraphs and requirements that were considered fully applicable as they are. The implicit considerations applying to the requirements are:
  - *‘The formulation of this Requirement is considered applicable as is’*, for requirements only composed by a title and the overarching requirement in bold text;
  - *‘The entire formulation of this Requirement is considered applicable as is, i.e. its title, the overarching requirement in bold text and the associated requirements set out in the subsequent paragraphs’*, for requirements having several paragraphs.

Regarding the paragraphs from the introductory sections 1 and 2 of SSR-2/1 (Rev. 1) [2], no changes or interpretations were identified as necessary; however, one comment to one specific paragraph (1.6) is provided in both appendices.

- The following format is used for the requirements having relevant considerations on applicability:
  - The ‘Requirement number’ appears underlined;
  - At the end of the formulation of the requirement, including its associated requirements set out in the subsequent paragraphs, a numbered text box is provided, indicating the result of the considerations on applicability with the following structure:
    - *Suggested changes*: The changes to the wording of the requirement are incorporated in the text (*italics*);
    - *Suggested interpretations*: These refer to terms, sentences or entire requirements that, in accordance to the view of the contributors, are to be interpreted in the suggested way when applied to the corresponding SMR technology;
    - *Justification of the suggested changes and/or interpretations*: Clarifications are provided about changes and/or justifications, as applicable.

Agreement regarding the considerations on applicability was reached among all the contributors in most cases. This affirmation is fully applicable in the case of the LW-SMRs (Appendix I). In the case of the HTG-SMRs (Appendix II), agreement was reached for most of the requirements. However, in some cases the contributors had two different views, mainly depending on the organization to which they belong; in these cases, both positions are provided in the text without further distinction.

The scope of the considerations provided has been adapted to the content of SSR-2/1 (Rev. 1) [2], although considerations of the novel design features (e.g. modularity) have been also taken into account. Aspects potentially necessitating the establishment of additional requirements are included after the last requirement (Requirement 82) in both Appendix I and Appendix II. Some additional definitions are proposed to clarify the concept of reactor module in the context of multi-module units.

#### 4. SUMMARY RESULTS AND CONCLUSION

The contributors to the preparation of this TECDOC evaluated the applicability of the introductory sections and the entire formulation of each of the 82 design safety requirements established in SSR-2/1 (Rev. 1) [2] to the two reactor technologies having SMR designs intended for near-term deployment, i.e. LW-SMRs and HTG-SMRs.

The considerations on applicability provided are mainly based on the design characteristics and safety considerations described in Section 2 and were developed in accordance to the approach and format indicated in Section 3. The results are provided in Appendix I for LW-SMRs and in Appendix II for HTG-SMRs. Table 1 provides a list highlighting the main result of the considerations on applicability (i.e. applicable ‘as is’; applicable with ‘changes’; applicable with ‘interpretation’).

In summary, regarding the introductory part (sections 1 and 2) of SSR-2/1 (Rev. 1) [2], one comment to paragraph 1.6 is provided. The number of safety requirements having suggestions for changes and interpretation is the following:

- Eight (8) of the existing safety requirements for LW-SMRs (Appendix I);
- Thirty (30) of the existing safety requirements for HTG-SMRs (Appendix II).

All the other safety requirements (i.e. 74 for the LW-SMRs and 52 for the HTG-SMRs) were considered fully applicable as they are without needing any change or interpretation.

Regarding multi-module units, considerations about aspects having potential for establishing additional safety requirements are provided at the end of Section 6 in each of the two appendices, Appendix 1 and Appendix 2.

The considerations confirmed that the main features of the set of safety requirements established for NPPs in SSR-2/1 (Rev. 1) [2], including the guiding principles, formulation (in general terms) and relevance to contribute to defence in depth and to fulfilment of the fundamental safety functions, remain valid when applied to the two SMR technologies evaluated in this publication.

Given the similarities between the design characteristics of SMRs that use light water technology and large NPPs that use the same reactor technology, the changes and/or interpretations identified as necessary for LW-SMRs amounts to less than 10 %. Conversely, taking into account the significant differences existing between the design characteristics of the HTG-SMRs and the light water reactors, around 35 % of the requirements need changes and/or interpretation. However, the applicability of the rationale behind the full set of safety requirements and behind each of the safety requirements established in SSR-2/1 (Rev. 1) [2] has been confirmed for the SMR technologies considered in this TECDOC.

The results included in this publication represent the views of the contributors. The contributors consider the results to be very useful for being taken into account in activities that are being implemented by their organizations or will be undertaken by other organizations in the near future. In addition, the results were also considered as a valuable input for future activities of the IAEA related to the enhancement and completion of the safety standards.

TABLE 1. SUMMARY RESULTS ON APPLICABILITY OF DESIGN SAFETY REQUIREMENTS OF SSR-2/1 (REV.1) TO LW-SMRS AND TO HTG-SMRS (APPENDICES I AND II)

Req. Nr.	Title	Applicability of each of the safety requirements	
		LW-SMRs (Appendix I)	HTG-SMRs (Appendix II)
<b>1. INTRODUCTION</b>			
N/A	Background (1.1–1.3)	As is	As is
	Objective (1.4–1.5)	As is	As is
	Scope		
	— Paragraph 1.6	Comment	Comment
	— Paragraphs 1.7–1.8	As is	As is
	Structure (1.9)	As is	As is
<b>2. APPLYING THE SAFETY PRINCIPLES AND CONCEPTS</b>			
N/A	(Paragraphs 2.1–2.5)	As is	As is
	Radiation protection in design (2.6–2.7)	As is	As is
	Safety in design (2.8–2.11)	As is	As is
	The concept of defence in depth (2.12–2.14)	As is	As is
	Maintaining the integrity of design of the plant throughout the lifetime of the plant (2.15–2.18)	As is	As is
<b>3. MANAGEMENT OF SAFETY IN DESIGN</b>			
1	Responsibilities in the management of safety in plant design (3.1)	As is	As is
2	Management system for plant design (3.2–3.4)	As is	As is
3	Safety of the plant design throughout the lifetime of the plant (3.5–3.6)	As is	As is
<b>4. PRINCIPAL TECHNICAL REQUIREMENTS</b>			
4	Fundamental safety functions (4.1–4.2)	As is	As is
5	Radiation protection in design (4.3–4.4)	As is	As is
6	Design for a nuclear power plant (4.5–4.8)	As is	As is
7	Application of defence in depth (4.9–4.13A)	As is	Change
8	Interfaces of safety with security and safeguards	As is	As is

TABLE 1. SUMMARY RESULTS ON APPLICABILITY OF DESIGN SAFETY REQUIREMENTS OF SSR-2/1 (REV.1) TO LW-SMRS AND TO HTG-SMRS (APPENDICES I AND II) (cont.)

Req. Nr.	Title	Applicability of each of the safety requirements	
		LW-SMRs (Appendix I)	HTG-SMRs (Appendix II)
9	Proven engineering practices (4.14–4.16)	As is	As is
10	Safety assessment (4.17–4.18)	As is	As is
11	Provision for construction (4.19)	Change	Change
12	Features to facilitate radioactive waste management and decommissioning (4.20)	As is	As is
<b>5. GENERAL PLANT DESIGN</b>			
<b>Design basis</b>			
13	Categories of plant states (5.1–5.2)	As is	Change
14	Design basis for items important to safety (5.3)	As is	As is
15	Design limits (5.4)	As is	As is
16	Postulated initiating events (5.5–5.15)	As is	As is
17	Internal and external hazards (5.15A–5.22)	Change	Change
18	Engineering design rules (5.23)	As is	As is
19	Design basis accidents (5.24–5.26)	As is	As is
20	Design extension conditions (5.27–5.32)	As is	Change
21	Physical separation and independence of safety systems (5.33)	As is	As is
22	Safety classification (5.34–5.36)	As is	As is
23	Reliability of items important to safety (5.37–5.38)	As is	As is
24	Common cause failures	As is	As is
25	Single failure criterion (5.39–5.40)	As is	As is
26	Fail-safe design (5.41)	As is	As is
27	Support service systems (5.42–5.43)	As is	As is
28	Operational limits and conditions for safe operation (5.44)	As is	As is

TABLE 1. SUMMARY RESULTS ON APPLICABILITY OF DESIGN SAFETY REQUIREMENTS OF SSR-2/1 (REV.1) TO LW-SMRS AND TO HTG-SMRS (APPENDICES I AND II) (cont.)

Req. Nr.	Title	Applicability of each of the safety requirements	
		LW-SMRs (Appendix I)	HTG-SMRs (Appendix II)
<b>Design for safe operation over the lifetime of the plant</b>			
29	Calibration, testing, maintenance, repair, replacement, inspection and monitoring of items important to safety (5.45–5.47)	As is	As is
30	Qualification of items important to safety (5.48–5.50)	As is	Change
31	Ageing management (5.51–5.52)	As is	As is
<b>Human factors</b>			
32	Design for optimal operator performance (5.53–5.62)	As is	As is
<b>Other design considerations</b>			
33	Safety systems, and safety features for design extension conditions, of units of a multiple unit nuclear power plant (5.63)	Change	Change
34	Systems containing fissile material or radioactive material	As is	As is
35	Nuclear power plants used for cogeneration of heat and power, heat generation or desalination	As is	Change
36	Escape routes from the plant (5.64–5.65)	As is	As is
37	Communication systems at the plant (5.66–5.67)	As is	As is
38	Control of access to the plant (5.68)	As is	As is
39	Prevention of unauthorized access to, or interference with, items important to safety	As is	As is
40	Prevention of harmful interactions of systems important to safety (5.69–5.70)	As is	As is
41	Interactions between the electrical power grid and the plant	As is	As is

TABLE 1. SUMMARY RESULTS ON APPLICABILITY OF DESIGN SAFETY REQUIREMENTS OF SSR-2/1 (REV.1) TO LW-SMRS AND TO HTG-SMRS (APPENDICES I AND II) (cont.)

Req. Nr.	Title	Applicability of each of the safety requirements	
		LW-SMRs (Appendix I)	HTG-SMRs (Appendix II)
<b>Safety analysis</b>			
42	Safety analysis of the plant design (5.71–5.76)	As is	Change
<b>6. DESIGN OF SPECIFIC PLANT SYSTEMS</b>			
<b>Reactor core and associated features</b>			
43	Performance of fuel elements and assemblies (6.1–6.3)	As is	Change
44	Structural capability of the reactor core	As is	Change
45	Control of the reactor core (6.4–6.6)	As is	Change
46	Reactor shutdown (6.7–6.12)	As is	Change
<b>Reactor coolant systems</b>			
47	Design of reactor coolant systems (6.13–6.16)	As is	Change
48	Overpressure protection of the reactor coolant pressure boundary	As is	Change
49	Inventory of reactor coolant	As is	As is
50	Cleanup of reactor coolant (6.17)	As is	Change
51	Removal of residual heat from the reactor core	As is	As is
52	Emergency cooling of the reactor core (6.18–6.19)	As is	Change
53	Heat transfer to an ultimate heat sink (6.19A–6.19B)	As is	As is
<b>Containment structure and containment system</b>			
54	Containment system for the reactor	As is	Change
55	Control of radioactive releases from the containment (6.20–6.21)	As is	Change
56	Isolation of the containment (6.22–6.24)	As is	Change
57	Access to the containment (6.25–6.26)	Interpretation	Change
58	Control of containment conditions (6.27–6.30)	As is	Change

TABLE 1. SUMMARY RESULTS ON APPLICABILITY OF DESIGN SAFETY REQUIREMENTS OF SSR-2/1 (REV.1) TO LW-SMRS AND TO HTG-SMRS (APPENDICES I AND II) (cont.)

Req. Nr.	Title	Applicability of each of the safety requirements	
		LW-SMRs (Appendix I)	HTG-SMRs (Appendix II)
<b>Instrumentation and control systems</b>			
59	Provision of instrumentation (6.31)	As is	As is
60	Control systems	As is	As is
61	Protection system (6.32–6.33)	As is	As is
62	Reliability and testability of instrumentation and control systems (6.34–6.36)	As is	As is
63	Use of computer based equipment in systems important to safety (6.37)	As is	As is
64	Separation of protection systems and control systems (6.38)	As is	As is
65	Control room (6.39–6.40A)	As is	As is
66	Supplementary control room (6.41)	As is	Change
67	Emergency response facilities on the site (6.42)	As is	As is
<b>Emergency power supply</b>			
68	Design for withstanding the loss of off-site power (6.43–6.45A)	Interpretation	Change
<b>Supporting systems and auxiliary systems</b>			
69	Performance of supporting systems and auxiliary systems	As is	As is
70	Heat transport systems (6.46)	As is	As is
71	Process sampling systems and post-accident sampling systems (6.47)	As is	As is
72	Compressed air systems	As is	As is
73	Air conditioning systems and ventilation systems (6.48–6.49)	Change	Change
74	Fire protection systems (6.50–6.54)	As is	As is
75	Lighting systems	As is	As is
76	Overhead lifting equipment (6.55)	Change	Change

TABLE 1. SUMMARY RESULTS ON APPLICABILITY OF DESIGN SAFETY REQUIREMENTS OF SSR-2/1 (REV.1) TO LW-SMRS AND TO HTG-SMRS (APPENDICES I AND II) (cont.)

Req. Nr.	Title	Applicability of each of the safety requirements	
		LW-SMRs (Appendix I)	HTG-SMRs (Appendix II)
<b>Other power conversion systems</b>			
77	Steam supply system, feedwater system and turbine generators (6.56–6.58)	As is	Change
<b>Treatment of radioactive effluents and radioactive waste</b>			
78	Systems for treatment and control of waste	Change	Change
79	Systems for treatment and control of effluents (6.61–6.63)	As is	As is
<b>Fuel handling and storage systems</b>			
80	Fuel handling and storage systems (6.64–6.68A)	As is	Change
<b>Radiation protection</b>			
81	Design for radiation protection (6.69–6.76)	As is	Change
82	Means of radiation monitoring (6.77–6.84)	As is	As is
New	Additional aspects regarding multi-module units for which new safety requirements could be provided	5 aspects	5 aspects
N/A	DEFINITIONS	Change	Change



## APPENDIX I. APPLICABILITY OF DESIGN SAFETY REQUIREMENTS TO LW-SMRS

This appendix includes specific considerations on the applicability of the IAEA design safety requirements established in SSR-2/1 (Rev. 1) [2] to LW-SMRs intended for near term deployment. Relevant aspects of the approach used to identify these considerations and the format adopted to present the results are described in the main body of this publication (see Section 3). In accordance to that section, no observations are provided to the paragraphs and requirements considered fully applicable as they are. For the requirements to which observations were made, the requirement number appears underlined, the changes to the wording are directly incorporated to the text of the safety requirement (in *italics*) and the other aspects (*'suggested interpretations'* and *'justification of the suggested changes and/or interpretations'*) are included in a text box placed at the end of the requirement.

The practical information provided in this publication represent the views of the contributors and cannot be considered as IAEA guidance or recommendations.

To clearly highlight the considerations of the applicability of the design safety requirements established in SSR-2/1 (Rev.1) [2] to SMRs, the entire text from SSR-2/1 (Rev.1) [2] is reproduced in full in this appendix, with the specific considerations identified inserted at relevant points within the text. For easier reading, the reproduced text that has no changes is shown in the original format (narrowed text) and the modified paragraphs in the format of this publication (full size text). The specific comments about the considerations on applicability are also reproduced in the format of this publication (full size text) and highlighted in boxes.

### 1. INTRODUCTION

#### BACKGROUND

1.1. The present publication supersedes the Safety Requirements publication Safety of Nuclear Power Plants: Design,<sup>1</sup> which was issued in 2012 as IAEA Safety Standards Series No. SSR-2/1. Account has been taken of the Fundamental Safety Principles [1], published in 2006. Requirements for nuclear safety are intended to ensure “the highest standards of safety that can reasonably be achieved” for the protection of workers, the public and the environment from harmful effects of ionizing radiation that could arise from nuclear power plants and other nuclear facilities [1]. It is recognized that technology and scientific knowledge advance, and that nuclear safety and the adequacy of protection against radiation risks need to be considered in the context of the present state of knowledge. Safety requirements will change over time; this Safety Requirements publication reflects the present consensus.

1.2. The designs of many existing nuclear power plants, as well as the designs for new nuclear power plants, have been enhanced to include additional measures to mitigate the consequences of complex accident sequences involving multiple failures and of severe accidents. Complementary systems and equipment with new capabilities have been backfitted to many existing nuclear power plants to aid in the prevention of severe accidents and the mitigation of their consequences. Guidance on the mitigation of the consequences of severe accidents has been provided at most existing nuclear power plants. The

---

<sup>1</sup> INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012)

design of new nuclear power plants now explicitly includes the consideration of severe accident scenarios and strategies for their management. Requirements related to the State system of accounting for, and control of, nuclear material and security related requirements are also taken into account in the design of nuclear power plants. Integration of safety measures and security measures will help to ensure that neither compromise the other.

1.3. It might not be practicable to apply all the requirements of this Safety Requirements publication to nuclear power plants that are already in operation or under construction. In addition, it might not be feasible to modify designs that have already been approved by regulatory bodies. For the safety analysis of such designs, it is expected that a comparison will be made with the current standards, for example as part of the periodic safety review for the plant, to determine whether the safe operation of the plant could be further enhanced by means of reasonably practicable safety improvements.

#### OBJECTIVE

1.4. This publication establishes design requirements for the structures, systems and components of a nuclear power plant, as well as for procedures and organizational processes important to safety that are required to be met for safe operation and for preventing events that could compromise safety, or for mitigating the consequences of such events, were they to occur.

1.5. This publication is intended for use by organizations involved in design, manufacture, construction, modification, maintenance, operation and decommissioning for nuclear power plants, in analysis, verification and review, and in the provision of technical support, as well as by regulatory bodies.

#### SCOPE

1.6. It is expected that this publication will be used primarily for land based stationary nuclear power plants with water cooled reactors designed for electricity generation or for other heat production applications (such as district heating or desalination). This publication may also be applied, with judgement, to other reactor types, to determine the requirements that have to be considered in developing the design.

#### **COMMENT TO PARAGRAPH 1.6**

Paragraph 1.6 indicates the ability to apply the safety requirements with judgement on a case by case basis. It is understood that judgement has to be informed by relevant and supportable evidence.

1.7. This publication does not address:

- (a) Requirements that are specifically covered in other IAEA Safety Requirements publications (e.g. IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), Safety Assessment for Facilities and Activities[2]);
  - (b) Matters relating to nuclear security or to the State system of accounting for, and control of, nuclear material;
  - (c) Conventional industrial safety that under no circumstances could affect the safety of the nuclear power plant;
  - (d) Non-radiological impacts arising from the operation of nuclear power plants.
- 1.8. Terms in this publication are to be understood as defined and explained in the IAEA Safety Glossary [3], unless otherwise stated here (see Definitions).

1.8. Terms in this publication are to be understood as defined and explained in the IAEA Safety Glossary [3], unless otherwise stated here (see Definitions).

## STRUCTURE

1.9. This Safety Requirements publication follows the relationship between the safety objective and safety principles, and between requirements for nuclear safety functions and design criteria for safety. Section 2 elaborates on the safety objective, safety principles and concepts that form the basis for deriving the safety function requirements that must be met for the nuclear power plant, as well as the safety design criteria. Sections 3–6 establish numbered overarching requirements (shown in bold type), with additional requirements as appropriate in the paragraphs that follow them. Section 3 establishes the general requirements to be satisfied by the design organization in the management of safety in the design process. Section 4 establishes: requirements for principal technical design criteria for safety, including requirements for the fundamental safety functions, the application of defence in depth and provision for construction; requirements for interfaces of safety with nuclear security and with the State system of accounting for, and control of, nuclear material; and requirements for ensuring that radiation risks arising from the plant are maintained as low as reasonably achievable. Section 5 establishes requirements for general plant design that supplement the requirements for principal technical design criteria to ensure that safety objectives are met and the safety principles are applied. The requirements for general plant design apply to all items (i.e. structures, systems and components) important to safety. Section 6 establishes requirements for the design of specific plant systems such as the reactor core, reactor coolant systems, containment system, and instrumentation and control systems.

## 2. APPLYING THE SAFETY PRINCIPLES AND CONCEPTS

2.1. The Fundamental Safety Principles [1] establish one fundamental safety objective and ten safety principles that provide the basis for requirements and measures for the protection of people and the environment against radiation risks and for the safety of facilities and activities that give rise to radiation risks.

2.2. This fundamental safety objective has to be achieved, and the ten safety principles have to be applied, without unduly limiting the operation of facilities or the conduct of activities that give rise to radiation risks. To ensure that nuclear power plants are operated and activities are conducted so as to achieve the highest standards of safety that can reasonably be achieved, measures have to be taken to achieve the following (see para. 2.1 of the Fundamental Safety Principles [1]):

- a) To control the radiation exposure of people and radioactive releases to the environment in operational states;
- b) To restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source, spent nuclear fuel, radioactive waste or any other source of radiation at a nuclear power plant;
- c) To mitigate the consequences of such events if they were to occur.

2.3. The fundamental safety objective applies for all stages in the lifetime of a nuclear power plant, including planning, siting, design, manufacture, construction, commissioning and operation, as well as decommissioning. This includes the associated transport of radioactive material and the management of spent nuclear fuel and radioactive waste (see para. 2.2 of the Fundamental Safety Principles [1]).

2.4. Paragraph 2.3 of the Fundamental Safety Principles [1] states that:

“Ten safety principles have been formulated, on the basis of which safety requirements are developed and safety measures are to be implemented in order to achieve the fundamental safety objective. The safety principles form a set that is applicable in its entirety; although in practice different principles may be more or less important in relation to particular circumstances, the appropriate application of all relevant principles is required.”

2.5. This Safety Requirements publication establishes requirements that apply those safety principles, which are particularly important in the design of nuclear power plants.

#### RADIATION PROTECTION IN DESIGN

2.6. In order to satisfy the safety principles, it is required to ensure that for all operational states of a nuclear power plant and for any associated activities, doses from exposure to radiation within the installation or exposure due to any planned radioactive release from the installation are kept below the dose limits and kept as low as reasonably achievable. In addition, it is required to take measures for mitigating the radiological consequences of any accidents, if they were to occur.

2.7. To apply the safety principles, it is also required that nuclear power plants be designed and operated so as to keep all sources of radiation under strict technical and administrative control. However, this principle does not preclude limited exposures or the release of authorized amounts of radioactive substances to the environment from nuclear power plants in operational states. Such exposures and radioactive releases are required to be strictly controlled and to be kept as low as reasonably achievable, in compliance with regulatory and operational limits as well as radiation protection requirements [4].

#### SAFETY IN DESIGN

2.8. To achieve the highest level of safety that can reasonably be achieved in the design of a nuclear power plant, measures are required to be taken to do the following, consistent with national acceptance criteria and safety objectives [1]:

- a) To prevent accidents with harmful consequences resulting from a loss of control over the reactor core or over other sources of radiation, and to mitigate the consequences of any accidents that do occur;
- b) To ensure that for all accidents taken into account in the design of the installation, any radiological consequences would be below the relevant limits and would be kept as low as reasonably achievable;
- c) To ensure that the likelihood of occurrence of an accident with serious radiological consequences is extremely low and that the radiological consequences of such an accident would be mitigated to the fullest extent practicable.

2.9. To demonstrate that the fundamental safety objective [1] is achieved in the design of a nuclear power plant, a comprehensive safety assessment [2] of the design is required to be carried out. Its objective is to identify all possible sources of radiation and to evaluate possible doses that could be received by workers at the installation and by members of the public, as well as possible effects on the environment, as a result of operation of the plant. The safety assessment is required in order to examine: (i) normal operation of the plant; (ii) the performance of the plant in anticipated operational occurrences; and accident conditions. On the basis of this analysis, the capability of the design to withstand postulated initiating events and accidents can be established, the effectiveness of the items important to safety can be demonstrated and the inputs (prerequisites) for emergency planning can be established.

2.10. Measures are required to be taken to control exposure for all operational states at levels that are as low as reasonably achievable and to minimize the likelihood of an accident that could lead to the loss of control over a source of radiation. Nevertheless, there will remain a possibility that an accident could happen. Measures are required to be taken to ensure that the radiological consequences of an accident would be mitigated. Such measures include the provision of safety features and safety systems, the establishment of accident management procedures by the operating organization and, possibly, the establishment of off-site protective actions by the appropriate authorities, supported as necessary by the operating organization, to mitigate exposures if an accident occurs.

2.11. The design for safety of a nuclear power plant applies the safety principle that practical measures must be taken to mitigate the consequences for human life and health and for the environment of nuclear or radiation accidents (Principle 8 of the Fundamental Safety Principles [1]). Plant event sequences that could result in high radiation doses or in a large radioactive release have to be ‘practically eliminated’<sup>2</sup> and plant event sequences with a significant frequency of occurrence have to have no, or only minor, potential radiological consequences. An essential objective is that the necessity for off-site protective actions to mitigate radiological consequences be limited or even eliminated in technical terms, although such measures might still be required by the responsible authorities.

#### THE CONCEPT OF DEFENCE IN DEPTH

2.12. The primary means of preventing accidents in a nuclear power plant and mitigating the consequences of accidents if they do occur is the application of the concept of defence in depth [1, 5, 6]. This concept is applied to all safety related activities, whether organizational, behavioural or design related, and whether in full power, low power or various shutdown states. This is to ensure that all safety related activities are subject to independent layers of provisions so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures. Application of the concept of defence in depth throughout design and operation provides protection against anticipated operational occurrences and accidents, including those resulting from equipment failure or human induced events within the plant, and against consequences of events that originate outside the plant.

2.13. Paragraph 3.31 of the Fundamental Safety Principles [1] states that:

“Defence in depth is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment. If one level of protection or barrier were to fail, the subsequent level or barrier would be available.... The independent effectiveness of the different levels of defence is a necessary element of defence in depth.”

There are five levels of defence:

- (1) The purpose of the first level of defence is to prevent deviations from normal operation and the failure of items important to safety. This leads to requirements that the plant be soundly and conservatively sited, designed, constructed, maintained and operated in accordance with quality management and appropriate and proven engineering practices. To meet these objectives, careful attention is paid to the selection of appropriate design codes and materials, and to the quality control of the manufacture of components and construction of the plant, as well as to its commissioning. Design options that reduce the potential for internal hazards contribute to the prevention of accidents at this level of defence. Attention is also paid to the processes and procedures involved in design, manufacture, construction, and in-service inspection, maintenance

---

<sup>2</sup> 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

and testing, to the ease of access for these activities, and to the way the plant is operated and to how operating experience is utilized. This process is supported by a detailed analysis that determines the requirements for operation and maintenance of the plant and the requirements for quality management for operational and maintenance practices.

- (2) The purpose of the second level of defence is to detect and control deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions. This is in recognition of the fact that postulated initiating events are likely to occur over the operating lifetime of a nuclear power plant, despite the care taken to prevent them. This second level of defence necessitates the provision of specific systems and features in the design, the confirmation of their effectiveness through safety analysis, and the establishment of operating procedures to prevent such initiating events, or otherwise to minimize their consequences, and to return the plant to a safe state.
- (3) For the third level of defence, it is assumed that, although very unlikely, the escalation of certain anticipated operational occurrences or postulated initiating events might not be controlled at a preceding level and that an accident could develop. In the design of the plant, such accidents are postulated to occur. This leads to the requirement that inherent and/or engineered safety features, safety systems and procedures be capable of preventing damage to the reactor core or preventing radioactive releases requiring off-site protective actions and returning the plant to a safe state.
- (4) The purpose of the fourth level of defence is to mitigate the consequences of accidents that result from failure of the third level of defence in depth. This is achieved by preventing the progression of such accidents and mitigating the consequences of a severe accident. The safety objective in the case of a severe accident is that only protective actions that are limited in terms of lengths of time and areas of application would be necessary and that off-site contamination would be avoided or minimized. Event sequences that would lead to an early radioactive release or a large radioactive release<sup>3</sup> are required to be 'practically eliminated'<sup>4</sup>.
- (5) The purpose of the fifth and final level of defence is to mitigate the radiological consequences of radioactive releases that could potentially result from accidents. This requires the provision of adequately equipped emergency response facilities and emergency plans and emergency procedures for on-site and off-site emergency response.

2.14. A relevant aspect of the implementation of defence in depth for a nuclear power plant is the provision in the design of a series of physical barriers, as well as a combination of active, passive and inherent safety features that contribute to the effectiveness of the physical barriers in confining radioactive material at specified locations. The number of barriers that will be necessary will depend upon the initial source term in terms of the amount and isotopic composition of radionuclides, the effectiveness of the individual barriers, the possible internal and external hazards, and the potential consequences of failures.

#### MAINTAINING THE INTEGRITY OF DESIGN OF THE PLANT THROUGHOUT THE LIFETIME OF THE PLANT

2.15. The design, construction and commissioning of a nuclear power plant might be shared between a number of organizations: the architect-engineer, the vendor of the reactor and its supporting systems,

---

<sup>3</sup> An 'early radioactive release' in this context is a radioactive release for which off-site protective actions would be necessary but would be unlikely to be fully effective in due time. A 'large radioactive release' is a radioactive release for which off-site protective actions that are limited in terms of lengths of time and areas of application would be insufficient for the protection of people and of the environment.

<sup>4</sup> 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.

the suppliers of major components, the designers of electrical systems, and the suppliers of other systems that are important to the safety of the plant.

2.16. The prime responsibility for safety rests with the person or organization responsible for facilities and activities that give rise to radiation risks (i.e. the operating organization) [1]. In 2003, the International Nuclear Safety Advisory Group suggested that the operating organization could set up a formal process to maintain the integrity of design of the plant throughout the lifetime of the plant (i.e. during the operating lifetime and into the decommissioning stage) [7]. A formally designated entity within the operating organization would take responsibility for this process.

2.17. In practice, the design of a nuclear power plant is complete only when the full plant specification (including site details) is produced for its procurement and licensing. Reference [7] emphasizes the need for a formally designated entity that has overall responsibility for the design process and is responsible for approving design changes and for ensuring that the requisite knowledge is maintained. Reference [7] also introduces the concept of ‘responsible designers’, to whom this formally designated entity could assign specific responsibilities for the design of parts of the plant. Prior to an application for authorization of a plant, the responsibility for the design will rest with the design organization (e.g. the vendor). Once an application for authorization of a plant has been made, the prime responsibility for safety will lie with the applicant, although detailed knowledge of the design will rest with the responsible designers. This balance will change as the plant is put into operation, since much of this detailed knowledge, such as the knowledge embodied in the safety analysis report, design manuals and other design documentation, will be transferred to the operating organization. To facilitate this transfer of knowledge, the structure of the formally designated entity that has overall responsibility for the design process would be established at an early stage.

2.18. The management system requirements that are placed on this formally designated entity would also apply to the responsible designers. However, the overall responsibility for maintaining the integrity of design of the plant would rest with the formally designated entity, and hence, ultimately, with the operating organization.

### 3. MANAGEMENT OF SAFETY IN DESIGN

#### **Requirement 1: Responsibilities in the management of safety in plant design**

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

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

#### **Requirement 2: Management system for plant design**

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

---

<sup>5</sup> The design organization is the organization responsible for preparation of the final detailed design of the plant to be built.

3.2. The management system<sup>6</sup> shall include provision for ensuring the quality of the design of each structure, system and component, as well as of the overall design of the nuclear power plant, at all times. This includes the means for identifying and correcting design deficiencies, for checking the adequacy of the design and for controlling design changes.

3.3. The design of the plant, including subsequent changes, modifications or safety improvements, shall be in accordance with established procedures that call on appropriate engineering codes and standards and shall incorporate relevant requirements and design bases. Interfaces shall be identified and controlled.

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

### **Requirement 3: Safety of the plant design throughout the lifetime of the plant**

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

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

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

- (a) That the plant design is fit for purpose and meets the requirement for the optimization of protection and safety by keeping radiation risks as low as reasonably achievable;
- (b) That the design verification, definition of engineering codes and standards and requirements, use of proven engineering practices, provision for feedback of information on construction and experience, approval of key engineering documents, conduct of safety assessments and maintaining a safety culture are included in the formal system for ensuring the continuing safety of the plant design;
- (c) That the knowledge of the design that is needed for safe operation, maintenance (including adequate intervals for testing) and modification of the plant is available, that this knowledge is maintained up to date by the operating organization, and that due account is taken of past operating experience and validated research findings;
- (d) That management of design requirements and configuration control are maintained;
- (e) That the necessary interfaces with responsible designers and suppliers engaged in design work are established and controlled;
- (f) That the necessary engineering expertise and scientific and technical knowledge are maintained within the operating organization;
- (g) That all design changes to the plant are reviewed, verified, documented and approved;
- (h) That adequate documentation is maintained to facilitate future decommissioning of the plant.

---

<sup>6</sup> Requirements on the management system are established in IAEA Safety Standards Series No. GS-R-3, The Management System for Facilities and Activities [8].

## 4. PRINCIPAL TECHNICAL REQUIREMENTS

### Requirement 4: Fundamental safety functions

**Fulfilment of the following fundamental safety functions for a nuclear power plant shall be ensured for all plant states: (i) control of reactivity; (ii) removal of heat from the reactor and from the fuel store; and (iii) confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.**

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

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

### Requirement 5: Radiation protection in design

**The design of a nuclear power plant shall be such as to ensure that radiation doses to workers at the plant and to members of the public do not exceed the dose limits, that they are kept as low as reasonably achievable in operational states for the entire lifetime of the plant, and that they remain below acceptable limits and as low as reasonably achievable in, and following, accident conditions.**

4.3. The design shall be such as to ensure that plant states that could lead to high radiation doses or to a large radioactive release have been 'practically eliminated'<sup>7</sup>, and that there would be no, or only minor, potential radiological consequences for plant states with a significant likelihood of occurrence.

4.4. Acceptable limits for purposes of radiation protection<sup>8</sup> associated with the relevant categories of plant states shall be established, consistent with the regulatory requirements.

### Requirement 6: Design for a nuclear power plant

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

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

---

<sup>7</sup> 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.

<sup>8</sup> Requirements on radiation protection and safety of radiation sources are established in IAEA Safety Standards Series No. GSR Part 3, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards [9]

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

4.7. The design shall take due account of the results of deterministic safety analyses and probabilistic safety analyses, to ensure that due consideration is given to the prevention of accidents and to mitigation of the consequences of any accidents that do occur.

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

#### **Requirement 7: Application of defence in depth**

**The design of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent as far as is practicable.**

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

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

4.11. The design:

- (a) Shall provide for multiple physical barriers to the release of radioactive material to the environment;
- (b) Shall be conservative, and the construction shall be of high quality, so as to provide assurance that failures and deviations from normal operation are minimized, that accidents are prevented as far as is practicable and that a small deviation in a plant parameter does not lead to a cliff edge effect<sup>9</sup>;
- (c) Shall provide for the control of plant behaviour by means of inherent and engineered features, such that failures and deviations from normal operation requiring actuation of safety systems are minimized or excluded by design, to the extent possible;
- (d) Shall provide for supplementing the control of the plant by means of automatic actuation of safety systems, such that failures and deviations from normal operation that exceed the capability of control systems can be controlled with a high level of confidence, and the need for operator actions in the early phase of these failures or deviations from normal operation is minimized;
- (e) Shall provide for systems, structures and components and procedures to control the course of and, as far as practicable, to limit the consequences of failures and deviations from normal operation that exceed the capability of safety systems;
- (f) Shall provide multiple means for ensuring that each of the fundamental safety functions is performed, thereby ensuring the effectiveness of the barriers and mitigating the consequences of any failure or deviation from normal operation.

---

<sup>9</sup> A 'cliff edge effect', in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input

4.12. To ensure that the concept of defence in depth is maintained, the design shall prevent, as far as is practicable:

- (a) Challenges to the integrity of physical barriers;
- (b) Failure of one or more barriers;
- (c) Failure of a barrier as a consequence of the failure of another barrier;
- (d) The possibility of harmful consequences of errors in operation and maintenance.

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

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

#### **Requirement 8: Interfaces of safety with security and safeguards**

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

#### **Requirement 9: Proven engineering practices**

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

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

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

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

#### **Requirement 10: Safety assessment**

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

4.17. The safety assessments<sup>10</sup> shall be commenced at an early point in the design process, with iterations between design activities and confirmatory analytical activities, and shall increase in scope and level of detail as the design programme progresses.

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

**Requirement 11: Provision for construction**

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

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

**BOX 1. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* See para. 4.19

*Suggested interpretations:* None

*Justification for the suggested changes:*

In many cases, NPPs incorporating SMRs are being designed to optimize off-site manufacture of major portions to leverage the value of this approach. With the implementation of factory manufacturing, there is a need for the inclusion of manufacturing as one of the provisions associated with this safety requirement.

**Requirement 12: Features to facilitate radioactive waste management and decommissioning**

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

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

- (a) The choice of materials, so that amounts of radioactive waste will be minimized to the extent practicable and decontamination will be facilitated;
- (b) The access capabilities and the means of handling that might be necessary;
- (c) The facilities necessary for the management (i.e. segregation, characterization, classification, pretreatment, treatment and conditioning) and storage of radioactive waste generated in operation, and provision for managing the radioactive waste that will be generated in the decommissioning of the plant.

---

<sup>10</sup> Requirements on safety assessment for facilities and activities are established in GSR Part 4 (Rev. 1) [2].

## 5. GENERAL PLANT DESIGN

### DESIGN BASIS

#### **Requirement 13: Categories of plant states**

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

5.1. Plant states shall typically cover:

- (a) Normal operation;
- (b) Anticipated operational occurrences, which are expected to occur over the operating lifetime of the plant;
- (c) Design basis accidents;
- (d) Design extension conditions, including accidents with core melting.

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

#### **Requirement 14: Design basis for items important to safety**

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

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

#### **Requirement 15: Design limits**

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

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

#### **Requirement 16: Postulated initiating events**

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

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

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

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

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

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

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

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

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

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

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

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

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

**Requirement 17: Internal and external hazards**

**All foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety of the nuclear power plant, shall be**

**identified and their effects shall be evaluated. Hazards shall be considered in designing the layout of the plant and in determining the postulated initiating events and generated loadings for use in the design of relevant items important to safety for the plant.**

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

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

*5.15C. For multi-module units, the design shall take due account of the potential for specific hazards to give rise to impacts on several or even all modules of the unit simultaneously and to the potential for hazards initiating from one reactor module impacting other reactor modules of the same unit.*

#### **Internal hazards**

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

#### **External hazards**

5.17. The design shall include due consideration of those natural and human induced external events<sup>11</sup> (i.e. events of origin external to the plant) that have been identified in the site evaluation process. Causation and likelihood shall be considered in postulating potential hazards. In the short term, the safety of the plant shall not be permitted to be dependent on the availability of off-site services such as electricity supply and firefighting services. The design shall take due account of site specific conditions to determine the maximum delay time by which off-site services need to be available.

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

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

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

5.21. The design of the plant shall provide for an adequate margin to protect items important to safety against levels of external hazards to be considered for design, derived from the hazard evaluation for the site, and to avoid cliff edge effects.<sup>12</sup>

---

<sup>11</sup> Requirements on site evaluation for nuclear installations are established in IAEA Safety Standards Series No. NS-R-3 (Rev. 1), Site Evaluation for Nuclear Installations [10].

<sup>12</sup> A 'cliff edge effect', in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.

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

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

## **BOX 2. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* See new para. 5.15C.

*Suggested interpretations:*

5.15A: The interpretation of the term ‘located’ has to allow for provisions to meet the requirement with separation by distance but also with other options, such as segregation by physical barriers.

5.16 and 5.17 (mainly): The potential impact of faults, hazards and transients occurring at coupled facilities (such as those for process heat applications) have to be considered as potential sources of hazards in the safety analyses.

*Justification for the suggested changes and interpretations:*

Regarding 5.15A: As SMRs are intended to be compact NPPs, protection against zonal effects can be provided by appropriate barriers as well as with separation by distance.

Regarding 5.15C: In a multiple modules design configuration (multi-module units), the potential for interactions between modules, or the simultaneous impact of all the modules due to internal and external hazards, has to be taken into account.

Regarding the interpretation of 5.16 and 5.17 (mainly): Future applications of SMRs include the direct use of process heat from the power plant, e.g. for district heating, heat processing or water desalination. These additional connections also represent potential sources of hazards and have to be taken into account.

### **Requirement 18: Engineering design rules**

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

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

### **Requirement 19: Design basis accidents**

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

5.24. Design basis accidents shall be used to define the design bases, including performance criteria, for safety systems and for other items important to safety that are necessary to control design

basis accident conditions, with the objective of returning the plant to a safe state and mitigating the consequences of any accidents.

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

5.26. The design basis accidents shall be analysed in a conservative manner. This approach involves postulating certain failures in safety systems, specifying design criteria and using conservative assumptions, models and input parameters in the analysis.

#### **Requirement 20: Design extension conditions**

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

5.27. An analysis of design extension conditions for the plant shall be performed.<sup>13</sup> The main technical objective of considering the design extension conditions is to provide assurance that the design of the plant is such as to prevent accident conditions that are not considered design basis accident conditions, or to mitigate their consequences, as far as is reasonably practicable. This might require additional safety features for design extension conditions, or extension of the capability of safety systems to prevent, or to mitigate the consequences of, a severe accident, or to maintain the integrity of the containment. These additional safety features for design extension conditions, or this extension of the capability of safety systems, shall be such as to ensure the capability for managing accident conditions in which there is a significant amount of radioactive material in the containment (including radioactive material resulting from severe degradation of the reactor core). The plant shall be designed so that it can be brought into a controlled state and the containment function can be maintained, with the result that the possibility of plant states arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated'.<sup>14</sup> The effectiveness of provisions to ensure the functionality of the containment could be analysed on the basis of the best estimate approach.

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

5.29. The analysis undertaken shall include identification of the features that are designed for use in, or that are capable<sup>15</sup> of preventing or mitigating, events considered in the design extension conditions. These features:

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

---

<sup>13</sup> The analysis of design extension conditions for the plant could be performed by means of a best estimate approach (more stringent approaches may be used according to States' requirements).

<sup>14</sup> 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.

<sup>15</sup> For returning the plant to a safe state or for mitigating the consequences of an accident, consideration could be given to the full design capabilities of the plant and to the temporary use of additional systems

- (b) Shall be capable of performing in the environmental conditions pertaining to these design extension conditions, including design extension conditions in severe accidents, where appropriate;
- (c) Shall have reliability commensurate with the function that they are required to fulfil.

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

5.31. The design shall be such that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated'.<sup>16</sup>

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

#### **Combinations of events and failures**

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

#### **Requirement 21: Physical separation and independence of safety systems**

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

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

#### **Requirement 22: Safety classification**

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

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

- (a) The safety function(s) to be performed by the item;
- (b) The consequences of failure to perform a safety function;
- (c) The frequency with which the item will be called upon to perform a safety function;
- (d) The time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function.

---

<sup>16</sup> 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.

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

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

**Requirement 23: Reliability of items important to safety**

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

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

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

**Requirement 24: Common cause failures**

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

**Requirement 25: Single failure criterion**

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

5.39. Spurious action shall be considered to be one mode of failure when applying the single failure criterion<sup>17</sup> to a safety group or safety system.

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

**Requirement 26: Fail-safe design**

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

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

**Requirement 27: Support service systems**

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

---

<sup>17</sup> A single failure is a failure that results in the loss of capability of a system or component to perform its intended safety function(s) and any consequential failure(s) that result from it. The single failure criterion is a criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure.

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

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

#### **Requirement 28: Operational limits and conditions for safe operation**

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

5.44. The requirements and operational limits and conditions established in the design for the nuclear power plant shall include (Requirement 6 of IAEA Safety Standards Series No. SSR-2/2 (Rev. 1), Safety of Nuclear Power Plants: Commissioning and Operation [4]):

- (a) Safety limits;
- (b) Limiting settings for safety systems;
- (c) Limits and conditions for normal operation;
- (d) Control system constraints and procedural constraints on process variables and other important parameters;
- (e) Requirements for surveillance, maintenance, testing and inspection of the plant to ensure that structures, systems and components function as intended in the design, to comply with the requirement for optimization by keeping radiation risks as low as reasonably achievable;
- (f) Specified operational configurations, including operational restrictions in the event of the unavailability of safety systems or safety related systems;
- (g) Action statements, including completion times for actions in response to deviations from the operational limits and conditions.

#### DESIGN FOR SAFE OPERATION OVER THE LIFETIME OF THE PLANT

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

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

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

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

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

- (a) Other proven alternative and/or indirect methods such as surveillance testing of reference items or use of verified and validated calculational methods shall be specified.
- (b) Conservative safety margins shall be applied or other appropriate precautions shall be taken to compensate for possible unanticipated failures.

### **Requirement 30: Qualification of items important to safety**

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

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

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

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

### **Requirement 31: Ageing management**

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

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

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

## **HUMAN FACTORS**

### **Requirement 32: Design for optimal operator performance**

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

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

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

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

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

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

- (a) To assess the general state of the plant in any condition;
- (b) To operate the plant within the specified limits on parameters associated with plant systems and equipment (operational limits and conditions);
- (c) To confirm that safety actions for the actuation of safety systems are automatically initiated when needed and that the relevant systems perform as intended;
- (d) To determine both the need for and the time for manual initiation of the specified safety actions.

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

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

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

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

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

#### OTHER DESIGN CONSIDERATIONS

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

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

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

***Requirement 33A: Safety systems, and safety features for design extension conditions, of modules of a multi-module unit***

***Each module of a multi-module unit shall have its own safety systems and shall have its own safety features for design extension conditions, as far as practicable. Where a safety system or a safety feature for design extension conditions is shared between reactor modules of a multi-module unit, the shared safety system or safety feature shall be functionally capable of fulfilling the safety requirements of each of these modules simultaneously, to protect against the consequences of events which have the potential to affect multiple modules.***

*5.63A. To further enhance safety, means allowing interconnections between modules of a multi-module unit shall be considered in the design.*

**BOX 3. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* To complement Requirement 33 (and 5.63) with Requirement 33A (and 5.63A).

*Suggested interpretations:* None.

*Justification for the suggested changes:*

SMR designs might consider sharing safety systems and safety features, especially safety features for design extension conditions and safety features designed to enhance safety and grace periods. However, it has to be made clear that safety cannot be negatively impacted by the sharing of safety systems or safety features.

**Requirement 34: Systems containing fissile material or radioactive material**

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

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

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

**Requirement 36: Escape routes from the plant**

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

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

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

**Requirement 37: Communication systems at the plant**

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

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

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

**Requirement 38: Control of access to the plant**

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

5.68. Provision shall be made in the design of the buildings and the layout of the site for the control of access to the nuclear power plant by operating personnel and/or for equipment, including emergency response personnel and vehicles, with particular consideration given to guarding against the unauthorized entry of persons and goods to the plant.

**Requirement 39: Prevention of unauthorized access to, or interference with, items important to safety**

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

**Requirement 40: Prevention of harmful interactions of systems important to safety**

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

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

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

**Requirement 41: Interactions between the electrical power grid and the plant**

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

**Requirement 42: Safety analysis of the plant design**

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

5.71. On the basis of a safety analysis, the design basis for items important to safety and their links to initiating events and event sequences shall be confirmed.<sup>18</sup> It shall be demonstrated that the nuclear power plant as designed is capable of complying with authorized limits on discharges with regard to radioactive releases and with the dose limits in all operational states, and is capable of meeting acceptable limits for accident conditions.

5.72. The safety analysis shall provide assurance that defence in depth has been implemented in the design of the plant.

5.73. The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects<sup>19</sup> and early radioactive releases or large radioactive releases.

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

**Deterministic approach**

5.75. The deterministic safety analysis shall mainly provide:

- (a) Establishment and confirmation of the design bases for all items important to safety;
- (b) Characterization of the postulated initiating events that are appropriate for the site and the design of the plant;
- (c) Analysis and evaluation of event sequences that result from postulated initiating events, to confirm the qualification requirements;
- (d) Comparison of the results of the analysis with acceptance criteria, design limits, dose limits and acceptable limits for purposes of radiation protection;
- (e) Demonstration that the management of anticipated operational occurrences and design basis accidents is possible by safety actions for the automatic actuation of safety systems in combination with prescribed actions by the operator;
- (f) Demonstration that the management of design extension conditions is possible by the automatic actuation of safety systems and the use of safety features in combination with expected actions by the operator.

**Probabilistic approach**

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

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

---

<sup>18</sup> Requirements on safety assessment for facilities and activities are established in GSR Part 4 (Rev. 1) [2].

<sup>19</sup> A 'cliff edge effect', in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.

- (b) Providing assurance that situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented;<sup>20</sup>
- (c) Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.

## 6. DESIGN OF SPECIFIC PLANT SYSTEMS

### REACTOR CORE AND ASSOCIATED FEATURES

#### **Requirement 43: Performance of fuel elements and assemblies**

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

6.1 The processes of deterioration to be considered shall include those arising from:

- Differential expansion and deformation;
- External pressure of the coolant;
- Additional internal pressure due to fission products and the buildup of helium in fuel elements;
- Irradiation of fuel and other materials in the fuel assembly;
- Variations in pressure and temperature resulting from variations in power demand;
- Chemical effects;
- Static and dynamic loading, including flow induced vibrations and mechanical vibrations;
- Variations in performance in relation to heat transfer that could result from distortion or chemical effects.

Allowance shall be made for uncertainties in data, in calculations and in manufacture.

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

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

#### **Requirement 44: Structural capability of the reactor core**

**The fuel elements and fuel assemblies and their supporting structures for the nuclear power plant shall be designed so that, in operational states and in accident conditions other than severe accidents, a geometry that allows for adequate cooling is maintained and the insertion of control rods is not impeded.**

#### **Requirement 45: Control of the reactor core**

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

---

<sup>20</sup> A 'cliff edge effect', in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.

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

6.5. In the design of reactivity control devices, due account shall be taken of wear out and of the effects of irradiation, such as burnup, changes in physical properties and production of gas.

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

#### **Requirement 46: Reactor shutdown**

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

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

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

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

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

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

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

#### REACTOR COOLANT SYSTEMS

#### **Requirement 47: Design of reactor coolant systems**

**The components of the reactor coolant systems for the nuclear power plant shall be designed and constructed so that the risk of faults due to inadequate quality of materials, inadequate design standards, insufficient capability for inspection or inadequate quality of manufacture is minimized.**

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

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

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

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

**Requirement 48: Overpressure protection of the reactor coolant pressure boundary**

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

**Requirement 49: Inventory of reactor coolant**

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

**Requirement 50: Cleanup of reactor coolant**

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

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

**Requirement 51: Removal of residual heat from the reactor core**

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

**Requirement 52: Emergency cooling of the reactor core**

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

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

- (a) The limiting parameters for the cladding or for integrity of the fuel (such as temperature) will not be exceeded;
- (b) Possible chemical reactions are kept to an acceptable level;
- (c) The effectiveness of the means of cooling of the reactor core compensates for possible changes in the fuel and in the internal geometry of the reactor core;
- (d) Cooling of the reactor core will be ensured for a sufficient time.

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

### **Requirement 53: Heat transfer to an ultimate heat sink**

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

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

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

## CONTAINMENT STRUCTURE AND CONTAINMENT SYSTEM

### **Requirement 54: Containment system for the reactor**

**A containment system shall be provided to ensure, or to contribute to, the fulfilment of the following safety functions at the nuclear power plant:**

**(i) confinement of radioactive substances in operational states and in accident conditions; (ii) protection of the reactor against natural external events and human induced events; and (iii) radiation shielding in operational states and in accident conditions.**

### **Requirement 55: Control of radioactive releases from the containment**

**The design of the containment shall be such as to ensure that any radioactive release from the nuclear power plant to the environment is as low as reasonably achievable, is below the authorized limits on discharges in operational states and is below acceptable limits in accident conditions.**

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

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

### **Requirement 56: Isolation of the containment**

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

6.22. Lines that penetrate the containment as part of the reactor coolant pressure boundary and lines that are connected directly to the containment atmosphere shall be fitted with at least two adequate containment isolation valves or check valves arranged in series<sup>21</sup> and shall be provided with suitable leak detection systems. Containment isolation valves or check valves shall be located as close to the containment as is practicable, and each valve shall be capable of reliable and independent actuation and of being periodically tested.

---

<sup>21</sup> In most cases, one containment isolation valve or check valve is outside the containment and the other is inside the containment. Other arrangements might be acceptable, however, depending on the design.

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

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

**Requirement 57: Access to the containment**

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

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

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

**BOX 4. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* None

*Suggested interpretations:*

In case of SMR designs that do not need access to the containment during power operation or in case of accident conditions, this requirement would not be applicable.

*Justification for the suggested interpretations:*

Containment in many SMR designs does not allow for any human access during operational states and accident conditions and many SMR designs are not equipped with large doors or equipment access hatches.

**Requirement 58: Control of containment conditions**

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

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

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

the containment shall have sufficient reliability and redundancy to ensure that this function can be fulfilled.

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

6.28B. The design shall also include features to enable the safe use of non-permanent equipment<sup>22</sup> for restoring the capability to remove heat from the containment.

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

- (a) To reduce the amounts of fission products that could be released to the environment in accident conditions;
- (b) To control the concentrations of hydrogen, oxygen and other substances in the containment atmosphere in accident conditions so as to prevent deflagration or detonation loads that could challenge the integrity of the containment.

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

## INSTRUMENTATION AND CONTROL SYSTEMS

### **Requirement 59: Provision of instrumentation**

**Instrumentation shall be provided for: determining the values of all the main variables that can affect the fission process, the integrity of the reactor core, the reactor coolant systems and the containment at the nuclear power plant; for obtaining essential information on the plant that is necessary for its safe and reliable operation; for determining the status of the plant in accident conditions; and for making decisions for the purposes of accident management.**

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

### **Requirement 60: Control systems**

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

### **Requirement 61: Protection system**

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

6.32. The protection system shall be designed:

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

---

<sup>22</sup> Non-permanent equipment need not necessarily be stored on the site.

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

6.33. The design:

- (a) Shall prevent operator actions that could compromise the effectiveness of the protection system in operational states and in accident conditions, but shall not counteract correct operator actions in accident conditions;
- (b) Shall automate various safety actions to actuate safety systems so that operator action is not necessary within a justified period of time from the onset of anticipated operational occurrences or accident conditions;
- (c) Shall make relevant information available to the operator for monitoring the effects of automatic actions.

#### **Requirement 62: Reliability and testability of instrumentation and control systems**

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

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

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

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

#### **Requirement 63: Use of computer based equipment in systems important to safety**

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

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

- (a) A high quality of, and best practices for, hardware and software shall be used, in accordance with the importance of the system to safety.
- (b) The entire development process, including control, testing and commissioning of design changes, shall be systematically documented and shall be reviewable.
- (c) An assessment of the equipment shall be undertaken by experts who are independent of the design team and the supplier team to provide assurance of its high reliability.
- (d) Where safety functions are essential for achieving and maintaining safe conditions, and the necessary high reliability of the equipment cannot be demonstrated with a high level of confidence, diverse means of ensuring fulfilment of the safety functions shall be provided.
- (e) Common cause failures deriving from software shall be taken into consideration.
- (f) Protection shall be provided against accidental disruption of, or deliberate interference with, system operation.

#### **Requirement 64: Separation of protection systems and control systems**

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

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

#### **Requirement 65: Control room**

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

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

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

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

#### **Requirement 66: Supplementary control room**

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

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

#### **Requirement 67: Emergency response facilities on the site**

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

6.42. Information about important plant parameters and radiological conditions at the nuclear power plant and in its immediate surroundings shall be provided to the relevant emergency response facilities<sup>23</sup>. Each facility shall be provided with means of communication with, as appropriate, the

---

<sup>23</sup> Emergency response facilities are addressed in IAEA Safety Standards Series No. GSR Part 7, Preparedness and Response for a Nuclear or Radiological Emergency [11]. For nuclear power plants, emergency response facilities (which are separate from the control room and the supplementary control room) include the technical support centre, the operational support centre and the emergency centre.

control room, the supplementary control room and other important locations at the plant, and with on-site and off-site emergency response organizations.

## EMERGENCY POWER SUPPLY

### **Requirement 68: Design for withstanding the loss of off-site power**

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

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

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

6.44A. The alternate power source shall be capable of supplying the necessary power to preserve the integrity of the reactor coolant system and to prevent significant damage to the core and to spent fuel in the event of the loss of off-site power combined with failure of the emergency power supply.

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

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

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

6.45. The design basis for any diesel engine or other prime mover<sup>24</sup> that provides an emergency power supply to items important to safety shall include:

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

6.45A. The design shall also include features to enable the safe use of non-permanent equipment to restore the necessary electrical power supply.<sup>25</sup>

---

<sup>24</sup> A prime mover is a component (such as a motor, solenoid operator or pneumatic operator) that converts energy into action when commanded by an actuation device.

<sup>25</sup> Non-permanent equipment need not necessarily be stored on the site.

## **BOX 5. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* None.

*Suggested interpretations:*

The term ‘necessary power’ used regarding emergency power supply and alternate power source has to be interpreted as applicable to all the safety functions and support functions that need power supply.

*Justification for the suggested interpretations:*

SMRs might be designed with passive or non-power dependent safety features and therefore might not be reliant on power in order to maintain safety. Nevertheless, an emergency or alternate power supply with adequate reliability has to be in place for monitoring the reactor under loss of off-site power supply and any other accidents, even for plants using extensive passive safety features.

### SUPPORTING SYSTEMS AND AUXILIARY SYSTEMS

#### **Requirement 69: Performance of supporting systems and auxiliary systems**

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

#### **Requirement 70: Heat transport systems**

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

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

#### **Requirement 71: Process sampling systems and post-accident sampling systems**

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

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

#### **Requirement 72: Compressed air systems**

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

#### **Requirement 73: Air conditioning systems and ventilation systems**

Systems for air conditioning, air heating, air cooling and ventilation shall be provided as appropriate in auxiliary rooms or other areas at the nuclear power plant to maintain the

**required environmental conditions for systems and components important to safety in all plant states.**

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

- (a) To prevent unacceptable dispersion of airborne radioactive substances within the plant;
- (b) To reduce the concentration of airborne radioactive substances to levels compatible with the need for access by personnel to the area;
- (c) To keep the levels of airborne radioactive substances in the plant below authorized limits and as low as reasonably achievable;
- (d) To ventilate rooms containing inert gases or noxious gases without impairing the capability to control radioactive effluents;
- (e) To control gaseous radioactive releases to the environment below the authorized limits on discharges and to keep them as low as reasonably achievable.

6.49. *The design shall minimize the spread of contamination from areas of high contamination to areas of low contamination, for example by maintaining areas of higher contamination at the plant ~~shall be maintained~~ at a negative pressure differential (partial vacuum) with respect to areas of lower contamination and other accessible areas.*

#### **BOX 6. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* See para. 6.49

*Suggested interpretations:* None.

*Justification for the suggested changes:*

Even though the negative pressure differential (partial vacuum) has been utilized for the minimization of contamination spread for the existing NPPs, other mechanisms can be utilized to achieve this aim. The original wording of the requirement describes the negative pressure differential as the only measure for the minimization of contamination spread and needs to be generalized for application to SMRs. The generalization is considered especially necessary for SMR designs incorporating passive safety systems, having the possibility of employing alternative means for isolating areas of contamination from clean areas, when an accident occurs.

#### **Requirement 74: Fire protection systems**

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

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

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

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

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

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

#### **Requirement 75: Lighting systems**

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

#### **Requirement 76: ~~Overhead~~ Lifting equipment**

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

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

- (a) Measures are taken to prevent the lifting of excessive loads;
- (b) Conservative design measures are applied to prevent any unintentional dropping of loads that could affect items important to safety;
- (c) The plant layout permits safe movement of the ~~overhead~~ lifting equipment and of items being transported;
- (d) Such equipment can be used only in specified plant states (by means of safety interlocks on the *lifting equipment-crane*);
  - (e) Such equipment for use in areas where items important to safety are located is seismically qualified.

### **BOX 7. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* See title, overarching requirement and para. 6.55, with items (c) and (d)

*Suggested interpretations:* None.

*Justification for the suggested changes:*

Limiting the lifting equipment to overhead equipment might have undesirable effects. Some SMR designs do not allow for the use of overhead lifting equipment because of a lack of overall volume to handle the items. Requirement 76 as it is currently formulated is not applicable to these SMR designs. The purpose of the suggested changes is to remove that limitation, allowing for other types of lifting equipment when appropriate, such as jacks, forklifts and cranes.

It is understood that the suggested changes have very little impact on the lifting equipment used in large scale NPPs, therefore it might be considered to incorporate them to the design safety requirements in the next revision

## OTHER POWER CONVERSION SYSTEMS

### **Requirement 77: Steam supply system, feedwater system and turbine generators**

**The design of the steam supply system, feedwater system and turbine generators for the nuclear power plant shall be such as to ensure that the appropriate design limits of the reactor coolant pressure boundary are not exceeded in operational states or in accident conditions.**

6.56. The design of the steam supply system shall provide for appropriately rated and qualified steam isolation valves capable of closing under the specified conditions in operational states and in accident conditions.

6.57. The steam supply system and the feedwater systems shall be of sufficient capacity and shall be designed to prevent anticipated operational occurrences from escalating to accident conditions.

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

## TREATMENT OF RADIOACTIVE EFFLUENTS AND RADIOACTIVE WASTE

### **Requirement 78: Systems for treatment and control of waste**

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

6.59. Systems and facilities shall be provided for the management and storage of radioactive waste on the nuclear power plant site *or at an off-site waste treatment facility* for a period of time consistent with the availability of the relevant disposal option.

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

## **BOX 8. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* See para. 6.59.

*Suggested interpretations:* None.

*Justification for the suggested changes:*

SMRs could be built in large numbers in a geographic area and therefore could enable a fleet solution to be derived for the effective and safe management of waste and the decommissioning process. This might enable consideration to be given to the construction of a single waste facility that would be built solely for that purpose. Such a fleet facility would have greater throughput of waste and therefore would offer a greater opportunity for the application of advanced processing technology to reduce environmental impact.

### **Requirement 79: Systems for treatment and control of effluents**

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

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

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

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

## FUEL HANDLING AND STORAGE SYSTEMS

### **Requirement 80: Fuel handling and storage systems**

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

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

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

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

- a) To prevent criticality by a specified margin, by physical means or by means of physical processes, and preferably by use of geometrically safe configurations, even under conditions of optimum moderation;
- b) To permit inspection of the fuel;
- c) To permit maintenance, periodic inspection and testing of components important to safety;
- d) To prevent damage to the fuel;
- e) To prevent the dropping of fuel in transit;
- f) To provide for the identification of individual fuel assemblies;
- g) To provide proper means for meeting the relevant requirements for radiation protection;
- h) To ensure that adequate operating procedures and a system of accounting for, and control of, nuclear fuel can be implemented to prevent any loss of, or loss of control over, nuclear fuel.

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

- (a) To permit adequate removal of heat from the fuel in operational states and in accident conditions;
- (b) To prevent the dropping of spent fuel in transit;
- (c) To avoid causing unacceptable handling stresses on fuel elements or fuel assemblies;
- (d) To prevent the potentially damaging dropping of heavy objects such as spent fuel casks, cranes or other objects onto the fuel;
- (e) To permit safe keeping of suspect or damaged fuel elements or fuel assemblies;
- (f) To control levels of soluble absorber if this is used for criticality safety;
- (g) To facilitate maintenance and future decommissioning of fuel handling and storage facilities;
- (h) To facilitate decontamination of fuel handling and storage areas and equipment when necessary;
- (i) To accommodate, with adequate margins, all the fuel removed from the reactor in accordance with the strategy for core management that is foreseen and the amount of fuel in the full reactor core;
- (j) To facilitate the removal of fuel from storage and its preparation for off-site transport.

6.68. For reactors using a water pool system for fuel storage, the design shall be such as to prevent the uncovering of fuel assemblies in all plant states that are of relevance for the spent fuel pool so that

the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated'<sup>26</sup> and so as to avoid high radiation fields on the site. The design of the plant:

- (a) Shall provide the necessary fuel cooling capabilities;
- (b) Shall provide features to prevent the uncovering of fuel assemblies in the event of a leak or a pipe break;
- (c) Shall provide a capability to restore the water inventory.

The design shall also include features to enable the safe use of non-permanent equipment to ensure sufficient water inventory for the long term cooling of spent fuel and for providing shielding against radiation.<sup>27</sup>

6.68A. The design shall include the following:

- (a) Means for monitoring and controlling the water temperature for operational states and for accident conditions that are of relevance for the spent fuel pool;
- (b) Means for monitoring and controlling the water level for operational states and for accident conditions that are of relevance for the spent fuel pool;
- (c) Means for monitoring and controlling the activity in water and in air for operational states and means for monitoring the activity in water and in air for accident conditions that are of relevance for the spent fuel pool;
- (d) Means for monitoring and controlling the water chemistry for operational states.

## RADIATION PROTECTION

### **Requirement 81: Design for radiation protection**

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

6.69. Radiation sources throughout the plant shall be comprehensively identified, and exposures and radiation risks associated with them shall be kept as low as reasonably achievable<sup>28</sup>, the integrity of the fuel cladding shall be maintained, and the generation and transport of corrosion products and activation products shall be controlled.

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

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

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

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

6.74. The plant layout shall be such that the doses received by operating personnel during normal operation, refuelling, maintenance and inspection can be kept as low as reasonably achievable, and

---

<sup>26</sup> 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.

<sup>27</sup> Non-permanent equipment need not necessarily be stored on the site.

<sup>28</sup> Requirements on radiation protection and the safety of radiation sources for facilities and activities are established in GSR Part 3 [9].

due account shall be taken of the necessity for any special equipment to be provided to meet these requirements.

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

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

#### **Requirement 82: Means of radiation monitoring**

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

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

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

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

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

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

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

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

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

- (a) Exposure pathways to people, including the food chain;
- (b) Radiological impacts, if any, on the local environment;
- (c) The possible buildup, and accumulation in the environment, of radioactive substances;
- (d) The possibility of there being any unauthorized routes for radioactive releases.

### **BOX 9. CONSIDERATIONS ON POTENTIAL ADDITIONAL REQUIREMENTS FOR MULTI-MODULE UNITS** *(These considerations are also applicable to HTG-SMRs)*

New requirements or additions to the existing requirements are deemed necessary to address particular safety considerations related to the use of multiple reactor modules within a single

unit (multi-module units). Some of these new requirements have already been captured in this appendix; however, the following additional aspects might be considered in further reviews of the design safety requirements:

**A) Interconnections among the reactor modules.** For purposes such as operation and accident management, multi-module units might include interconnections between reactor modules. In this case, specific considerations are necessary to ensure that such interconnections will not be detrimental to the safety of each reactor module and of the overall plant.

**B) Control and protection systems.** The control and protection systems of each module and of all the modules have to ensure that a clear actuation logic is reliably implemented so that an initiating event or accident occurring within one reactor module will not propagate to accident conditions in other reactor modules and that the reactor modules will not have detrimental effects on each other under accident conditions.

**C) Human factors engineering.** This covers aspects relating to the main control room, supplementary control and other emergency response facilities and locations; maintenance of the multiple modules; potential remote control of the main control room; one operator managing several modules; more than one module supplying the same turbine.

**D) Emergency preparedness and response.** This includes aspects relating to the design of multi-module units to enable the emergency response under all relevant conditions.

**E) Capacity for the addition of future modules, plant lay-out and construction.** Some design schemes consider a plant lay-out which allows a consecutive and serialized construction of the reactor modules. This new practice has to involve additional important safety considerations. Some SMR designs adopt extension of power capacity during plant lifetime through additional module installation. Changes in specifications or capability might result in the addition of new equipment which could, for example, increase the load on heating, ventilating and air conditioning systems. Therefore, consideration might need to be given to including margins in the design capability of relevant support systems to allow for the potential addition of new equipment at a later date.

*Justification for the suggestion of adding new requirements in these areas:*

The safety requirements established in SSR-2/1 (Rev. 1) [2] are primarily applicable to land based stationary NPPs that comprise a single nuclear reactor or more nuclear reactors which are to a great extent independent of each other. When there are interconnections among the reactors, the number of the interconnections is very limited and usually the interconnections are meant to cope with complex plant conditions for safety considerations.

For SMR designs, there are more design configurations and application options than for land based stationary NPPs. An SMR unit might comprise more than one reactor module having, for example, a common control room, or might be housed in one common reactor building. These aspects are not covered in SSR-2/1 (Rev. 1) [2] and therefore pose new challenges in establishing design safety requirements.

## REFERENCES<sup>29</sup>

- [1] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR Part 4 Rev. 1), IAEA, Vienna (2016).
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection (2007 Edition), IAEA, Vienna (2007).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Commissioning and Operation, IAEA Safety Standards Series No. SSR-2/2 (Rev. 1), IAEA, Vienna (2016).
- [5] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).
- [6] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna (1999).
- [7] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life, INSAG-19, IAEA, Vienna (2003).
- [8] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-R-3, IAEA, Vienna (2006). (A revision of this publication is in preparation, to be issued as GSR Part 2.)
- [9] EUROPEAN COMMISSION, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards, IAEA Safety Standards Series No. GSR Part 3, IAEA, Vienna (2014).
- [10] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. NS-R-3 (Rev. 1), IAEA, Vienna (2016).
- [11] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR- TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015).

---

<sup>29</sup>List of references copied from SSR-2/1 (Rev. 1) [2].



## DEFINITIONS<sup>30</sup>

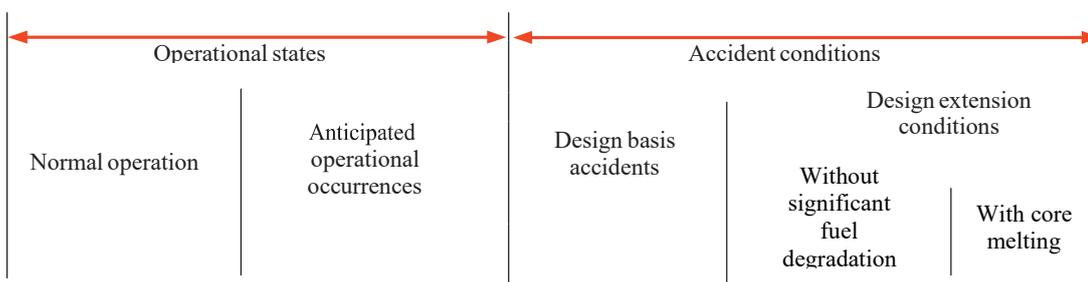
*The following new and revised definitions differ from those in the IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection (2007 Edition), IAEA, Vienna (2007):*

*<http://www-pub.iaea.org/books/IAEABooks/7648/IAEA-Safety-Glossary>*

*The symbol '(i)' denotes an information note.*

**controlled state.** Plant state, following an anticipated operational occurrence or accident conditions, in which the fundamental safety functions can be ensured and which can be maintained for a time sufficient to effect provisions to reach a safe state.

**plant states** (*considered in design*)



**accident conditions.** Deviations from normal operation that are less frequent and more severe than anticipated operational occurrences.

(i) Accident conditions comprise design basis accidents and design extension conditions.

**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.

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

(i) Design extension conditions comprise conditions in events without significant fuel degradation and conditions in events with core melting.

**safe state.** Plant state, following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time.

**safety feature for design extension conditions.** Item designed to perform a safety function or which has a safety function in design extension conditions.

**safety system settings.** Settings for levels at which safety systems are automatically actuated in the event of anticipated operational occurrences or design basis accidents, to prevent safety limits from being exceeded.

<sup>30</sup> List of definitions copied from SSR-2/1 (Rev. 1) [2].

## **BOX 10. CONSIDERATIONS ABOUT THE APPLICABILITY OF ‘DEFINITIONS’**

*Suggested changes: To add the definition of the following new terms:*

**Multi-module unit.** *A unit having the possibility of including more than one reactor module.*

- (i) *A multi-module unit might include only one reactor module in the first stage of its planned development*
- (ii) *Features of the multi-module unit approach typically include the following:*
  - a. *Allow the addition of several modules in close proximity to the same infrastructure;*
  - b. *The modules might be deployed in compact configurations and share structures, systems and components to a larger extent than in units using a single reactor design approach, provided fulfilment of corresponding requirements;*
  - c. *Each module can be operated mostly independently of the state of completion or operating condition of any other module of the multi-module unit;*
  - d. *The different modules are essentially identical.*

**Reactor module (sometimes abbreviated as ‘module’).** *A nuclear reactor with its associated structures, systems and components. This term is used in multi-module units.*

*Suggested interpretations: None*

*Justification for the suggested changes:*

The use of these terms is necessary in this publication and also in future publications related to design safety and safety assessment of SMRs

## APPENDIX II. APPLICABILITY OF DESIGN SAFETY REQUIREMENTS TO HTG-SMRS

This appendix includes specific considerations on the applicability of the IAEA design safety requirements established in SSR-2/1 (Rev. 1) [2] to HTG-SMRs. Relevant aspects of the approach used to identify these considerations and the format adopted to present the results are described in the main body of this publication (see Section 3). In accordance to that Section, no observations are provided to the paragraphs and requirements considered fully applicable as they are. For the requirements to which observations were made, the requirement number appears underlined, the changes to the wording are directly incorporated to the text of the safety requirement (in *italics*) and the other aspects (*'suggested interpretations'* and *'justification of the suggested changes and/or interpretations'*) are included in a text box placed at the end of the requirement.

The practical information provided in this publication represent the views of the contributors and cannot be considered as IAEA guidance or recommendations.

To clearly highlight the considerations of the applicability of the design safety requirements established in SSR-2/1 (Rev.1) [2] to SMRs, the entire text from SSR-2/1 (Rev.1) [2] is reproduced in full in this appendix, with the specific considerations identified inserted at relevant points within the text. For easier reading, the reproduced text that has no changes is shown in the original format (narrowed text) and the modified paragraphs in the format of this publication (full size text). The specific comments about the considerations on applicability are also reproduced in the format of this publication (full size text) and highlighted in boxes.

### 1. INTRODUCTION

#### BACKGROUND

1.1. The present publication supersedes the Safety Requirements publication Safety of Nuclear Power Plants: Design,<sup>1</sup> which was issued in 2012 as IAEA Safety Standards Series No. SSR-2/1. Account has been taken of the Fundamental Safety Principles [1], published in 2006. Requirements for nuclear safety are intended to ensure “the highest standards of safety that can reasonably be achieved” for the protection of workers, the public and the environment from harmful effects of ionizing radiation that could arise from nuclear power plants and other nuclear facilities [1]. It is recognized that technology and scientific knowledge advance, and that nuclear safety and the adequacy of protection against radiation risks need to be considered in the context of the present state of knowledge. Safety requirements will change over time; this Safety Requirements publication reflects the present consensus.

1.2. The designs of many existing nuclear power plants, as well as the designs for new nuclear power plants, have been enhanced to include additional measures to mitigate the consequences of complex accident sequences involving multiple failures and of severe accidents. Complementary systems and equipment with new capabilities have been backfitted to many existing nuclear power plants to aid in the prevention of severe accidents and the mitigation of their consequences. Guidance on the mitigation

---

<sup>1</sup> INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012)

of the consequences of severe accidents has been provided at most existing nuclear power plants. The design of new nuclear power plants now explicitly includes the consideration of severe accident scenarios and strategies for their management. Requirements related to the State system of accounting for, and control of, nuclear material and security related requirements are also taken into account in the design of nuclear power plants. Integration of safety measures and security measures will help to ensure that neither compromise the other.

1.3. It might not be practicable to apply all the requirements of this Safety Requirements publication to nuclear power plants that are already in operation or under construction. In addition, it might not be feasible to modify designs that have already been approved by regulatory bodies. For the safety analysis of such designs, it is expected that a comparison will be made with the current standards, for example as part of the periodic safety review for the plant, to determine whether the safe operation of the plant could be further enhanced by means of reasonably practicable safety improvements.

#### OBJECTIVE

1.4. This publication establishes design requirements for the structures, systems and components of a nuclear power plant, as well as for procedures and organizational processes important to safety that are required to be met for safe operation and for preventing events that could compromise safety, or for mitigating the consequences of such events, were they to occur.

1.5. This publication is intended for use by organizations involved in design, manufacture, construction, modification, maintenance, operation and decommissioning for nuclear power plants, in analysis, verification and review, and in the provision of technical support, as well as by regulatory bodies.

#### SCOPE

1.6. It is expected that this publication will be used primarily for land based stationary nuclear power plants with water cooled reactors designed for electricity generation or for other heat production applications (such as district heating or desalination). This publication may also be applied, with judgement, to other reactor types, to determine the requirements that have to be considered in developing the design.

#### **COMMENT TO PARAGRAPH 1.6**

Paragraph 1.6 indicates the ability to apply the safety requirements with judgement on a case by case basis. It is understood that judgement has to be informed by relevant and supportable evidence.

1.7. This publication does not address:

- (e) Requirements that are specifically covered in other IAEA Safety Requirements publications (e.g. IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), Safety Assessment for Facilities and Activities[2]);
- (f) Matters relating to nuclear security or to the State system of accounting for, and control of, nuclear material;
- (g) Conventional industrial safety that under no circumstances could affect the safety of the nuclear power plant;

- (h) Non-radiological impacts arising from the operation of nuclear power plants. 1.8. Terms in this publication are to be understood as defined and explained in the IAEA Safety Glossary [3], unless otherwise stated here (see Definitions).

1.8. Terms in this publication are to be understood as defined and explained in the IAEA Safety Glossary [3], unless otherwise stated here (see Definitions).

## STRUCTURE

1.9. This Safety Requirements publication follows the relationship between the safety objective and safety principles, and between requirements for nuclear safety functions and design criteria for safety. Section 2 elaborates on the safety objective, safety principles and concepts that form the basis for deriving the safety function requirements that must be met for the nuclear power plant, as well as the safety design criteria. Sections 3–6 establish numbered overarching requirements (shown in bold type), with additional requirements as appropriate in the paragraphs that follow them. Section 3 establishes the general requirements to be satisfied by the design organization in the management of safety in the design process. Section 4 establishes: requirements for principal technical design criteria for safety, including requirements for the fundamental safety functions, the application of defence in depth and provision for construction; requirements for interfaces of safety with nuclear security and with the State system of accounting for, and control of, nuclear material; and requirements for ensuring that radiation risks arising from the plant are maintained as low as reasonably achievable. Section 5 establishes requirements for general plant design that supplement the requirements for principal technical design criteria to ensure that safety objectives are met and the safety principles are applied. The requirements for general plant design apply to all items (i.e. structures, systems and components) important to safety. Section 6 establishes requirements for the design of specific plant systems such as the reactor core, reactor coolant systems, containment system, and instrumentation and control systems.

## **2. APPLYING THE SAFETY PRINCIPLES AND CONCEPTS**

2.1. The Fundamental Safety Principles [1] establish one fundamental safety objective and ten safety principles that provide the basis for requirements and measures for the protection of people and the environment against radiation risks and for the safety of facilities and activities that give rise to radiation risks.

2.2. This fundamental safety objective has to be achieved, and the ten safety principles have to be applied, without unduly limiting the operation of facilities or the conduct of activities that give rise to radiation risks. To ensure that nuclear power plants are operated and activities are conducted so as to achieve the highest standards of safety that can reasonably be achieved, measures have to be taken to achieve the following (see para. 2.1 of the Fundamental Safety Principles [1]):

- (a) To control the radiation exposure of people and radioactive releases to the environment in operational states;
- (b) To restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source, spent nuclear fuel, radioactive waste or any other source of radiation at a nuclear power plant;
- (c) To mitigate the consequences of such events if they were to occur.

2.3. The fundamental safety objective applies for all stages in the lifetime of a nuclear power plant, including planning, siting, design, manufacture, construction, commissioning and operation, as well as

decommissioning. This includes the associated transport of radioactive material and the management of spent nuclear fuel and radioactive waste (see para. 2.2 of the Fundamental Safety Principles [1]).

2.4. Paragraph 2.3 of the Fundamental Safety Principles [1] states that:

“Ten safety principles have been formulated, on the basis of which safety requirements are developed and safety measures are to be implemented in order to achieve the fundamental safety objective. The safety principles form a set that is applicable in its entirety; although in practice different principles may be more or less important in relation to particular circumstances, the appropriate application of all relevant principles is required.”

2.5. This Safety Requirements publication establishes requirements that apply those safety principles, which are particularly important in the design of nuclear power plants.

## RADIATION PROTECTION IN DESIGN

2.6. In order to satisfy the safety principles, it is required to ensure that for all operational states of a nuclear power plant and for any associated activities, doses from exposure to radiation within the installation or exposure due to any planned radioactive release from the installation are kept below the dose limits and kept as low as reasonably achievable. In addition, it is required to take measures for mitigating the radiological consequences of any accidents, if they were to occur.

2.7. To apply the safety principles, it is also required that nuclear power plants be designed and operated so as to keep all sources of radiation under strict technical and administrative control. However, this principle does not preclude limited exposures or the release of authorized amounts of radioactive substances to the environment from nuclear power plants in operational states. Such exposures and radioactive releases are required to be strictly controlled and to be kept as low as reasonably achievable, in compliance with regulatory and operational limits as well as radiation protection requirements [4].

## SAFETY IN DESIGN

2.8. To achieve the highest level of safety that can reasonably be achieved in the design of a nuclear power plant, measures are required to be taken to do the following, consistent with national acceptance criteria and safety objectives [1]:

- (a) To prevent accidents with harmful consequences resulting from a loss of control over the reactor core or over other sources of radiation, and to mitigate the consequences of any accidents that do occur;
- (b) To ensure that for all accidents taken into account in the design of the installation, any radiological consequences would be below the relevant limits and would be kept as low as reasonably achievable;
- (c) To ensure that the likelihood of occurrence of an accident with serious radiological consequences is extremely low and that the radiological consequences of such an accident would be mitigated to the fullest extent practicable.

2.9. To demonstrate that the fundamental safety objective [1] is achieved in the design of a nuclear power plant, a comprehensive safety assessment [2] of the design is required to be carried out. Its objective is to identify all possible sources of radiation and to evaluate possible doses that could be received by workers at the installation and by members of the public, as well as possible effects on the environment, as a result of operation of the plant. The safety assessment is required in order to examine: (i) normal operation of the plant; (ii) the performance of the plant in anticipated operational occurrences; and accident conditions. On the basis of this analysis, the capability of the design to withstand postulated

initiating events and accidents can be established, the effectiveness of the items important to safety can be demonstrated and the inputs (prerequisites) for emergency planning can be established.

2.10. Measures are required to be taken to control exposure for all operational states at levels that are as low as reasonably achievable and to minimize the likelihood of an accident that could lead to the loss of control over a source of radiation. Nevertheless, there will remain a possibility that an accident could happen. Measures are required to be taken to ensure that the radiological consequences of an accident would be mitigated. Such measures include the provision of safety features and safety systems, the establishment of accident management procedures by the operating organization and, possibly, the establishment of off-site protective actions by the appropriate authorities, supported as necessary by the operating organization, to mitigate exposures if an accident occurs.

2.11. The design for safety of a nuclear power plant applies the safety principle that practical measures must be taken to mitigate the consequences for human life and health and for the environment of nuclear or radiation accidents (Principle 8 of the Fundamental Safety Principles [1]). Plant event sequences that could result in high radiation doses or in a large radioactive release have to be ‘practically eliminated’<sup>2</sup> and plant event sequences with a significant frequency of occurrence have to have no, or only minor, potential radiological consequences. An essential objective is that the necessity for off-site protective actions to mitigate radiological consequences be limited or even eliminated in technical terms, although such measures might still be required by the responsible authorities.

#### THE CONCEPT OF DEFENCE IN DEPTH

2.12. The primary means of preventing accidents in a nuclear power plant and mitigating the consequences of accidents if they do occur is the application of the concept of defence in depth [1, 5, 6]. This concept is applied to all safety related activities, whether organizational, behavioural or design related, and whether in full power, low power or various shutdown states. This is to ensure that all safety related activities are subject to independent layers of provisions so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures. Application of the concept of defence in depth throughout design and operation provides protection against anticipated operational occurrences and accidents, including those resulting from equipment failure or human induced events within the plant, and against consequences of events that originate outside the plant.

2.13. Paragraph 3.31 of the Fundamental Safety Principles [1] states that:

“Defence in depth is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment. If one level of protection or barrier were to fail, the subsequent level or barrier would be available.... The independent effectiveness of the different levels of defence is a necessary element of defence in depth.”

There are five levels of defence:

- (1) The purpose of the first level of defence is to prevent deviations from normal operation and the failure of items important to safety. This leads to requirements that the plant be soundly and conservatively sited, designed, constructed, maintained and operated in accordance with quality management and appropriate and proven engineering practices. To meet these objectives, careful attention is paid to the selection of appropriate design codes and materials, and to the quality control of the manufacture of components and construction of the plant, as well as to its commissioning. Design options that reduce the potential for internal hazards

---

<sup>2</sup> 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

contribute to the prevention of accidents at this level of defence. Attention is also paid to the processes and procedures involved in design, manufacture, construction, and in-service inspection, maintenance and testing, to the ease of access for these activities, and to the way the plant is operated and to how operating experience is utilized. This process is supported by a detailed analysis that determines the requirements for operation and maintenance of the plant and the requirements for quality management for operational and maintenance practices.

- (2) The purpose of the second level of defence is to detect and control deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions. This is in recognition of the fact that postulated initiating events are likely to occur over the operating lifetime of a nuclear power plant, despite the care taken to prevent them. This second level of defence necessitates the provision of specific systems and features in the design, the confirmation of their effectiveness through safety analysis, and the establishment of operating procedures to prevent such initiating events, or otherwise to minimize their consequences, and to return the plant to a safe state.
- (3) For the third level of defence, it is assumed that, although very unlikely, the escalation of certain anticipated operational occurrences or postulated initiating events might not be controlled at a preceding level and that an accident could develop. In the design of the plant, such accidents are postulated to occur. This leads to the requirement that inherent and/or engineered safety features, safety systems and procedures be capable of preventing damage to the reactor core or preventing radioactive releases requiring off-site protective actions and returning the plant to a safe state.
- (4) The purpose of the fourth level of defence is to mitigate the consequences of accidents that result from failure of the third level of defence in depth. This is achieved by preventing the progression of such accidents and mitigating the consequences of a severe accident. The safety objective in the case of a severe accident is that only protective actions that are limited in terms of lengths of time and areas of application would be necessary and that off-site contamination would be avoided or minimized. Event sequences that would lead to an early radioactive release or a large radioactive release<sup>3</sup> are required to be ‘practically eliminated’<sup>4</sup>.
- (5) The purpose of the fifth and final level of defence is to mitigate the radiological consequences of radioactive releases that could potentially result from accidents. This requires the provision of adequately equipped emergency response facilities and emergency plans and emergency procedures for on-site and off-site emergency response.

2.14. A relevant aspect of the implementation of defence in depth for a nuclear power plant is the provision in the design of a series of physical barriers, as well as a combination of active, passive and inherent safety features that contribute to the effectiveness of the physical barriers in confining radioactive material at specified locations. The number of barriers that will be necessary will depend upon the initial source term in terms of the amount and isotopic composition of radionuclides, the effectiveness of the individual barriers, the possible internal and external hazards, and the potential consequences of failures.

#### MAINTAINING THE INTEGRITY OF DESIGN OF THE PLANT THROUGHOUT THE LIFETIME OF THE PLANT

2.15. The design, construction and commissioning of a nuclear power plant might be shared between a number of organizations: the architect–engineer, the vendor of the reactor and its supporting systems,

---

<sup>3</sup> An ‘early radioactive release’ in this context is a radioactive release for which off-site protective actions would be necessary but would be unlikely to be fully effective in due time. A ‘large radioactive release’ is a radioactive release for which off-site protective actions that are limited in terms of lengths of time and areas of application would be insufficient for the protection of people and of the environment.

<sup>4</sup> 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.

the suppliers of major components, the designers of electrical systems, and the suppliers of other systems that are important to the safety of the plant.

2.16. The prime responsibility for safety rests with the person or organization responsible for facilities and activities that give rise to radiation risks (i.e. the operating organization) [1]. In 2003, the International Nuclear Safety Advisory Group suggested that the operating organization could set up a formal process to maintain the integrity of design of the plant throughout the lifetime of the plant (i.e. during the operating lifetime and into the decommissioning stage) [7]. A formally designated entity within the operating organization would take responsibility for this process.

2.17. In practice, the design of a nuclear power plant is complete only when the full plant specification (including site details) is produced for its procurement and licensing. Reference [7] emphasizes the need for a formally designated entity that has overall responsibility for the design process and is responsible for approving design changes and for ensuring that the requisite knowledge is maintained. Reference [7] also introduces the concept of 'responsible designers', to whom this formally designated entity could assign specific responsibilities for the design of parts of the plant. Prior to an application for authorization of a plant, the responsibility for the design will rest with the design organization (e.g. the vendor). Once an application for authorization of a plant has been made, the prime responsibility for safety will lie with the applicant, although detailed knowledge of the design will rest with the responsible designers. This balance will change as the plant is put into operation, since much of this detailed knowledge, such as the knowledge embodied in the safety analysis report, design manuals and other design documentation, will be transferred to the operating organization. To facilitate this transfer of knowledge, the structure of the formally designated entity that has overall responsibility for the design process would be established at an early stage.

2.18. The management system requirements that are placed on this formally designated entity would also apply to the responsible designers. However, the overall responsibility for maintaining the integrity of design of the plant would rest with the formally designated entity, and hence, ultimately, with the operating organization.

### 3. MANAGEMENT OF SAFETY IN DESIGN

#### **Requirement 1: Responsibilities in the management of safety in plant design**

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

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

#### **Requirement 2: Management system for plant design**

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

---

<sup>5</sup> The design organization is the organization responsible for preparation of the final detailed design of the plant to be built

3.2. The management system<sup>6</sup> shall include provision for ensuring the quality of the design of each structure, system and component, as well as of the overall design of the nuclear power plant, at all times. This includes the means for identifying and correcting design deficiencies, for checking the adequacy of the design and for controlling design changes.

3.3. The design of the plant, including subsequent changes, modifications or safety improvements, shall be in accordance with established procedures that call on appropriate engineering codes and standards and shall incorporate relevant requirements and design bases. Interfaces shall be identified and controlled.

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

### **Requirement 3: Safety of the plant design throughout the lifetime of the plant**

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

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

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

- (a) That the plant design is fit for purpose and meets the requirement for the optimization of protection and safety by keeping radiation risks as low as reasonably achievable;
- (b) That the design verification, definition of engineering codes and standards and requirements, use of proven engineering practices, provision for feedback of information on construction and experience, approval of key engineering documents, conduct of safety assessments and maintaining a safety culture are included in the formal system for ensuring the continuing safety of the plant design;
- (c) That the knowledge of the design that is needed for safe operation, maintenance (including adequate intervals for testing) and modification of the plant is available, that this knowledge is maintained up to date by the operating organization, and that due account is taken of past operating experience and validated research findings;
- (d) That management of design requirements and configuration control are maintained;
- (e) That the necessary interfaces with responsible designers and suppliers engaged in design work are established and controlled;
- (f) That the necessary engineering expertise and scientific and technical knowledge are maintained within the operating organization;
- (g) That all design changes to the plant are reviewed, verified, documented and approved;
- (h) That adequate documentation is maintained to facilitate future decommissioning of the plant.

---

<sup>6</sup> Requirements on the management system are established in IAEA Safety Standards Series No. GS-R-3, The Management System for Facilities and Activities [8].

## 4. PRINCIPAL TECHNICAL REQUIREMENTS

### Requirement 4: Fundamental safety functions

**Fulfilment of the following fundamental safety functions for a nuclear power plant shall be ensured for all plant states: (i) control of reactivity; (ii) removal of heat from the reactor and from the fuel store; and (iii) confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.**

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

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

### Requirement 5: Radiation protection in design

**The design of a nuclear power plant shall be such as to ensure that radiation doses to workers at the plant and to members of the public do not exceed the dose limits, that they are kept as low as reasonably achievable in operational states for the entire lifetime of the plant, and that they remain below acceptable limits and as low as reasonably achievable in, and following, accident conditions.**

4.3. The design shall be such as to ensure that plant states that could lead to high radiation doses or to a large radioactive release have been ‘practically eliminated’<sup>7</sup>, and that there would be no, or only minor, potential radiological consequences for plant states with a significant likelihood of occurrence.

4.4. Acceptable limits for purposes of radiation protection<sup>8</sup> associated with the relevant categories of plant states shall be established, consistent with the regulatory requirements.

### Requirement 6: Design for a nuclear power plant

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

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

---

<sup>7</sup> 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.

<sup>8</sup> Requirements on radiation protection and safety of radiation sources are established in IAEA Safety Standards Series No. GSR Part 3, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards [9]

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

4.7. The design shall take due account of the results of deterministic safety analyses and probabilistic safety analyses, to ensure that due consideration is given to the prevention of accidents and to mitigation of the consequences of any accidents that do occur.

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

#### **Requirement 7: Application of defence in depth**

**The design of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent as far as is practicable.**

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

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

4.11. The design:

- (a) Shall provide for multiple physical barriers to the release of radioactive material to the environment;
- (b) Shall be conservative, and the construction shall be of high quality, so as to provide assurance that failures and deviations from normal operation are minimized, that accidents are prevented as far as is practicable and that a small deviation in a plant parameter does not lead to a cliff edge effect<sup>9</sup>;
- (c) Shall provide for the control of plant behaviour by means of inherent and engineered features, such that failures and deviations from normal operation requiring actuation of safety systems are minimized or excluded by design, to the extent possible;
- (d) Shall provide for supplementing the control of the plant by means of automatic actuation of safety systems, such that failures and deviations from normal operation that exceed the capability of control systems can be controlled with a high level of confidence, and the need for operator actions in the early phase of these failures or deviations from normal operation is minimized;
- (e) Shall provide for systems, structures and components and procedures to control the course of and, as far as practicable, to limit the consequences of failures and deviations from normal operation that exceed the capability of safety systems;
- (f) Shall provide multiple means for ensuring that each of the fundamental safety functions is performed, thereby ensuring the effectiveness of the barriers and mitigating the consequences of any failure or deviation from normal operation.

4.12. To ensure that the concept of defence in depth is maintained, the design shall prevent, as far as is practicable:

- (a) Challenges to the integrity of physical barriers;
- (b) Failure of one or more barriers;
- (c) Failure of a barrier as a consequence of the failure of another barrier;

---

<sup>9</sup> A 'cliff edge effect', in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input

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

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

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

## **BOX 1. CONSIDERATIONS ABOUT THE APPLICABILITY**

### **POSITION A**

*Suggested changes:*

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

*Suggested interpretations:* None.

*Justification for the suggested changes:*

The second sentence of this requirement (4.13A) is considered applicable in general terms to HTG-SMRs, although the formulation of the example provided takes into account the background and experience from light water reactor technologies. For HTG-SMRs no fault sequences have yet been identified causing accident conditions that might lead to large-scale fuel particles damage and, consequently, to large-scale releases of radioactive material. At present, caution has to be taken in the absence of sufficient practical experience.

### **POSITION B**

*Suggested changes:*

“4.13A. The levels of defence in depth shall be independent as far as practicable to avoid the failure of one level reducing the effectiveness of other levels. In particular, safety features for design extension conditions (especially features for mitigating the consequences of accidents involving ~~the melting of fuel~~ *significant fuel damage or core degradation*) shall as far as is practicable be independent of safety systems.”

*Suggested interpretations:* None.

*Justification for the suggested changes:*

The second sentence of this requirement (4.13A) is considered applicable in general terms to HGT-SMRs, although the formulation of the example provided takes into account the background and experience of light water reactor technologies. For HTG-SMRs no fault sequences have yet been identified causing accident conditions that would involve the melting of fuel or the melting of the reactor core. Although accident scenarios that might lead to large scale fuel particles damage and, consequently, to large scale releases of radioactive material have not been found in the case of HTG-SMRs, caution has to be taken in the absence of sufficient practical experience. In addition, consideration has to be given to the establishment of a physical barrier similar to the containment used in light water reactors.

#### **Requirement 8: Interfaces of safety with security and safeguards**

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

#### **Requirement 9: Proven engineering practices**

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

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

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

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

#### **Requirement 10: Safety assessment**

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

4.17. The safety assessments<sup>10</sup> shall be commenced at an early point in the design process, with iterations between design activities and confirmatory analytical activities, and shall increase in scope and level of detail as the design programme progresses.

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

#### **Requirement 11: Provision for construction**

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

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

---

<sup>10</sup> Requirements on safety assessment for facilities and activities are established in GSR Part 4 (Rev. 1) [2].

## **BOX 2. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* See para. 4.19

*Suggested interpretations:* None

*Justification for the suggested changes:*

In many cases, NPPs incorporating SMRs are being designed to optimize off-site manufacture of major portions to leverage the value of this approach. With the implementation of factory manufacturing, there is a need for the inclusion of manufacturing as one of the provisions associated with this safety requirement.

### **Requirement 12: Features to facilitate radioactive waste management and decommissioning**

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

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

- (a) The choice of materials, so that amounts of radioactive waste will be minimized to the extent practicable and decontamination will be facilitated;
- (b) The access capabilities and the means of handling that might be necessary;
- (c) The facilities necessary for the management (i.e. segregation, characterization, classification, pretreatment, treatment and conditioning) and storage of radioactive waste generated in operation, and provision for managing the radioactive waste that will be generated in the decommissioning of the plant.

## **5. GENERAL PLANT DESIGN**

### DESIGN BASIS

#### **Requirement 13: Categories of plant states**

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

5.1. Plant states shall typically cover:

- (a) Normal operation;
- (b) Anticipated operational occurrences, which are expected to occur over the operating lifetime of the plant;
- (c) Design basis accidents;
- (d) Design extension conditions, including accidents with core melting;

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

## **BOX 3. CONSIDERATIONS ABOUT THE APPLICABILITY**

### **POSITION A**

*Suggested changes:*

5.1 (d) Design extension conditions, ~~including accidents with core melting~~;

*Suggested interpretations:* None.

*Justification for the suggested changes:* (See also the justification provided for Requirement 7)

In reference to design extension conditions, fuel melting is considered not applicable to HTG-SMRs. In addition, scenarios with significant fuel damage or core degradation might also not be applicable, provided that the ‘practical elimination’ of these scenarios is adequately demonstrated.

### **POSITION B**

*Suggested changes:*

5.1 (d) Design extension conditions, *including accidents with significant fuel damage or core degradation*;

*Suggested interpretation:*

5.1 (d) Fuel melting is considered not applicable to HTG-SMRs; however, there could be a need to consider potential failures of the identified levels of defence in depth, which could result in a requirement to consider scenarios with significant fuel damage or core degradation.

*Justification for the suggested interpretation:*

Fuel melting is not considered to be applicable to HTG-SMRs.

#### **Requirement 14: Design basis for items important to safety**

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

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

#### **Requirement 15: Design limits**

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

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

#### **Requirement 16: Postulated initiating events**

**The design for the nuclear power plant shall apply a systematic approach to identifying a comprehensive set of postulated initiating events such that all foreseeable events with the potential**

**for serious consequences and all foreseeable events with a significant frequency of occurrence are anticipated and are considered in the design.**

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

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

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

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

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

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

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

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

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

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

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

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

**Requirement 17: Internal and external hazards**

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

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

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

*5.15C. For multi-module units, the design shall take due account of the potential for specific hazards to give rise to impacts on several or even all modules of the unit simultaneously and to the potential for hazards initiating from one reactor module impacting other reactor modules of the same unit.*

**Internal hazards**

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

**External hazards**

5.17. The design shall include due consideration of those natural and human induced external events<sup>11</sup> (i.e. events of origin external to the plant) that have been identified in the site evaluation process. Causation and likelihood shall be considered in postulating potential hazards. In the short term, the safety of the plant shall not be permitted to be dependent on the availability of off-site services such as electricity supply and firefighting services. The design shall take due account of site specific conditions to determine the maximum delay time by which off-site services need to be available.

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

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

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

---

<sup>11</sup> Requirements on site evaluation for nuclear installations are established in IAEA Safety Standards Series No. NS-R-3 (Rev. 1), Site Evaluation for Nuclear Installations [10].

5.21. The design of the plant shall provide for an adequate margin to protect items important to safety against levels of external hazards to be considered for design, derived from the hazard evaluation for the site, and to avoid cliff edge effects<sup>12</sup>.

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

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

#### **BOX 4. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* See new para. 5.15C.

*Suggested interpretations:*

5.15A: The interpretation of the term ‘located’ has to allow for provisions to meet the requirement with separation by distance but also with other options, such as segregation by physical barriers.

5.16 and 5.17 (mainly): The potential impact of faults, hazards, and transients occurring at coupled facilities (such as those for process heat applications) have to be considered as potential sources of hazards in the safety analyses.

*Justification for the suggested changes and interpretations:*

5.15A: As SMRs are intended to be compact NPPs, protection against zonal effects can be provided by appropriate barriers as well as with separation by distance.

*Regarding 5.15C:* In a multiple modules design configuration (multi-module units), the potential for interactions between modules, or the simultaneous impact of all the modules due to internal and external hazards, has to be taken into account.

Regarding the interpretation of 5.16 and 5.17 (mainly): Future applications of SMRs include the direct use of process heat from the power plant, e.g. for district heating, heat processing, hydrogen production or water desalination. These additional connections also represent potential sources of hazards and have to be taken into account.

#### **Requirement 18: Engineering design rules**

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

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

---

<sup>12</sup> A ‘cliff edge effect’, in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.

### **Requirement 19: Design basis accidents**

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

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

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

5.26. The design basis accidents shall be analysed in a conservative manner. This approach involves postulating certain failures in safety systems, specifying design criteria and using conservative assumptions, models and input parameters in the analysis.

### **Requirement 20: Design extension conditions**

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

5.27. An analysis of design extension conditions for the plant shall be performed.<sup>13</sup> The main technical objective of considering the design extension conditions is to provide assurance that the design of the plant is such as to prevent accident conditions that are not considered design basis accident conditions, or to mitigate their consequences, as far as is reasonably practicable. This might require additional safety features for design extension conditions, or extension of the capability of safety systems to prevent, or to mitigate the consequences of, a severe accident, or to maintain the integrity of the containment. These additional safety features for design extension conditions, or this extension of the capability of safety systems, shall be such as to ensure the capability for managing accident conditions in which there is a significant amount of radioactive material in the containment (including radioactive material resulting from severe degradation of the reactor core). The plant shall be designed so that it can be brought into a controlled state and the containment function can be maintained, with the result that the possibility of plant states arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated'.<sup>14</sup> The effectiveness of provisions to ensure the functionality of the containment could be analysed on the basis of the best estimate approach.

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

---

<sup>13</sup> The analysis of design extension conditions for the plant could be performed by means of a best estimate approach (more stringent approaches may be used according to States' requirements).

<sup>14</sup> 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.

5.29. The analysis undertaken shall include identification of the features that are designed for use in, or that are capable<sup>15</sup> of preventing or mitigating, events considered in the design extension conditions. These features:

- (a) Shall be independent, to the extent practicable, of those used in more frequent accidents;
- (b) Shall be capable of performing in the environmental conditions pertaining to these design extension conditions, including design extension conditions in severe accidents, where appropriate;
- (c) Shall have reliability commensurate with the function that they are required to fulfil.

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

5.31. The design shall be such that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated'.<sup>16</sup>

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

### Combinations of events and failures

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

## BOX 5. CONSIDERATIONS ABOUT THE APPLICABILITY

### POSITION A

#### *Suggested changes:*

1) "5.27. An analysis of design extension conditions for the plant shall be performed\*. The main technical objective of considering the design extension conditions is to provide assurance that the design of the plant is such as to prevent accident conditions not considered design basis accident conditions, or to mitigate their consequences, as far as is reasonably practicable. This might require additional safety features for design extension conditions, or extension of the capability of safety systems to prevent, or to mitigate the consequences of, a design extension condition, or to maintain the ~~integrity of the containment confinement function~~. These additional safety features for design extension conditions, or this extension of the capability of safety systems, shall be such as to ensure the capability for managing accident conditions ~~in which there is a significant amount of radioactive material in the containment (including radioactive material resulting from severe degradation of the reactor core)~~. The plant shall be designed so that it can be brought into a controlled state and the ~~containment confinement~~ function can be maintained, with the result that the possibility of plant states arising that could lead to an early radioactive release or a large radioactive release is practically eliminated\*\*. The

---

<sup>15</sup> For returning the plant to a safe state or for mitigating the consequences of an accident, consideration could be given to the full design capabilities of the plant and to the temporary use of additional systems

<sup>16</sup> 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.

effectiveness of provisions to ensure the *functionality of the containment confinement function* could be analysed on the basis of the best estimate approach.”

(\*) “13: The analysis of design extension conditions for the plant could be performed by means of a best estimate approach (more stringent approaches may be used according to States’ requirements).”

(\*\*) “14: 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.”

2) ~~“5.30 In particular, the containment and its safety features shall be able to withstand extreme scenarios that include, among other things, melting of the reactor core. These scenarios shall be selected by using engineering judgement and input from probabilistic safety assessments.”~~

*Suggested interpretations:* None

*Justification for the suggested changes:*

- The terms ‘core melting’, ‘severe degradation of the reactor core’ and ‘significantly degraded fuel’ are not applicable to design extension conditions of HTG-SMRs.

- The technical basis for inherent safety of HTG-SMRs is the TRISO coated particle fuel, the graphite as the core structure, the helium coolant, as well as the dedicated core layout and lower power density to remove decay heat in a natural way. These features keep the maximum fuel temperature below the safety limit in all conceivable accidents so as to efficiently contain fission products inside the fuel. Therefore, early and large releases of radioactive materials are practically eliminated by the fuel efficiently retaining the fission product, which eliminates the possibility of significant fuel damage, including core melting.

- Regarding design extension conditions: Taking into account that no cliff edge effect is expected as significant fuel damage or fuel melt within design extension conditions, it is appropriate to redefine design extension conditions for HTG-SMRs, having only one level instead of two.

- Regarding containment: Among the basic barriers of a traditional NPP (fuel pellets, fuel cladding, primary loop and containment), the containment is regarded as the last and most significant confinement to retain the radioactive release, especially in case of design extension conditions with core melting, when core melting is assumed. However, for the HTG-SMR, the fuel acts as the main contributor to the confinement function (the SiC layer of a fuel particle is considered as a micro-containment). The degree of importance of an HTG-SMR containment in terms of confinement is, therefore, not as high as that of an LWR containment.

- Regarding para. 5.30: The original spirit of this requirement is to address the importance of the containment of a traditional NPP to withstand a core melting scenario. According to the above-mentioned justifications, this requirement is not applicable to HTG-SMRs.

## **POSITION B**

*Suggested changes:*

1) “5.27. An analysis of design extension conditions for the plant shall be performed\*. The main technical objective of considering the design extension conditions is to provide assurance that the design of the plant is such as to prevent accident conditions not considered design basis accident conditions, or to mitigate their consequences, as far as is reasonably practicable. This might require additional safety features for design extension conditions, or extension of the capability of safety systems to prevent, or to mitigate the consequences of, a severe accident, or to maintain the integrity of the containment. These additional safety features for design extension conditions, or this extension of the capability of safety systems, shall be such as to ensure the capability for managing accident conditions in which *the integrity of the fuel and the core is significantly degraded* ~~there is a~~

~~significant amount of radioactive material in the containment (including radioactive material resulting from severe degradation of the reactor core)~~. The plant shall be designed so that it can be brought into a controlled state and the containment function can be maintained, with the result that the possibility of plant states arising that could lead to an early radioactive release or a large radioactive release is practically eliminated\*\*. The effectiveness of provisions to ensure the functionality of the containment could be analysed on the basis of the best estimate approach.”

(\*) “13: The analysis of design extension conditions for the plant could be performed by means of a best estimate approach (more stringent approaches may be used according to States’ requirements)”.

(\*\*) “14: 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.”

2) “5.30. In particular, the containment and its safety features shall be able to withstand extreme scenarios ~~that include, among other things, melting of the reactor core~~. These scenarios shall be selected by using engineering judgement and input from probabilistic safety assessments.”

*Suggested interpretations:*

5.30: The structures providing or contributing to the safety functions of a typical LWR containment, including protection against external events, radiation shielding, and confinement of radioactive material are not consistently named in HTG-SMR designs. For example, in the case of HTG-SMRs such structures could be called ‘containment’, ‘reactor building’ or ‘confinement structure’; in addition, the fuel also contributes significantly to the confinement function.

It is important to note that the functional intent of the original requirements is not lost in the choice of terminology. In SSR-2/1 (Rev. 1) [2], the term ‘containment’ is used both to describe the confinement function and to refer to the structure which provides the functions captured in Requirement 54.

*Justification for the suggested changes and interpretations:*

- The principles of design extension conditions are applicable to all types of reactor, but the wording of Requirement 20 has to be amended to replace reference to ‘core melting’ with ‘significant core degradation’ (and the associated large radioactivity inventory outside the fuel and in the containment building).

Note: There may be other examples of concern, e.g. manufacturing issues, which could potentially result in significant core degradation under accident conditions. The demonstration of the tolerance of the fuel and the quality of its manufacture will need to be sufficient to demonstrate that the relevant requirements are met.

- In large LWRs the containment building is identified as the final confinement barrier to early and large radioactivity releases. In some HTG-SMRs, the coated particle fuel is claimed to be fundamental in delivering the final confinement barrier to radioactivity release and thus the coated particle fuel has to be the focus and the main safety aspect relevant to such HTG-SMRs.

## **Requirement 21: Physical separation and independence of safety systems**

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

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

**Requirement 22: Safety classification**

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

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

- (a) The safety function(s) to be performed by the item;
- (b) The consequences of failure to perform a safety function;
- (c) The frequency with which the item will be called upon to perform a safety function;
- (d) The time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function.

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

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

**Requirement 23: Reliability of items important to safety**

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

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

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

**Requirement 24: Common cause failures**

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

**Requirement 25: Single failure criterion**

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

5.39. Spurious action shall be considered to be one mode of failure when applying the single failure criterion<sup>17</sup> to a safety group or safety system.

---

<sup>17</sup> A single failure is a failure that results in the loss of capability of a system or component to perform its intended safety function(s) and any consequential failure(s) that result from it. The single failure criterion is a criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure.

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

**Requirement 26: Fail-safe design**

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

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

**Requirement 27: Support service systems**

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

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

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

**Requirement 28: Operational limits and conditions for safe operation**

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

5.44. The requirements and operational limits and conditions established in the design for the nuclear power plant shall include (Requirement 6 of IAEA Safety Standards Series No. SSR-2/2 (Rev. 1), Safety of Nuclear Power Plants: Commissioning and Operation [4]):

- (a) Safety limits;
- (b) Limiting settings for safety systems;
- (c) Limits and conditions for normal operation;
- (d) Control system constraints and procedural constraints on process variables and other important parameters;
- (e) Requirements for surveillance, maintenance, testing and inspection of the plant to ensure that structures, systems and components function as intended in the design, to comply with the requirement for optimization by keeping radiation risks as low as reasonably achievable;
- (f) Specified operational configurations, including operational restrictions in the event of the unavailability of safety systems or safety related systems;
- (g) Action statements, including completion times for actions in response to deviations from the operational limits and conditions.

**DESIGN FOR SAFE OPERATION OVER THE LIFETIME OF THE PLANT**

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

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

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

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

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

- (a) Other proven alternative and/or indirect methods such as surveillance testing of reference items or use of verified and validated calculational methods shall be specified.
- (b) Conservative safety margins shall be applied or other appropriate precautions shall be taken to compensate for possible unanticipated failures.

**Requirement 30: Qualification of items important to safety**

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

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

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

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

**BOX 6. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* None.

*Suggested interpretations:*

5.50: For some HTG-SMR designs, the containment might not be designed as a pressure retaining structure and might not require periodic testing of the containment leak rate. Some HTG-SMR designs include alternative confinement systems, which might also require periodic testing.

*Justification for the suggested interpretations:*

The requirement covers environmental conditions that could be reasonably anticipated. The text in para. 5.50 "...such as in periodic testing of the containment leak rate..." is an LWR-specific

example where it is assumed that the containment structure provides a significant contribution to the confinement function and therefore the example of periodic testing might not apply to some HTG-SMR.

#### **Requirement 31: Ageing management**

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

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

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

#### HUMAN FACTORS

#### **Requirement 32: Design for optimal operator performance**

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

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

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

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

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

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

- (a) To assess the general state of the plant in any condition;
- (b) To operate the plant within the specified limits on parameters associated with plant systems and equipment (operational limits and conditions);
- (c) To confirm that safety actions for the actuation of safety systems are automatically initiated when needed and that the relevant systems perform as intended;
- (d) To determine both the need for and the time for manual initiation of the specified safety actions.

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

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

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

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

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

#### OTHER DESIGN CONSIDERATIONS

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

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

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

#### ***Requirement 33A: Safety systems, and safety features for design extension conditions, of modules of a multi-module unit.***

***Each module of a multi-module unit shall have its own safety systems and shall have its own safety features for design extension conditions, as far as practicable. Where a safety system or a safety feature for design extension conditions is shared between reactor modules of a multi-module unit, the shared safety system or safety feature shall be functionally capable of fulfilling the safety requirements of each of these modules simultaneously, to protect against the consequences of events which have the potential to affect multiple modules.***

5.63A. To further enhance safety, means allowing interconnections between modules of a multi-module unit shall be considered in the design.

#### **BOX 7. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* To complement Requirement 33 (and 5.63) with Requirement 33A (and 5.63A).

*Suggested interpretation:* None.

*Justification for the suggested changes:*

SMR designs might consider sharing safety systems and safety features, especially safety features for design extension conditions and safety features designed to enhance safety and

grace periods. However, it has to be made clear that safety cannot be negatively impacted by the sharing of safety systems or safety features.

**Requirement 34: Systems containing fissile material or radioactive material**

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

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

Nuclear power plants coupled with heat utilization units (such as for *process heat, hydrogen production, district heating*) ~~and/or~~ water desalination *units*) shall be designed to ~~prevent processes that limit the~~ transport of radionuclides from the nuclear plant to the ~~desalination unit or the district heating unit~~ *heat utilization units* ~~application to ensure that defined regulatory limits are not exceeded~~ under conditions of operational states and in accident conditions.

5.63B. *The design of the nuclear power plant shall take account of the potential impact of coupled facilities on nuclear safety.*

**BOX 8. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* See the overarching requirement and the new para. 5.63B.

*Suggested interpretations:* None.

*Justification for the suggested changes:*

1) Overarching requirement: Some heat utilization units (such as for process heat) operate in high temperatures, which makes it more challenging to control radionuclides. Therefore, it is necessary to define the requirement to "prevent processes that transport radionuclides from the nuclear plant" as *'to ensure that defined regulatory limits are not exceeded.'*

2) New para 5.63B:

- Coupled facilities might contain large amount of flammable, corrosive and toxic chemicals. The impact of leakage of such chemicals through the heat transport line, back to the nuclear plant has to be considered in the design.
- Where a coupled facility might affect the safety of a NPP, the design of the NPP has to take into account the potential effects caused by the coupled facility.
- The additional criterion to exclude the facility coupled with the NPP from the nuclear regulation has to be addressed. If normal operation, abnormal events and accidents in the coupled facility do not affect the operation of the NPP, safety requirements for the NPP do not need to be applied to the design of the coupled facility, even though the coupled facility is connected with the nuclear plant by some means. In this case, abnormal events in the coupled facility shall be defined as external hazards against the nuclear plant. The coupled

facility has to be physically separated from the nuclear plant to prevent harmful disturbances over the nuclear plant if abnormal events occur.

**Requirement 36: Escape routes from the plant**

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

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

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

**Requirement 37: Communication systems at the plant**

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

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

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

**Requirement 38: Control of access to the plant**

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

5.68. Provision shall be made in the design of the buildings and the layout of the site for the control of access to the nuclear power plant by operating personnel and/or for equipment, including emergency response personnel and vehicles, with particular consideration given to guarding against the unauthorized entry of persons and goods to the plant.

**Requirement 39: Prevention of unauthorized access to, or interference with, items important to safety**

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

**Requirement 40: Prevention of harmful interactions of systems important to safety**

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

5.69. In the analysis of the potential for harmful interactions of systems important to safety, due account shall be taken of physical interconnections and of the possible effects of one system's operation, maloperation or malfunction on local environmental conditions of other essential systems, to ensure that

changes in environmental conditions do not affect the reliability of systems or components in functioning as intended.

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

#### **Requirement 41: Interactions between the electrical power grid and the plant**

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

#### SAFETY ANALYSIS

#### **Requirement 42: Safety analysis of the plant design**

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

5.71. On the basis of a safety analysis, the design basis for items important to safety and their links to initiating events and event sequences shall be confirmed.<sup>18</sup> It shall be demonstrated that the nuclear power plant as designed is capable of complying with authorized limits on discharges with regard to radioactive releases and with the dose limits in all operational states, and is capable of meeting acceptable limits for accident conditions.

5.72. The safety analysis shall provide assurance that defence in depth has been implemented in the design of the plant.

5.73. The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects<sup>19</sup> and early radioactive releases or large radioactive releases.

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

#### **Deterministic approach**

5.75. The deterministic safety analysis shall mainly provide:

- (a) Establishment and confirmation of the design bases for all items important to safety;
- (b) Characterization of the postulated initiating events that are appropriate for the site and the design of the plant;
- (c) Analysis and evaluation of event sequences that result from postulated initiating events, to confirm the qualification requirements;
- (d) Comparison of the results of the analysis with acceptance criteria, design limits, dose limits and acceptable limits for purposes of radiation protection;
- (e) Demonstration that the management of anticipated operational occurrences and design basis accidents is possible by *inherent safety features, safety features and* safety actions for the automatic actuation of safety systems in combination with prescribed actions by the operator;

---

<sup>18</sup> Requirements on safety assessment for facilities and activities are established in GSR Part 4 (Rev. 1) [2].

<sup>19</sup> A 'cliff edge effect', in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.

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

#### **Probabilistic approach**

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

- (a) Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent;
- (b) Providing assurance that situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented;<sup>20</sup>
- (c) Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.

### **BOX 9. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* See para. 5.75, items (e) and (f)

*Suggested interpretations:* None.

*Justification for the suggested changes:*

The accident management for HTG-SMRs could rely more on its design features than on automatic safety actions and prescribed operator actions to maintain the main safety functions

## **6. DESIGN OF SPECIFIC PLANT SYSTEMS**

### REACTOR CORE AND ASSOCIATED FEATURES

#### **Requirement 43: Performance of fuel *particles and* elements ~~*and assemblies*~~**

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

6.1. The processes of deterioration to be considered shall include those arising from:

- ~~*Thermal effect;*~~
- ~~*Differential expansion and deformation;*~~
- ~~*External pressure of the coolant;*~~
- ~~*Additional*~~ Internal pressure due to fission products and ~~*other gasses the buildup of helium*~~ in coated fuel particles ~~*elements*~~;
- ~~*Kernel migration in coated fuel particle due to temperature gradient;*~~
- ~~*Chemical attack of coating layers of coated fuel particle by metallic fission products;*~~

---

<sup>20</sup> A 'cliff edge effect', in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.

- Irradiation of fuel *particles* and other materials in the fuel *element assembly*;
- ~~Variations in pressure and temperature resulting from variations in power demand;~~
- ~~Abrasion (for pebble bed design);~~
- ~~Coolant chemical effects;~~
- Static and dynamic loading, ~~including flow induced vibrations and mechanical vibrations;~~
- ~~Variations in performance in relation to heat transfer that could result from distortion or chemical effects.~~

Allowance shall be made for uncertainties in data, in calculations and in manufacture.

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

6.2a. *Fuel particles and elements shall be designed for adequate radionuclide retention in accident conditions.*

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

## **BOX 10. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* See the title, overarching requirement, para. 6.1, the new para. 6.2a and para. 6.3.

*Suggested interpretations:*

Overarching requirement:

- The terms ‘fuel particle’ and ‘fuel elements’ have to be interpreted in accordance with the descriptions provided in Section 2.3 (a) of this TECDOC.
- The term ‘accident conditions’ has to be interpreted in accordance with the definition of design extension conditions. If design extension conditions include two subcategories, then ‘accident conditions’ will refer to design basis accidents and design extension conditions without significant fuel degradation; otherwise it refers to design basis accidents and design extension conditions without subcategories. (See definitions of design extension conditions in the section on ‘Definitions’, at the end of this appendix).

Paragraph 6.1: The specific mechanisms referred to in the requirement are those of LWRs. This has to be changed to reflect processes of deterioration of HTG-SMR coated particle fuel.

Paragraph 6.2: The fuel design limits of HTG-SMRs might also include key fuel manufacturing parameters, such as the coated fuel particles defect fraction and heavy metal contamination.

*Justification for the suggested changes and interpretations:*

Title, overarching requirement and para. 6.3: In HTG-SMR, only the terms fuel particles and fuel elements are used.

Fuel particles (overarching requirement): HTG-SMR fuel elements contain large amounts of fuel particles (TRISO) and their integrity is the most important factor to prevent the release of radionuclides.

6.1: The processes of deterioration of HTG-SMR fuel are different from those of light water reactors and are considered well understood in several countries through implemented research and development [4–9]. ‘Coolant chemical effects’ refers to deterioration processes, such as those due to the presence of impurities.

6.2a: As the fuel elements of HTG-SMRs, which include the fuel particles, are the dominant contributors to the confinement function in all plant states, requirements on the confinement function of fuel elements are also necessary for accident conditions.

Interpretation of para. 6.2: Given the very large number of coated fuel particles, it is not realistic to assure that zero defects exist in the manufactured fuel particles. In addition, there is a potential for heavy metal contamination of the coated fuel particles during the manufacturing process. These key fuel manufacturing parameters have to be taken into account for the fuel design limit.

#### **Requirement 44: Structural capability of the reactor core**

**The fuel elements and fuel assemblies and their supporting structures for the nuclear power plant shall be designed so that, in operational states and in accident conditions other than severe accidents, a geometry that allows for adequate cooling is maintained and the insertion of control rods is not impeded.**

### **BOX 11. CONSIDERATIONS ABOUT THE APPLICABILITY**

#### **POSITION A**

*Suggested changes:*

“The fuel elements ~~and fuel assemblies~~ and their supporting structures for the nuclear power plant shall be designed so that, in operational states and in accident conditions ~~other than severe accidents, unacceptable loads to the coated fuel particles are prevented, a geometry that allows for~~ adequate core cooling can be achieved and maintained, and the core temperature remains within acceptable limits ~~is maintained and the insertion of control rods is not impeded.~~”

*Suggested interpretations:* None.

*Justification for the suggested changes and/or interpretations:*

The functional requirements of the HTG-SMRs’ core and its supporting structures under accident conditions are explained as follows:

- With the objective of no large release of radioactivity from the coated particle fuel, the geometry of the HTG-SMR core and its supporting structures shall be designed to prevent the occurrence of events that could lead to unacceptable loads to the coated fuel particles.
- Under accident conditions, the core residual heat is removed from the core to the outside of the reactor pressure vessel merely by natural or passive means, i.e., heat conduction, natural convection and radiation. Therefore, the residual heat removal is adequate as long as the geometry of the HTG-SMR core and its supporting structures do not impede the passive core cooling. It may be argued that even some geometrical changes will not impede heat removal (i.e. heat conduction is dominated by the presence of the material and not by its geometry).
- Under accident conditions of the HTG-SMR, the reactor can be automatically scrammed by the self-acting (and much larger than light water reactors) negative temperature feedback, so

the reactor shutdown and sub-criticality might not rely on the control rod system. The specific reference to the control rod is thus not applicable. Some means of long term shutdown will be needed in design extension conditions after some time and thus measures can be taken to achieve this.

## POSITION B

*Suggested changes:*

“The fuel elements ~~and fuel assemblies~~ and their supporting structures for the nuclear power plant shall be designed so that, in operational states and in accident conditions ~~other than severe accidents, unacceptable loads on the coated fuel particles are prevented,~~ a geometry that allows for adequate core cooling is maintained *to ensure that the core temperature remains within acceptable limits and the ability to bring the core sub-critical, with sufficient margin and the insertion of control rods* is not impeded.”

*Suggested interpretations:* None.

*Justification for the suggested changes:*

For operational states, one requirement on the HTG-SMR core and its supporting structures is to maintain the structural integrity.

For accident conditions, it is suggested to maintain the geometry of the HTG-SMR core and its supporting structures, to make sure that the necessary means allowing for core sub-criticality and for adequate core cooling remain available.

### **Requirement 45: Control of the reactor core**

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

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

6.5. In the design of reactivity control devices, due account shall be taken of wear out and of the effects of irradiation, such as burnup, changes in physical properties and production of gas.

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

## BOX 12. CONSIDERATIONS ABOUT THE APPLICABILITY

### POSITION A

*Suggested changes:*

“Distributions of neutron flux that can arise in any state of the reactor core in the nuclear power plant, including states arising after shutdown and during or after refuelling, and states arising from anticipated

operational occurrences and from accident conditions *not involving degradation of the reactor core*, shall be inherently stable. ...”

“6.4 Adequate means of detecting *and controlling* the neutron flux distributions in the reactor core and their changes shall be provided *as necessary* for the purpose of ensuring that there are no regions of the core in which the design limits could be exceeded.”

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

*Suggested interpretations:*

The existing text is only accepted when a different interpretation is accepted for HTG-SMRs:

- ‘After refuelling’ might not be applicable to a pebble bed reactor with on-line refuelling. However, it could be interpreted as referring to the minor variations in core content and reactivity due to the online refuelling, that may only take place for a few hours per day, or less frequently for small pebble bed reactors.
- Paragraph 6.4: It is not to be assumed that “Adequate means of detecting and controlling the neutron flux distribution” are only achievable by in-core instrumentation. Flux measurements outside the reactor vessel can be shown to be adequate to confirm that the large margins will not be exceeded.

*Justification for the suggested changes and interpretations:*

For pebble bed HTG-SMRs, the on-line refuelling mode during normal operation is adopted, so there is no specific state of refuelling. However, refuelling activities take place for prismatic HTG-SMRs as well as for LWRs and, therefore, the suggested changes and interpretations are only applicable to prismatic HTG-SMRs.

Whether for pebble bed HTG-SMRs or for prismatic HTG-SMRs, nuclear measurement devices adopted by the current designs are used for monitoring the reactor power level via detecting the neutron flux. However, in contrast to LWRs, there are no in-core measurement means to capture the fine flux distribution.

Paragraph 6.4: It is not to be assumed (and prescribed) that “Adequate means of detecting and controlling the neutron flux distribution” imply in-core measurements as the ones used in LWRs. The requirement is to know the flux distribution and changes in the distribution to an adequate level of accuracy to ensure that design limits are not exceeded. In HTG-SMRs with their small lumped fuel and graphite moderator and reflector, we have very long neutron mean free paths and large margins (in power and temperatures) for the fuel. The derived distribution from ex-core (i.e. external to the reactor vessel) flux measurements has to be shown as being adequate to derive the in-core flux distributions and the resultant non-exceedance of the design limits. No localized points with elevated neutronic flux exist in an HTG-SMR core in contrast to LWR designs, where a neighboring pin might represent a considerable power peak (and flux variation). The neutron and gamma flux measurements in LWRs are typically conducted by positioning the measuring equipment in the center of the assembly and, thus, many mean free path lengths away from many of the pins in the reactor. In LWRs, the flux levels and distributions (to ensure that limits are not exceeded) are similarly derived, but with a much

stricter stipulation on accuracy since the margins are quite small (assembly misloading can lead to fuel damage).

Paragraph 6.6: The requirements for the reactivity control system to maintain the structural integrity of the reactor coolant pressure boundary are not applicable to HTG-SMRs, because the fuel-coolant reaction caused by the energy produced in the fuel by positive reactivity is not postulated.

## **POSITION B**

*Suggested changes:* None.

*Suggested interpretations:*

The existing text is only applicable when a different interpretation is accepted for HTG-SMRs:

- ‘After refuelling’ might not be applicable to a pebble bed reactor with on-line refuelling. However, it could be interpreted as referring to the minor variations in core content and reactivity due to the on-line refuelling, that might take place for a few hours per day, or less frequently for small pebble bed reactors.
- Paragraph 6.4: It is not to be assumed that “Adequate means of detecting flux distribution” are only achievable by in-core instrumentation, if flux measurements outside the reactor vessel can be shown to be adequate.

*Justification for the suggested interpretations:*

For pebble bed HTG-SMRs, the online refuelling mode during normal operation might be adopted, so there is no specific state of refuelling in contrast to prismatic HTG-SMRs and LWRs.

Whether for pebble bed HTG-SMRs or for prismatic ones, nuclear measurement devices adopted by the current designs are used for monitoring the reactor power level via detecting the neutron flux. However, in contrast to LWRs, there are currently no reliable in-core measurement means to capture the fine flux distribution.

Paragraph 6.4 The use of the term ‘adequate means’ in this paragraph does not need to imply in-core measurements as in the case of LWRs. The requirement is to know the flux distribution and changes in the distribution to an adequate level of accuracy to ensure that design limits are not exceeded. HTG-SMRs with small lumped fuel graphite moderator and reflector have long neutron mean free paths and large margins (in power and temperatures) for the fuel. As such, the derived distribution from ex-core (i.e. external to the reactor vessel) flux measurements might be shown to be adequate to derive the in-core flux distributions whilst permitting non-exceedance of the design limits.

### **Requirement 46: Reactor shutdown**

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

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

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

6.9. The *design provisions means* for shutting down the reactor shall consist of at least two diverse and independent *means systems*.

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

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

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

### **BOX 13. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* See paras 6.9 and 6.10

*Suggested interpretations:*

Regarding para. 6.10, in the event of failure of the shutdown system, a recriticality transient may be permitted, provided that the specified fuel and component limits are not exceeded.

For HTG-SMRs, it is possible that the negative temperature feedback following shutdown of helium circulators and subsequent rise in core temperature will bring the reactor sub-critical. Although a subsequent recriticality transient has been predicted for some designs, this is claimed not to lead to fuel damage. The grace time available for operator actions following a transient is expected to be long, and as the passive shutdown means might provide enhanced safety by reducing the instantaneous demand on the engineered shutdown systems or operator actions. In addition, the continued pebble bed refuelling strategy allows the minimization of excess reactivity in the reactor core.

*Justification for the suggested changes and interpretations:*

The change from ‘shutdown system’ to ‘shutdown means’ is suggested in recognition that HTG-SMR designs might not rely exclusively on control rods to rapidly shut down the reactor.

#### **ADDITIONAL CONSIDERATIONS**

An alternative formulation to the interpretation of the changes incorporated to para. 6.10, with corresponding justifications, was also suggested by the contributors.

*Suggested interpretation:*

6.10: The term ‘shutdown means’ can refer to a shutdown system (e.g. control rods), or to a combination of inherent plant responses and active or passive safety systems.

*Justification for the suggested interpretation:*

The means for shutting down a reactor (including an HTG-SMR), might refer to a shutdown system (such as control rods), or might include an inherent reactivity feedback response to

manage the short-term transient, coupled with a system (or systems) to bring the reactor permanently sub-critical and maintain a long-term stable shutdown condition.

Replacing 'shutdown systems' with 'shutdown means' is considered to be a more flexible terminology; however, the operating organization would still be expected to demonstrate that adequate control of the plant reactivity in operational states and accident conditions is achieved by the design

## REACTOR COOLANT SYSTEMS

### **Requirement 47: Design of reactor coolant systems**

**The components of the reactor coolant systems for the nuclear power plant shall be designed and constructed so that the risk of faults due to inadequate quality of materials, inadequate design standards, insufficient capability for inspection or inadequate quality of manufacture is minimized.**

- 6.13. Pipework connected to the pressure boundary of the reactor coolant systems for the nuclear power plant shall be equipped with adequate isolation devices to limit any loss of radioactive fluid (primary coolant) and to prevent the loss of coolant through interfacing systems.
- 6.14. The design of the reactor coolant pressure boundary shall be such that flaws are very unlikely to be initiated, and any flaws that are initiated would propagate in a regime of high resistance to unstable fracture and to rapid crack propagation, thereby permitting the timely detection of flaws.
- 6.15. The design of the reactor coolant systems shall be such as to ensure that plant states in which components of the reactor coolant pressure boundary could exhibit embrittlement are avoided.
- 6.16. The design of the components contained inside the reactor coolant pressure boundary, such as ~~pump~~ *circulator or turbine* impellers and valve parts, shall be such as to minimize the likelihood of failure and consequential damage to other components of the primary coolant system that are important to safety, in all operational states and in design basis accident conditions, with due allowance made for deterioration that might occur in service.

## **BOX 14. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* See para 6.16.

*Suggested interpretations:* See below two positions.

*Justification for the suggested changes (para. 6.16):*

In the HTG-SMR design, there are no pumps inside the reactor coolant pressure boundary. The examples of components contained inside the reactor coolant pressure boundary corresponding to ‘pump’ of LWR are ‘circulator’ (‘blower’ in other terminology) and ‘turbine’ for direct gas cycle.

### **POSITION A**

*Suggested interpretations:* None.

### **POSITION B**

*Additional changes suggested:*

New paragraph: “6.16A. The design of the reactor coolant system shall consider prevention of reactivity insertion by core overcooling, the mitigation and limitation of air and water ingress, and the protection of the reactor coolant pressure boundary from overheating, to ensure the appropriate design limits are not exceeded during anticipated operational occurrences or accident conditions.”

*Suggested interpretations:*

6.13: The term ‘reactor coolant system’ is to be interpreted as including the ‘reactor helium pressure boundary’.

*Justification for these suggested changes and interpretations:*

Paragraph 6.13 and new para. 6.16A: In terms of reactor core cooling, the isolation function of the reactor coolant system pressure boundary is less focussed on preventing the loss of coolant than on limiting the air ingress into the reactor core after a depressurization accident, through the pipework connected to the reactor coolant system pressure boundary.

In HTG-SMR designs, it might be required to stop the circulation of primary coolant under specified conditions and not to restart the circulation during anticipated operational occurrences and accident conditions. The reasons for these measures include the following:

- Protection of the reactor coolant system pressure boundary from overheating;
- Minimization of water ingress into the core due to water vaporization by heating;
- Prevention of reactivity insertion by core overcooling;

Mitigation of air ingress into the core due to the suction of air from the pipe breach.

### **Requirement 48: Overpressure protection of the reactor coolant pressure boundary**

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

## **BOX 15. CONSIDERATIONS ABOUT THE APPLICABILITY**

### **POSITION A**

*Suggested changes:*

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

*Suggested interpretations:* None.

*Justification for the suggested changes:*

In HTG-SMRs, the reactor coolant can be directly released into the reactor building atmosphere when the pressure relief device is actuated by overpressure or by the overpressure protection signal, and there are no means to remove radioactive materials from the reactor coolant released from the pressure relief device.

### **POSITION B**

*Suggested changes:* None.

*Suggested interpretations:*

To meet the last part of the requirement (“... will not lead to the release of radioactive material from the nuclear power plant directly to the environment”) it might be necessary to use additional means to avoid the direct release of the overpressure relief devices to the environment; the additional means have to reduce the released radioactivity as low as is reasonably practicable.

*Justification for the suggested interpretations:*

This interpretation meets the two intents of the original requirement

#### **Requirement 49: Inventory of reactor coolant**

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

#### **Requirement 50: Cleanup of reactor coolant**

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

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

## BOX 16. CONSIDERATIONS ABOUT THE APPLICABILITY

### POSITION A

*Suggested changes:*

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

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

*Suggested interpretations:* None.

*Justification for the suggested changes:*

The deletion of the term ‘corrosion’ allows the requirement to encompass radioactive graphite dust, which is not a ‘corrosion product’.

For the HTG-SMRs, the helium purification system is designed to control the level of chemical impurities, with the objective of reducing corrosion in both fuel and reactor internals. Usually, chemical impurities include H<sub>2</sub>O, O<sub>2</sub>, CO<sub>2</sub>, CO, H<sub>2</sub>, CH<sub>4</sub>, N<sub>2</sub>, H<sub>3</sub> (tritium) and graphite dust. Therefore, the design basis of the purification system is the design limit of the chemical impurities and the system is non-safety grade.

Although the purification system could also be used to reduce the amount of radioactive materials in the primary circuit, it is considered that controlling the level of activity in the circuit is out of the scope of the requirements to this system.

### POSITION B

*Suggested changes:*

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

*Suggested interpretations:* None.

*Justification for the suggested changes:*

The deletion of the term ‘corrosion’ allows the requirement to encompass radioactive graphite dust, which is not a ‘corrosion product’.

For HTG-SMRs, the helium purification system is designed to control the level of chemical impurities, with the objective of reducing corrosion in both fuel and reactor internals. Usually, chemical impurities include H<sub>2</sub>O, O<sub>2</sub>, CO<sub>2</sub>, CO, H<sub>2</sub>, CH<sub>4</sub>, N<sub>2</sub>, H<sub>3</sub> (tritium) and graphite dust.

Paragraph 6.17 is considered fully applicable to HTG-SMRs, noting that there will be a certain fraction of failed fuel kernels in fresh fuel. Controlling the radioactivity of the helium

coolant is expected to be an important function of the helium purification system, to maintain releases during normal operations and accident conditions as low as reasonably practicable, especially considering that many current HTG-SMR designs propose to discharge the initial helium release directly to the atmosphere (unfiltered) in the event of a depressurization accident.

**Requirement 51: Removal of residual heat from the reactor core**

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

**Requirement 52: Emergency cooling of the reactor core**

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

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

- (a) The limiting parameters for the ~~cladding or for~~ integrity of the fuel (such as temperature) will not be exceeded;
  - (b) Possible chemical reactions are kept to an acceptable level;
  - (c) The effectiveness of the means of cooling of the reactor core compensates for possible changes in the fuel and in the internal geometry of the reactor core;
  - (d) Cooling of the reactor core will be ensured for a sufficient time.

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

**BOX 17. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* See 6.18, item (a)

*Suggested interpretations:*

Paragraph 6.18: The ‘means provided for cooling of the reactor core’ can include passive heat removal mechanisms.

*Justification for the suggested changes:*

There is no ‘cladding’ on HTG-SMR fuel.

**Requirement 53: Heat transfer to an ultimate heat sink**

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

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

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

**Requirement 54: Containment system for the reactor**

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

**BOX 18. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:*

To change the marking of the items, placing item (i) “confinement of radioactive substances in operational states and in accident conditions” at the end of the requirement and marking it as (iii).

*Suggested interpretations:*

The term ‘containment system’ is to be interpreted here as a ‘reactor functional containment’ consisting of multiple barriers, internal and external to the reactor, including the reactor building.

*Justification for the suggested changes and interpretations:*

The expected contribution of the different barriers of the containment system of HTG-SMRs to the fulfilment of the safety functions of the NPP is different than in the case of the traditional LWRs.

In HTG-SMRs, the fuel acts as the dominant contributor to the confinement function, and less importance is placed on the containment structure (reactor building). Multiple barriers are provided to control the release of radioactivity to the environment and to ensure that the ‘reactor functional containment’ design conditions important to safety are not exceeded in any of the plant states.

**Requirement 55: Control of radioactive releases from the containment system**

The design of the containment *system* shall be such as to ensure that any radioactive release from the nuclear power plant to the environment is as low as reasonably achievable, is below the authorized limits on discharges in operational states and is below acceptable limits in accident conditions.

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

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

## BOX 19. CONSIDERATIONS ABOUT THE APPLICABILITY

### POSITION A

The general considerations about the applicability of requirements 55–58 are provided in common at the end of Requirement 58.

### POSITION B (for Requirement 55)

*Suggested changes:* See title, overarching requirement and para. 6.20

*Suggested interpretations:* None.

*Justification of the suggested changes:*

Title and overarching requirement: The term ‘containment’ is renamed as ‘containment system’ to be consistent with the interpretation of ‘functional containment’ as outlined in Box 18 for Requirement 54. The concept of the TRISO fuel constituting the primary fission product barriers is intertwined with the concept of a functional containment for HTG-SMRs.

6.20: This supporting requirement mainly refers to traditional NPPs, where a leaktight containment is needed. However, it is important to preserve the intent of this requirement when other reactor technologies are considered, which is to facilitate periodic confirmation that the confinement function is being adequately maintained and has not been compromised by some of the potential degradation mechanisms, such as ageing and/or irradiation. In addition, the leak rate is an important assumption in safety analysis and has to be confirmed by testing at an appropriate pressure.

- This requirement focuses to minimizing the potential for compromising the integrity of the functional containment. The design has to include provisions to ensure that the confinement of radioactive material cannot be lost due to effects of internal or external hazards.
- Users potentially interested in keeping and applying this requirement to HTG-SMRs can consider the modification of its current wording, to reflect the differences in purpose and function of the reactor building in this type of reactor technology.

### **Requirement 56: Isolation of the containment building**

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

6.22. Lines that penetrate the containment as part of the reactor coolant pressure boundary and lines that are connected directly to the containment atmosphere shall be fitted with at least two adequate containment isolation valves or check valves arranged in series<sup>21</sup> and shall be provided with suitable leak detection systems. Containment isolation valves or check valves shall be located as close to the containment as is practicable, and each valve shall be capable of reliable and independent actuation and of being periodically tested.

---

<sup>21</sup> In most cases, one containment isolation valve or check valve is outside the containment and the other is inside the containment. Other arrangements might be acceptable, however, depending on the design.

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

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

## **BOX 20. CONSIDERATIONS ABOUT THE APPLICABILITY**

### **POSITION A**

The general considerations about the applicability of requirements 55–58 are provided in common at the end of Requirement 58.

### **POSITION B (for Requirement 56)**

*Suggested changes:* See the overarching requirement

*Suggested interpretations and corresponding justifications:*

In the context of Requirement 56, the term ‘containment’ has to be considered as related to the ‘reactor building’.

General: The current formulation of this requirement might not be fully applicable to HTG-SMRs. However, the ‘as low as reasonably practicable’ principle has still to be considered, if additional design measures associated with the reactor building can be implemented to further reduce the release of radioactive material. In addition, specific considerations for HTG-SMRs can be made, such as a requirement to limit the ingress of air (oxygen) to minimize the oxidation of the core in the event of a depressurization accident.

Overarching requirement: The existing formulation of this requirement would permit a licensee to demonstrate that there are no accidents in which the leaktightness of the containment (reactor building) is essential to prevent radioactive releases to the environment, taking into account that this function is provided by the fuel barriers. However, as indicated above, the reliable closure of penetrations might be necessary to prevent air (oxygen) ingress in the event of a depressurization accident.

Paragraphs 6.22, 6.23 and 6.24: The intent of these supporting requirements about minimizing the risk of containment bypass (direct release from the primary circuit to the environment) remains applicable for HTG-SMRs, taking into account that radioactive releases directly to the environment have to be avoided as far as is reasonably practicable. In addition, as penetrations might be a source of air (oxygen) ingress in the event of a depressurization accident combined with pipe failure, isolation means have to be considered.

In HTG-SMRs, the leaktightness function is performed by the multiple barriers of the functional containment.

### **Requirement 57: Access to the containment**

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

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

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

## **BOX 21. CONSIDERATIONS ABOUT THE APPLICABILITY**

### **POSITION A**

The general considerations about the applicability of requirements 55–58 are provided in common at the end of Requirement 58.

### **POSITION B (for Requirement 57)**

*Suggested changes:* None.

*Suggested interpretation and corresponding justifications:*

In the context of Requirement 57, the term ‘containment’ has to be considered as related to the ‘reactor building’.

General: As indicated in Requirement 56, the current formulation of Requirement 57 might not be fully applicable to HTG-SMRs. However, the ‘as low as reasonably practicable’ principle has still to be considered, if additional design measures associated with the reactor building can be implemented to further reduce the release of radioactive material. In addition, specific considerations for HTG-SMRs can be made, such as a requirement to limit the ingress of air (oxygen) to minimize the oxidation of the core in the event of a depressurization accident.

Overarching requirement: Although a licensee may indicate that airlocks are not needed for contamination control, access routes have to be designed in such a way that zoning systems, if included, are not compromised by the access (e.g. ventilation cascades are not affected by the opening of doors).

Paragraph 6.25: The intent of this supporting requirement about providing protection to operating personnel entering the reactor building remains fully applicable.

Paragraph 6.26: The requirement for rapid closure of openings in the reactor building might not be necessary for an HTG-SMR; however, the reliable closure may be important to minimize air (oxygen) ingress in the event of a primary circuit depressurization accident.

### **Requirement 58: Control of containment conditions**

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

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

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

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

6.28B. The design shall also include features to enable the safe use of non-permanent equipment<sup>22</sup> for restoring the capability to remove heat from the containment.

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

- (a) To reduce the amounts of fission products that could be released to the environment in accident conditions;
- (b) To control the concentrations of hydrogen, oxygen and other substances in the containment atmosphere in accident conditions so as to prevent deflagration or detonation loads that could challenge the integrity of the containment.

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

## **BOX 22. CONSIDERATIONS ABOUT THE APPLICABILITY**

### **POSITION A**

The general considerations about the applicability of requirements 55–58 are provided in common below.

### **POSITION B (for Requirement 58)**

*Suggested changes:* None.

*Suggested interpretation and corresponding justifications:*

In the context of Requirement 58, the term ‘containment’ has to be considered as related to the ‘reactor building’.

The purpose of Requirement 58 can be summarized as ‘to ensure that the functionality or integrity of structures, systems and components (SSCs) important to safety inside the containment (reactor building), are not compromised by environmental conditions (e.g. pressure, temperature or radiation levels)’.

6.27: The intention of this supporting requirement is fully applicable to releases of high energy fluids into the reactor building.

6.28: The use of the term ‘acceptably low levels’ allows a graded approach depending on the requirements about the SSCs credited in the safety case.

6.28A: It can be considered that this supporting requirement applies to the reactor building, which for HTG-SMR designs is typically fitted with a pressure relief device.

---

<sup>22</sup> Non-permanent equipment need not necessarily be stored on the site.

6.28B: This supporting requirement might be necessary to ensure heat removal from the reactor building, to respect the design limits of SSCs important to safety (including the reactor building itself), if the designed heat removal pathway is lost (e.g. due to an extreme external event).

6.29: This supporting requirement applies to HTG-SMRs. It includes the term ‘as necessary’, allowing a licensee to put forward an argument not to include such design features for control of releases into the reactor building where not relevant to nuclear safety.

6.30: This supporting requirement applies to HTG-SMRs; however, in the reactor building of this reactor technology, relatively limited interferences with other safety functions from degradation of coverings, thermal insulation and coatings can be expected.

## **POSITION A**

### **General considerations about the applicability of requirements 55–58:**

*Suggested changes:* To consider these requirements not applicable (i.e. to delete requirements 55–58).

*Suggested interpretations:*

The intention of Requirement 58 is only broadly applicable to HTG-SMRs.

*Justification for the suggested changes and interpretations:*

Requirements 55–58 generally address the importance of the containment to perform confinement function, which is specific to the traditional water-cooled reactors. However, for HTG-SMRs, the fuel is considered as the dominant contributor to the confinement function, and such confinement function of the containment is less relevant. Therefore, the requirements 55–58 are generally considered as not applicable to HTG-SMRs.

Notwithstanding the above, it is recognized that further discussions are necessary in the near future to formulate additional requirements, specific for the containment of HTG-SMRs and replacing the existing ones, to address their unique features in terms of confinement function.

## INSTRUMENTATION AND CONTROL SYSTEMS

### **Requirement 59: Provision of instrumentation**

**Instrumentation shall be provided for: determining the values of all the main variables that can affect the fission process, the integrity of the reactor core, the reactor coolant systems and the containment at the nuclear power plant; for obtaining essential information on the plant that is necessary for its safe and reliable operation; for determining the status of the plant in accident conditions; and for making decisions for the purposes of accident management.**

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

### **Requirement 60: Control systems**

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

### **Requirement 61: Protection system**

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

- 6.32. The protection system shall be designed:
- (a) To be capable of overriding unsafe actions of the control system;
  - (b) With fail-safe characteristics to achieve safe plant conditions in the event of failure of the protection system.
- 6.33. The design:
- (a) Shall prevent operator actions that could compromise the effectiveness of the protection system in operational states and in accident conditions, but shall not counteract correct operator actions in accident conditions;
  - (b) Shall automate various safety actions to actuate safety systems so that operator action is not necessary within a justified period of time from the onset of anticipated operational occurrences or accident conditions;
  - (c) Shall make relevant information available to the operator for monitoring the effects of automatic actions.

### **Requirement 62: Reliability and testability of instrumentation and control systems**

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

- 6.34. Design techniques such as testability, including a self-checking capability where necessary, fail-safe characteristics, functional diversity and diversity in component design and in concepts of operation shall be used to the extent practicable to prevent the loss of a safety function.
- 6.35. Safety systems shall be designed to permit periodic testing of their functionality when the plant is in operation, including the possibility of testing channels independently for the detection of failures and losses of redundancy. The design shall permit all aspects of functionality testing for the sensor, the input signal, the final actuator and the display.
- 6.36. When a safety system, or part of a safety system, has to be taken out of service for testing, adequate provision shall be made for the clear indication of any protection system bypasses that are necessary for the duration of the testing or maintenance activities.

### **Requirement 63: Use of computer based equipment in systems important to safety**

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

- 6.37. For computer based equipment in safety systems or safety related systems:
- (a) A high quality of, and best practices for, hardware and software shall be used, in accordance with the importance of the system to safety.
  - (b) The entire development process, including control, testing and commissioning of design changes, shall be systematically documented and shall be reviewable.
  - (c) An assessment of the equipment shall be undertaken by experts who are independent of the design team and the supplier team to provide assurance of its high reliability.

- (d) Where safety functions are essential for achieving and maintaining safe conditions, and the necessary high reliability of the equipment cannot be demonstrated with a high level of confidence, diverse means of ensuring fulfilment of the safety functions shall be provided.
- (e) Common cause failures deriving from software shall be taken into consideration.
- (f) Protection shall be provided against accidental disruption of, or deliberate interference with, system operation.

#### **Requirement 64: Separation of protection systems and control systems**

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

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

#### **Requirement 65: Control room**

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

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

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

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

#### **Requirement 66: Supplementary control room**

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

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

## BOX 23. CONSIDERATIONS ABOUT THE APPLICABILITY

*Suggested changes:* None.

*Suggested interpretations:*

For HTG-SMRs, the supplementary control room might be of less importance compared to the existing water cooled nuclear power plants. The main function of the supplementary control room would be the safe shutdown of the reactor and the periodic monitoring of safety related data from the reactor after shutdown.

*Justification for the suggested interpretations:*

Some HTG-SMR designs aim not to rely on operator actions for the safety of the reactor.

### **Requirement 67: Emergency response facilities on the site**

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

6.42. Information about important plant parameters and radiological conditions at the nuclear power plant and in its immediate surroundings shall be provided to the relevant emergency response facilities<sup>23</sup>. Each facility shall be provided with means of communication with, as appropriate, the control room, the supplementary control room and other important locations at the plant, and with on-site and off-site emergency response organizations.

### EMERGENCY POWER SUPPLY

#### **Requirement 68: Design for withstanding the loss of off-site power**

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

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

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

6.44A. The alternate power source shall be capable of supplying the necessary power to preserve the integrity of the reactor coolant system and to prevent significant damage to the core and to spent fuel in the event of the loss of off-site power combined with failure of the emergency power supply.

6.44B. Equipment that is necessary to mitigate the consequences of *design extension conditions* ~~melting of the reactor core~~ shall be capable of being supplied by any of the available power sources.

---

<sup>23</sup> Emergency response facilities are addressed in IAEA Safety Standards Series No. GSR Part 7, Preparedness and Response for a Nuclear or Radiological Emergency [11]. For nuclear power plants, emergency response facilities (which are separate from the control room and the supplementary control room) include the technical support centre, the operational support centre and the emergency centre.

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

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

6.45. The design basis for any diesel engine or other prime mover<sup>24</sup> that provides an emergency power supply to items important to safety shall include:

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

6.45A. The design shall also include features to enable the safe use of non-permanent equipment to restore the necessary electrical power supply.<sup>25</sup>

## **BOX 24. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* See para. 6.44B

*Suggested interpretations:*

The term ‘necessary power’ used regarding emergency power supply and alternate power source has to be interpreted as applicable to all the safety functions and support functions that need power supply.

*Justification for the suggested changes and interpretations:*

SMRs may be designed with passive or non-power dependent safety features and, therefore, might not be reliant on power to maintain safety. Nevertheless, an emergency or alternate power supply with adequate reliability has to be in place for monitoring the reactor under loss of off-site power supply and any other accidents, even for plants using extensive passive safety features.

## SUPPORTING SYSTEMS AND AUXILIARY SYSTEMS

### **Requirement 69: Performance of supporting systems and auxiliary systems**

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

---

<sup>24</sup> A prime mover is a component (such as a motor, solenoid operator or pneumatic operator) that converts energy into action when commanded by an actuation device.

<sup>25</sup> Non-permanent equipment need not necessarily be stored on the site.

#### **Requirement 70: Heat transport systems**

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

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

#### **Requirement 71: Process sampling systems and post-accident sampling systems**

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

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

#### **Requirement 72: Compressed air systems**

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

#### **Requirement 73: Air conditioning systems and ventilation systems**

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

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

- (a) To prevent unacceptable dispersion of airborne radioactive substances within the plant;
- (b) To reduce the concentration of airborne radioactive substances to levels compatible with the need for access by personnel to the area;
- (c) To keep the levels of airborne radioactive substances in the plant below authorized limits and as low as reasonably achievable;
- (d) To ventilate rooms containing inert gases or noxious gases without impairing the capability to control radioactive effluents;
- (e) To control gaseous radioactive releases to the environment below the authorized limits on discharges and to keep them as low as reasonably achievable.

6.49. *The design shall minimize the spread of contamination from areas of high contamination to areas of low contamination, for example by maintaining areas of higher contamination at the plant ~~shall be maintained~~ at a negative pressure differential (partial vacuum) with respect to areas of lower contamination and other accessible areas.*

## **BOX 25. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* See para. 6.49.

*Suggested interpretations:* None.

*Justification for the suggested changes:*

Even though the negative pressure differential (partial vacuum) has been utilized for the minimization of contamination spread for the existing NPPs, other mechanisms can be utilized to achieve this aim. The original wording of the requirement describes the negative pressure differential as the only measure for the minimization of contamination spread and needs to be generalized for application to SMRs. The generalization is considered especially necessary for SMR designs incorporating passive safety systems, having the possibility of employing alternative means for isolating areas of contamination from clean areas, when an accident occurs.

### **Requirement 74: Fire protection systems**

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

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

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

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

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

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

### **Requirement 75: Lighting systems**

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

### **Requirement 76: ~~Overhead~~ Lifting equipment**

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

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

- (a) Measures are taken to prevent the lifting of excessive loads;
- (b) Conservative design measures are applied to prevent any unintentional dropping of loads that could affect items important to safety;

- (c) The plant layout permits safe movement of the ~~overhead~~ lifting equipment and of items being transported;
- (d) Such equipment can be used only in specified plant states (by means of safety interlocks on the ~~crane~~ lifting equipment);
  - (e) Such equipment for use in areas where items important to safety are located is seismically qualified.

## **BOX 26. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* See title, overarching requirement and para. 6.55, items (c) and (d).

*Suggested interpretations:* None.

*Justification for the suggested changes:*

Limiting the lifting equipment to overhead equipment might have undesirable effects. Some SMR designs do not allow for the use of overhead lifting equipment because of a lack of overall volume to handle the items. Requirement 76 as it is currently formulated is not applicable to these SMR designs. The purpose of the suggested changes is to remove that limitation, allowing for other types of lifting equipment when appropriate, such as jacks, forklifts and cranes.

It is understood that the suggested changes have very little impact on the lifting equipment used in large scale NPPs, therefore it might be considered to incorporate them to the design safety requirements in the next revision.

## OTHER POWER CONVERSION SYSTEMS

### **Requirement 77: Steam supply system, feedwater system and turbine generators**

**The design of the steam supply system, feedwater system and turbine generators for the nuclear power plant shall be such as to ensure that the appropriate design limits of the reactor coolant pressure boundary are not exceeded in operational states or in accident conditions.**

6.56. The design of the steam supply system shall provide for appropriately rated and qualified steam isolation valves capable of closing under the specified conditions in operational states and in accident conditions.

6.57. The steam supply system and the feedwater systems shall be of sufficient capacity and shall be designed to prevent anticipated operational occurrences from escalating to accident conditions.

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

## **BOX 27. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* None.

*Suggested interpretations:*

Paragraph 6.56: Regarding the scenario of water ingress, the isolation of the steam supply system in HTG-SMRs might also contribute to the mitigation of water ingress into the core in the case that heat exchanger and/or steam generator tube rupture occurs. In addition, HTG-SMR designs might also include a system that provides fast drainage of the water from the

heat exchanger and/or steam generator, which is the major contributor to the mitigation of water ingress.

*Justification for the suggested interpretations:*

The supporting requirement provided in para. 6.56 and addressing the isolation of the steam supply system, is applicable to limit the water ingress. However, it is insufficient. The isolation of the feedwater system, fast drainage of water and other design features has also to be addressed elsewhere.

Paragraph 6.58 is applicable to HTG-SMRs with either steam turbine or gas turbine. However, it is noted that there are different possible HTG-SMR secondary system configurations that might be different from that of LWRs (e.g. gas turbines). Therefore, the specific requirements related to the design of the secondary coolant system using water and steam might not always be applicable.

## TREATMENT OF RADIOACTIVE EFFLUENTS AND RADIOACTIVE WASTE

### **Requirement 78: Systems for treatment and control of waste**

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

6.59. Systems and facilities shall be provided for the management and storage of radioactive waste on the nuclear power plant site *or at an off-site waste treatment facility* for a period of time consistent with the availability of the relevant disposal option.

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

### **BOX 28. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* See para. 6.59

*Suggested interpretations:* None.

*Justification for the suggested changes:*

SMRs could be built in large numbers in a geographic area and therefore could enable a fleet solution to be derived for the effective and safe management of waste and the decommissioning process. This might enable consideration to be given to the construction of a single waste facility that would be built solely for that purpose. Such a fleet facility would have greater throughput of waste and therefore would offer a greater opportunity for the application of advanced processing technology to reduce environmental impact.

### **Requirement 79: Systems for treatment and control of effluents**

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

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

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

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

## FUEL HANDLING AND STORAGE SYSTEMS

### **Requirement 80: Fuel handling and storage systems**

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

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

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

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

- (a) To prevent criticality by a specified margin, by physical means or by means of physical processes, and preferably by use of geometrically safe configurations, even under conditions of optimum moderation;
- (b) To permit inspection of the fuel;
- (c) To permit maintenance, periodic inspection and testing of components important to safety;
- (d) To prevent damage to the fuel;
- (e) To prevent the dropping of fuel in transit;
- (f) To provide for the identification of individual fuel assemblies;
- (g) To provide proper means for meeting the relevant requirements for radiation protection;
- (h) To ensure that adequate operating procedures and a system of accounting for, and control of, nuclear fuel can be implemented to prevent any loss of, or loss of control over, nuclear fuel.

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

- (a) To permit adequate removal of heat from the fuel in operational states and in accident conditions;
- (b) To prevent the dropping of spent fuel in transit;
- (c) To avoid causing unacceptable handling stresses on fuel elements or fuel assemblies;
- (d) To prevent the potentially damaging dropping of heavy objects such as spent fuel casks, cranes or other objects onto the fuel;
- (e) To permit safe keeping of suspect or damaged fuel elements or fuel assemblies;
- (f) To control levels of soluble absorber if this is used for criticality safety;
- (g) To facilitate maintenance and future decommissioning of fuel handling and storage facilities;
- (h) To facilitate decontamination of fuel handling and storage areas and equipment when necessary;
- (i) To accommodate, with adequate margins, all the fuel removed from the reactor in accordance with the strategy for core management that is foreseen and the amount of fuel in the full reactor core;
- (j) To facilitate the removal of fuel from storage and its preparation for off-site transport.

6.68. For reactors using a water pool system for fuel storage, the design shall be such as to prevent the uncovering of fuel assemblies in all plant states that are of relevance for the spent fuel pool so that the

possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is ‘practically eliminated’<sup>26</sup> and so as to avoid high radiation fields on the site. The design of the plant:

- (a) Shall provide the necessary fuel cooling capabilities;
- (b) Shall provide features to prevent the uncovering of fuel assemblies in the event of a leak or a pipe break;
- (c) Shall provide a capability to restore the water inventory.

The design shall also include features to enable the safe use of non-permanent equipment to ensure sufficient water inventory for the long term cooling of spent fuel and for providing shielding against radiation.<sup>27</sup>

*6.68bis. For reactors using an air cooling system for fuel storage, the design shall be such as to provide adequate cooling of fuel elements in all plant states of relevance for the spent fuel storage, so that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is ‘practically eliminated’ and so as to avoid high radiation fields on the site. The design of the plant:*

- (a) Shall provide the necessary fuel cooling capabilities;*
- (b) Shall provide features to ensure adequate cooling of fuel elements in the event of a leak of the air-cooling system;*

*The design shall also include features to provide shielding against radiation and the necessary confinement capability of radioactive material for dry cask.*

6.68A. The design for reactors using a water pool system for fuel storage shall include the following:

- (a) Means for monitoring and controlling the water temperature for operational states and for accident conditions that are of relevance for the spent fuel pool;
- (b) Means for monitoring and controlling the water level for operational states and for accident conditions that are of relevance for the spent fuel pool;
- (c) Means for monitoring and controlling the activity in water and in air for operational states and means for monitoring the activity in water and in air for accident conditions that are of relevance for the spent fuel pool;
- (d) Means for monitoring and controlling the water chemistry for operational states.

*6.68B. The design for reactors using an air cooling system for fuel storage shall include the following:*

- (a) Means for monitoring and controlling the air temperature for operational states and for accident conditions that are of relevance for the spent fuel storage region;*
- (b) Means for monitoring and controlling the activity in air for operational states and means for monitoring the activity in air for accident conditions that are of relevance for the spent fuel storage region;*

---

<sup>26</sup> 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.

<sup>27</sup> Non-permanent equipment need not necessarily be stored on the site.

## BOX 29. CONSIDERATIONS ABOUT THE APPLICABILITY

*Suggested changes:* See the new paras 6.68bis, 6.68A and 6.68B.

*Suggested interpretations:*

Note: Further supporting requirements on fuel handling and storage systems, additionally to those proposed above for air cooled fuel storage, appear to be necessary and might need to be developed. For example, the need for further requirements will depend on the method for providing cooling (active or passive) and might need to account for potential issues, such as air intake blockage or water ingress.

*Justification for the suggested changes and interpretations:*

The HTG-SMRs might use air cooling for the spent fuel storage.

As compared to large water-cooled reactors, the fuel power density of HTG-SMRs is low, the safety margin of fuel particle temperature is large, and the cooling of spent fuel is thus potentially less challenging.

### RADIATION PROTECTION

#### **Requirement 81: Design for radiation protection**

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

6.69. Radiation sources throughout the plant shall be comprehensively identified, and exposures and radiation risks associated with them shall be kept as low as reasonably achievable<sup>28</sup>, the integrity of the fuel ~~cladding~~ shall be maintained, and the generation and transport of corrosion products and activation products shall be controlled.

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

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

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

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

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

---

<sup>28</sup> Requirements on radiation protection and the safety of radiation sources for facilities and activities are established in GSR Part 3 [9].

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

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

### **BOX 30. CONSIDERATIONS ABOUT THE APPLICABILITY**

*Suggested changes:* See para. 6.69.

*Suggested interpretation:* None

*Justification for the suggested changes:*

The term 'fuel cladding' is LWR-specific.

#### **Requirement 82: Means of radiation monitoring**

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

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

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

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

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

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

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

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

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

- (a) Exposure pathways to people, including the food chain;
- (b) Radiological impacts, if any, on the local environment;
- (c) The possible buildup, and accumulation in the environment, of radioactive substances;
- (d) The possibility of there being any unauthorized routes for radioactive releases.

**BOX 31. CONSIDERATIONS ON POTENTIAL ADDITIONAL REQUIREMENTS FOR MULTI-MODULE UNITS** *(These considerations are also applicable to LW-SMRs)*

**Considerations regarding multi-module units**

New requirements or additions to the existing requirements are deemed necessary to address particular safety considerations related to the use of multiple reactor modules within a single unit (multi-module units). Some of these new requirements have already been captured in this appendix; however, the following additional aspects might be considered in further reviews of the design safety requirements:

- A) Interconnections among the reactor modules.** For purposes such as operation and accident management, multi-module units might include interconnections between reactor modules. In this case, specific considerations are necessary to ensure that such interconnections will not be detrimental to the safety of each reactor module and of the overall plant.
- B) Control and protection systems.** The control and protection systems of each module and of all the modules have to ensure that a clear actuation logic is reliably implemented so that an initiating event or accident occurring within one reactor module will not propagate to accident conditions in other reactor modules and that the reactor modules will not have detrimental effects on each other under accident conditions.
- C) Human factors engineering.** This covers aspects relating to the main control room, supplementary control and other emergency response facilities and locations; maintenance of the multiple modules; potential remote control of the main control room; one operator managing several modules; more than one module supplying the same turbine.
- D) Emergency preparedness and response.** This includes aspects relating to the design of multi-module units to enable the emergency response under all relevant conditions.
- E) Capacity for the addition of future modules, plant lay-out and construction.** Some design schemes consider a plant lay-out which allows a consecutive and serialized construction of the reactor modules. This new practice has to involve additional, important, safety considerations. Some SMR designs adopt extension of power capacity during plant lifetime through additional module installation. Changes in specifications or capability might result in the addition of new equipment which could, for example, increase the load on heating, ventilating and air conditioning systems. Therefore, consideration might need to be given to including margins in the design capability of relevant support systems to allow for the potential addition of new equipment at a later date.

*Justification for the suggestion of adding new requirements in these areas:*

The safety requirements established in SSR-2/1 (Rev. 1) [2] are primarily applicable to land based stationary NPPs that comprise a single nuclear reactor or more nuclear reactors which are to a great extent independent from each other. When there are interconnections among the reactors, the number of the interconnections is very limited and usually the interconnections are meant to cope with complex plant conditions for safety considerations.

For SMR designs, there are more design configurations and application options than for land based stationary NPPs. An SMR unit might comprise more than one reactor module having, for example, a common control room, or might be housed in one common reactor building. These aspects are not covered in SSR-2/1 (Rev. 1) [2] and therefore pose new challenges in establishing design safety requirements.



## REFERENCES<sup>29</sup>

- [1] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR Part 4 Rev. 1), AEA, Vienna (2016).
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection (2007 Edition), IAEA, Vienna (2007).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Commissioning and Operation, IAEA Safety Standards Series No. SSR-2/2 (Rev. 1), IAEA, Vienna (2016).
- [5] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).
- [6] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna (1999).
- [7] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life, INSAG-19, IAEA, Vienna (2003).
- [8] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-R-3, IAEA, Vienna (2006). (A revision of this publication is in preparation, to be issued as GSR Part 2.)
- [9] EUROPEAN COMMISSION, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards, IAEA Safety Standards Series No. GSR Part 3, IAEA, Vienna (2014).
- [10] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. NS-R-3 (Rev. 1), IAEA, Vienna (2016).
- [11] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR- TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015).

---

<sup>29</sup> List of references copied from SSR-2/1 (Rev. 1) [2].



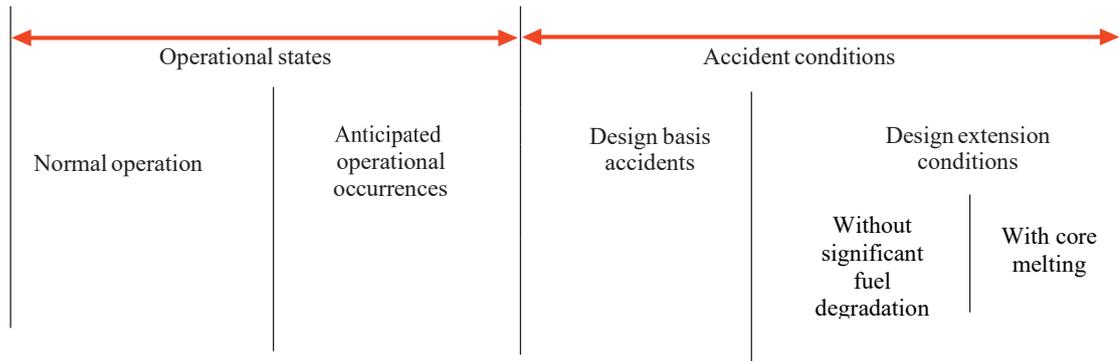
## DEFINITIONS<sup>30</sup>

*The following new and revised definitions differ from those in the IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection (2007 Edition), IAEA, Vienna (2007):*  
<http://www-pub.iaea.org/books/IAEABooks/7648/IAEA-Safety-Glossary>

*The symbol '(i)' denotes an information note.*

**controlled state.** Plant state, following an anticipated operational occurrence or accident conditions, in which the fundamental safety functions can be ensured and which can be maintained for a time sufficient to effect provisions to reach a safe state.

**plant states** (*considered in design*)



**accident conditions.** Deviations from normal operation that are less frequent and more severe than anticipated operational occurrences.

(i) Accident conditions comprise design basis accidents and design extension conditions.

**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.

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

(i) Design extension conditions comprise conditions in events without significant fuel degradation and conditions in events with core melting.

**safe state.** Plant state, following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time.

**safety feature for design extension conditions.** Item designed to perform a safety function or which has a safety function in design extension conditions.

**safety system settings.** Settings for levels at which safety systems are automatically actuated in the event of anticipated operational occurrences or design basis accidents, to prevent safety limits from being exceeded.

---

<sup>30</sup> List of definitions copied from SSR-2/1 (Rev. 1) [2].

## BOX 32. CONSIDERATIONS ABOUT THE APPLICABILITY OF DEFINITIONS

### COMMON POSITION

*Suggested changes: To add the definition of the following new terms:*

**Multi-module unit.** *A unit having the possibility of including more than one reactor module.*

- (i) *A multi-module unit might include only one reactor module in the first stage of its planned development*
- (ii) *Features of the multi-module unit approach typically include the following:*
  - a. *Allow the addition of several modules in close proximity to the same infrastructure;*
  - b. *The modules might be deployed in compact configurations and share structures, systems and components to a larger extent than in units using a single reactor design approach, provided fulfilment of corresponding requirements;*
  - c. *Each module can be operated mostly independently of the state of completion or operating condition of any other module of the multi-module unit;*
  - d. *The different modules are essentially identical.*

**Reactor module (sometimes abbreviated as ‘module’).** *A nuclear reactor with its associated structures, systems and components. This term is used in multi-module units.*

*Suggested interpretations: None*

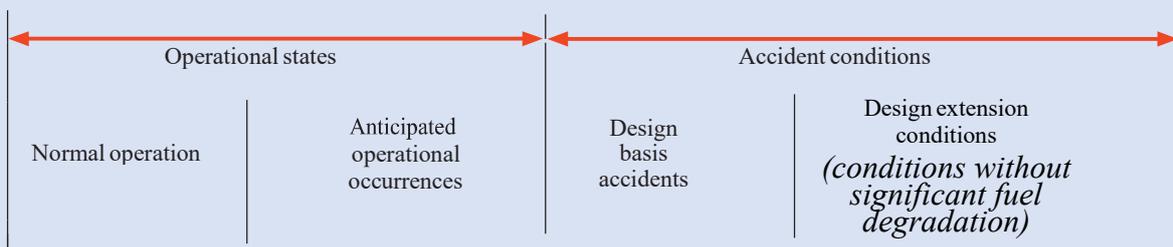
*Justification for the suggested changes:*

The use of these terms is necessary in this publication and also in future publications related to design safety and safety assessment of SMRs.

### POSITION A

*Suggested changes:*

**plant states** (*considered in design*):



- (i) *Design extension conditions refer to ~~comprise~~ conditions ~~in events~~ without significant fuel degradation and conditions ~~in events with core melting~~.*

*Suggested interpretations: None*

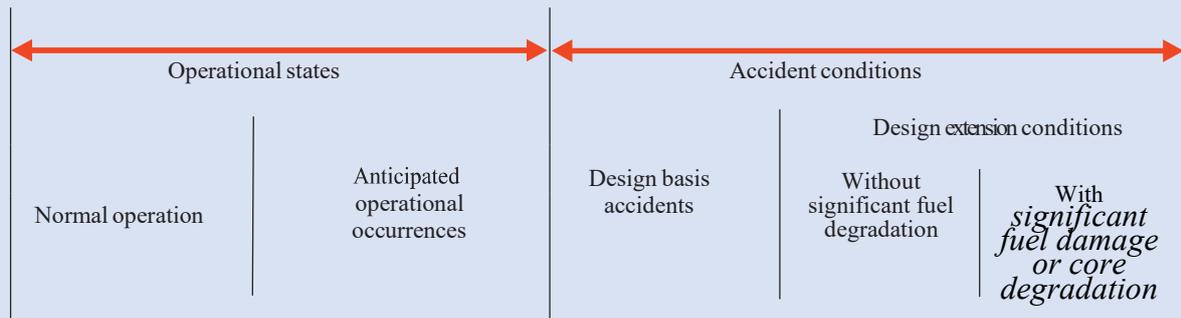
*Justification for the suggested changes:*

See the ones provided in Box 5, position A, of this appendix (Requirement 20)).

## **POSITION B**

*Suggested changes:*

**plant states** (*considered in design*):



- (i) Design extension conditions comprise conditions in events without significant fuel degradation and conditions in events with *significant fuel damage or core degradation* ~~core melting~~.

*Suggested interpretations:* None

*Justification for the suggested changes:*

See the ones provided in Box 5, position B, of this appendix (Requirement 20)).



## REFERENCES

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY, Advances in Small Modular Reactor Technology Developments, a Supplement to IAEA Advanced Reactors Information System (ARIS), IAEA Booklet, 2020 Edition, IAEA, Vienna (2020).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Analysis for Nuclear Power Plants with Modular High Temperature Gas Cooled Reactors, Safety Report Series No. 54, IAEA, Vienna (2008).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, Fuel Performance and Fission Product Behavior in Gas Cooled Reactors, IAEA-TECDOC-978, IAEA, Vienna (1997).
- [5] INTERNATIONAL ATOMIC ENERGY AGENCY, High Temperature Gas Cooled Reactor Fuels and Materials, IAEA-TECDOC-CD-1645, IAEA, Vienna (2010).
- [6] REUTLER H, LOHNERT GH, Advantages of going modular in HTRs, NEDEAU, 78 (1984) 129-136.
- [7] LOHNERT GH, Technical design features and essential safety-related properties of the HTR-Module. NEDEAU, 121 (1990) 259-275.
- [8] LOHNERT GH, The consequences of water ingress into the primary circuit of an HTR-Module – From design basis accident to hypothetical postulates. NEDEAU, 134 (1992) 159-176.
- [9] SAITO, S., et al., Design of High Temperature Engineering Test Reactor (HTTR), Report of the Japan Atomic Energy Research Institute, JAERI 1332 (1994).



## ANNEX I. APPLICABILITY OF DESIGN SAFETY REQUIREMENTS RELATED TO THE REACTOR CONTAINMENT TO HTG-SMRS

This annex includes a structured approach used to determine the applicability of the design safety requirements established in SSR-2/1 (Rev. 1) [I-1] relating to containment structure and containment system, mainly requirements 55 to 58, for HTG-SMRs (See Table A–1 and Figure A–1). The results of the considerations on applicability for each of these requirements are provided in Appendix II (see ‘position B’ in Boxes 19-22).

TABLE A–1. STRUCTURED APPROACH TO DETERMINE THE APPLICABILITY OF SAFETY REQUIREMENTS ON THE REACTOR CONTAINMENT TO HTG-SMRs

Req. Nr and title Or Para. Nr	Requirement wording at SSR-2/1 (Rev. 1)	Underlying principle(s)	Safety Function(s)	Contributing SSCs <sup>a</sup>	Observations
<b>55</b> <b>Control of radioactive releases from the containment</b>	<b>The design of the containment shall be such as to ensure that any radioactive release from the nuclear power plant to the environment is as low as reasonably achievable, is below the authorized limits on discharges in operational states and is below acceptable limits in accident conditions.</b>	To ensure that radioactive releases are as low as reasonably achievable and below authorized limits.	Confinement of radioactive substances in operational states and in accident conditions.	Fuel; Pressure boundary; Concrete reactor building and its internal and associated structures.	The underlying principle is applicable to all reactor designs.
6.20	The containment structure and the systems and components affecting the leaktightness of the containment system shall be designed and constructed so that the leak rate can be tested after all penetrations through the containment have been installed and, if necessary, during the operating lifetime of the plant, so that the leak rate can be tested at the containment design pressure.	To confirm the leaktightness assumed in the safety analysis and to ensure that it remains valid throughout the lifetime of the NPP.	Confinement of radioactive substances in operational states and in accident conditions.	Fuel; Pressure boundary; Concrete reactor building and its internal and associated structures.	Paragraph 6.20 refers to the reactor building. In HTG-SMRs the reactor building contributes to the ‘confinement’ of radioactive materials, along with the fuel and the reactor pressure boundary. Therefore, in HTG-SMRs adequate leaktightness has to be assured by the ‘confinement system’ (e.g. by applying the concept of ‘functional containment’, which can be defined as a barrier or set of barriers taken together, that effectively limits the physical release of radioactive substances to the environment); this typically includes the fuel, the pressure boundary and the reactor building. The effectiveness of a ‘functional containment’ has to be demonstrated at commissioning and throughout the lifetime of the plant, as necessary.

<sup>a</sup> SSC: Structures, Systems and Components

TABLE A-1. STRUCTURED APPROACH TO DETERMINE THE APPLICABILITY OF SAFETY REQUIREMENTS ON THE REACTOR CONTAINMENT TO HTG-SMRs (cont.)

Req. Nr and title Or Para. Nr	Requirement wording at SSR-2/1 (Rev. 1)	Underlying principle(s)	Safety Function(s)	Contributing SSCs <sup>b</sup>	Observations
6.21	<p>The number of penetrations through the containment shall be kept to a practical minimum and all penetrations shall meet the same design requirements as the containment structure itself. The penetrations shall be protected against reaction forces caused by pipe movement or accidental loads such as those due to missiles caused by external or internal events, jet forces and pipe whip.</p>	<p>Likelihood of compromising the integrity of SSCs supporting confinement and/or containment functions is to be minimized by design. For example, penetrations may be weak spots of the containment boundary, and, as such, need to be minimized and to have adequate protection against various reaction forces.</p>	<p>Confinement of radioactive substances in operational states and in accident conditions.</p>	<p>Fuel; Pressure boundary; Concrete reactor building and its internal and associated structures.</p>	<p>Paragraph 6.21 mainly refers to the reactor building. In HTG-SMRs, R/B contributes to confinement, along with fuel and reactor coolant pressure boundary (RCPB). This para. still contains a useful design objective for HTG-SMRs.</p> <p>The application of the wording "... <i>all penetrations shall meet the same design requirements as the containment structure itself</i>" can be commensurate with the consequences of failure of the penetrations, taking into account the allowable leak rate of the containment envelope.</p>
<p><b>56 Isolation of the containment</b></p>	<p><b>Each line that penetrates the containment at a nuclear power plant as part of the reactor coolant pressure boundary or that is connected directly to the containment atmosphere shall be automatically and reliably sealable in the event of an accident in which the leak tightness of the containment is essential to preventing radioactive releases to the environment that exceed acceptable limits.</b></p>	<p>Ensure that radioactive releases are as low as reasonably achievable and below authorized limits. Main concern addressed is containment bypass, caused by either coolant pressure boundary or pipes and penetrations that cross the containment boundary.</p>	<p>Confinement of radioactive substances in operational states and in accident conditions.</p>	<p>Concrete reactor building and its internal and associated structures.</p>	<p>The requirement can be applied in an objective based manner. The HTG-SMR designer has to demonstrate that other barriers, which contribute to the 'containment function', are effective in case sealing of one or more penetrations fail. For a pebble bed reactor, the long term management of dust and other radioactive debris will be a relevant factor in management of releases within the SSCs of the plant if a penetration fails.</p>

<sup>b</sup> SSC: Structures, Systems and Components

TABLE A-1. STRUCTURED APPROACH TO DETERMINE THE APPLICABILITY OF SAFETY REQUIREMENTS ON THE REACTOR CONTAINMENT TO HTG-SMRs (cont.)

Req. Nr and title Or Para. Nr	Requirement wording at SSR-2/1 (Rev. 1)	Underlying principle(s)	Safety Function(s)	Contributing SSCs <sup>c</sup>	Observations
6.22	Lines that penetrate the containment as part of the RCPB and lines that are connected directly to the containment atmosphere shall be fitted with at least two adequate containment isolation valves or check valves arranged in series and shall be provided with suitable leak detection systems. Containment isolation valves or check valves shall be located as close to the containment as is practicable, and each valve shall be capable of reliable and independent actuation and of being periodically tested.	Maintenance of the containment function and minimization of containment bypass. Confirmation of adequate leaktightness.	Confinement of radioactive substances in operational states and in accident conditions.	Concrete reactor building and its internal and associated structures.	A vendor can make a case that the requirement be applied in a way commensurate to the consequences of failure of the penetration taking into account the allowable leak rate of the containment envelope. For example, for an HTGR, if the helium gas is kept very clean and dust is managed, a blow-out of a penetration may not result in significant consequences.
6.23	Exceptions to the requirements for containment isolation stated in para. 6.22 shall be permissible for specific classes of lines such as instrumentation lines, or in cases in which application of the methods of containment isolation specified in para. 6.22 would reduce the reliability of a safety system that includes a penetration of the containment.	States exceptions from application of para. 6.22.			Definition of 'safety systems' relates to the approach adopted for safety classification.
6.24	Each line that penetrates the containment and is neither part of the RCPB nor connected directly to the containment atmosphere shall have at least one adequate containment isolation valve. The containment isolation valves shall be located outside the containment and as close to the containment as is practicable.	Maintenance of the containment function and/or prevention of containment bypass.	Confinement of radioactive substances in operational states and in accident conditions.	Concrete reactor building and its internal and associated structures.	This requirement has to be considered in the designs of all SMR technologies. Main reasons for that include maintenance and provisions to facilitate equipment replacement and removal (e.g. for outages or, more importantly, for decommissioning of SSCs).
<b>57 Access to the containment</b>	<b>Access by operating personnel to the containment at a nuclear power plant shall be through airlocks equipped with doors that are interlocked to ensure that at least one of the doors is closed during reactor power operation and in accident conditions.</b>	Ensure that radioactive releases are as low as reasonably achievable and below authorized limits. Minimizing containment bypass.	Confinement of radioactive substances in operational states and in accident conditions.	Concrete reactor building and its internal and associated structures.	All functions of an airlock (including confinement, access control, safety and security) have to be considered, if a case is made that the requirement might not be applicable.

<sup>c</sup> SSC: Structures, Systems and Components

TABLE A-1. STRUCTURED APPROACH TO DETERMINE THE APPLICABILITY OF SAFETY REQUIREMENTS ON THE REACTOR CONTAINMENT TO HTG-SMRs (cont.)

Req. Nr and title Or Para. Nr	Requirement wording at SSR-2/1 (Rev. 1)	Underlying principle(s)	Safety Function(s)	Contributing SSCs <sup>d</sup>	Observations
6.25	Where provision is made for entry of operating personnel for surveillance purposes, provision for ensuring protection and safety for operating personnel shall be specified in the design. Where equipment airlocks are provided, provision for ensuring protection and safety for operating personnel shall be specified in the design.	Protection of operating personnel.	Protection of operating personnel.	Concrete reactor building and its internal and associated structures.	
6.26	Containment openings for the movement of equipment or material through the containment shall be designed to be closed quickly and reliably in the event that isolation of the containment is required.	To ensure that radioactive releases are as low as reasonably achievable and below authorized limits.	Confinement of radioactive substances in operational states and in accident conditions.	Concrete reactor building and its internal and associated structures.	It applies to HTG-SMR. The term 'quickly' has to be interpreted according to the specifications of the containment (i.e. in the context of the internal event progression). For example, for HTG-SMRs, prevention of moisture or air ingress, as per the assumptions of the safety analysis, might require additional constraints to reactor building isolations.
<b>58 Control of containment conditions</b>	<b>Provision shall be made to control the pressure and temperature in the containment at a nuclear power plant and to control any buildup of fission products or other gaseous, liquid or solid substances that might be released inside the containment and that could affect the operation of systems important to safety.</b>	To ensure integrity of the reactor building structure and the equipment important to safety protected or contained by this structure.	All safety functions provided by the containment (see Req. 54). It also contributes to other safety functions (e.g. control, cooling and monitoring) fulfilled by the containment and/or provided by the SSCs the containment protects.	Concrete reactor building and its internal and associated structures.	The underlying principle is applicable to all SMR technologies.  Systems 'important to safety' are technology dependent and have to be determined through a comprehensive and systematic safety classification process.

<sup>d</sup> SSC: Structures, Systems and Components

TABLE A-1. STRUCTURED APPROACH TO DETERMINE THE APPLICABILITY OF SAFETY REQUIREMENTS ON THE REACTOR CONTAINMENT TO HTG-SMRs (cont.)

Req. Nr and title Or Para. Nr	Requirement wording at SSR-2/1 (Rev. 1)	Underlying principle(s)	Safety Function(s)	Contributing SSCs <sup>e</sup>	Observations
6.27	The design shall provide for sufficient flow routes between separate compartments inside the containment. The cross-sections of openings between compartments shall be of such dimensions as to ensure that the pressure differentials occurring during pressure equalization in accident conditions do not result in unacceptable damage to the pressure bearing structure or to systems that are important in mitigating the effects of accident conditions.	Ensure the integrity of the reactor building structure by adequate flow paths between reactor building compartments and thus preventing unacceptable loads during accidents involving release of high energy fluids.	All safety functions provided by the containment. It also contributes indirectly to other safety functions (e.g. control, cooling and monitoring) provided by the SSCs that the containment protects.	Concrete reactor building and its internal and associated structures.	
6.28, 6.28 A, 6.28 B	<p>6.28. The capability to remove heat from the containment shall be ensured, in order to reduce the pressure and temperature in the containment, and to maintain them at acceptably low levels after any accidental release of high energy fluids. The systems performing the function of removal of heat from the containment shall have sufficient reliability and redundancy to ensure that this function can be fulfilled.</p> <p>6.28A. Design provision shall be made to prevent the loss of the structural integrity of the containment in all plant states. The use of this provision shall not lead to an early radioactive release or a large radioactive release.</p> <p>6.28B. The design shall also include features to enable the safe use of non-permanent equipment for restoring the capability to remove heat from the containment.</p>	<p>To ensure integrity of the R/B structure.</p> <p>This requirement focuses on heat removal from the containment to ensure that pressures and temperatures in the reactor building are acceptable, so that early or large release of radioactivity are minimized.</p>	All safety functions provided by the containment.	Concrete reactor building and its internal and associated structures.	<p>6.28A. remains a valuable design rule as part of defence in depth, even if it is not necessary. It helps with plant recovery following initiating events.</p> <p>Provisions have to be considered for non-permanent connections to fulfil the safety functions provided by the containment.</p>

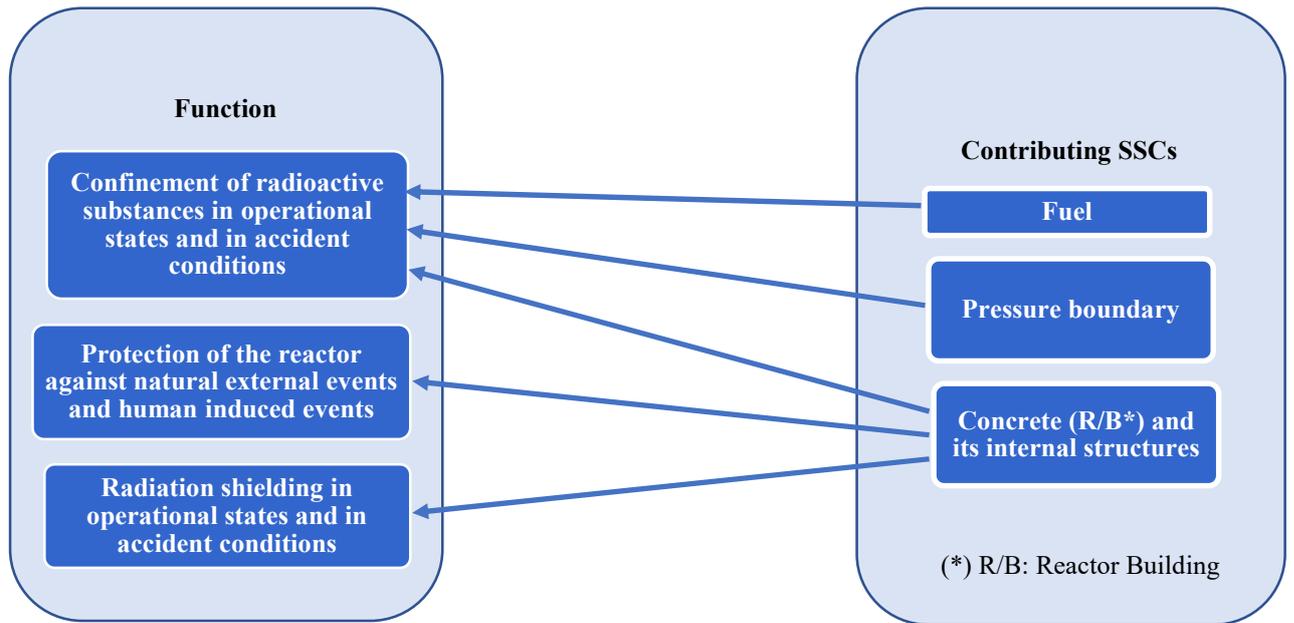
<sup>e</sup> SSC: Structures, Systems and Components

TABLE A-1. STRUCTURED APPROACH TO DETERMINE THE APPLICABILITY OF SAFETY REQUIREMENTS ON THE REACTOR CONTAINMENT TO HTG-SMRs (cont.)

Req. Nr and title Or Para. Nr	Requirement wording at SSR-2/1 (Rev. 1)	Underlying principle(s)	Safety Function(s)	Contributing SSCs <sup>f</sup>	Observations
6.29	<p>Design features to control fission products, hydrogen, oxygen and other substances that might be released into the containment shall be provided as necessary:</p> <p>(a) To reduce the amounts of fission products that could be released to the environment in accident conditions;</p> <p>(b) To control the concentrations of hydrogen, oxygen and other substances in the containment atmosphere in accident conditions so as to prevent deflagration or detonation loads that could challenge the integrity of the containment.</p>	<p>To ensure the integrity of the reactor building structure and the equipment important to safety protected and contained by this structure.</p>	<p>All safety functions provided by the containment.</p> <p>It also contributes indirectly to other safety functions (e.g. control, cooling and monitoring) provided by the SSCs that the containment protects.</p>	<p>Concrete reactor building and its internal and associated structures.</p>	
6.30	<p>Coverings, thermal insulations and coatings for components and structures within the containment system shall be carefully selected and methods for their application shall be specified to ensure the fulfilment of their safety functions and to minimize interference with other safety functions in the event of deterioration of the coverings, thermal insulations and coatings.</p>	<p>The design of reactor building has to consider the effect its components (e.g. thermal insulation and coatings) might have on the effectiveness of other items important to safety.</p>	<p>Other safety functions (e.g. control, cooling and monitoring) provided by the SSCs that the containment protects.</p>	<p>Concrete reactor building and its internal and associated structures.</p>	<p>The requirement mainly refers to LWR, for which the containment might impair long term ECIS<sup>g</sup> if debris and other contaminants clog the ECIS pump suction. Nevertheless, it might still be applicable to HTG-SMRs (e.g. coatings cannot lead to adverse events such as generation of corrosive gases, formation of hot spots on structures important to safety or degradation of components).</p>

<sup>f</sup> SSC: Structures, Systems and Components

<sup>g</sup> ECIS: Emergency coolant injection system



*FIG. A-1. Contribution of SSCs to the fulfilment of the safety functions in the containment of HTG-SMRs*

## REFERENCES TO ANNEX I

[I-1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).



## CONTRIBUTORS TO DRAFTING AND REVIEW

### CONTRIBUTORS TO THE TECDOC

Bernard, M.	Électricité de France, France
Calle Vives, P.	Office for Nuclear Regulation, United Kingdom
Chen, F.	Institute of Nuclear and New Energy Technology, China, People's Republic of
Flower, A.	Rolls-Royce plc, United Kingdom
Gimenez, M.	National Atomic Energy Commission, Argentina
Ingersoll, D.	NuScale Power Inc., United States of America
Madni, I.	Nuclear Regulatory Commission, United States of America
Muzikova, E.	Ultra-Safe Nuclear Corporation, South Africa
Ohashi, H.	Japan Atomic Energy Agency, Japan
Plummer, D.	Office for Nuclear Regulation, United Kingdom
Purba, J.	National Nuclear Energy Agency, Indonesia
Sato, H.	Japan Atomic Energy Agency, Japan
Shiba, S.	Nuclear Regulation Authority, Japan
Sinegribov, S.	Scientific and Engineering Centre for Nuclear and Radiation Safety, Russian Federation
Song, D.	Nuclear Power Institute of China, China, People's Republic of
Spitzer, C.	International Atomic Energy Agency
Tanase, A.	Canadian Nuclear Safety Commission, Canada
Villalibre Ares, P.	International Atomic Energy Agency
Wang, H.	Institute of Nuclear and New Energy Technology, China, People's Republic of
Wu, J.	National Nuclear Safety Administration, China, People's Republic of
Yang, Z.	National Nuclear Safety Administration, China, People's Republic of
Yllera Sanchez, J.	International Atomic Energy Agency
Zhong, F.	Nuclear Power Institute of China, China, People's Republic of

### Consultants Meetings

Vienna, Austria: 2-6 July 2018; 22-25 October 2018; 13-17 May 2019

## CONTRIBUTORS TO THE STUDY

Arnold, R.	International Atomic Energy Agency
Beck, R. (*)	Bechtel, United States of America
Bowser, R. (*)	Westinghouse Electric Company, United States of America
Boyes, D. (*)	Steenkampskraal Thorium Limited, South Africa
Burns, E. (*)	X-Energy, United States of America
Chen, F.	Institute of Nuclear and New Energy Technology, China, People's Republic of
Cook, S.	Canadian Nuclear Safety Commission, Canada
Gimenez, M.	National Atomic Energy Commission, Argentina
Flauw, Y.	Institute for Radiological Protection and Nuclear Safety, France
Fletcher, J.	Ultra-Safe Nuclear Corporation, South Africa
Flower, A.	Rolls-Royce plc, United Kingdom
Harkness, A. (*)	Westinghouse Electric Company, United States of America
Hirnuma, N.	International Atomic Energy Agency
Ingersoll, D.	NuScale Power Inc., United States of America
Kang, H.	Korea Atomic Energy Research Institute, Korea, Republic of
Lee, D. (*)	BWX Technology, United States of America
Madden, K.	International Atomic Energy Agency
Magruder, S.	International Atomic Energy Agency
Monti, S.	International Atomic Energy Agency
Moor, S.	Rolls-Royce plc, United Kingdom
Mount, J.	Rolls-Royce plc, United Kingdom
Mulder, E. (*)	X-Energy, United States of America
Ohashi, H.	Japan Atomic Energy Agency, Japan
Parada, F.	International Atomic Energy Agency
Park, J. S.	Korea Institute of Nuclear Safety, Korea, Republic of
Park, H. O. (*)	Korea Institute of Nuclear Safety, Korea, Republic of
Purba, J.	National Nuclear Energy Agency, Indonesia
Reitsma, F.	International Atomic Energy Agency
Rickman, R.	Terrestrial Energy, United States of America
Song, D.	Nuclear Power Institute of China, China, People's Republic of

Spitzer, C.	International Atomic Energy Agency
Subki, H.	International Atomic Energy Agency
Sun, Y.	Institute of Nuclear and New Energy Technology, China, People's Republic of
Trotta, R. (*)	Holtec International, United States of America
Villalibre Ares, P.	International Atomic Energy Agency
Wu, J.	National Nuclear Safety Administration, China, People's Republic of
Yllera Sanchez, J.	International Atomic Energy Agency

(\*) Main contribution provided by answering an inquiry form distributed at the start of the study.

### **Consultants Meetings**

Vienna, Austria: 20-24 February 2017; 12-16 June 2017



**IAEA**

International Atomic Energy Agency

No. 26

## ORDERING LOCALLY

IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

### NORTH AMERICA

***Bernan / Rowman & Littlefield***

15250 NBN Way, Blue Ridge Summit, PA 17214, USA

Telephone: +1 800 462 6420 • Fax: +1 800 338 4550

Email: [orders@rowman.com](mailto:orders@rowman.com) • Web site: [www.rowman.com/bernan](http://www.rowman.com/bernan)

### REST OF WORLD

Please contact your preferred local supplier, or our lead distributor:

***Eurospan Group***

Gray's Inn House  
127 Clerkenwell Road  
London EC1R 5DB  
United Kingdom

***Trade orders and enquiries:***

Telephone: +44 (0)176 760 4972 • Fax: +44 (0)176 760 1640

Email: [eurospan@turpin-distribution.com](mailto:eurospan@turpin-distribution.com)

***Individual orders:***

[www.eurospanbookstore.com/iaea](http://www.eurospanbookstore.com/iaea)

***For further information:***

Telephone: +44 (0)207 240 0856 • Fax: +44 (0)207 379 0609

Email: [info@eurospangroup.com](mailto:info@eurospangroup.com) • Web site: [www.eurospangroup.com](http://www.eurospangroup.com)

### Orders for both priced and unpriced publications may be addressed directly to:

Marketing and Sales Unit

International Atomic Energy Agency

Vienna International Centre, PO Box 100, 1400 Vienna, Austria

Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 26007 22529

Email: [sales.publications@iaea.org](mailto:sales.publications@iaea.org) • Web site: [www.iaea.org/publications](http://www.iaea.org/publications)

**International Atomic Energy Agency  
Vienna**