IAEA Nuclear Energy Series

No. NP-T-2.2

Design Features to Achieve Defence in Depth in Small and Medium Sized Reactors

IAEA
International Atomic Energy Agency

DESIGN FEATURES TO ACHIEVE DEFENCE IN DEPTH IN SMALL AND MEDIUM SIZED REACTORS

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

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHRAIN
BANGLADESH
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BULGARIA
BURKINA FASO
BURUNDI
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LATVIA
LEBANON
LIBERIA
LIBYAN ARAB JAMAHIRIYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TUNISIA
TURKEY
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VENEZUELA
VIETNAM
YEMEN
ZAMBIA
ZIMBABWE

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 NUCLEAR ENERGY SERIES No. NP-T-2.2

DESIGN FEATURES TO ACHIEVE DEFENCE IN DEPTH IN SMALL AND MEDIUM SIZED REACTORS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2009

Sales and Promotion, Publishing Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
1400 Vienna, Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/books

Printed by the IAEA in Austria
June 2009
STI/PUB/1399

IAEA Library Cataloguing in Publication Data

Design features to achieve defence in depth in small and medium sized reactors. — Vienna : International Atomic Energy Agency, 2009.
p. ; 29 cm. — (IAEA nuclear energy series, ISSN 1995–7807 ; no. NP-T-2.2)
STI/PUB/1399
ISBN 978–92–0–104209–5
Includes bibliographical references.

1. Nuclear reactors — Safety measures. 2. Nuclear reactors — Design and construction. I. International Atomic Energy Agency. II. Series.

IAEAL 09–00588

FOREWORD

There is a continued interest among Member States in the development and application of small and medium sized reactors (SMRs). In the very near term, most new nuclear power plants (NPPs) are likely to be evolutionary water cooled reactor designs building on proven systems while incorporating technological advances and often economies of scale, resulting in outputs of up to 1600 MW(e) from the reactor. For the longer term, the focus is on innovative designs to provide increased benefits in the areas of safety and security, non-proliferation, waste management, resource utilization and economics, as well as to offer a variety of energy products and flexibility in design, siting and fuel cycle options. Many innovative designs are implemented in reactors within the small to medium size range having equivalent electric power of less than 700 MW(e) or even less than 300 MW(e).

Incorporation of inherent and passive safety design features has become a 'trademark' of many advanced reactor concepts, including several evolutionary designs and nearly all innovative SMR design concepts. Ensuring adequate defence in depth is important for reactors with smaller output because many of them are being designed to allow greater proximity to the user, specifically when non-electrical energy products are targeted.

The IAEA provides a forum for the exchange of information by experts and policy makers from industrialized and developing countries on the technical, economic, environmental, and social aspects of SMR development and implementation. It makes this information available to all interested Member States by producing status reports and other publications focusing on advances in SMR design and technology development.

The objective of this report is to assist developers of SMRs in Member States in defining consistent defence in depth approaches regarding the elimination of accident initiators/prevention of accident consequences through design and incorporation of inherent and passive safety features and passive systems into safety design concepts of such reactors. Another objective is to assist potential users in Member States in their evaluation of the overall technical potential of SMRs with inherent and passive safety design features, including possible implications in areas other than safety.

This report is intended for different categories of stakeholders, including designers and potential users of innovative SMRs, as well as officers in ministries or atomic energy commissions in Member States responsible for implementing nuclear power development programmes or evaluating nuclear power deployment options in the near, medium, and longer term.

The main sections of this report present state of the art advances in defence in depth approaches based on the incorporation of inherent and passive safety features into the design concepts of pressurized water reactors, pressurized light water cooled heavy water moderated reactors, high temperature gas cooled reactors, liquid metal cooled fast reactors, and non-conventional designs within the SMR range. They also highlight benefits and negative impacts in areas other than safety arising from the incorporation of such features.

The annexes provide descriptions of the design features of 11 representative SMR concepts used to achieve defence in depth and patterned along a common format reflecting the definitions and recommendations of the IAEA safety standards. The annexes were prepared by designers of the corresponding SMRs.

The IAEA officer responsible for this publication was V. Kuznetsov of the Division of Nuclear Power.

EDITORIAL NOTE

This report has been edited by the editorial staff of the IAEA to the extent necessary for the reader's assistance.

This report does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.

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.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

1.1.1. Rationale and developments in Member States

According to classifications adopted by the IAEA, small reactors are reactors with an equivalent electric output of less than 300 MW; medium sized reactors are reactors with an equivalent electric power of between 300 and 700 MW [1].

Small and medium sized reactors (SMRs) are not intended to benefit from economics of scale. In most cases, deployment potential of SMRs is supported by their ability to fill niches in which they address markets or market situations different from those of currently operated large-capacity nuclear power plants, e.g., situations demanding better distributed electrical supplies or a better match between capacity increments and investment capability or demand growth, or more flexible siting and greater product variety [2, 3].

It is important to note that the term small or medium sized reactor does not necessarily mean small or medium sized nuclear power plant. Like any nuclear power plants, those with SMRs can be built many at a site, or as twin units. In addition to this, innovative SMR concepts provide for power plant configurations with two, four, or more reactor modules. Units or modules can be added incrementally over time, reaping the benefits of experience, timing, and construction schedules (see Fig. 1), and creating an attractive investment profile with minimum capital at risk.

Sometimes it is perceived that SMRs are meant to address users in countries which currently either do not have a nuclear infrastructure, or which have it on a small scale, and which are contemplating either introduction or significant expansion of nuclear power for the first time. However, this is not the case – most innovative SMR designs are intended to fulfil a broad variety of applications in developed and developing countries alike, irregardless of whether they have already embarked on a nuclear power programme or are only planning to do so [1–3].

Finally, it should be emphasized that SMRs are not the only prospective nuclear option; it must be recognized that a diverse portfolio of reactors of different capacities and applications are required if nuclear power is to make a meaningful contribution to global sustainable development. The anticipated role of SMRs

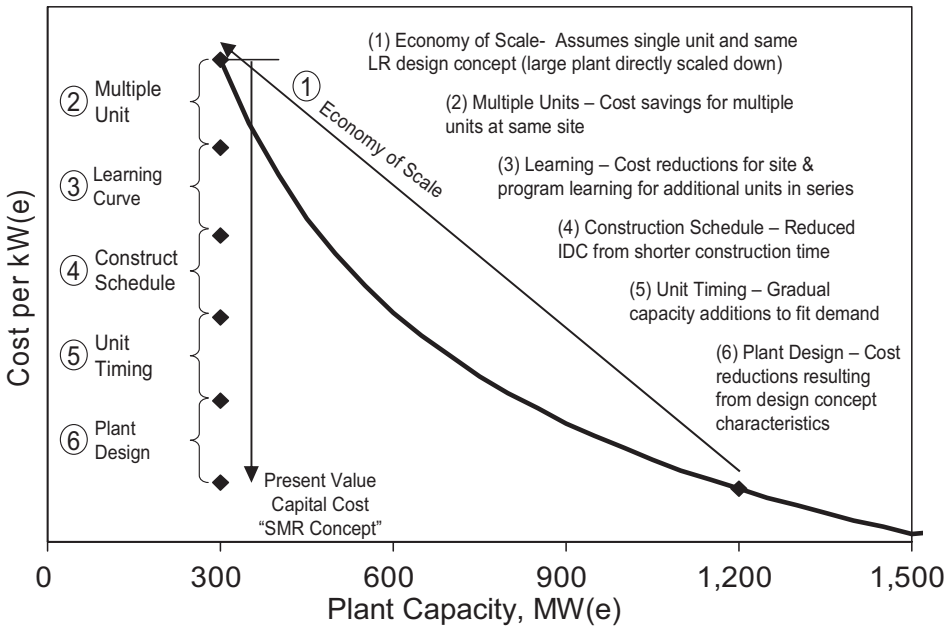


FIG. 1. A generic scheme illustrating potential SMR economic factor advantages (Westinghouse, USA).

within the global nuclear energy system could be to increase the availability of clean energy in usable form in all regions of the world, to broaden access to clean, affordable and diverse energy products and, in this way, to contribute to the eradication of poverty and support of a peaceful and stable world.

In 2008, more than 45 innovative[1] SMR concepts and designs were developed within national or international research and development (R&D) programmes involving Argentina, Brazil, China, Croatia, France, India, Indonesia, Italy, Japan, the Republic of Korea, Lithuania, Morocco, the Russian Federation, South Africa, Turkey, the USA, and Vietnam [2, 3].

Innovative SMRs are being developed for all principal reactor lines and some non-conventional combinations thereof. The target dates of readiness for deployment range from 2010 to 2030.

Strong reliance on inherent and passive safety design features has become a trademark of many advanced reactor designs, including several evolutionary designs [4] and nearly all innovative SMR designs [2, 3]. Reactors with smaller unit output require adequate defence in depth to benefit from more units being clustered on a site or to allow more proximity to the user, specifically when non-electrical energy products are targeted and the user is a process heat application facility such as a chemical plant.

This report is intended to present state of the art design approaches with the aim to achieve defence in depth in SMRs. Preparation of this report is supported by IAEA General Conference resolution GC(51)/14/B2(k) of September 2007.

1.1.2. Previous IAEA publications

Direct predecessors of this report are: IAEA-TECDOC-1485, entitled Status of Innovative Small and Medium Sized Reactor Designs 2005*:* Reactors with Conventional Refuelling Schemes [2], published in March 2006, and IAEA-TECDOC-1536, Status of Innovative Small Reactor Designs Without On-Site Refuelling [3], published in January 2007. These reports presented the design and technology development status and design descriptions for concepts of innovative SMRs developed worldwide. Design descriptions of SMRs in these reports incorporated descriptions of safety concepts prepared according to a common outline. However, these descriptions were rather limited in detail because of limited space in the reports, which were also dedicated to the presentation of other aspects of innovative SMRs, including descriptions of design, economics, proliferation resistance and security, fuel cycle options, and innovative infrastructure provisions. More importantly, descriptions of SMR safety design concepts in these reports were not always structured according IAEA safety standard recommendations, specifically regarding defence in depth strategies

Another predecessor of this report is IAEA-TECDOC-1487, Advanced Nuclear Plant Design Options to Cope with External Events [5, 6], published in February 2006, which provided structured descriptions and explanations of the design features of 14 advanced nuclear power plants incorporating protection against the impacts of natural and human induced external events. The designs considered in that report included several SMRs.

The present report, therefore, provides an in-depth description of safety design features used to achieve defence in depth in 11 innovative SMR concepts selected to represent all major reactor lines with near to medium and longer term deployment potential. These descriptions are structured to follow the definitions and recommendations of IAEA safety standard NS-R-1, Safety of the Nuclear Power Plants: Design Requirements [7] and include some references to other IAEA safety guides and documents, including NS-G-3.3, Evaluation of Seismic Hazard for Nuclear Power Plants [8], and NS-G-1.5, External Events Excluding Earthquakes in the Design of Nuclear Power Plants [9], as well as recommendations by the International Nuclear Safety Advisory Group [10 11], and non-consensus definitions suggested in IAEA publications [5, 12]. The basic definitions recommended or suggested in the above mentioned IAEA publications are reproduced in Appendix 2 of this report.

In September 2007, the IAEA published IAEA-TECDOC-1570, Proposal for a Technology-Neutral Safety Approach for New Reactor Designs [13]. Based on a critical review of IAEA safety standard NS-R-1,

[1] IAEA-TECDOC-936 [5] defines an innovative design as a design "that incorporates radical conceptual changes in design approaches or system configuration in comparison with existing practice" and would, therefore, "require substantial R&D, feasibility tests and a prototype or demonstration plant to be implemented".

Safety of the Nuclear Power Plants: Design Requirements [7], IAEA-TECDOC-1570 outlines a methodology/ process to develop a new framework for the safety approach based on quantitative safety goals (a probability-consequences curve correlated with each level of defence in depth), fundamental safety functions, and generalized defence in depth, which includes probabilistic considerations. Further elaboration of IAEA safety standards suggested in reference [13] could facilitate expansion of design development and safety qualifications of several medium and longer term SMRs addressed in the present report, thus recommendations in this publication are referenced in Section 3, which highlights design features of selected SMRs. Limited information provided by Member States for this report made it impossible to consider in full the recommendations of IAEA safety standards and guides. Where possible, references to other recently published IAEA reports are included, when such recommendations may be considered in more detail; see Ref. [6].

1.2. OBJECTIVE

This report is intended for different categories of stakeholders, including designers and potential users of innovative SMRs, as well as officers in ministries of atomic energy commissions in Member States responsible for implementing nuclear power development programmes or evaluating nuclear power deployment options in the near, medium, and longer term.

The overall objectives of this report are:

(1) To assist developers of innovative SMRs in defining consistent defence in depth approaches regarding the elimination of accident initiators/ prevention of accident consequences through design and the incorporation of inherent and passive safety features and passive systems in safety design concepts of such reactors;
(2) To assist potential users of innovative SMRs in their evaluation of the overall technical potential of SMRs with inherent and passive safety design features, including their possible implications in areas other than safety.

The specific objectives of this report are:

— To present the state of the art in design approaches used to achieve defence in depth in pressurized water reactors, pressurized light water cooled heavy water moderated reactors, high temperature gas cooled reactors, sodium cooled and lead cooled fast reactors, and non-conventional designs within the SMR range;
— To highlight benefits and negative impacts in areas other than safety arising from the implementation of inherent and passive safety design features;
— To identify issues of performance reliability assessment for passive safety systems in advanced reactors, and to highlight further research and development needs arising therefrom.

Designers of SMRs not considered in the present report (currently a minimum of 45 innovative SMR concepts and designs are being analysed or developed worldwide [2, 3]) could benefit from the information published here, which is structured to follow the definitions and recommendations established in IAEA safety standards or suggested in other IAEA publications. It should be noted that IAEA safety standards are used as the base for national nuclear regulations in many developing countries, and that this trend will likely continue into the future.

The information presented in this report could be used in assessment studies for innovative nuclear energy systems (INSs) involving SMRs, as conducted by the IAEA's International Project on Innovative Reactors and Nuclear Fuel Cycles (INPRO) [14].

Part of this report is elaborated upon through participation of research teams in Member States involved in the development of methodologies for reliability assessments of passive safety systems in advanced reactors. This part (see Appendix I) provides justification for the coordinated research project on Development of Methodologies for the Assessment of Passive Safety System Performance in Advanced Reactors, which is being implemented by the IAEA in its programme during the 2008-2009 budget cycle.

1.3. SCOPE

This report addresses 11 representative SMR concepts/designs originating from seven IAEA Member States, including Argentina, France, India, Italy, Japan, the Russian Federation, and the USA. The concepts have been selected to include:

— As many concepts as possible for which noticeable progress toward advanced design stages or deployment is observed;
— Concepts representing different reactor lines;
— Those concepts that could be deployed in the near term.

Presentation of certain SMR concepts in this report was also conditioned by the agreement of their developers to cooperate. In some cases, the designers considered the subject of this report too sensitive and withdrew from the cooperation.

1.4. STATUS OF CONSIDERED SMR DESIGNS AND CONCEPTS

The SMR concepts included represent pressurized water reactors (5 inputs), pressurized light water cooled heavy water moderated reactors (1 input); high temperature gas cooled reactors (HTGRs, 1 input); liquid metal cooled fast reactors (1 input for sodium and 1 input for lead cooled reactors), and a single non-conventional design, which is a lead-bismuth cooled very high temperature reactor with pin-in-block HTGR type fuel.

Of the pressurized water reactors included, the KLT-40S (Annex I) has entered the deployment stage — construction began in 2007 in the Russian Federation of a pilot floating cogeneration plant of 400 MW(th)/ 70 MW(e) with two KLT-40S reactors. Actual deployment is scheduled for 2010.

Two reactors with integrated design of the primary circuit are in advanced design stages, and their commercialization could start around 2015. These are the 335 MW(e) IRIS design (Annex II) developed by the international consortium led by Westinghouse, USA; and the prototype 27 MW(e) CAREM (Annex III) developed in Argentina, for which construction is scheduled to be complete in 2011.

Two other PWR type designs, the SCOR (France) and the MARS (Italy) have the potential to be developed and deployed in the short term but show no substantial progress toward deployment. The SCOR, with 630 MW(e) (Annex IV), is in the conceptual design stage, and is of interest as it represents a larger capacity integral-design PWR. The modular MARS, with 150 MW(e) per module (Annex V), is at the basic design stage, and is of interest as it represents an alternative solution to other pressurized water SMRs, the solution based on the primary pressure boundary being enveloped by a protective shell with slowly moving low enthalpy water.

Advanced pressurized light water cooled heavy water moderated reactors are represented by one design – the AHWR, with 300 MW(e) (Annex VI). The AHWR (India) is at the detailed design stage with the start-up of construction related actions expected before 2010.

The GT-MHR, with 287.5 MW(e), a collaborative US–Russian concept of an HTGR with pin-in-block type fuel, is at the basic design stage (Annex VII). Its progress toward deployment may be not so advanced as that of some other HTGRs (e.g., the PBMR of South Africa or the HTR-PM of China [2]), however, as passive safety design features of all HTGRs have much in common, the GT-MHR is quite representative of the passive safety design options implemented in other HTGRs.

Sodium and lead cooled fast SMRs are represented by the 4S-LMR concept of a sodium cooled small reactor without on-site refuelling developed by the Central Research Institute of Electric Power Industry (CRIEPI) and Toshiba in Japan (Annex VIII) and by the SSTAR and STAR-LM concepts of small lead cooled reactors without on-site refuelling developed by the Argonne National Laboratory in the USA (both described in Annex IX). Of the two designs, the 4S-LMR with 50 MW(e) and a 10-year core lifetime is at a more advanced stage because the conceptual design and major parts of the system design have already been completed for a similar design differing essentially in the type of fuel and named the 4S. A pre-application review by the US NRC started in the fall of 2007. Construction of a demonstration reactor and safety tests are planned for early 2010 [3]. Different from this reactor type, both the SSTAR with 19.7 MW(e) and a 30-year core lifetime and the STAR-LM with 181 MW(e) and a 15-year core lifetime are at the pre-conceptual stage [3]. In 2008, due to

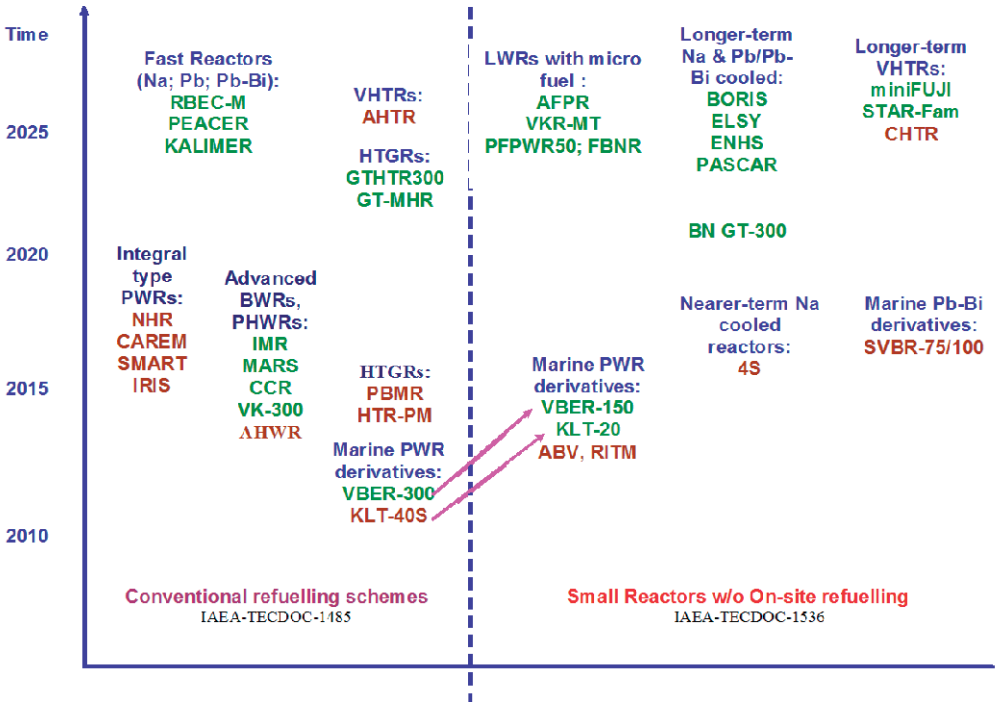


FIG. 2. Deployment potential map of innovative SMRs [2,3].

reduced funding, activities in the USA refocused on a lead cooled fast reactor (LFR) Technology Pilot Plant (a demonstration plant) under a GNEP programme.

Finally, non-conventional designs are represented by the CHTR with 100 kW(th) and a 15-year core lifetime (Annex X). The CHTR (India) is a small reactor without on-site refuelling designed to be a semi-autonomous 'power pack' for operation in remote areas and, specifically, for advanced non-electrical applications, such as hydrogen production. The CHTR is a non-conventional reactor merging the technologies of high temperature gas cooled reactors and lead-bismuth cooled reactors. The core uses ^{233}U-Th based pin-in-block fuel of the HTGR type with BeO moderator blocks, while the coolant is lead-bismuth. When this report was prepared, an extensive research and development programme including both analytical studies and testing was in progress for the CHTR at the Bhabha Atomic Research Centre (BARC) in India [3].

Detailed design descriptions of the abovementioned and other SMRs, as well as some results of safety analyses performed for these reactors are provided in Refs [2, 3]. Figure 2 illustrates deployment potential of innovative SMRs. Brown indicates concepts with noticeable progress towards advanced design stages and deployment.

1.5. STRUCTURE

The report includes an introduction, 6 Sections, 4 appendices and 10 annexes.

The introduction (Section 1) describes the background and identifies the objectives, the scope and the structure of this report, as well as the approach used in its preparation and the design status of the SMRs considered.

Section 2 provides an overview of the considerations for the incorporation of inherent and passive safety features into safety design concepts of SMRs. These considerations, presented in a generic way and for each reactor line separately, were elaborated at the IAEA technical meetings in June 2005 and in October 2006.

Section 3 presents the design approaches applied by the designers to achieve defence in depth in SMRs. Both passive and active safety design features and systems are included to highlight the role of inherent and passive features and show how they may affect the design/function of the active safety systems. This section is based on the information and data provided by the designers of SMRs in Member States and presented, in a

structured form, in Annexes I–X in this report. The common format used to describe passive and active safety design features of SMRs is given in Appendix IV.

Section 3 is structured as follows. First, a common general approach is described. Then a description is provided for each reactor line addressed in the present report, including pressurized water reactors, pressurized light water cooled heavy water moderated reactors, high temperature gas cooled reactors, liquid metal cooled fast reactors, and non-conventional designs. For each reactor line, a short summary of the design features of one or more of the corresponding SMRs presented in the annexes is included, followed by summary tables and discussions of the safety design features contributing to each level of defence in depth. In this, dedicated passive and active safety systems are discussed in more detail in conjunction with defence in depth level 3. After that, summary tables and discussions follow on design basis and beyond design basis events, on acceptance criteria, and on features for plant protection against external event impacts. Each section winds-up with a summary table and a discussion of the measures planned in response to severe accidents.

Section 4 provides a review of the benefits and negative impacts in areas other than safety that in view of the SMR designers arise from incorporation of the corresponding inherent and passive safety design features. The discussion is structured along the reviewed reactor lines, in the same way as in Section 3.

Section 5 summarizes the approaches and considerations applied in the selection of combinations of passive and active safety systems in the considered SMRs.

Section 7 is the conclusion. It is elaborated as an executive summary of the report.

Appendix 1 addresses the issue of performance assessment of passive safety systems by providing a summary of background and experience, a short description of the two methodologies for reliability assessment of passive safety systems, and a recommendation for further research and development based on the outputs of a dedicated IAEA technical meeting on June 2006. This appendix is referenced from Section 5.

Appendix 2 includes a paper on periodic confirmation of passive safety feature effectiveness, contributed by D.C. Wade of the Argonne National Laboratory (ANL), USA. This paper is referenced from Appendix 1.

Appendix 3 includes consensus and non-consensus definitions from the IAEA safety standards and other publications relevant to the subject of this report, and also highlights some non-conventional terms used by Member States.

Appendix 4 gives a common format for description of the design features of SMRs as used in Annexes I–X.

Annexes I–X provide descriptions of the design features of the considered SMRs used to achieve defence in depth. The descriptions were contributed by Member States and are done according to the common outline in Appendix 3. The order of the inputs corresponds to that used in Sections 3 and 4, with pressurized water SMRs going first (Annexes I–V), followed by a pressurized light water cooled heavy water moderated reactor (Annex VI), a high temperature gas cooled reactor (Annex VII), the liquid metal cooled fast-spectrum SMRs (Annexes VIII, IX), and the non-conventional design (Annex X).

Contributors to drafting and review of this report are listed on the last page.

1.6. APPROACH

All structured descriptions of SMR design features used to achieve defence in depth were prepared and reviewed first hand by the designers of SMRs in Member States, in communication with international experts and the IAEA Secretariat.

Appendix 1 of this report was elaborated upon through participation of research teams involved in development of methodologies for the reliability assessment of passive safety systems in advanced reactors.

The introductory and cross-cutting sections were developed by international experts and the Secretariat, and reviewed by SMR designers in Member States. The conclusions were elaborated through the effort of the two IAEA technical meetings convened in June 2005 and October 2006.

2. CONSIDERATIONS FOR THE INCORPORATION OF INHERENT AND PASSIVE SAFETY DESIGN FEATURES INTO SMRs

2.1. GENERAL CONSIDERATIONS

General considerations for the incorporation of inherent and passive safety design features into SMRs are not different from those of advanced reactors of any capacity and type. Clearly, the implementation of inherent and passive safety design features can facilitate improved defence in depth. It can also positively affect plant economy through:

- Reduced design complexity and reduced necessity for human intervention resulting in fewer potentially unsafe actions;
- Reduced investment requirements, due to a reduction in qualifications as well as operation and maintenance and, depending on specific design and regulations, reduced off-site emergency planning;
- Increased operability and capacity factors.

It is also noted that the use of inherent and passive safety features can facilitate advantages in areas other than economy, for example:

- Reduced adverse environmental impacts, for example through a reduced number of systems requiring maintenance and associated waste;
- Reduced vulnerability to sabotage through semi-autonomous operation, better reactor self-control in accidents, and 'passive shutdown'[2] capabilities;
- Deployment in developing countries through simplified infrastructure requirements matching human resource limitations in such countries.

In the view of SMR designers, smaller capacity reactors have the following generic features, potentially contributing to a particular effectiveness in the implementation of inherent and passive safety features:

- Larger surface-to-volume ratio, facilitating easier decay heat removal, specifically, with a single phase coolant;
- An option to achieve compact primary coolant system design, e.g. the integral pool type primary coolant system, which could contribute to the effective suppression of certain initiating events;
- Reduced core power density, facilitating easy use of many passive features and systems, not limited to natural convection based systems;
- Lower potential hazard that generically results from lower source term owing to lower fuel inventory, less non-nuclear energy stored in the reactor, and a lower decay heat generation rate.

Section 2.2. below summarizes considerations of SMR designers regarding inherent and passive safety features that could be easier to achieve in a reactor of smaller capacity for each reactor line considered in this report.

[2] Throughout this report, 'passive shutdown' denotes bringing the reactor to a safe, low-power state with balanced heat production and passive heat removal, with no failure to barriers preventing radioactivity releases to the environment; all relying on inherent and passive safety features only, with no operator intervention, no active safety systems involved, and no requirement for external power and water supplies, as well as with the grace period infinite for practical purpose.

2.2. REACTOR LINE SPECIFIC CONSIDERATIONS

2.2.1. Pressurized water reactors

The designers of pressurized water SMRs cumulatively mention the following inherent and passive safety design features as facilitated by smaller reactor capacity and size:

- Integral design of the primary circuit with in-vessel location of steam generators and control rod drives, to eliminate large diameter piping, minimize reactor vessel penetrations, and prevent large-break loss of coolant accidents (LOCA) and reactivity initiated accidents with control rod ejection, as well as to limit the scope of small and medium-break LOCA;
- Compact modular loop-type designs with reduced piping length, an integral reactor cooling system accommodating all main and auxiliary systems within a leaktight pressure boundary, and leak restriction devices, all to prevent LOCA or limit their scope and hazard;
- A primary pressure boundary enclosed in an enveloping shell with low enthalpy slow moving water, intended to prevent LOCA or limit their scope and hazard;
- Increased thermal inertia at a reasonable reactor vessel size, contributing to long response time in transients and accidents;
- Enhanced levels of natural convection, sufficient to passively remove decay heat from a shutdown reactor over an indefinite time;
- In-vessel retention of core melt through, for example, passive external cooling of the reactor pressure vessel;
- Compact design of the primary circuit and the containment, to facilitate protection against missiles and aircraft crash.

2.2.2. Pressurized light water cooled heavy water moderated reactors

For the boiling light water cooled heavy water moderated reactor considered in the present report (the AHWR, incorporating pressure channels and calandria; see Annex VI), smaller capacity — in view of the designers — facilitates:

- The use of natural convection for heat removal in normal operation, eliminating, for example, main circulation pumps;
- Achievement of a slightly negative void coefficient of reactivity;
- Provision of a relatively large coolant inventory in the main coolant system to ensure its high thermal inertia and slow pace of transients;
- Provision of a relatively large inventory of water in a reasonably sized gravity driven water pool (GDWP), located inside the containment and intended for passive emergency injection of cooling water, passive containment cooling, and passive decay heat removal via the isolation condensers.

2.2.3. High temperature gas cooled reactors

For high temperature gas cooled reactors (HTGRs) with pebble bed or pin-in-block tristructural-isotropic (TRISO) fuel and helium coolant, smaller reactor capacity facilitates:

- Long term passive decay heat removal from the core to the outside of the reactor vessel based on natural processes of conduction, radiation and convection, with natural convection based heat removal from the outside of the reactor vessel to an ultimate heat sink;
- Achievement of a large temperature margin between the operation limit and the safe operation limit, owing to inherent fission product confinement properties of TRISO fuel at high temperatures and fuel burnups;
- De-rating of accident scenarios rated as potentially severe in reactors of other types, including loss of coolant (LOCA), loss of flow (LOFA), and reactivity initiated accidents; for example, helium release from

the core in the GT-MHR can be a safety action and not the initiating event for a potentially severe accident;
— Achievement of increased reactor self-control in anticipated transients without scram, without exceeding safe operation limits for fuel;
— Relatively high heat capacity of the reactor core and reactor internals and low core power density, resulting in slow progression of the transients.

It should be noted that, in view of currently known reactor vessel materials, an HTGR unit capacity below ~600 MW(th) is a necessary condition to ensure long-term passive decay heat removal from the core as described in the first item of this listing. Therefore, all currently known concepts of HTGR with TRISO based fuel and gas coolant belong to the SMR range [2].

2.2.4. Sodium cooled and lead cooled fast reactors

For both sodium cooled and lead cooled fast reactors, smaller unit capacity could facilitate:

— Effective use of auxiliary passive decay heat removal systems with environmental air in natural draught acting as an ultimate heat sink;
— Achievement of a relatively high heat capacity of the primary (or primary and adjacent intermediate) coolant system at its reasonable size, resulting in a slower progression of transients.

Specifically for sodium cooled fast reactors, smaller reactor capacity could facilitate achieving a negative whole core void coefficient of reactivity to prevent the progression of design basis accidents into severe incidents, otherwise possible at a start of sodium boiling.

Specifically for lead cooled fast reactors, smaller reactor capacity could facilitate simplified seismic protection and improved seismic response [2].

2.2.5. Non-conventional designs

The only non-conventional reactor concept considered in this report, the Compact High Temperature Reactor (CHTR) of BARC (India), is based on a synthesis of the technology of ^{233}U-Th HTGR type pin-in-block fuel and that of a lead-bismuth coolant; see Annex X. The CHTR is a very high temperature reactor concept. Smaller reactor capacity facilitates:

— Passive heat removal from the core in normal operation, with no main circulation pumps being employed; as well as passive and passively actuated heat removal from the core during and after accidents, including those based on the use of heat pipe systems;
— Relatively high heat capacity of the ceramic core, resulting in slow temperature transients, at a reasonable reactor size;
— Prevention of the consequences of transient overpower events;
— Passive power regulation and increased reactor self-control in transients without scram.

3. DESIGN APPROACHES TO ACHIEVE DEFENCE IN DEPTH IN SMRs

3.1. GENERAL APPROACH

In SMR designs, as in larger reactor designs, the defence in depth strategy is used to protect the public and environment from accidental releases of radiation. Nearly all SMR designs seek to strengthen the first and subsequent levels of defence by incorporating inherent and passive safety features. Certain common characteristics of smaller reactors lend themselves to inherent and passive safety features, such as relatively smaller core sizes enabling integral coolant system layouts and larger reactor surface-to-volume ratios or lower core power densities which facilitate passive decay heat removal. Using the benefits of such features, the main goal is to eliminate or prevent, through design, as many accident initiators and accident consequences as possible. Remaining plausible accident initiators and consequences are then addressed by appropriate combinations of active and passive safety systems. The intended outcome is greater plant simplicity with high safety levels that, in turn, may allow reduced emergency requirements off-site.

It should be noted that an approach to maximize the use of inherent safety features in order to minimize the number of accident initiators in a reactor concept, and then to deal with the remaining accidents using reasonable combinations of active and passive safety systems is being pursued by the Generation IV International Forum, in line with Generation IV Technology Goals [15]. To a limited extent, such an approach is also realized in several near term designs of large capacity water cooled reactors, such as the AP1000, the ESBWR, and the VVER1000, the goal being to achieve a high level of safety in a cost effective way [4].

3.2. APPROACHES FOR SPECIFIC REACTOR LINES

For each of the reactor lines considered (pressurized water reactors, pressurized light water cooled heavy water moderated reactors, high temperature gas cooled reactors, sodium cooled and lead cooled fast reactors, and non-conventional designs), the design features contributing to different levels of defence in depth are summarized and structured as described below.

The first five tables for each reactor line give a summary of design features contributing to Level 1 through Level 5 of defence in depth with a short explanation of the nature of these contributions, in line with the definitions given in [7]. Passive and active safety systems are highlighted in more detail in conjunction with Level 3 defence in depth.

It should be noted that original safety design concepts of the considered SMRs do not always follow the defence in depth concept recommended in by IAEA safety standards [7]. Although all designers were requested to follow the recommendations of [7] when providing descriptions of SMR safety design features enclosed as Annexes I–X, the results are non-uniform. For example, some Level 4 features were in several cases attributed to Level 5 for PWRs, etc. To provide a uniform basis for descriptions, the attribution of safety design features to certain levels of defence in depth was harmonized for all SMRs considered, following the recommendations of [7], and in this way presented in all tables of this section. Therefore, attribution indicated in the tables below may be in some cases different from that originally provided by designers in the corresponding annexes.

The sixth table for each reactor line summarizes the degree of detail in the definition of design basis and beyond design basis events, as observed in the corresponding annexes, and highlights the events specific to a particular SMR, but not to the corresponding reactor line.

The seventh table gives a summary of deterministic and probabilistic acceptance criteria for design basis and beyond design basis events as applied by the designers, and specifically highlights cases when a risk-informed approach is being used or targeted.

The eighth table for each reactor line summarizes design features for plant protection against external event impacts, with a focus on aircraft crashes and earthquakes, and refers to recent IAEA publications of relevance [6], when applicable.

Finally, the ninth table gives a summary of measures planned in response to severe accidents.

The final paragraph in each of the following subsections provides a summary of safety design approaches pursued by designers of SMRs, using the above mentioned tables as references, with a link to IAEA safety standards [7] and other publications of relevance.

3.2.1. Pressurized water reactors

Pressurized water small and medium sized reactors are represented by three concepts using integral layout of the primary circuit with in-vessel location of steam generators and control rod drives; one compact modular loop-type design features reduced length piping, an integral reactor cooling system accommodating all main and auxiliary systems within a leaktight pressure boundary, and leak restriction devices, and one design, originating from the mid 1980s, has the primary pressure boundary enclosed in an enveloping shell with low enthalpy, slow moving water.

The concepts with integral primary circuit layout include the CAREM-25 with 27 MW(e), a prototype for a series of larger capacity SMRs being developed by the CNEA (Argentina), the IRIS with 335 MW(e), being developed by the international consortium led by Westinghouse (USA), and the SCOR concept with 630 MW(e), being developed by CEA (France). The CAREM-25 and the IRIS have reached detailed design stages with deployments targeted for 2011 and 2015 respectively, while the SCOR is just a conceptual design. Detailed design descriptions of the CAREM-25, IRIS, and SCOR are presented in [2], and corresponding structured descriptions of their passive safety design features are given in Annexes II, III, and IV. Figure 3 provides an illustration of the primary coolant system layout for the indicated designs.

Compact modular loop-type concepts are represented by the KLT-40S, a 35 MW(e)/150 MW(th) reactor for a twin-unit floating heat and power plant, the construction of which started in the Russian Federation in April 2007. The power circuits of the two units are separate, with each producing more heat power than required to generate the rated electrical output; the remaining heat power is to be used for district heating (as provided for in 'Lomonosov', a first of a kind floating nuclear power plant under construction in Russia) or for seawater desalination (it is foreseen future units will be deployed outside of the Russian Federation). A detailed description of the KLT-40S design, developed by OKBM and several other Russian organizations, is provided in [4]; a structured design description of passive safety design features is given in Annex I. IAEA publications [2, 3] provide descriptions of several other floating reactors as well as land-based NPPs, employing a design concept similar to that of the KLT-40S. Layout of the KLT-40S reactor is shown in Fig. 4.

The MARS reactor with 150 MW(e) per module, in which the primary pressure boundary is enclosed in a pressurized low enthalpy containment, was developed by a consortia of academic, research and industrial organizations in Italy. The detailed design stage was reached, and several testing programmes were completed. A design description of the MARS is presented in [2]; passive safety design features of the MARS are described in Annex V. Layout of the MARS primary coolant system is shown in Fig. 5.

Design features of pressurized water SMRs contributing to enhancement of Level 1 of defence in depth are summarized in Table 1; subsequent levels are summarized in Tables 2, 3, 4 and 5, respectively.

At Level 1 of defence in depth, "Prevention of abnormal operation and failure", the dominant tendency is to exclude loss of coolant accidents (LOCA) or limit their scope and hazard by applying certain features in reactor design, such as:

- In-vessel location of steam generators in PWRs with integral design of the primary circuit (CAREM-25, IRIS, SCOR), eliminating large diameter piping and, hence, large-break LOCA;
- In-vessel location of the control rod drive mechanism (CAREM-25, IRIS, SCOR), which reduces the number and diameter of necessary in-vessel penetrations;
- Compact modular design of the reactor unit, eliminating long pipelines in the reactor coolant system, leak restriction devices in the primary pipelines, and a so-called 'leaktight' reactor coolant system with packless canned pumps, welded joints, and leaktight bellows sealed valves (KLT-40S, based on submarine and icebreaker reactor experiences); internal, fully immersed pumps are also applied in the IRIS and the SCOR reactors with integral design of the primary circuit;
- Primary pressure boundary enclosed in a pressurized, low enthalpy containment (a shell) with only a single, small diameter pipeline between the primary coolant pressure boundary and the auxiliary systems (MARS).

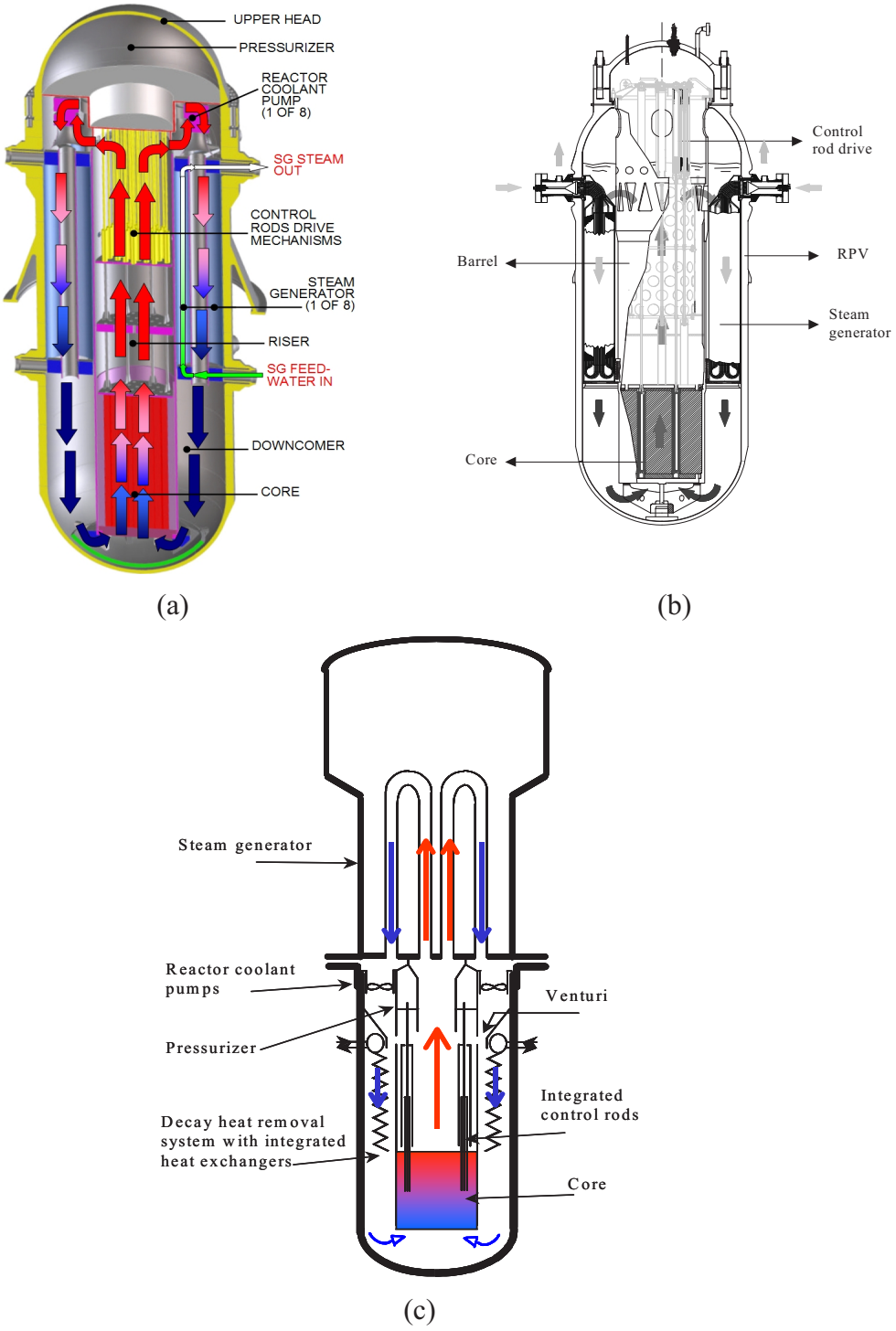


FIG. 3. Schematics of the primary coolant system for (a) IRIS; (b) CAREM-25; and (c) SCOR.

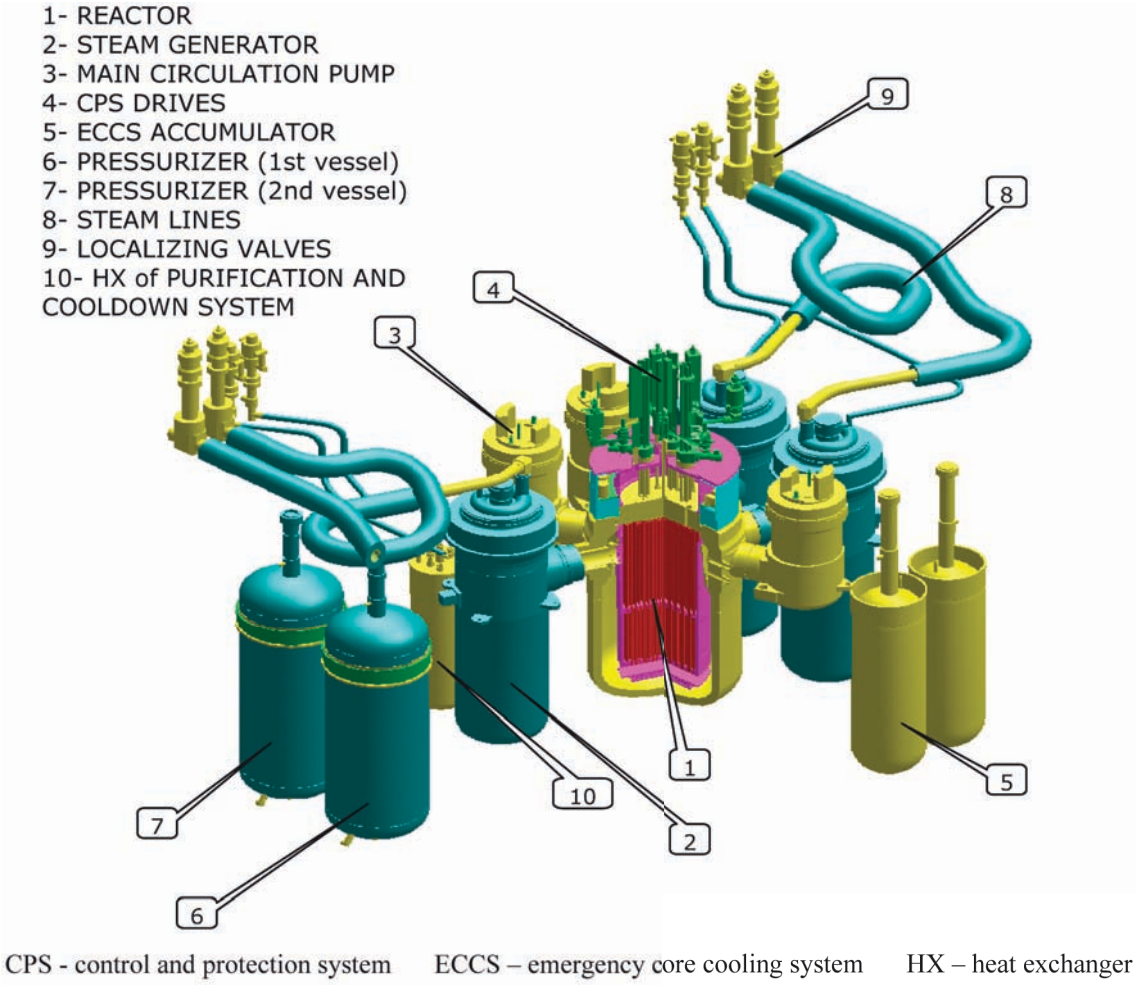


FIG. 4. Layout of the KLT-40S reactor.

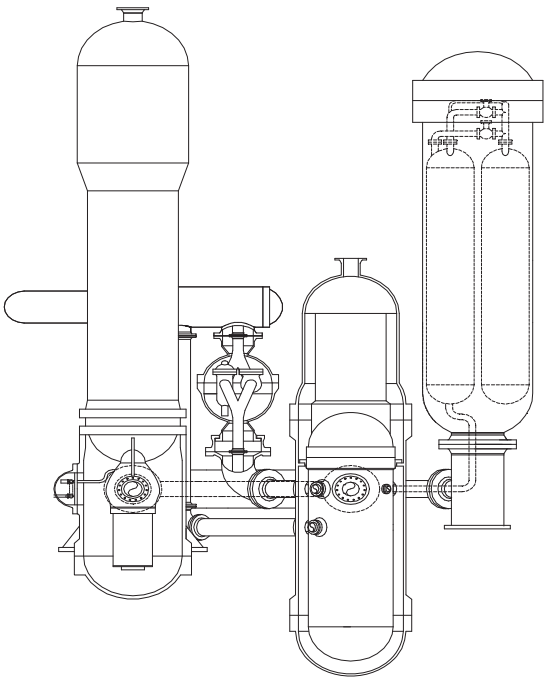


FIG. 5. Layout of the MARS reactor with pressurized containment for primary loop protection.

TABLE 1. DESIGN FEATURES OF PRESSURIZED WATER SMR CONCEPTS CONTRIBUTING TO LEVEL 1 OF DEFENCE IN DEPTH

#	Design features	What is targeted	SMR designs
1	Elimination of liquid boron reactivity control system	Exclusion of inadvertent reactivity insertion as a result of boron dilution	KLT-40S, CAREM-25, SCOR
2	Relatively low core power density	Larger thermal-hydraulic margins	MARS, IRIS, CAREM-25, SCOR
3	Integral design of primary circuit with in-vessel location of steam generators and (hydraulic) control rod drive mechanisms	Exclusion of large-break loss of coolant accidents (LOCA), exclusion of inadvertent control rod ejection, larger coolant inventory and thermal inertia	CAREM-25, IRIS, SCOR
4	Compact modular design of the reactor unit, eliminating long pipelines in the reactor coolant system	Decreased probability of LOCA	KLT-40S
5	Primary pressure boundary enclosed in a pressurized, low enthalpy containment	Elimination of LOCA resulting from failure of the primary coolant pressure boundary, elimination of control rod ejection accidents	MARS
6	Leaktight reactor coolant system (welded joints, packless canned pumps, and leaktight bellows, sealed valves, etc.)	Decreased probability of LOCA	KLT-40S
7	Internal, fully immersed pumps	Elimination of pump seizure, rotor lock, and seal LOCA	MARS, IRIS, SCOR
8	Leak restriction devices in the primary pipelines	Limitation of the break flow in case of a pipeline guillotine rupture	KLT-40S
9	A single, small diameter double connecting line between the primary coolant pressure boundary and auxiliary systems	Prevention of LOCA caused by rupture of the connecting line	MARS
10	Natural circulation based heat removal from the core in normal operation, eliminating main circulation pumps	Elimination of loss of flow accidents (LOFA)	CAREM-25
11	Steam generator with lower pressure inside the tubes in normal operation mode	Reduced probability of a steam tube rupture; prevention or downgrading of a steam line break or a feed line break	MARS, KLT-40S, IRIS
12	Steam generator designed for a full primary system pressure	Prevention or downgrading of a steam line break or a feed line break	IRIS, MARS

As already mentioned, all PWRs with integral design of the primary circuit incorporate in-vessel control rod drives, which is not only a design feature intended to minimize reactor vessel penetration but which is meant primarily to exclude reactivity initiated accidents with inadvertent control rod excursion (otherwise potentially facilitated by high primary pressure). Integral design of the primary circuit with in-vessel steam generators and control rod drives[3] apparently necessitates using a relatively low core power density, which in turn contributes to providing larger thermal-hydraulic margins.

[3] Some PWRs use primary circuit with internal steam generators but have external control rod drives, such as the Republic of Korea's SMART [2].

Elimination of liquid boron reactivity control, which facilitates prevention of inadvertent reactivity excursion as the result of boron dilution, can not be attributed to a certain class of reactor concepts; it is applied in the KLT-40S and the CAREM-25 but not in other concepts considered.

Finally, the use of natural convection for heat removal in normal operation, which eliminates loss of flow accidents owing to pump failure, is not a preferable feature of PWR type small and medium sized reactors; it is applied only in the small-powered CAREM-25 design (with 27 MW(e)).

Four of the considered reactors have applied design features to prevent steam generator tube rupture, see Table 1. The KLT-40S, the MARS and the IRIS use steam generators with lower pressure inside the tubes in normal operation mode. Also in the IRIS and the MARS, steam generators are designed for full primary system pressure.

All in all, PWRs with integral design of the primary circuit have a tangible and transparent approach to the elimination of several accident initiators caused by design. The question of whether this can only be applied to reactors within the small to medium power range is, however, open. For example, the French SCOR has up to 630 MW(e), credited to a steam generator of original design borrowing from the experience of marine propulsion reactors [2]. A recent paper on SCOR [16] points to the option to develop a PWR of integral design with as much as 1000 MW(e). In the latter case, however, the reactor vessel height would exceed 30 m (actually, two vertically adjusted half-vessels are used in SCOR). It should also be noted that the SCOR is at a conceptual design stage, while the IRIS and CAREM-25 have reached detailed design stages.

At Level 2 of defence in depth, "Control of abnormal operation and detection of failure", active systems of instrumentation and control and negative reactivity coefficients over the whole burnup cycle are common to all designs. These are features typical of all state of the art reactor designs, independent of their unit power range.

A relatively large coolant inventory in the primary circuit and high heat capacity of the nuclear installation as a whole, resulting from integral (IRIS, CAREM-25, SCOR) or compact modular (KLT-40S) design of the nuclear installation, are factors contributing to large thermal inertia and a slow pace of transients, altogether allowing more time for failure detection or corrective actions. Larger coolant inventory and higher heat capacity of the primary circuit are related to relatively large reactor vessels and internals or lower core power density as compared to a typical large PWR.

TABLE 2. DESIGN FEATURES OF PRESSURIZED WATER SMR CONCEPTS CONTRIBUTING TO LEVEL 2 OF DEFENCE IN DEPTH

#	Design feature	What is targeted	SMR designs
1	Active systems of instrumentation and control	Timely detection of abnormal operation and failures	All designs
2	Negative reactivity coefficients over the whole cycle	Prevention of transient over-criticality due to abnormal operation and failures	All designs
3	A relatively large coolant inventory in the primary circuit, resulting in large thermal inertia	Slow progression of transients due to abnormal operation and failures	CAREM-25, SCOR, IRIS, MARS
4	High heat capacity of nuclear installation as a whole	Slow progression of transients due to abnormal operation and failures	KLT-40S
5	Favourable conditions for implementation of the leak before break concept, through design of the primary circuit	Facilitate implementation of leak before break concept	KLT-40S
6	Little coolant flow in the low temperature pressurized water containment enclosing the primary pressure boundary	Facilitate implementation of leak before break concept	MARS
7	Redundant and diverse passive or active shutdown systems	Reactor shutdown	All designs

TABLE 3. DESIGN FEATURES OF PRESSURIZED WATER SMR CONCEPTS CONTRIBUTING TO LEVEL 3 OF DEFENCE IN DEPTH

#	Design feature	What is targeted	SMR designs
1	Negative reactivity coefficients over the whole cycle	Prevention of transient over-criticality and bringing the reactor to a sub-critical state in design basis accidents	All designs
2	Relatively low core power density	Larger thermal-hydraulic margins	MARS, IRIS, CAREM-25, SCOR
3	Relatively low primary coolant temperature	Larger thermal-hydraulic margins	MARS
4	A relatively large coolant inventory in the primary circuit (or primary circuit and the pressurized low enthalpy containment, enclosing the primary pressure boundary; or primary circuit and the reactor building), resulting in large thermal inertia	Slow progression of transients in design basis accidents	CAREM-25, SCOR, IRIS, MARS
5	High heat capacity of nuclear installation as a whole	Limitation of temperature increase in design basis accidents	KLT-40S
6	Restriction devices in pipelines of the primary circuit, with primary pipelines being connected to the hot part of the reactor	Limitation of scope and slower progression of LOCA	KLT-40S
7	Use of once-through steam generators	Limitation of heat rate removal in a steam line break accident	KLT-40S
8	Steam generator designed for full primary pressure	Limitation of the scope of a steam generator tube rupture accident	IRIS, MARS
9	A dedicated steam dump pool located in the containment building	Prevention of steam release to the atmosphere in case of a steam generator tube rupture	SCOR
10	Enclosure of the relief tank of a steam generator safety valve in a low temperature pressurized water containment enclosing the primary pressure boundary	Prevention of steam release to the atmosphere in the case of a steam generator tube rupture	MARS
11	'Soft' pressurizer system[a]	Damping pressure perturbations in design basis accidents	KLT-40S
12	Self-pressurization, large pressurizer volume, elimination of sprinklers, etc.	Damping pressure perturbations in design basis accidents	CAREM-25, IRIS, SCOR
13	Limitation of inadvertent control rod movement by an overrunning clutch and by the limiters	Limitation of the scope of reactivity insertion in an accident with control rod drive bar break	KLT-40S
14	Redundant and diverse reactor shutdown and heat removal systems	Increased reliability in carrying out safety functions	All designs
15	Insertion of control rods to the core, driven by gravity	Reactor shutdown	KLT-40S, CAREM-25
16	Insertion of control rods to the core, driven by force of springs	Reactor shutdown	KLT-40S
17	Non-safety-grade control rod system with internal control rod drives	Reactor shutdown	IRIS
18	One shutdown system based on gravity driven insertion of control rods to the core	Reactor shutdown	SCOR

TABLE 3. DESIGN FEATURES OF PRESSURIZED WATER SMR CONCEPTS CONTRIBUTING TO LEVEL 3 OF DEFENCE IN DEPTH (cont.)

#	Design feature	What is targeted	SMR designs
19	Safety-grade active mechanical control rod scram system	Reactor shutdown	MARS
20	Additional (optional) passive scram system actuated by a bimetallic core temperature sensor and operated by gravity	Reactor shutdown	MARS
21	Gravity driven high pressure borated water injection device (as a second shutdown system)	Reactor shutdown	CAREM-25
22	Injection of borated water from the emergency boron tank at high pressure (as an auxiliary shutdown measure)	Reactor shutdown	IRIS
23	Active safety injection system based on devices with a small flow rate	Reactor shutdown	SCOR
24	Emergency injection system (with borated water), actuated by rupture disks	Reactor shutdown plus prevention of core uncovery in LOCA	CAREM-25
25	Natural convection core cooling in all modes	Passive heat removal	CAREM-25
26	Natural convection level in the primary circuit with operating passive residual heat removal systems sufficient to remove decay heat under a station blackout	Passive heat removal	IRIS, SCOR
27	Level of natural circulation sufficient for adequate core cooling in a condition with all main circulation pumps switched off	Passive heat removal	KLT-40S
28	Passive emergency (or residual) core heat removal system with natural convection of coolant in all circuits, with water evaporation in water (e.g., storage) tanks	Passive decay heat removal	KLT-40S, IRIS, CAREM-25
29	Residual heat removal through the steam generator. The steam is discharged to the atmosphere, and the steam generator is fed by the startup shutdown system (SSS). This system is not safety grade.	Passive decay heat removal	SCOR
30	Redundant passive residual heat removal systems on the primary circuit with two diverse heat sinks; infinite autonomy achieved with the air-cooling tower heat sink	Passive decay heat removal	SCOR
31	Passive emergency core cooling system with infinite grace period, using natural draught of air as an ultimate heat sink; actuated upon flow rate decrease	Passive decay heat removal	MARS
32	Decay heat removal through a steam line of the steam generator, requiring no action to be initiated	Passive decay heat removal	SCOR
33	A small automatic depressurization system from the pressurizer steam space	Depressurization of the reactor vessel when in-vessel coolant inventory drops below a specified level	IRIS
34	Safety (relief) valves	Protection of reactor vessel from overpressurization	IRIS, CAREM-25

TABLE 3. DESIGN FEATURES OF PRESSURIZED WATER SMR CONCEPTS CONTRIBUTING TO LEVEL 3 OF DEFENCE IN DEPTH (cont.)

#	Design feature	What is targeted	SMR designs
35	Long term gravity make-up system	Assures that the core remains covered indefinitely following a LOCA	IRIS
36	Emergency injection system (with borated water), actuated by rupture disks	Prevention of core uncovery in LOCA	CAREM-25

[a] A 'soft' pressurizer system is characterized by small changes in primary pressure under a primary coolant temperature increase. This quality, due to a large volume of gas in the pressurizing system, results in a period of pressure increase up to the limit value under the total loss of heat removal from the primary circuit.

Compact modular design of a reactor unit, eliminating long pipelines in the reactor coolant system, with leak restriction devices in the primary pipelines and a so-called 'leaktight' reactor coolant system with packless canned pumps, welded joints, and leaktight bellows sealed valves, implemented in the KLT-40S, are mentioned as factors contributing to effective realization of the leak before break concept. In the MARS design, implementation of leak before break is facilitated by maintaining a small coolant flow in the low temperature pressurized water shell (containment) enclosing the primary pressure boundary.

Finally, redundant and diverse passive or active shutdown systems are provided in all designs in case abnormal operation runs out of control or the source of failure is not detected in a timely and adequate fashion.

As discussed above, certain design features provided at Level 1 of defence in depth in PWR type SMRs contribute to prevention or de-rating of certain design basis accidents, such as large break or medium break LOCA, core uncovery in LOCA, steam generator tube rupture, reactivity accidents with inadvertent ejection of a control rod or loss of flow, thus narrowing the scope of events to be dealt with at Level 3 of defence in depth, "Control of accidents within design basis". For the remaining events, a variety of design features are specified at Level 3. Altogether, these features fit into the following main groups:

(1) Inherent safety features provided by design and contributing to larger thermal margins, lower parameter variation, better reactor self-control, slower pace of transients, and damping of perturbations in design basis events. These features are highlighted in numbers 1–13 of Table 3;
(2) All designs incorporate at least two redundant and diverse shutdown systems; see numbers 14–24 of Table 3. These systems may be passive, such as those using mechanical control rods inserted into the core driven by gravity or by the force of springs, or active, such as those using standard mechanical control rods. Some passive systems are passively actuated, e.g., by system de-energization, by core temperature sensor, or other means. The role of safety injection systems with borated water is essentially reduced in some cases, e.g., in the IRIS and SCOR, or the function of a safety injection is coupled with core uncovery prevention, e.g., in the CAREM-25. Safety injection may be passive (IRIS) or active (SCOR); it may also be actuated passively, by disk rupture due to an overpressure situation (CAREM-25). For some designs (KLT-40S), safety injection of borated water is not indicated at all;
(3) All pressurized water SMRs incorporate passive residual heat removal systems of various design, often redundant, based on natural convection of the coolant; see numbers 25–32 of Table 3. Features of PWR type SMRs such as reduced core power density, relatively large coolant inventory in the primary circuit, or a taller reactor vessel, discussed in more details above, in conjunction with levels 1 and 2 of defence in depth, contribute to passive residual heat removal that is effective under a total power station blackout, with an increased or practically infinite grace period. It can be emphasized that all decay heat removal systems in all PWR type SMRs are passive, and most of them require no operator action to become actuated;
(4) Finally, numbers 33–36 of Table 3 indicate design features or systems dedicated to prevention of core uncovery in design basis accidents. These may include automatic depressurization systems, safety relief valves, long term gravity make-up systems and emergency boron injection systems also acting as make-up systems. All of the indicated systems are passive and passively actuated.

TABLE 4. DESIGN FEATURES OF PRESSURIZED WATER SMR CONCEPTS CONTRIBUTING TO LEVEL 4 OF DEFENCE IN DEPTH

#	Design feature	What is targeted	SMR designs
1	Relatively low core power density	Limitation or postponement of core melting	IRIS, CAREM-25, SCOR, MARS
2	Relatively low temperature of reactor coolant	Limitation or postponement of core melting	MARS
3	Low heat-up rate of fuel elements predicted in a hypothetical event of core uncovery, owing to design features	Prevention of core melting due to core uncovery	CAREM-25
4	Low enthalpy pressurized water containment embedding the primary pressure boundary	Additional barrier to possible radioactivity release into the environment	MARS
5	Passive emergency core cooling, often with increased redundancy and grace period (up to infinite in time)	Provision of sufficient time for accident management, e.g., in the case of failure of active emergency core cooling systems	KLT-40S, IRIS, CAREM-25 SCOR, MARS
6	Passive system of reactor vessel bottom cooling	In-vessel retention of core melt	KLT-40S
7	Natural convection of water in flooded reactor cavity	In-vessel retention of core melt	SCOR
8	Passive flooding of the reactor cavity following a small LOCA	Prevention of core melting due to core uncovery; in-vessel retention	IRIS
9	Flooding of the reactor cavity, dedicated pool for steam condensation under a steam generator tube rupture	Reduction of radioactivity release to the environment due to increased retention of fission products	SCOR
10	Containment and protective enclosure (shell) or double containment	Prevention of radioactive release in severe accidents; protection against external event impacts (aircraft crash, missiles)	KLT-40S, IRIS, CAREM-25 MARS
11	Containment building	Prevention of radioactive release in severe accidents; protection against external event impacts (aircraft crash, missiles)	All designs
12	Very low leakage containment; elimination or reduction of containment vessel penetrations	Prevention of radioactivity release to the environment	IRIS
13	Reasonably oversized reactor building, in addition to a primary coolant pressure boundary and additional water filled pressurized containment	Prevention of radioactivity release to the environment in unforeseen LOCA and severe accidents (LOCAs are prevented by design through the CPP	MARS
14	Indirect core cooling via containment cooling	Prevention of core melting; in-vessel retention	IRIS
15	Passive containment cooling system	Reduction of containment pressure and limitation of radioactivity release	KLT-40S
16	Relatively small, inert, pressure suppression containment	Prevention of hydrogen combustion	SCOR
17	Inert containment	Prevention of hydrogen combustion	IRIS
18	Reduction of hydrogen concentration in the containment by catalytic recombiners and selectively located igniters	Prevention of hydrogen combustion	CAREM-25
19	Sufficient floor space for cooling of molten debris; extra layers of concrete to avoid containment basement exposure directly to such debris	Prevention of radioactivity release to the environment	CAREM-25

The approaches for using safety grade or non-safety-grade systems vary between different SMR concepts.

In the IRIS (Annex II), all passive safety systems are safety grade; all safety grade systems are passive. For example, the refuelling water storage tank is safety grade. All active systems are non-safety-grade.

In the CAREM-25 (Annex III), all safety systems are passive and safety grade; auxiliary active systems are safety grade also.

In the SCOR (Annex IV), redundant residual heat removal systems on the primary coolant system with pool as a heat sink (RRPp) are safety grade; similar designation systems with air as a heat sink (RRPa) are safety grade, except for the chilled water pool and pumps. The startup shutdown system is non-safety-grade. The safety injection system is the only active safety system that is safety grade. In the case of a steam generator line rupture, there is no need for a safety grade auxiliary feedwater system, because normal operation systems are used in this case.

In the MARS (Annex V), all nuclear components of the reactor core are safety grade. CPP — the enveloping primary circuit boundary — is non-safety-grade. The hydraulic connections to the primary coolant boundary are safety grade. The steam generator tubes are safety grade. The containment building is safety grade. SCCS — the passive core cooling system — is safety grade. The optional passive scram system is safety grade, as well as the active scram system.

No information on the grade of safety systems was provided for the KLT-40S.

The design features of PWR type SMRs contributing to Level 4 of defence in depth, "Control of severe plant conditions, including prevention of accident progression and mitigation of consequences of severe accidents", could be categorized as follows:

(1) Inherent or passive safety features, provided by design, contributing to the limitation or postponing of core melting, or the prevention of core melting due to core uncovery, or providing additional barriers to possible radioactivity release to the environment. These are highlighted in numbers 1–4 of Table 4;
(2) Passive emergency core cooling systems, often redundant and offering an increased grace period up to infinite autonomy. These are intended to provide sufficient time for accident management. Passive emergency core cooling systems and passive decay heat removal systems are highlighted in more detail in Table 3;
(3) Passive systems of reactor vessel cooling based on natural convection of water in a flooded reactor cavity, intended to secure in-vessel retention of the corium; see numbers 6–9 of Table 4. It should be noted that features of smaller reactors such as reduced core power density or relatively larger or taller reactor vessels, discussed above in conjunction with Level 1 of defence in depth, facilitate effective in-vessel retention of corium and allow exclusion of core catchers from the reactor design;
(4) Containment buildings, in most cases a containment and a protective shell or a double containment, typical of all PWR type SMRs, are highlighted in numbers 10–13 of Table 4. Similar to reactors of other types and capacities, these are intended to prevent radioactivity release to the environment in severe accidents, and are also designed to provide protection against the impacts of external events (discussed later in this section). The containments for PWR type SMRs are more compact than for large PWRs, providing a smaller target for external aircraft missiles. However, they can be made reasonably oversized to confine hydrogen and other gaseous products in case of a severe accident;
(5) Design features to prevent hydrogen combustion of limited hydrogen concentration inside the containment; see numbers 16–18 of Table 4;
(6) In the CAREM-25, sufficient floor space for cooling of molten debris and extra layers of concrete to avoid containment basement exposure directly to such debris provides a kind of substitute to the core catcher.

For Level 5 of defence in depth, "Mitigation of radiological consequences of significant release of radioactive materials", the designers of several PWR type SMRs considered in the present report mention smaller source terms, possibly resulting from relatively smaller fuel inventory, less non-nuclear energy stored in the reactor, and lower integral decay heat rates compared to a typical large PWR; see Table 5. The designers also suggest that design features for Levels 1–4 of defence in depth could be sufficient to achieve the goal of defence in depth Level 5. However, such a suggestion needs to be proven and accepted by regulators, which had not occurred at the time this report was prepared. Certain activities of PWR type SMR designers targeted at proving the option of a reduced emergency planning zone were, however, in progress. One such activity, generic for

TABLE 5. DESIGN FEATURES AND MEASURES OF PRESSURIZED WATER SMR CONCEPTS CONTRIBUTING TO LEVEL 5 OF DEFENCE IN DEPTH

#	Design feature	What is targeted	SMR designs
1	Mainly administrative measures	Mitigation of radiological consequences resulting in significant release of radioactive materials	KLT-40S
2	Relatively small fuel inventory, less non-nuclear energy stored in the reactor, and lower integral decay heat rate	Smaller source term	Several designs
3	Design features of Levels 1–4 could be sufficient to achieve defence in depth Level 5[a]	Exclusion of a significant release of radioactive materials beyond the plant boundary or essential reduction of the zone of off-site emergency planning	KLT-40S, IRIS, CAREM,-25 MARS, SCOR

[a] Some features mentioned by contributors to Annexes II, III, IV as contributing to defence in depth level 5 generically belong to the defence in depth level 4.

many innovative SMRs, is being carried out under the IAEA coordinated research project Small Reactors without On-site Refuelling, using the IRIS reactor as an example.

Table 6 summarizes information on design basis and beyond design basis events provided by the designers of PWR type SMRs in Annexes I–V, and highlights events specific to a given SMR but not for generic PWR reactor lines. De facto, such events are mentioned only for the KLT-40S, for which two groups of specific events are specified, the first group of two related to the 'soft' pressurizer system operated by gas from a gas balloon, and the latter group of five specific to a floating (barge-mounted) NPP. For an IRIS design version under consideration for future licensing without off-site emergency planning, consideration of such rare hypothetical events as rupture of the reactor vessel and failure of all safety systems is made. It should be noted that this will not be the case for first of a kind plant licensing. In several cases, a qualitative comparison of the progression of transients in a given SMR and in a typical PWR is provided; see Annexes I–V for details.

Table 7 summarizes the information on acceptance criteria for design basis and beyond design basis events, provided by the designers of PWR type SMRs in Annexes I–V. Deterministic acceptance criteria for design basis accidents (DBA) are in most cases similar to those used for typical PWRs. Probabilistic acceptance criteria for beyond design basis accidents (BDBA) are specified as numbers for core damage frequency and large (early) release frequency in all cases except for the CAREM-25, where the requirement is to meet nationally established risk informed criteria set by the annual probability-effective dose curve shown in Fig. 6. For one design, the MARS of Italy, notwithstanding the fact that the probabilistic safety assessment granted a much lower value, core damage frequency is still accepted at 10^{-7} 1/year level, in view of a possible common cause failure resulting from ultra-catastrophic, natural events (meteorite impact).

Table 8 summarizes the information on design features for protection against external event impacts provided by the designers of PWR type SMRs in Annexes I–V, with a focus on protection against aircraft crash and seismic events. Regarding other natural and human induced external events, more detailed information on the IRIS and the CAREM-25 designs is provided in a dedicated IAEA report Advanced Nuclear Plant Design Options to Cope with External Events, IAEA-TECDOC-1487 [6]. The requirements for plant protection against external hazards, excluding seismic hazard, are in the IAEA safety standard [9].

Protection against aircraft crash is generally provided by the containment or a double containment (or the containment and a protective shell), with relatively small containment size rated as a factor that reduces the probability of an external missile impact on the plant. In the case of the IRIS, the reactor building is half-embedded underground; thus, the reactor additionally appears to be a low profile, minimum sized target from an aircraft.

Structures, systems, and components of the KLT-40S are designed taking into account possible impacts of natural and human induced external events typical of floating NPP installation sites and transportation routes; see details in Table 6. Crash landing of a helicopter is mentioned as an event considered in the design. For the

TABLE 6. SUMMARY OF DESIGN BASIS AND BEYOND DESIGN BASIS EVENTS, INCLUDING THOSE SPECIFIC FOR A PARTICULAR SMR

#	SMR design	Lists of initiating events	Events specific to a particular SMR
1	KLT-40S	Detailed lists of initiating events for abnormal operation occurrences (AOO), design basis accidents (DBA), and beyond design basis accidents (BDBA) are presented (Annex I)	(1) Disconnection of gas balloons from the pressurizer during power operation (2) Rupture of a pipeline connecting a gas balloon to a pressurizer (3) Explosion of gas balloons (4) Collision with another ship (5) Sinking of a floating power unit (6) Grounding of a floating power unit, including on rocky ground (7) Helicopter crash landing
2	IRIS	List of design basis events corresponds to that considered by the US NRC for a typical PWR (Annex II) Beyond design basis events are defined on a preliminary basis: – Hypothetical reactor pressure vessel break – Transient with failure of all safety systems.	No design specific events identified
3	CAREM-25	List of DBA defined; list of BDBA is said to be defined with no details presented (Annex III); Argentine's risk informed regulatory approach to BDBA outlined (Annex III)	No design specific events identified
4	SCOR	DBA and BDBA lists defined and presented; for DBA, the progression of transients in comparison with a typical PWR is qualitatively analyzed (Annex IV)	No design specific events identified
5	MARS	A complete safety analysis is performed, based on a preliminary HAZOP; the general approach used and some selected points are highlighted (Annex V)	No design specific events identified

CAREM-25, protection against aircraft crash is assumed to be provided by appropriate site selection, while the MARS containment is designed to withstand the worst aircraft impact.

Seismic design corresponds to 0.4–0.5 g peak ground acceleration (PGA); for the KLT-40S, the equipment, machinery, and systems important to safety, and their mounting, are designed to withstand 3 g PGA. Where indicated, the approach to seismic design is in line with IAEA safety standards [8].

The designers of all SMR type PWRs foresee that, eventually, their designs could be licensed with reduced or even eliminated off-site emergency planning measures, or at least without evacuation measures beyond the plant boundary; see Table 9.

As a desired or possible feature, reduced off-site emergency planning is mentioned in the Technology Goals of the Generation IV International Forum [15] in the User Requirements of the IAEA's International Project on Innovative Reactors and Nuclear Fuel Cycles (INPRO) [14], and in the recommendations of the International Nuclear Safety Advisory Group (INSAG-12) [11], with a caution that full elimination of off-site emergency planning may be difficult to achieve or with a recommendation that Level 5 of defence in depth still needs to be kept, notwithstanding its possibly decreased role [11].

Achieving the goal of reduced off-site emergency planning would require both development of a methodology to prove that such reduction is possible in the specific case of a plant design and siting, and adjustment of existing regulations. A risk-informed approach to reactor qualification and licensing could be of value here, once it gets established. Within the deterministic safety approach it might be very difficult to justify reduced emergency planning in view of a prescribed consideration of a postulated severe accident with

TABLE 7. SUMMARY OF ACCEPTANCE CRITERIA

#	SMR design	Deterministic acceptance criteria	Probabilistic acceptance criteria (or targets)
1	KLT-40S	Detailed lists of acceptance criteria for pre-accident situations, DBA and BDBA (Annex I)	Probabilistic acceptance criteria defined in compliance with Russian regulatory document OPB-87/97 (see Annex I): Core damage frequency (CDF) 10^{-5} 1/year; Probability of large radioactivity release 10^{-6}1/year The probabilistic risk assessment (PRA) has demonstrated CDF to be one order of magnitude less than the prescribed limit, taking into account uncertainties
2	IRIS	Deterministic acceptance criteria for DBA are assumed to be the same as for conventional PWRs Deterministic acceptance criteria for BDBA, defined on a preliminary basis, include in-vessel retention of core melt by passive means (Annex II)	The probabilistic acceptance criteria are: Core damage frequency $< 10^{-7}$1/year; Large early release frequency $<10^{-9}$1/year
3	CAREM-25	Deterministic acceptance criteria for DBA are assumed to be the same as for conventional PWRs	Risk-informed criteria set by the annual probability — effective dose curve are applied to BDBA (Annex III)
4	SCOR	The qualitative and quantitative objectives of radiological protection of the population and the environment developed for Generation III reactors, e.g., the EPR, are applied	No details have been provided
5	MARS	Deterministic acceptance criteria for DBA are assumed to be the same as for conventional PWRs	Core damage frequency accepted at 10^{-7} 1/year, taking into account possible common cause failure because of ultra-catastrophic events.

radioactivity release to the environment, e.g., owing to a common cause failure, such a catastrophic natural disaster. Probabilistic safety assessment (PSA), as a supplement to the deterministic approach, might help justify very low core damage frequency (CDF) or large early release frequency (LERF), but it does not address the consequences and, therefore, does not provide for assessment of the source terms. Risk informed approach that introduces quantitative safety goals based on the probability-consequences curve, could help solve the dilemma by providing for a quantitative measure for the consequences of severe accidents and by applying a rational technical and non-prescriptive basis to define a severe accident.

It is worth mentioning that nuclear regulations in some countries, e.g., Argentina, already incorporate provisions for applying a risk-informed approach in the analysis of severe accidents, see Fig. 6 and Annex III.

The IAEA has recently published a report entitled Proposal for a Technology-Neutral Safety Approach for New Reactor Designs, IAEA-TECDOC-1570 [13]. Based on a critical review of the IAEA safety standard NS-R-1 Safety of the Nuclear Power Plants: Design Requirements [7], IAEA-TECDOC-1570 outlines a methodology/process to design a new framework for development of the safety approach based on quantitative safety goals (a probability-consequences curve correlating to each level of defence in depth), fundamental safety functions, and generalized defence in depth, which includes probabilistic considerations. Different from this, the current safety approach [7] is based on qualitative safety goals, fundamental safety functions, application of defence in depth, and application of probabilistic safety assessments complementing deterministic methods.

Future IAEA publications and, specifically, a report of the above mentioned coordinated research project, will provide more details on the progress of justification for limiting measures of Level 5 of defence in depth to plant sites.

In the meantime, the designers of PWR type SMRs accept that licensing of their plants in the near term could be accomplished in line with existing regulations prescribing standard measures for the mitigation of

TABLE 8. SUMMARY OF DESIGN FEATURES FOR PROTECTION AGAINST EXTERNAL EVENT IMPACTS

#	SMR design	Aircraft crash / Earthquakes	Other external events
1	KLT-40S	No details provided regarding aircraft crash; crash-landing of a helicopter is considered in the design. The equipment, machinery, and systems important to safety and their mounting are designed to withstand 3 g peak ground acceleration (PGA). Seismic design: 7 on the MSK scale at 10^{-2} 1/year frequency for design earthquakes; 8 on the MSK scale at 10^{-4} 1/year frequency for maximum design earthquakes	Structures, systems, and components designed taking into account possible impacts of natural and human induced external events typical of a floating NPP installation site and transportation routes. Specific external events for a floating NPP are summarized in Table 6
2	IRIS	The reactor, the containment, the passive safety systems, the fuel storage, the control room, and the back-up control room located in the reinforced concrete auxiliary building are half-embedded underground. The reactor appears as a low-profile, minimum sized target from an aircraft; 0.5g PGA	Design features for protection against the impacts of natural and human induced external events are described in more detail in [6]
3	CAREM-25	Aircraft crash is not considered in the CAREM-25 design – protection is assumed to be provided by site selection and administrative measures; there are two shells (containment, confinement), and the nuclear module is compact and small, which reduces the probability of an external missile impact on the containment; 0.4 g PGA; 'probable earthquake' is similar to operating basis earthquake (US NRC) or L-S1 (IAEA classification); 'severe earthquake' is similar to safe shutdown earthquake (US NRC) or L-S2 (IAEA classification)	Design features for protection against the impacts of natural and human induced external events are described in more detail in [6]
4	SCOR	No information was provided	No information was provided
5	MARS	Designed against aircraft crash/seismic loads under reference site conditions	No further information was provided

TABLE 9. SUMMARY OF MEASURES PLANNED IN RESPONSE TO SEVERE ACCIDENTS

#	SMR design	Measures
1	KLT-40S	– Exclusion of staff presence in compartments adjacent to the containment and in other compartments with high radiation levels. – To limit radiation dose to the population living within a 1 km radius of the floating NPP it may be required (depending on the actual radiation situation) that some protective measures, such as iodine prophylaxis or sheltering, are implemented. – As a protective measure, temporary limits could be established on the consumption of separate agricultural products grown in an radius of up to 5 km from the floating NPP contaminated by radioactive products. –Evacuation of the population is not required at any distance from the floating NPP.
2	IRIS	– Measures essentially not needed. An option to license IRIS with reduced or eliminated off-site emergency planning is under consideration; otherwise, the plant could be licensed using measures typical of a conventional PWR.
3	CAREM-25	– Measures essentially not needed. An option to license CAREM with simplified or abandoned off-site emergency planning requirements is considered, with a link to the risk-informed regulatory criteria for BDBA (see Fig. 6 and Annex III).
4	SCOR	– No information was provided except for that on passive safety design features eliminating or preventing radioactivity releases beyond the plant boundary.
5	MARS	– Deterministic and probabilistic safety analyses performed conclude that licensing of MARS may not require any off-site emergency planning.

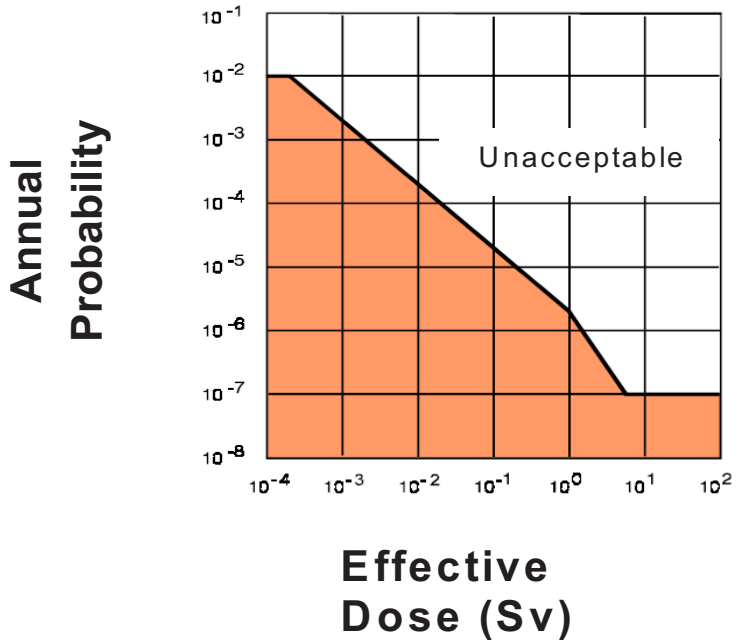


FIG. 6. Acceptance criteria for beyond design basis accidents as provided for by regulations in Argentina (see Annex III).

radiological consequences of significant release of radioactive materials. These measures are mostly of an administrative character. In particular, the KLT-40S designers mention that administrative measures are foreseen for plant personnel and the population within a 1 km radius of the plant, but indicate that evacuation is not required at any distance from the floating NPP; for more details see Annex I.

Design approaches used to achieve defence in depth in pressurized water SMRs considered in this report are generally in line with recommendations of the IAEA Safety Standards Series No. NS-R-1, Safety of the Nuclear Power Plants: Design Requirements [7]. Specifically, designers often refer to [7] when discussing safety objectives, safety functions, defence in depth concepts, accident prevention, radiation protection and acceptance criteria, safety classifications, safety assessment and single failure criterion, common cause failure and redundancy, diversity and independence, conservatism in design, and human factors. It should be noted that, because of limited information obtained from Member States, this report is not intended to provide a review of safety design approaches applied by SMR designers against IAEA safety standards.

Designers anticipate that future revisions of safety standards with more focus on a risk informed approach to design qualification, such as suggested in IAEA-TECDOC-1570 [13], could facilitate the goal of achieving plant qualification and licensing with reduced off-site emergency planning requirements.

3.2.2. Pressurized light water cooled heavy water moderated reactors

This reactor line is represented by only one design considered in the present report, which is the Advanced Heavy Water Reactor (AHWR) developed by the Bhabha Atomic Research Centre (BARC) of India; see Annex VI for details. The AHWR uses boiling light water as a coolant in pressure channels and heavy water as a moderator in the calandria. On-line refuelling is applied, and the fuel is Pu-Th based. Figure 7 gives a schematic of the main heat transport system and passive decay heat removal system of the AHWR.

Design features contributing to different levels of defence in depth are summarized in Tables 10–14.

A distinct feature of the AHWR contributing to all levels of defence in depth is the absence of dedicated active safety systems. Heat is removed by natural convection in all modes, including normal operation mode. In case the main condenser and passive Isolation Condensers (ICs) would be unavailable to remove decay heat, decay heat could be removed using purification coolers of the main heat transport system in an active mode. Two independent, fast acting shutdown systems are Category D [12] passive systems. All passive systems are safety grade.

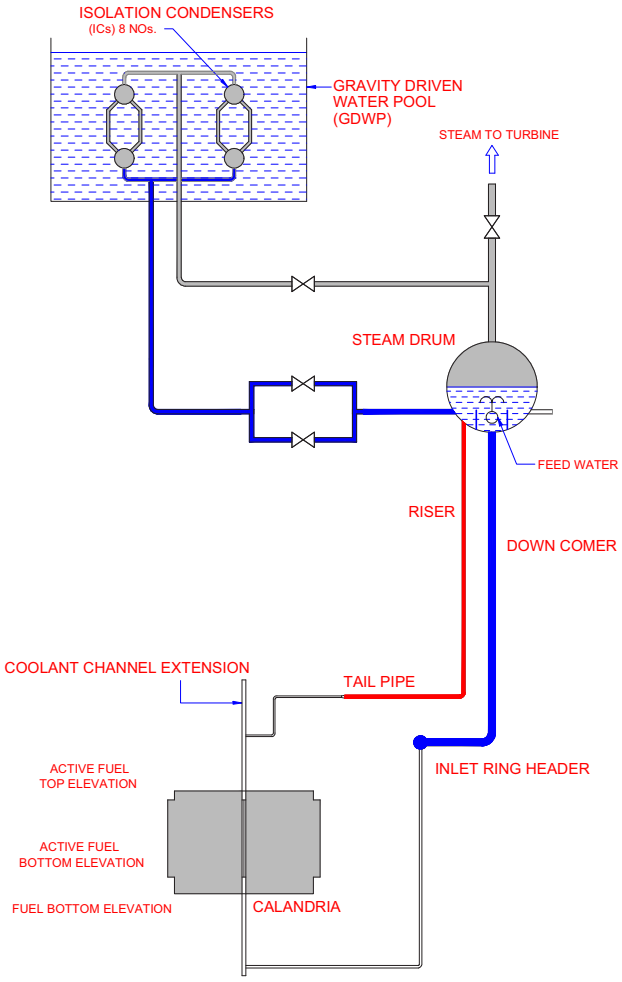


FIG. 7. Heat transport systems of AHWR.

TABLE 10. DESIGN FEATURES OF AHWR CONTRIBUTING TO LEVEL 1 OF DEFENCE IN DEPTH

#	Design features	What is targeted
1	Heat removal from the core under both normal operation and shutdown conditions performed by natural convection of the coolant	Elimination of loss of flow hazard
2	Slightly negative void coefficient of reactivity	Reduction of the extent of transient overpower accidents
3	Relatively low core power density	
4	Negative fuel temperature coefficient of reactivity	
5	Low excess reactivity due to the use of Pu-Th based fuel and on-line refuelling	

TABLE 11. DESIGN FEATURES OF AHWR CONTRIBUTING TO LEVEL 2 OF DEFENCE IN DEPTH

#	Design feature	What is targeted
1	Large coolant inventory in the main coolant system	Increased thermal inertia; slower progression of transients
2	Digital control systems using advanced information technology	Increased reliability of the control system
3	Advanced displays and diagnostics using artificial intelligence and expert systems	Increased operator reliability
4	Two independent and diverse shutdown systems, one based on mechanical control rods and another employing injection of liquid poison into the low pressure moderator, each with 100% shutdown capacity	Reactor shutdown

TABLE 12. DESIGN FEATURES OF AHWR CONTRIBUTING TO LEVEL 3 OF DEFENCE IN DEPTHX

#	Design feature	What is targeted
1	Large inventory of water inside the containment (about 6000 m^3 of water in the gravity driven water pool (GDWP))	Prolonged core cooling with increased grace period
2	Passive injection of cooling water, first from the accumulator and later from the overhead GDWP, directly into the fuel cluster through four independent parallel trains	Increased reliability of emergency core cooling systems
3	Passive decay heat removal system, which transfers of decay heat to GDWP using natural convection	Increased reliability of decay heat removal
4	Two independent and diverse shutdown systems, one based on mechanical control rods and another employing injection of liquid poison into the low pressure moderator; each with 100% shutdown capacity	Increased reliability of reactor shutdown
5	Additional passive shutdown device for the injection of a poison using steam pressure	Increased reliability of reactor shutdown

TABLE 13. DESIGN FEATURES OF AHWR CONTRIBUTING TO LEVEL 4 OF DEFENCE IN DEPTH

#	Design feature	What is targeted
1	Use of the moderator as a heat sink	Establishing additional path for heat removal
2	Flooding of the reactor cavity following a LOCA	Prevention of core melt
3	Double containment	Prevention of radioactivity release to the environment; protection against external events
4	Passive containment isolation system	Prevention of core melt
5	Passive containment cooling	Prevention of core melt
6	Vapour suppression in GDWP	Prevention of failure of the primary coolant system and containment under severe plant conditions

TABLE 14. DESIGN FEATURES OF AHWR CONTRIBUTING TO LEVEL 5 OF DEFENCE IN DEPTH

#	Design feature	What is targeted
1	Design features of Levels 1–4 could be sufficient to achieve the goal of defence in depth Level 5[a]	Elimination of the need for any intervention in the public domain beyond plant boundaries as a consequence of any accident condition within the plant

[a] Some features mentioned in ANNEXES II, III, IV as contributing to defence in depth Level 5 generically belong to defence in depth Level 4.

Natural convection in normal operation mode contributes to elimination of loss of flow hazard; see Table 10. Negative void reactivity coefficient, relatively low core power density, negative fuel temperature coefficient of reactivity, and low excess reactivity owing to the use of Pu-Th fuel with on-line refuelling contribute to a reduction of the extent of transient overpower accidents. Relatively large coolant inventory in the main coolant system contributes to increased thermal inertia and slower progression of transients (see Table 12), while large inventory of water inside the containment contributes to a prolonged reactor cooling with increased grace period (see Table 11).

Flooding of the reactor cavity following a LOCA, use of the passive containment isolation system and passive containment cooling contribute to the prevention of core melting (see Table 13). Vapour suppression in the Gravity Driven Water Pool (GDWP), located inside the containment, contributes to prevention of a failure of the primary coolant system and containment under severe plant conditions.

Altogether, design features of Levels 1–4 of the defence in depth are indicated by the designers as sufficient to achieve the goal of defence in depth Level 5 (see Table 14).

Small power rating of the AHWR obviously contributes to the extended use of natural convection based passive systems for normal and emergency reactor cooling. Other inherent and passive features of the AHWR are generically independent of reactor capacity.

Tables 15 and 16 summarize design basis events and acceptance criteria for the AHWR. An event specific to the AHWR is instability during a start-up owing to the natural convection cooling mode (see Table 15).

Table 17 gives a summary of design features to protect against external event impacts; for more details see [6]. Double containment is used for protection against aircraft crash. Seismic design is in line with IAEA safety standards [8].

According to information provided in Table 18, the design target for the AHWR is to eliminate the need for any intervention in the public domain beyond the plant boundary as a consequence of any accident condition within the plant (see also Table 14).

Issues of achieving plant licensing with reduced off-site emergency planning requirements are discussed in more detail in Section 3.2.1., in conjunction with measures planned in response to severe accidents for pressurized water type SMRs. This discussion is also relevant to pressurized light water moderated heavy water cooled reactors considered in this section.

TABLE 15. SUMMARY OF DESIGN BASIS AND BEYOND DESIGN BASIS EVENTS, INCLUDING THOSE SPECIFIC FOR A PARTICULAR SMR

SMR design	Lists of initiating events	Events specific to a particular SMR
AHWR	Forty-three postulated initiating events have been identified for the AHWR; short summary of design basis and beyond design basis event groups is given in Annex VI	Instability during a startup

TABLE 16. SUMMARY OF ACCEPTANCE CRITERIA

SMR design	Deterministic acceptance criteria	Probabilistic acceptance criteria (or targets)
AHWR	Deterministic acceptance criteria are defined. It is noted that a large number of accident scenarios that would conventionally fall within the category of beyond design basis accidents have been demonstrated, via safety analysis, to prevent violation of acceptance criteria established for design basis accidents	The probability of unacceptable radioactivity release beyond plant boundaries is expected not to exceed 1×10^{-7} 1/year

TABLE 17. SUMMARY OF DESIGN FEATURES FOR PROTECTION AGAINST EXTERNAL EVENT IMPACTS

SMR design	Aircraft crash / Earthquakes	Other external events
AHWR	Double containment is used for protection against aircraft crash. The AHWR structures, systems and components are being designed for high level and low probability seismic events such as operating basis earthquakes (OBE) and safe shutdown earthquakes (SSE); seismic instrumentation is planned in accordance with national and international standards	Safety design features of the AHWR intended to cope with external events are described in more detail in [6]. Specifically, the AHWR is being designed to cope with floods (high grade elevation); trajectory missiles (adequate protection of all safety related buildings); ingress of toxic gases; etc. Combinations of internal and external events are considered. Important nuclear auxiliary systems are located inside the reactor building and in the basement to the extent possible. The plant incorporates many passive safety features ensuring a grace period of 3 days

TABLE 18. SUMMARY OF MEASURES PLANNED IN RESPONSE TO SEVERE ACCIDENTS

SMR design	Measures
AHWR	Measures essentially not needed; one of the design objectives of the AHWR is to eliminate the need for any intervention in the public domain beyond the plant boundaries as a consequence of any postulated accident condition within the plant

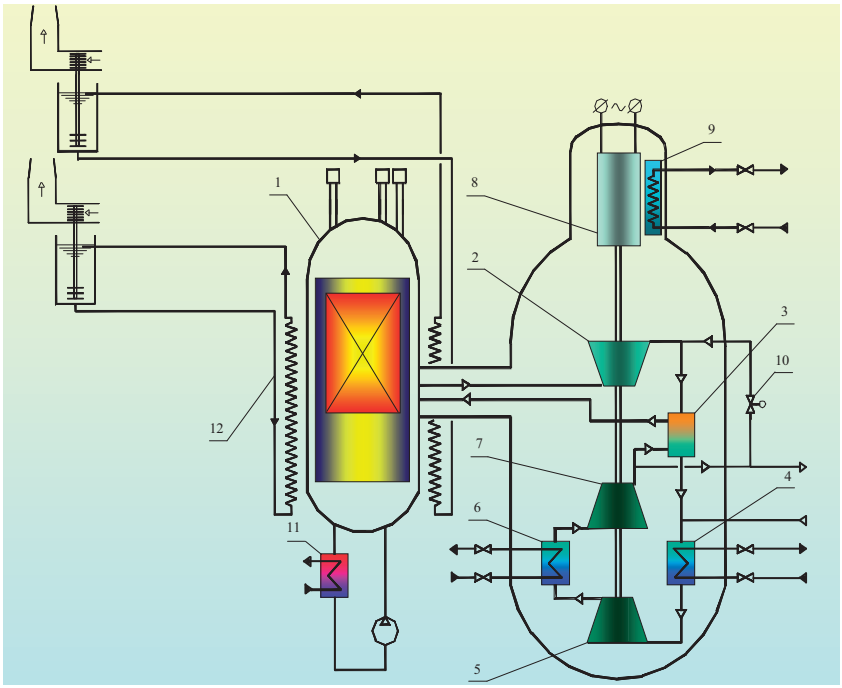
The IAEA safety standard NS-R-1, Safety of Nuclear Power Plants: Design [7], provides a basis for national nuclear regulations in India.

Because the AHWR uses only passive natural convection based systems for both heat removal in normal operation (boiling light water coolant in channels) and heat removal in emergency conditions, including long term decay heat removal, performance qualification and, specifically, justification of reliability of passive safety systems are required to justify low targeted values of core damage frequency (CDF) and large early release frequency (LERF). Assessment methodologies that could facilitate achieving such a justification are discussed in Appendix 1 of the present report.

As in the case with PWR type SMRs, future revisions of IAEA safety standards with more focus on a risk-informed safety approach, e.g., such as suggested in IAEA-TECDOC-1570 Proposal for a Technology-Neutral Safety Approach for New Reactor Designs [13] could be helpful in facilitating achievement of the goal of plant licensing with reduced off-site emergency planning requirements.

3.2.3. High temperature gas cooled reactors

All high temperature gas cooled reactors (HTGRs) use tristructural-isotropic (TRISO) coated fuel particles. Each particle consists of a fuel kernel coated with, among other layers, a ceramic layer of SiC that retains fission products at high temperatures and high fuel burnups. Some HTGR designs, e.g., the PBMR [2], use graphite spheres (pebbles) in which thousands of TRISO fuel particles are embedded, but other HTGR designs use pin-in-block type fuel with graphite TRISO particles incorporated in graphite pins. An example of such designs is the GT-MHR addressed in the present report; see Annex VII. The ability of TRISO fuel particles to contain fission products at high temperatures creates additional opportunities, relative to established practices in light water reactors, to design safety systems and mitigation measures and essentially makes it possible to eliminate the adverse consequences of many severe accidents by design. Passive decay heat removal in HTGRs can be accomplished by heat conduction through the graphite holding TRISO particles, followed by convection and radiation in the structures and other media in the absence of primary coolant. Also, due to the large heat capacity of graphite in the HTGR core, HTGRs have a slow and stable response to transients caused by initiating events, facilitating better reactor self-control at all levels of defence in depth. A requirement of



1–Reactor; 2–Turbine; 3–Recuperator; 4, 6–Precooler and intercoolers;
5, 7–Low and high pressure compressors; 8–Generator; 9–Cooler; 10–Bypass valve;
11–Reactor shutdown cooling system; 12–Reactor cavity cooling system.

FIG. 8. Flow diagram of the GT-MHR cooling system.

passive decay heat removal through the reactor vessel wall and the properties of known materials for use in the reactor pressure vessel limit the unit power of HTGRs by approximately 600 MW(th); thus all HTGR designs fall within the SMR unit size range [2].

Figure 8 shows the flow diagram of the GT-MHR (see Annex VII for more details).

Tables 19-23 summarize the design features of the GT-MHR contributing to Levels 1–5 of defence in depth.

For Level 1 of defence in depth, "Prevention of abnormal operation and failure", design features of the GT-MHR cumulatively result in an essential de-rating of accident scenarios rated as potentially severe in reactors of other types, including LOCA, LOFA, and reactivity initiated accidents. For example, helium release from the core in the GT-MHR can be a safety action and not the initiating event of a potentially severe accident, with indefinite passive decay heat removal from the core possible via convection, conduction and radiation in all structures and media.[4] Also, use of a direct gas turbine cycle eliminates accident initiators otherwise associated with a steam-water power circuit, such as steam generator tube rupture in PWRs or water ingress into the core in indirect cycle HTGRs. Absence of large diameter piping in the primary circuit reduces the scope of possible loss of coolant accidents. Helium properties exclude transient overpower events owing to coolant density variation.

For Level 2 of defence in depth, "Control of abnormal operation and detection of failure", the contribution comes from advanced instrumentation and control and operator support systems, but also from inherent safety features owing to the reactor design. The latter security increases self-control properties of the reactor under a large temperature margin between the operation limit and the safe operation limit. Finally, two independent and diverse passive reactor shutdown systems and one active system of normal operation, capable of performing reactor shutdown, are available to contribute to this level.

[4] Long term passive decay heat removal may cause degradation of core structures, e.g., via graphite oxidation, etc., therefore, early restart of normal operation systems is targeted in management of design basis accidents to facilitate continuation of normal operation of the plant after the accident.

TABLE 19. DESIGN FEATURES OF GT-MHR CONTRIBUTING TO LEVEL 1 OF DEFENCE IN DEPTH

#	Design features	What is targeted
1	Use of TRISO fuel	Reliable operation, high temperatures and high fuel burnups
2	Use of helium coolant	– Good heat transfer properties; no dissociation and phase changes; low activation; chemical inertness – Eliminates the option of transient overpower at coolant density variation
3	Use of direct closed gas turbine cycle	– Design simplification, with minimization of necessary plant equipment and systems; – Exclusion of the steam turbine power circuit and associated impacts of its possible failures
4	Relatively low power density of the core + large volume of graphite inside the reactor Vessel + high temperature TRISO fuel + neutronic properties of helium + negative reactivity feedbacks on reactor temperature and power increase	Large temperature margin between the operation limit and the safe operation limit, and large Thermal inertia of the reactor core and improved self-control properties of the reactor, cumulatively resulting in an essential de-rating of accident scenarios rated as potentially severe in reactors of other types and facilitating better reactor self-control. For example, helium release from the core in the GT-MHR is a safety action, with long-term passive decay heat removal from the core possible via convection, conduction and radiation in all structures and media of the voided reactor
5	No large diameter pipelines in the primary circuit	Limitation of the scope of LOCA

TABLE 20. DESIGN FEATURES OF GT-MHR CONTRIBUTING TO LEVEL 2 OF DEFENCE IN DEPTH

#	Design feature	What is targeted
1	Relatively low power density of the core + large volume of graphite inside the reactor vessel + high temperature TRISO fuel + neutronic properties of helium + negative reactivity feedbacks on reactor temperature and power increase	Increased self-control properties of the reactor under a large temperature margin between the operation limit and the safe operation limit
2	Use of reliable automated control systems with a self-diagnostics capability	Increased reliability in controlling abnormal operation and prevention of failure
3	Use of state of the art operator information support system	Increased reliability of the control of abnormal operation and prevention of failure
4	Two diverse and independent passive shutdown systems; One active system of normal operation, capable of reactor shutdown	Reactor shutdown

TABLE 21. DESIGN FEATURES OF GT-MHR CONTRIBUTING TO LEVEL 3 OF DEFENCE IN DEPTH

#	Design feature	What is targeted
1	Increased role of inherent safety features, such as negative reactivity feedback on reactor power and temperature and natural processes of conduction, radiation and convection, provided by design	Slow progression of transients resulting from large thermal inertia of the core; large temperature margin between operation limit and safe operation limit; and slow temperature variation at power variation
2	Preferential use of passive safety systems (see Section 7.2. in Annex VII)	Increased reliability in carrying out of safety functions
3	Mechanical control rod system providing gravity driven insertion of control rods to the core and the reflector, operated in the case of de-energization actuated by the control system	Reactor scram
4	Reactor emergency shutdown system based on gravity driven insertion of spherical absorbing elements to the dedicated channels located within the core stack, initiated by supplying power from diesel generators to the drive motors	Effective shutdown of the reactor and maintenance of a subcritical status in a cold unpoisoned state
5	Active electromechanical reactivity control system, which is a normal operation system shouldering the functions of a safety system	Reactivity control and hot reactor shutdown
6	Passive residual heat removal from the core based on natural processes of conduction, radiation and convection, requiring no external power sources, control signals, or human intervention, and leading to heat removal from outside of the reactor vessel to the environment through the always effective passive reactor cavity cooling system	Increased reliability of accident control within the design basis; Securing fuel safe operation limits at passive shutdown and cooling of the reactor
7	Low core power density; Annular reactor core with a high surface to volume ratio; Central reflector; High heat capacity of the reactor core and internals; Heat resistant steel used for the reactor internals and vessel	Facilitate effective operation of the reactor cavity cooling system

As already mentioned, an increased role of inherent safety features, such as negative reactivity feedbacks on reactor power and temperature; high thermal inertia of the reactor core; and natural processes of conduction, radiation and convection, provided by HTGR design, facilitates a high degree of reactor self-control at all levels of defence in depth and secures safe operation limits of fuel, and ensures that passive shutdown and cooling of the reactor are provided for in the case of a variety of postulated initiating events; see Annex VII. These features are also effective at Level 3 of defence in depth, "Control of accidents within design basis". Long term passive decay heat removal accomplished via natural processes of conduction, convection and radiation and through operation of the reactor cavity cooling system, even in the absence of helium coolant in the reactor coolant system, is facilitated by the GT-MHR design features listed explicitly in number 7 of Table 21. For Level 3 of defence in depth, the reactor incorporates two independent and diverse reactor shutdown systems, which operate on passive principles and are passively actuated. In addition to them, an active electromechanical reactivity control system, which is a normal operation system, is capable of accomplishing the function of hot reactor shutdown.

The GT-MHR design provides for no dedicated active safety systems. Active systems of normal operation, such as the power conversion unit (PCU), the shutdown cooling system (SCS), and the electromechanical reactivity control system can be used for safety purposes; see Annex VII. These systems remove heat under abnormal operation conditions, and in design basis and beyond design basis accidents. All main passive safety systems are safety grade. The electromechanical reactivity control system (an active system of normal operation) is safety grade too.

TABLE 22. DESIGN FEATURES OF GT-MHR CONTRIBUTING TO LEVEL 4 OF DEFENCE IN DEPTH

#	Design feature	What is targeted
1	Additional physical barriers provided by the design of fuel with multilayer TRISO coatings	Mitigation of consequences of severe accidents
2	Inherent and passive safety features and passive safety systems incorporated in plant design, cumulatively (see Annex VII)	Securing that final stable and safe conditions are reached when the chain reaction of fission is suppressed and when continuous cooling of nuclear fuel and retention of radioactive substances within established boundaries are provided
3	Use of helium in reactor core cooling, as a safety action	Passive residual heat removal from the core based on natural processes of conduction, radiation and convection, requiring no external power sources, control signals, or human intervention, ending up with heat removal from outside of the reactor vessel to the environmental air by the always effective passive reactor cavity cooling system
4	Option of beyond design basis accident management by personnel in the case of failure of safety components and systems, secured by: Safety design features of the reactor that limit the progression of accidents; Characteristics of the passive systems; Capabilities of the normal operation systems; Large time margins for implementation of accident management measures	Increased confidence that the objectives of defence in depth Level 4 will be fulfilled
5	Containment designed to retain the helium-air fluid and to withstand external loads	Increased confidence that the objectives of defence in depth Level 4 will be fulfilled under impacts of internal and external events and combinations thereof

TABLE 23. DESIGN FEATURES OF GT-MHR CONTRIBUTING TO LEVEL 5 OF THE DEFENCE IN DEPTH

#	Design feature	What is targeted
1	Design features of Levels 1–4 could be sufficient to achieve the goal of defence in depth Level 5	No accident mitigation measures required both within and beyond the NPP site

The GT-MHR features contributing to increased confidence that the objective of Level 4 of defence in depth, "Mitigation of radiological consequences of significant release of radioactive materials", will be fulfilled are (see Table 22):

- Additional physical barriers provided by the design of fuel with TRISO multilayer coatings, securing short term fission product confinement capability at temperatures as high as 2100°C, and long term fission product confinement capability at 1600°C — essentially, each micro fuel element in the HTGR has its own containment;
- Safety design features of the reactor that limit the progression of accidents (see more detailed discussion for levels 2 and 3 of defence in depth);
- Characteristics of passive systems (long term passive decay heat removal capability via conduction, convection and radiation even in the absence of helium in the core, but with the operation of a passive cavity cooling system);

- Capabilities of normal operation systems. Although passive decay heat removal can be practically infinite, retaining the capability to restart the reactor for normal operation after an emergency may be facilitated by on-time restart of some normal operation systems during the emergency process, e.g., to prevent graphite oxidation, see Annex VII for details;
- Large time margins for implementation of accident management measures (see more detailed discussion for Level 3 of defence in depth);
- Use of the containment designed to retain the helium-air fluid.

The designers of the GT-MHR foresee that the design features of Levels 1–4 of defence in depth could be sufficient to achieve the goal of defence in depth Level 5, "Mitigation of radiological consequences of significant release of radioactive materials".

Tables 24 and 25 summarize information on design basis and beyond design basis accidents and acceptance criteria provided by designers of the GT-MHR in Annex VII. The event (abnormal operation occurrence) specific to the GT-MHR, but not necessarily to other HTGRs, is inadvertent insertion of absorbing elements from the reserve shutdown system hoppers into the reactor core.

Table 26 summarizes design features of the GT-MHR contributing to plant protection against external event impacts.

TABLE 24. SUMMARY OF DESIGN BASIS AND BEYOND DESIGN BASIS EVENTS, INCLUDING THOSE SPECIFIC TO A PARTICULAR SMR

SMR design	Lists of initiating events	Events specific to a particular SMR
GT-MHR	Detailed lists of initiating events for abnormal operation occurrences, DBA, and BDBA are presented (Annex VII)	Abnormal operation occurrence: Inadvertent insertion of absorbing elements from the reserve shutdown system (RSS) hoppers into the reactor core

TABLE 25. SUMMARY OF ACCEPTANCE CRITERIA

SMR design	Deterministic acceptance criteria	Probabilistic acceptance criteria (or targets)
GT-MHR	The acceptance criteria are radiation safety criteria (deterministic criteria related to dose limits of irradiation to personnel and the population). In addition to this, operation limits and safe operation limits are defined for process parameters; operation limits are defined for the equipment; design limits are specified to the analysis of design basis accidents; and the acceptance criteria are introduced for different operation modes, see Annex VII	Probabilistic acceptance criteria are defined as follows: The overall probability of severe beyond design basis accidents less than 10^{-5} per reactor per year; Probability of large radioactivity release less than 10^{-7} per reactor per year

TABLE 26. SUMMARY OF DESIGN FEATURES FOR PROTECTION AGAINST EXTERNAL EVENT IMPACTS

SMR design	Aircraft crash / Earthquakes	Other external events
GT-MHR	The design of the GT-MHR ensures protection against an aircraft crash involving a 20 t aircraft falling with 200 m/s speed and producing a 7 m^2 impact area; the maximum design basis earthquake corresponds to 8 on the MSK scale (horizontal PGA component is 0.2 g; vertical component is 2/3 of the horizontal component); design basis earthquake corresponds to 7 on the MSK scale (PGA components are two times lower than for the maximum design basis earthquake)	Other external events considered in the GT-MHR design are winds, low and high environmental temperatures, shock wave impacts, etc. The reactor plant is arranged in a monolithic ferroconcrete underground containment that provides protection against external event impacts. Apart from external events, the containment provides protection against internal impacts, such as those caused by jets and missiles

TABLE 27. SUMMARY OF MEASURES PLANNED IN RESPONSE TO SEVERE ACCIDENTS

SMR design	Measures
GT-MHR	Design features and inherent properties of the GT-MHR ensure that the temperature of the coated particle fuel is kept below 1600 °C in any accidents involving heat removal failure, including complete failure of all active means of the reactor emergency protection and shutdown. At this temperature, the integrity of the fuel element coatings is maintained, thus no protective measures would be required for the population beyond the buffer area

Table 27 gives a summary of the measures planned in response to severe accidents. As in the case of several other SMRs in this report, the designers foresee no need for measures to protect the population beyond a certain buffer area around the plant in any accidents with heat removal failure accompanied by failure of all active means of reactor emergency protection and shutdown.

Issues of achieving plant licensing with reduced off-site emergency planning requirements are discussed in more detail in section 3.2.1., in conjunction with measures planned in response to severe accidents for pressurized water type SMRs. This discussion is also relevant to high temperature gas cooled reactors considered in this section.

Although the ultimate goal is to prove that no accident mitigation measures would be required both within and beyond the NPP site, licensing of a first of a kind plant is likely to be carried out in compliance with existing regulatory rules and practices.

It is expected that a technology neutral approach may facilitate assessment of the design features of HTGRs, including the GT-MHR. Specifically, IAEA-TECDOC-1570 Proposal for a Technology-Neutral Safety Approach for New Reactor Designs [13] suggests that *"in the design of innovative reactors it may be possible, by following the risk-informed approach, to provide justification that a confinement system designed to the same standards that have been established for LWR technology would not be needed. This may be because, for example, there are mitigating features of the design of the fuel which limit the quantity of radioactive materials released, and allow the reactor to return to a stable state without impairing the ability of the fuel to be maintained within its design matrix with little or no release of fission products. Another consideration may be that of the timescale before the plant state escalates to a condition where corrective action, e.g., initiation of cooling systems, is necessary."*

Certain passive decay heat removal mechanisms of the GT-MHR (and HTGRs), such as natural convection, conduction and radiation, are rated reliable and independent of possible disruptions of core configuration. Their reliability, as well as passive response of the reactor to unprotected accidents, such as LOCA or control rod ejection, could be proven via a 'license-by-test' approach, e.g., as demonstrated in tests performed at the HTR-10 reactor in China [17].

3.2.4. Liquid metal cooled fast reactors

All fast reactor designs in the SMR family offer design flexibility in setting desired combinations of reactivity coefficients and effects. This flexibility, coupled with the inherent properties of advanced types of fuel, creates a potential to prevent transient overpower accidents, to ensure increased reactor self-control in a variety of other anticipated transients without scram and combinations thereof, and to enable 'passive shutdown' (see definition at the end of Appendix 2) and passive load following capabilities of a plant.[5] Smaller specific core power or relatively tall reactor vessels facilitate the use of natural convection of a single phase liquid metal coolant to remove decay heat or even the heat produced in normal operation (for heavy liquid metal cooled SMRs). For sodium cooled

[5] It should be noted that features of liquid metal cooled reactors such as passive load following and 'passive shutdown' have been more analyzed in the past for smaller reactors, such as EBR-II with 65 MW(th) or PRISM with 850 MW(th). However, for sodium and lead cooled fast reactors, there is no reason such features can't be realized in larger reactors with nitride or metallic fuel. Certain analytical studies carried out in the past provide preliminary proof of this [26, 27, 28].

reactors, smaller reactor size facilitates achievement of negative whole core sodium void reactivity effect. For lead cooled reactors, there could be a certain size limit to ensure reliable seismic design [2].

Figure 9 and 10 show general layouts of the 4S-LMR and the SSTAR, respectively.

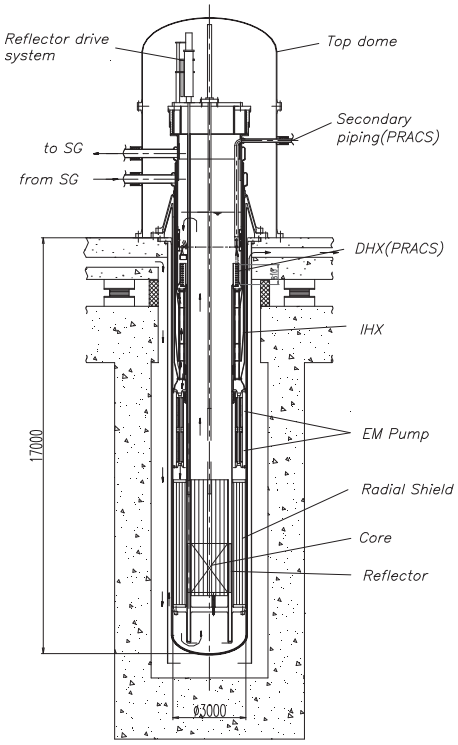


FIG. 9. Vertical view of the 4S-LMR layout.

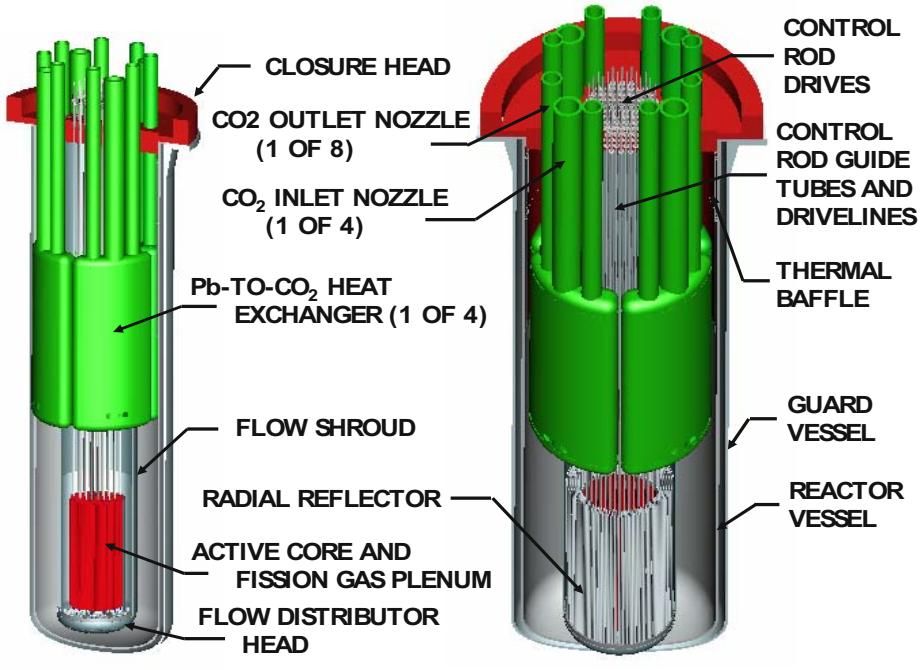


FIG. 10. General view of the SSTAR layout.

Fast spectrum liquid metal cooled SMR designs are represented by the 4S-LMR concept of a sodium cooled small reactor without on-site refuelling developed by the Central Research Institute of Electric Power Industry (CRIEPI) and Toshiba in Japan (see Annex VIII) and by the SSTAR and STAR-LM concepts of small lead cooled reactors without on-site refuelling developed by the Argonne National Laboratory (ANL) in the USA (see Annex IX). Lead cooled SMR concepts use CO_2 as the working media in the Brayton cycle power circuit, and incorporate no intermediate heat transport system. Although essentially different in several important features, both the sodium cooled and the lead cooled SMR concepts belong to a family of pool type integral design liquid metal cooled fast reactors, and close cooperation between their designers was established long ago [3]. Of the two designs, the 4S-LMR is in a more advanced stage, because for a similar design — different essentially in the type of fuel used and named the 4S — the conceptual design and major parts of the system design have been completed [3]. A pre-application review by the US NRC was initiated in the fall of 2007. Construction of a demonstration reactor and safety tests are planned for early 2010 [3]. Different from the 4S-LMR, both the SSTAR and STAR-LM are at a pre-conceptual stage. It should be noted that the small size and capacity of fast reactors considered in this section are, first of all, conditioned by the requirement for operation without on-site refuelling (see [3] for more detail) and not by the a priori considerations of achieving a somewhat higher degree of passive response in accidents.

Tables 28–32 summarize the design features of the 4S-LMR, the SSTAR and the STAR-LM contributing to defence in depth Levels 1–5.

Design features contributing to Level 1 of defence in depth, "Prevention of abnormal operation and failure", are summarized in Table 28.

TABLE 28. DESIGN FEATURES OF SODIUM COOLED AND LEAD COOLED FAST SMRs CONTRIBUTING TO LEVEL 1 OF DEFENCE IN DEPTH

#	Design feature	What is targeted	SMR designs
1	Low pressure primary coolant system	Little non-nuclear energy stored in the primary coolant system — elimination of a potential of release of this energy	4S-LMR, SSTAR, STAR-LM
2	Use of metallic fuel with high thermal conductivity (relatively low temperature)	High margin to fuel failure	4S-LMR
3	Use of nitride fuel with high thermal conductivity (relatively low temperature)	High margin to fuel failure	SSTAR, STAR-LM
4	Relatively low linear heat rate of fuel	Higher margin to fuel failure	4S-LMR
5	Power control via pump flow rate in the power circuit, with no control rods in the core	Elimination of an accident with control rod ejection	4S-LMR
6	Large negative feedback from fast spectrum core plus natural convection of coolant in all modes, enabling passive load following and 'passive shutdown'[a]	Essential prevention or de-rating of initiating events resulting from malfunctioning of systems or components, or operator actions that would otherwise need to be considered sources of failure	SSTAR, STAR-LM
7	Low burnup reactivity swing over long core lifetime/refuelling interval	Elimination of transient overpower accident due to control rod ejection	SSTAR, STAR-LM
8	Elimination of feedback control of moveable reflectors (that compensate for reactivity changes due to fuel burnup); a pre-programmed reflector drive system is used	Prevention of transient overpower	4S-LMR
9	Electromagnetic impulsive force used in the reflector driving system	Intrinsic limitation of the speed of positive reactivity insertion	4S-LMR
10	Intermediate heat transport system	Prevention of a sodium-water reaction	4S-LMR

TABLE 28. DESIGN FEATURES OF SODIUM COOLED AND LEAD COOLED FAST SMRs CONTRIBUTING TO LEVEL 1 OF DEFENCE IN DEPTH (cont.)

#	Design feature	What is targeted	SMR designs
11	Pb coolant not reacting chemically with CO_2 working fluid; no intermediate heat transport system	Elimination of a chemical interaction between the primary coolant and the working fluid of a power circuit	SSTAR, STAR-LM
12	Natural convection of coolant plus open fuel element lattice (large fuel element pitch to diameter ratio)	Elimination of loss of flow accidents; Prevention of flow blockage accidents	SSTAR, STAR-LM
13	Primary electromagnetic (EM) pumps arranged in two units connected in series, with each unit capable of taking on one half of the pump head	Prevention of loss of flow	4S-LMR
14	Reactor vessel enclosed in a guard vessel to prevent loss of the primary coolant; pool type design with intermediate heat exchangers located inside the main reactor vessel	Prevention of loss of coolant (LOCA)	4S-LMR
15	Use of double piping, double tubes and double vessels for secondary sodium, including heat transfer tubes from the steam generator	Prevention of LOCA Prevention of a sodium-water reaction	4S-LMR
16	Reactor vessel enclosed in a guard vessel such that even in the case of primary vessel boundary rupture, the faulted level of lead will always exceed Pb entrances to the PB to CO_2 heat exchangers; High boiling point of the Pb coolant (1740°C), exceeding the point at which stainless steel core structures melt; Pool type design configuration; High density of Pb coolant limits void growth and downward penetration following a postulated in-vessel heat exchanger tube rupture	Prevention of loss of coolant (LOCA) and its possible consequences	SSTAR, STAR-LM
17	Highly reliable system of control of dissolved oxygen potential in the Pb coolant	Maintenance of the integrity of stainless steel cladding in all modes of operation by preventing corrosion;[b] Prevention of the formation of corrosion debris with a potential to block the coolant area	SSTAR, STAR-LM

[a] 'Passive shutdown' is used to denote bringing a reactor to a safe low power state with balanced heat production and passive heat removal, with no failure of the barriers preventing radioactivity release to the environment. The shutdown should take place using inherent and passive safety features only, with no operator intervention, no active safety systems involved, no requirement for external power and water supplies, and with a practically infinite grace period.

[b] Corrosion/erosion is generally a slow and easily detectable process.

A low pressure primary coolant system, securing low non-nuclear energy stored in the primary coolant system is a common feature of all liquid metal cooled reactors, irrespective of their size and capacity. In addition to this, like many innovative liquid metal cooled reactors of a variety of capacities and sizes, all SMRs considered in this section rely on advanced fuel designs with high thermal conductivity, ensuring increased margins to fuel failure.

The lead cooled SSTAR and STAR-LM reactors incorporate optimum sets of reactivity feedbacks, provided by design and contributing to the elimination of transient overpower, as well as to the prevention or de-rating of the initiating events resulting from malfunctioning of systems or operator actions. Specifically, the designers of the SSTAR and STAR-LM mention the so-called 'passive shutdown' capability of their reactors as provided by design.

TABLE 29. DESIGN FEATURES OF SODIUM COOLED AND LEAD COOLED FAST SMRs CONTRIBUTING TO LEVEL 2 OF DEFENCE IN DEPTH

#	Design feature	What is targeted	SMR designs
1	All-negative temperature reactivity coefficients	Increased self-control of abnormal operation	4S-LMR
2	Large negative feedback in fast spectrum core; natural convection of coolant in all modes; physical properties of Pb coolant and nitride fuel with high heat conductivity	Increased self-control in case of abnormal operation, including passive load following and 'passive shutdown'	SSTAR, STAR-LM
3	Large thermal inertia of the coolant and the shielding structure	Slow pace of transients due to abnormal operation	4S-LMR, SSTAR, STAR-LM
4	Sodium leak detection system in heat transfer tubes of the steam generator, capable of detecting both inner and outer tube failures	Enhanced detection of failure of the secondary sodium boundary	4S-LMR
5	Two redundant power monitoring systems; balance of plant temperature monitoring system; electromagnetic pump performance monitoring system; cover gas radioactivity monitoring system, etc.	Enhanced control of abnormal operation and detection of failure	4S-LMR
6	System of monitoring dissolved oxygen potential in the Pb coolant	Control of the corrosion/erosion processes of stainless steel claddings in Pb flow and detection of failures	SSTAR, STAR-LM
7	Independent and redundant shutdown systems (see Table 30 for details)	Reactor shutdown	All designs

The sodium cooled 4S-LMR provides for power control via pump flow rate in the power circuit, with no control rods in the core, and for pre-programmable movement of axial reflectors with no feedback control, contributing to burnup reactivity compensation. Both of these features contribute to the prevention of transient overpower accidents.

To prevent a sodium-water reaction, the 4S-LMR incorporates an intermediate heat transport system, like most of sodium cooled fast reactors. As the CO_2 is used as a working medium in the power circuits of the SSTAR and STAR-LM, which does not react chemically with Pb, these reactors do not incorporate an intermediate transport system.

Natural convection is used in the SSTAR and STAR-LM to remove heat under normal operation, eliminating loss of flow accidents. De-rating of loss of flow in the 4S-LMR is achieved by a scheme with two electromagnetic pumps connected in series.

Both sodium and lead cooled SMRs incorporate guard vessel to prevent LOCA; the 4S-LMR also incorporates double piping and double vessels for secondary sodium, including heat transfer tubes of the steam generator.

Finally, a reliable system of corrosion control is assumed to be provided for the SSTAR and STAR-LM to maintain the integrity of stainless steel claddings and to prevent the formation of corrosion debris with the potential of coolant area blockage. For these reactors it is important to maintain the oxygen potential in the correct regime to prevent the formation of PbO, which needs to be avoided. There could also be corrosion debris such as Fe that migrates into the coolant where it forms iron oxide, which should be filtered out.

For Level 2 of defence in depth, "Control of abnormal operation and prevention of failure", contributions come from large thermal inertia of the primary coolant system and reactor internals, resulting in the slow progress of transients, and from optimum negative feedback, provided by design and ensuring a high-degree of reactor self-control. Specifically, passive load following and 'passive shutdown' capabilities are mentioned for the SSTAR and STAR-LM. Monitoring and detection systems are other important contributors. Finally,

TABLE 30. DESIGN FEATURES OF SODIUM COOLED AND LEAD COOLED FAST SMRs CONTRIBUTING TO LEVEL 3 OF DEFENCE IN DEPTH

#	Design feature	What is targeted	SMR designs
1	Use of metallic fuel with high thermal conductivity (relatively low temperature)	High margin to fuel failure; larger grace period	4S-LMR
2	Use of nitride fuel with high thermal conductivity (relatively low temperature)	High margin to fuel failure; larger grace period	SSTAR, STAR-LM
3	Relatively low linear heat rate of fuel	Higher margin to fuel failure; larger grace period	4S-LMR
4	All-negative temperature reactivity coefficients	Increased reactor self-control in design basis accidents	4S-LMR
5	Large negative feedback from fast spectrum core, natural convection of coolant in all modes, physical properties of Pb coolant and nitride fuel with high heat conductivity	Increased self-control of the reactor in design basis accidents, including passive load following and 'passive shutdown' (in the case of a failure of both scram systems)	SSTAR, STAR-LM
6	Negative whole core void worth	Prevention of design basis accidents propagation into beyond design basis conditions (due to coolant boiling or loss)	4S-LMR
7	– Very high boiling point of Pb coolant (1740°C); – Escape path for gas/void to reach free surface provided by design; – The reactor vessel is enclosed in a guard vessel such that even in the case of primary vessel boundary rupture, the faulted level of lead will always exceed Pb entrances to the PB to CO_2 heat exchangers	Prevention of core void as the extension of design basis accidents; securing of normal heat removal path through Pb/CO_2 heat exchangers in DBA	SSTAR, STAR-LM
8	Large specific (per unit of power) inventory of the primary coolant	Increased grace period	4S-LMR, SSTAR, STAR-LM
9	Effective radial expansion of the core (negative feedback), provided by design	Increased reactor self-control in design basis accidents; prevention of DBA propagation into beyond design basis conditions	4S-LMR, SSTAR, STAR-LM
10	Low pressure loss in the core region, provided by design	Increased level of natural circulation to remove decay heat from the core	4S-LMR
11	A combined system of electromagnetic pumps and synchronous motors (SM), ensuring favourable flow coast-down characteristics	Increased grace period in the case of pump failure	4S-LMR
12	Natural convection of coolant in all modes of operation plus open fuel element lattice (large fuel element pitch to diameter ratio)	Increased reliability of heat removal through natural convection of coolant via Pb-CO_2 heat exchangers and, in the case of their failure, by natural convection based decay heat removal systems RVACS and DRACS	SSTAR, STAR-LM
13	Two independent systems of reactor shutdown, each capable of shutting down the reactor by: – A drop of several sectors of the reflector; or – Gravity-driven insertion of the ultimate shutdown rod	Reactor shutdown	4S-LMR
14	Two independent and redundant active safety grade shutdown systems	Reactor shutdown[a]	SSTAR, STAR-LM

TABLE 30. DESIGN FEATURES OF SODIUM COOLED AND LEAD COOLED FAST SMRs CONTRIBUTING TO LEVEL 3 OF DEFENCE IN DEPTH (cont.)

#	Design feature	What is targeted	SMR designs
15	Redundant and diverse passive auxiliary cooling systems (RVACS and IRACS or PRACS), both using draught of environmental air as an ultimate heat sink	Increased reliability of decay heat removal from the core	4S-LMR
16	Two or more safety grade independent Direct Reactor Auxiliary Cooling System (DRACS) providing independent paths for decay heat removal. The reactor vessel auxiliary cooling system (RVACS), if present, will be a single safety grade decay heat removal system. If RVACS and DRACS are both present, an even greater diversity is provided. However, if DRACS are effective, the role of RVACS would be reduced. All systems will use natural draught of air as an ultimate heat sink	Increased reliability of decay heat removal from the core (especially when the normal path via Pb-CO_2 heat exchangers becomes unavailable)	SSTAR, STAR-LM
17	Use of double piping, double tubes and double vessels for the secondary sodium, including heat transfer tubes of the steam generator	Prevention of steam generator tube rupture, sodium-water reaction, and pressure increase in the intermediate heat transport system	4S-LMR
18	Passive pressure relief from the primary coolant system	Protection of the reactor vessel and enclosure from over-pressurization when one or more in-vessel Pb to CO_2 heat exchanger tubes fail	SSTAR, STAR-LM

[a] It is noted that the operation of these systems may actually be unnecessary because the inherent and passive features are in any case capable of ensuring a 'passive shutdown', i.e., bringing the reactor to a safe low power state with balanced heat production and passive heat removal, with no failure of the barriers preventing radioactivity release to the environment, and with a practically indefinite grace period.

independent and redundant active or passive shutdown systems are available for cases in which all other measures of control and prevention turn out to be ineffective.

For Level 3 of defence in depth, "Control of accidents within design basis", the contribution comes from the following main groups of design features:

(1) Inherent safety features, highlighted in numbers 1–8 of Table 30. In addition to the features already discussed in conjunction with defence in depth Levels 1 and 2, it is important to note negative whole core void worth provided by design in the 4S-LMR and inherent features of the lead cooled SSTAR and STAR-LM, practically eliminating the option of coolant boiling or gas bubbles arriving at the core (preventing the propagation of a design basis accident into a severe accident with transient overpower);
(2) By-design provisions for certain passive mechanisms such as radial expansion or enhanced levels of natural convection in the primary coolant system, highlighted in numbers 9–12 of Table 30;
(3) Two independent systems of reactor shutdown, provided in each design; see numbers 13–14 of Table 30. These operate based on gravity in the 4S-LMR, while in the SSTAR and the STAR-LM both systems are active and safety grade. For the SSTAR and STAR-LM, it is mentioned that the operation of these systems may actually be unnecessary because inherent and passive features are in any case capable of ensuring a 'passive shutdown' of the reactor;
(4) Not less than two redundant and diverse passive decay heat removal systems in each design, with some of them, possibly, providing several passive decay heat removal paths, and all using natural draught of air as an ultimate heat sink; see numbers 15–16 of Table 30;
(5) Special design features provided to prevent or mitigate the effects of pressurized medium from the power circuit getting into the primary circuit; see numbers 17–18 of Table 30.

TABLE 31. DESIGN FEATURES OF SODIUM COOLED AND LEAD COOLED FAST SMRs CONTRIBUTING TO LEVEL 4 OF DEFENCE IN DEPTH

#	Design feature	What is targeted	SMR designs
1	Inherent safety features of a metal or nitride fuelled core, such as high thermal conductivity and low accumulated enthalpy	Prevention of core melting	4S-LMR, SSTAR, STAR-LM
2	Large negative feedback from a fast spectrum core, natural convection of coolant in all modes, physical properties of Pb coolant and nitride fuel with high heat conductivity	Prevention of core melting	SSTAR, STAR-LM
3	Relatively low linear heat rate of fuel	Prevention of core melting	4S-LMR
4	Large specific (per unit of power) inventory of the primary coolant, contributing to high heat capacity of the primary coolant system	Increased capability of the coolant system to absorb heat; prevention of core melting	4S-LMR, SSTAR, STAR-LM
5	Negative whole core void worth	Prevention of transient overpower in the case of coolant boiling or void penetration to the core	4S-LMR, SSTAR[a]
6	Redundant and diverse passive auxiliary cooling systems (RVACS and IRACS or PRACS), both using draught of environmental air as an ultimate heat sink	Increased reliability of decay heat removal from the core	4S-LMR
7	Two redundant and diverse passive decay heat removal systems, reactor vessel auxiliary cooling system (RVACS) and, perhaps, direct reactor auxiliary cooling system (DRACS), both using draught of environmental air as an ultimate heat sink	Increased reliability of decay heat removal from the core	SSTAR, STAR-LM
8	Effective mechanism of fuel carry-over from the core in the case of fuel element cladding failure	Prevention of recriticality	4S-LMR
9	High effective density of the Pb coolant (~11 g/cm^3) plus pool type design	In the case of melting, fuel is moved to an upper free level of lead, preventing recriticality	SSTAR, STAR-LM
10	Fast acting system of sodium drain from the steam generator to the dump tank	Mitigation of a sodium-water reaction	4S-LMR
11	Reactor vessel enclosed in a guard vessel to prevent loss of primary sodium; pool type design with intermediate heat exchangers located inside the main reactor vessel	Prevention of radioactivity release to the environment	4S-LMR
12	Use of double piping, double tubes and double vessels for secondary sodium, including heat transfer tubes of the steam generator	Prevention of radioactivity release to the environment	4S-LMR
13	The guard vessel surrounds the reactor vessel, and an upper enclosure head covers both the reactor vessel and the guard vessel. A hermetic seal is established between the upper closure head and the guard vessel. In the event of a rupture of one or more Pb to CO_2 heat exchangers, CO_2 would vent through an upper closure head into the volume of the containment structure	Prevention of radioactivity release to the environment; securing of the integrity of the reactor vessel and a heat removal path contributing to core melt prevention	SSTAR, STAR-LM
14	The containment	Prevention of radioactivity release to the environment	4S-LMR, SSTAR, STAR-LM
15	Reactor located in a concrete silo below ground level	Prevention of radioactivity release to the environment	4S-LMR, SSTAR, STAR-LM

[a] In both the SSTAR and STAR-LM, generation of void in the core is practically excluded by design; in addition to this, Pb boiling temperature (1740°C) exceeds the melting temperature of core structures made of stainless steel.

The 4S-LMR incorporates no active safety systems. However, there are several active systems providing normal operation of the reactor at rated or de-rated power, e.g., electromagnetic pumps providing forced convention of sodium coolant to remove core heat, or a burnup reactivity compensation system based on slow upward movement of the reflector, using an advanced pre-programmed drive mechanism. These systems can contribute to performing safety functions in certain accident scenarios. No information was provided on which systems of the 4S-LMR are safety grade.

All passive and active safety systems in the SSTAR and the STAR-LM are assumed to be safety grade.

The design features contributing to Level 4 of defence in depth, "Control of severe plant conditions, including prevention of accident progression and mitigation of consequences of severe accidents" fit in the following main groups; see Table 31:

(1) Inherent safety features contributing to prevention of core melting, numbers 1–5 of Table 31;

(2) Redundant and diverse passive decay heat removal systems with natural draught of air used as an ultimate heat sink, discussed in more detail in conjunction with Level 3 of defence in depth;

(3) Inherent and passive design features for the prevention of recriticality, numbers 8–9 of Table 31. These include an effective mechanism of fuel carry-over from the core in case of fuel element cladding failure (4S-LMR) and high density of the Pb coolant securing movement of molten fuel to the upper free level of lead (SSTAR and STAR-LM);

(4) Guard vessels in addition to the main vessels, for all designs, and double piping for the 4S-LMR; see numbers 11–13 of Table 31;

(5) Location of the containment and reactor in a concrete silo below ground level, for all designs considered.

For Level 5 of defence in depth, "Mitigation of radiological consequences of significant release of radioactive materials", the designers of the 4S-LMR foresee no measures needed beyond the plant boundary in response to any severe accidents or combinations thereof, even when there is no operator intervention, no emergency team actions, and no external power and water supply. The designers of the SSTAR and STAR-LM take a more conservative approach, suggesting that standard measures may still be applicable, but within the exclusion zone reduced against that of present day reactors; see Table 32 and Table 35.

Issues of achieving plant licensing with reduced off-site emergency planning requirements are discussed in more detail in section 3.2.1., in conjunction with measures planned in response to severe accidents for pressurized water type SMRs. This discussion is also relevant to sodium cooled and lead cooled fast reactors considered in this section.

Tables 33 and 34 summarize the information on design basis and beyond design basis accidents and acceptance criteria.

TABLE 32. DESIGN FEATURES OF SODIUM COOLED AND LEAD COOLED FAST SMRs CONTRIBUTING TO LEVEL 5 OF DEFENCE IN DEPTH

#	Design feature	What is targeted	SMR designs
1	Inherent and passive safety features ensure the plant will survive all postulated design basis and beyond design basis accidents, including anticipated transients without scram and combinations thereof, without operator intervention, emergency team actions, and external power and water supply	Eliminate the need for any intervention in the public domain beyond plant boundaries as a consequence of any accident condition within the plant	4S-LMR
2	Inherent and passive safety features ensure lower probability of radioactivity material release to the environment (compared to present day light water reactors)	To reduce the exclusion zone compared to that provided for currently operated reactors	SSTAR, STAR-LM

TABLE 33. SUMMARY OF DESIGN BASIS AND BEYOND DESIGN BASIS EVENTS, INCLUDING THOSE SPECIFIC FOR A PARTICULAR SMR

SMR design	Lists of initiating events	Events specific to a particular SMR
4S-LMR	Lists of initiating events for DBA and BDBA have been defined and are presented as a summary or examples (Annex VIII). The events were identified systematically based on consideration of the 4S operation cycle and events postulated for the MONJU and DFBR sodium cooled fast reactors (Japan). The lists of events typical of LWRs were also taken into account. On a broad scale, the BDBA are divided into two big groups that are anticipated transients without scram (ATWS) and accidents without scram (AWS). The ATWS comprise the sequences in which one of the reactor shutdown systems does not operate for any reason. The AWS includes sequences more severe than ATWS, such as failure of more than one redundant system, e.g. failures of both pumps, both shutdown systems, and one or both of the decay heat removal systems	– Failure in insertion of the ultimate shutdown rod; – Failure in the operation of pre-programmed moveable reflector
SSTAR, STAR-LM	With the new 10 CFR Part 53 regulation being considered currently (see Annex IX), a limited set of traditional design basis accidents have been identified, including loss of heat sink, in-vessel heat exchanger tube rupture, transient overcooling, transient overpower/reactivity insertion, and loss of load; The list of beyond design basis accidents has also been identified that includes failure to scram due to the assumed failure of both safety grade active shutdown systems	– Cessation of heat removal from in-vessel heat exchangers by CO_2 working fluid with or without scram; – Transient overcooling due to initiating event on supercritical CO_2 Brayton cycle secondary side

TABLE 34. SUMMARY OF ACCEPTANCE CRITERIA

SMR design	Deterministic acceptance criteria	Probabilistic acceptance criteria (or targets)
4S-LMR	Acceptance criteria for DBA are based on the experience with conventional light water reactors and previous design experience with sodium cooled fast reactors; specifically, the criteria that have been applied in the Clinch River Breeder reactor project are used (see Annex VIII); Acceptance criteria for ATWS and AWS are presented explicitly; see Annex VIII.	The acceptance criteria for DBA are risk-informed, as indicated by Table VIII-4 in Annex VIII, and envelop both normal operation, anticipated events and unlikely and very unlikely events (frequency down to 10^{-6}/year), which in the 4S are treated as design basis events; The acceptance criteria for ATWS and AWS are specified in a deterministic way, with no frequency being indicated.
SSTAR, STAR-LM	It is expected that development of the SSTAR (and even more so the STAR-LM) would take place on a timescale consistent with application of the new risk-informed and technology-neutral 10 CFR 53 regulations, which would provide a basis for the definition of acceptance criteria. No further details have been provided.	

Table 33 also lists the features that are specific for the considered SMRs but not for a reactor line as a whole. For the sodium cooled 4S-LMR, these are failure in insertion of the ultimate shutdown rod and failure in the operation of the pre-programmed moveable reflector, in view of the fact that these design features are unique to the 4S-LMR. As both SSTAR and STAR-LM are being designed with a non-conventional CO_2 based Brayton cycle power circuit, specific events are indicated as those related to disruption in the operation of this power circuit.

The 4S-LMR appears to be the only SMR concept in this report for which the acceptance criteria for design basis accidents are specified in a risk-informed way; see Annex VIII. Addressed within the design basis are events with a frequency as low as $10^{-6} \times 1$/year. In contrast, the acceptance criteria for severe accidents, which

in the case of the 4S-LMR include extremely rare failures of more than one redundant system, are specified in a deterministic way, with no frequency indicated.

For the SSTAR and STAR-LM, an expectation of new technology neutral and risk informed regulations to arrive in time for design completion is mentioned, but no details are provided regarding the acceptance criteria themselves.

Table 35 summarizes design features for protection against external event impacts, while Table 36 lists measures foreseen in response to severe accidents.

For both the 4S-LMR and the SSTAR and STAR-LM, strong reliance on inherent and passive safety features expected to render unnecessary operator intervention, emergency team actions and external power and water supplies, while ensuring a 'passive shutdown' capability of the reactor, are mentioned as factors important for protection against both internal and external event impacts and combinations thereof.

The design features of sodium cooled and lead cooled fast SMRs addressed in this report fit in within the fundamental requirements suggested in the IAEA safety standard Safety of Nuclear Power Plants: Design Requirements [7].

However, all considered fast spectrum SMR designs are being developed to offer several unique qualities, such as:

(1) A 'passive shutdown' capability, i.e., the capability to bring the reactor to a safe low power state with balanced heat production and passive heat removal, and with no failure to barriers preventing radioactivity release to the environment; all relying on inherent and passive safety features only, and with practically indefinite grace period;

TABLE 35. SUMMARY OF DESIGN FEATURES FOR PROTECTION AGAINST EXTERNAL EVENT IMPACTS

SMR design	Aircraft crash / Earthquakes	Other external events
4S-LMR	The reactor vessel is located in a shaft below the ground level, which, together with the containment and a relatively small footprint of the plant, contributes to increased protection against aircraft crash. The reactor building is isolated horizontally by seismic isolators; the 'tiny' shaped reactor results in a higher characteristic frequency; thus, the design is expected to be rigid against a vertical shock	The capability of the plant to survive all postulated accidents relying only on inherent and passive safety features without the need for operator intervention, emergency team actions, and an external power and water supply, is rated as an important feature contributing to protection of the plant against external event impacts. No further details were provided
SSTAR, STAR-LM	The reactor vessel is located in a shaft below the ground level, which, together with the containment and a relatively small footprint of the plant, contributes to increased protection against aircraft crash. No information was provided regarding seismic design	The capability of passive load following and 'passive shutdown' provided by inherent and passive safety features could be viewed as an important feature contributing to protection of the plant against external event impacts. No further details were provided

TABLE 36. SUMMARY OF MEASURES PLANNED IN RESPONSE TO SEVERE ACCIDENTS

SMR design	Measures
4S-LMR	Safety analyses have shown that 4S-LMR fuel never melts under any hypothetically postulated conditions, such as ATWS or AWS. Some fuel pins with maximum cladding temperature might fail in more severe AWS events; Analyses performed for hypothetical conditions when all fuel element claddings fail show the dose equivalent to be 0.01 Sv at a distance of 20 m from the reactor. No measures beyond this boundary are required
SSTAR, STAR-LM	It is envisioned that the exclusion zone for SSTAR and STAR-LM may at least be reduced in size as a result of inherent safety features and the expected low probability of radioactive material release relative to light water reactor designs with a similar power level. No further details were provided

(2) Very low pressure in the primary coolant system, challenging the notion of a primary pressure boundary used throughout the safety standard [7];
(3) Design basis events encompassing events with occurrence frequencies as low as 10^{-6} 1/year and including combinations of unprotected transients [2, 3], each of which is rated severe for the current generation of light water reactors.

The designers of fast spectrum SMRs target licensing within the currently established national regulatory framework but mention that further elaboration of national regulatory norms toward technology-neutral and risk-informed approach could facilitate licensing considerations and further design improvements.

As an example, the recently published IAEA report Proposal for a Technology-Neutral Safety Approach for New Reactor Designs [13] suggests that "the means for shutting down the reactor shall consist of a minimum of two lines of protection (shutdown mechanisms — whether they be control rods or inherent feedback features of the core design) required to achieve the mission within the reliability requirements for safety".

3.2.5. Non-conventional designs

Non-conventional designs are represented in this report by the Compact High Temperature Reactor (CHTR) concept of a small very high temperature reactor developed by the Bhabha Atomic Research Centre (BARC) of India. Description of the passive safety design features of the CHTR is provided in Annex X; more detailed design description of the CHTR is given in the report [3].

The CHTR, with 100 kW(th), is being designed as a semi-autonomous 'power pack' for operation in remote areas and, specifically, for advanced non-electrical applications, such as hydrogen production. The CHTR could also be viewed as a prototype of somewhat larger, but still fitting into a SMR range, future reactors. It is a non-conventional reactor merging the technologies of high temperature reactors with pin-in-block type TRISO fuel and lead-bismuth cooled reactors. The core uses ^{233}U-Th based fuel of HTGR type with BeO moderator blocks, while the coolant is lead-bismuth eutectic. The reactor has an essentially thermal spectrum of neutrons and uses heat pipe systems to deliver heat to process heat applications, as well as to remove heat from the core during postulated accident conditions.

Figure 11 shows a schematic of the CHTR primary circuit loop.

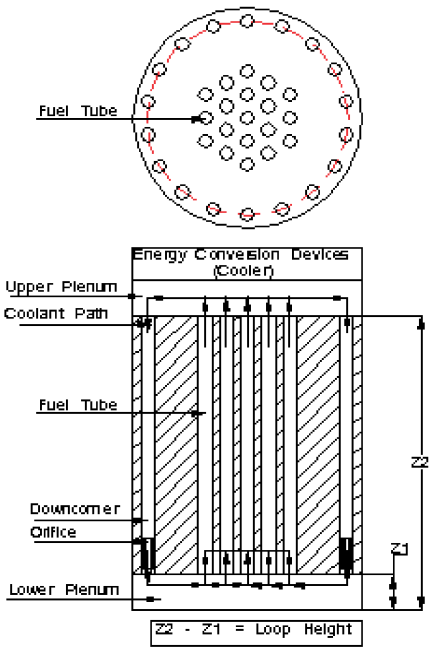


FIG. 11. Schematic view of CHTR primary circuit loop.

Tables 37 to 41 summarize the design features of the CHTR contributing to different defence in depth levels.

The design features contributing to Level 1 of defence in depth, "Prevention of abnormal operation and failure", listed in Table 37, are intended to provide high margins to fuel failure, a low overall reactivity margin in the reactor core, and to exclude loss of flow accidents by relying on heat removal by natural circulation in all operation modes.

To achieve Level 2 of defence in depth, "Control of abnormal operation and detection of failure", there are negative reactivity effects, high thermal inertia of the core structures, a passive power regulation system (based on a gas expansion device), and two independent passive shutdown systems; see Table 38. It is remarkable that the objectives of Level 2 of defence in depth are expected to be fully met by passive means, independent of operator intervention.

For Level 3 of defence in depth, "Control of accidents within design basis", there are three groups of features that make a major contribution:

(1) Inherent safety features, provided by design and intended to prevent accident propagation into BDBA conditions, with an increased grace period; see numbers 1–2 of Table 39;
(2) Three independent passive systems for heat removal in postulated accident conditions, two based on heat pipes, and one providing for the filling of the gas gap around the reactor by lead-bismuth to increase heat conductivity and facilitate heat removal to the environment. Of these, one heat pipe based system and the system based on gas gap filling, are dedicated passive safety systems; another heat pipe based system is a normal operation heat removal system capable of carrying out a safety function in accidents;

TABLE 37. DESIGN FEATURES OF CHTR CONTRIBUTING TO LEVEL 1 OF DEFENCE IN DEPTH

#	Design feature	What is targeted
1	Low core power density	Prevention of failure through increased temperature margin; lower non-nuclear (thermal) energy stored in the core
2	Heat removal from the core by natural circulation under normal operating conditions	Elimination of loss of flow accidents
3	Low overall reactivity margin of the reactor core, provided by design and, specifically, by the use of burnable poison to compensate for reactivity change due to fuel burnup	Limitation of the scope of transient overpower accidents due to inadvertent control rod withdrawal by reducing the worth of control rods
4	Use of an all-ceramic core with high heat capacity and high temperature margins	Prevention of failure through increased temperature margins

TABLE 38. DESIGN FEATURES OF CHTR CONTRIBUTING TO LEVEL 2 OF DEFENCE IN DEPTH

#	Design feature	What is targeted
1	Negative reactivity effects (void, power, temperature, etc.) achieved with the use of the lead-bismuth coolant; specifically, high negative Doppler coefficient, achieved through the selection of an appropriate fuel composition	Higher degree of reactor self-control in abnormal operation
2	Use of an all-ceramic core with high heat capacity and high temperature margins	Slow progression of transients due to abnormal operation, simplification of control
3	Increased reliability of the control system achieved through the use of a passive power regulation system; this system passively inserts negative reactivity to the core when temperature increases beyond allowable limits	Passive control of power and temperature
4	The use of two independent passively operating shutdown systems	Prevention of abnormal operation progression into a design basis accident

TABLE 39. DESIGN FEATURES OF CHTR CONTRIBUTING TO LEVEL 3 OF DEFENCE IN DEPTH

#	Design feature	What is targeted
1	Very high boiling point of the Pb-Bi coolant (1670°C)	Prevention of coolant boiling in design basis accidents that otherwise might result in accident propagation to beyond design basis conditions
2	The use of a high heat capacity ceramic core	Increased grace period
3	The use of two independent passive systems to transfer reactor core heat to the outside environment, one comprising a gas gap filling system, and the other a heat pipe based system	Increased reliability of heat removal from the reactor core in design basis accidents
4	The use of an independent system based on carbon-carbon composite heat pipes to transfer heat from the reactor core to the atmosphere in the case of a loss of coolant (in addition to the two systems mentioned in item 2[a])	Increased reliability of heat removal from the reactor core in design basis accidents
5	The use of two independent shutdown systems, one comprising passively activated gravity driven drop of mechanical shut-off rods, and the other employing temperature feedback gas expansion	Reactor shutdown

[a] Each of the indicated passive decay heat removal systems is capable of dissipating 200% of the rated reactor power

TABLE 40. DESIGN FEATURES OF CHTR CONTRIBUTING TO LEVEL 4 OF DEFENCE IN DEPTH

#	Design feature	What is targeted
1	Low pressure of the Pb-Bi coolant; coolant flows out very slowly in the case of a break of the primary boundary and eventually solidifies	Prevention of radioactivity release to the environment through reliance on relatively low non-nuclear energy stored in the primary coolant system
2	Proven fission product confinement capability of the TRISO coated particle fuel at high temperatures (1600°C in the long term and up to 2100°C in the short term)	Prevention of core melting; and Limitation of fission product release in severe accidents
3	Large heat capacity of the ceramic core	Slow fuel temperature rise with more than 50 minutes available even when all heat sinks are lost
4	The use of heat sink located outside of the outer steel shell of the reactor	Increased reliability of heat removal in severe accidents
5	Reactor located in an underground pit and covered by a reinforced concrete barrier (the confinement structure); additionally, a steel vessel is foreseen	Prevention of radioactivity release to the environment; protection from the impacts of severe external events
6	High density of Pb-Bi coolant, comparable to the density of the fuel	Prevention of re-criticality — in the case of a severe accident with fuel failure, the fuel would be carried over to the upper part of the reactor, preventing re-criticality

TABLE 41. DESIGN FEATURES OF CHTR CONTRIBUTING TO LEVEL 5 OF DEFENCE IN DEPTH

#	Design feature	What is targeted
1	Passive safety design features contributing to Levels 1–4 of defence in depth are expected to prevent any significant release of radioactive materials in any design basis and beyond design basis accident	No evacuation or relocation measure needed outside of the plant boundary

(3) Two independent passive shutdown systems, one based on the passively activated gravity driven drop of mechanical rods, and the other using the effects of a temperature feedback gas-expansion to increase neutron leakage from the core and insert negative reactivity.

All passive safety systems of the CHTR are safety grade. The CHTR active safety systems, which are the reset systems of passive shutdown and passive gas gap heat removal, as well as the system of liquid metal draining from the gas gaps to a reservoir, and a defuelling and refuelling system, are all non-safety-grade.

For Level 4 of defence in depth, "Control of severe plant conditions, including prevention of accident progression and mitigation of consequences of severe accidents", intrinsic features are in place, such as low Pb-Pi coolant pressure; proven fission product confinement capability of the high temperature HTGR type fuel, and; large heat capacity of the ceramic core ensuring slow fuel temperature rise even if all heat sinks are lost; see numbers 1–3 of Table 39. In addition to this, heat sink is located outside of the outer steel shell of the reactor, and the reactor itself is located in an underground pit covered by a reinforced confinement structure. The steel shell (vessel) of the reactor is expected to act as a second containment. Finally, as with lead cooled fast reactors, re-criticality is prevented by high density of the Pb-Bi coolant via passive carry over of molten fuel or fuel debris to the upper part of the reactor.

The designers of the CHTR rate passive safety design features contributing to Levels 1–4 of defence in depth as sufficient to meet the objective of defence in depth Level 5; see Table 41.

Issues of achieving plant licensing with reduced off-site emergency planning requirements are discussed in more detail in Section 3.2.1., in conjunction with measures planned in response to severe accidents for pressurized water type SMRs. This discussion is also relevant to reactors of non-conventional design considered in this section.

Tables 42 and 43 summarize information provided by the designers of the CHTR on design basis and beyond design basis events and on the corresponding acceptance criteria.

Table 44 summarizes the design features of the CHTR contributing to plant protection against external event impacts, while Table 45 summarizes measures planned in response to severe accidents.

Seismic design of the CHTR corresponds to the recommendations of IAEA safety standards [8]. Protection against aircraft crash is provided by locating the reactor in an underground pit with low exterior profile of the reactor building. Additionally, the reactor would be provided with a low leakage thick steel vessel to absorb energy in case of a postulated aircraft impact. This leaktight vessel with minimum penetrations is also meant to provide protection against flooding. The reactor, including the steel vessel, is located in the reinforced confinement structure.

TABLE 42. SUMMARY OF DESIGN BASIS AND BEYOND DESIGN BASIS EVENTS FOR CHTR, INCLUDING THOSE SPECIFIC FOR A PARTICULAR SMR

SMR design	Lists of initiating events	Events specific to a particular SMR
CHTR	A preliminary list of design basis and beyond design basis events has been compiled, with a short summary provided in Annex X	Nothing in particular has been specified (apparently, because the CHTR concept is unique and has no analogues)

TABLE 43. SUMMARY OF ACCEPTANCE CRITERIA

SMR design	Deterministic acceptance criteria	Probabilistic acceptance criteria (or targets)
CHTR	Top level acceptance criteria for DBA and BDBA have been formulated, see Annex X	The probability of unacceptable radioactivity release beyond the plant boundary is targeted at less than 1×10^{-7}/year

TABLE 44. SUMMARY OF DESIGN FEATURES FOR PROTECTION AGAINST EXTERNAL EVENT IMPACTS

SMR design	Aircraft crash / Earthquakes	Other external events
CHTR	For protection against aircraft crash and missiles, the CHTR would be installed in an underground pit with low exterior profile of the reactor building; additionally, the reactor would be first provided with a low leakage thick steel vessel to absorb energy in the case of a postulated aircraft impact. CHTR structures, systems and components are being designed for high level and low probability seismic events such as operating basis earthquakes (OBE) and safe shutdown earthquakes (SSE); seismic isolators and dampers are also planned	Design features for protection against the impacts of natural and human induced external events are described in detail in [6]. The external events considered in plant design include earthquakes, aircraft crash, cyclones, and flooding. For protection against flooding, the reactor would be provided with a low leakage thick steel vessel with a reduced number and size of penetrations; additional water tight barriers and a duct would be provided for systems communicating to the control room

TABLE 45. SUMMARY OF MEASURES PLANNED IN RESPONSE TO SEVERE ACCIDENTS

SMR design	Measures
CHTR	The safety analyses performed indicate the inherent and passive features of the CHTR might be able to prevent the TRISO coated particle fuel from exceeding the limiting temperatures in postulated accidents. The design objective is that no emergency evacuation or relocation measures in the public domain would be required

A design objective of the CHTR is that no emergency evacuation or relocation measures in the public domain would be required in any accidents without operator intervention and emergency team actions, and without external water and power supplies.

According to its designers, the CHTR is being developed in line with the recommendations of IAEA safety standard NS-R-1 Safety of the Nuclear Power Plants: Design Requirements [7], which is the basis for currently adopted national nuclear regulations in India. In view of the designers, further design development could be facilitated by technology neutral revisions of the indicated standard, such as suggested in the recently published IAEA-TECDOC-1570 Proposal of a Technology-Neutral Safety Approach for New Reactor Designs [13]. In addition to this, the risk-informed approach suggested in the above mentioned document includes quantitative safety goals linked to defence in depth levels which could facilitate assessment of claimed qualities of the CHTR, such as absence of the need for off-site emergency planning and reactor self-control in accidents relying on the inherent and passive safety features only, as provided by design.

4. BENEFITS AND NEGATIVE IMPACTS ARISING FROM THE INCORPORATION OF INHERENT AND PASSIVE SAFETY DESIGN FEATURES INTO SMRs

Discussed below are the specific positive and negative effects of incorporating inherent and passive safety design features that, in view of the SMR designers, affect plant characteristics in areas other than safety.

4.1. WATER COOLED SMRS

Table 46 summarizes the positive and negative effects of the inherent and passive safety design features of pressurized water type SMRs in areas other than safety, based on inputs provided by SMR designers in Annexes I–V of this report.

As can be seen from Table 46, relying more on inherent and passive safety features and passive safety systems as compared to traditional solutions based on active safety systems is in all cases a trade-off regarding plant economy.

TABLE 46. SUMMARY OF POSITIVE AND NEGATIVE EFFECTS FROM INCORPORATION OF INHERENT AND PASSIVE SAFETY DESIGN FEATURES INTO PRESSURIZED WATER TYPE SMRs — AREAS OTHER THAN SAFETY

#	Design feature	Positive effects	Negative effects	SMR designs
1	Elimination of liquid boron reactivity control system	– Decrease in capital and operation costs; plant simplification; – Relaxed concerns with relation to human actions of a malevolent character	Certain deterioration of fuel cycle characteristics	KLT-40S, CAREM-25, SCOR
2	Integral primary circuit with internal steam generators and control rod drives	– Core damage frequency (CDF) and large early release frequency (LERF) are reduced, allowing the economy of twin unit and multiunit plants and, potentially, positive economic effects from reduced or eliminated emergency planning;	Increased cost owing to the limited power of a single module[a]	IRIS, CAREM-25, SCOR
		– Decreased plant costs, resulting from a compact primary circuit, the use of a compact steel containment, and a reduced siting area;	Increased cost of a larger reactor pressure vessel[b]	IRIS, SCOR
		– Reduced operation and maintenance costs resulting from simplified operation and maintenance;		IRIS
		– Higher capacity factor;		IRIS
		– Possibly reduced security costs resulting from ‘inherent security’		IRIS
		– Certain economic benefits achieved via longer reactor pressure vessel lifetime owing to a reduced fast neutron fluence		CAREM-25, IRIS
		– Reduced plant costs resulting from simplification of certain safety systems		CAREM-25, IRIS
3	Modular design of the reactor unit	Decrease in plant costs resulting from compactness of the reactor unit and smaller dimensions of the containment	Certain deterioration of maintainability as compared to loop type plants	KLT-40S
4	Totally leaktight reactor coolant system	Decrease in the operation costs resulting from a decrease in the amount of radioactive waste		KLT-40S

TABLE 46. SUMMARY OF POSITIVE AND NEGATIVE EFFECTS FROM INCORPORATION OF INHERENT AND PASSIVE SAFETY DESIGN FEATURES INTO PRESSURIZED WATER TYPE SMRs — AREAS OTHER THAN SAFETY (cont.)

#	Design feature	Positive effects	Negative effects	SMR designs
5	Primary coolant pressure boundary enclosed in a pressurized low enthalpy water containment	– Could facilitate cost reduction via plant licensing without off-site emergency planning; – Complicates unauthorized access to fuel.	Negatively affects plant costs via the incorporation of: – Additional pressure vessel; – Control rod drive mechanisms able to operate in cold water; – Complicates plant maintainability through lower accessibility of the primary pressure boundary	MARS
6	Reduced number of safety grade systems and components requiring maintenance	Improved plant economy owing to simplified operation and maintenance and reduced operation waste		MARS
7	Incorporation of passive safety systems		Increase in plant construction and maintenance costs	KLT-40S
8	Use of self-actuated devices in passive systems		Increase in plant construction and maintenance costs	KLT-40S
9	All safety grade safety systems are passive	– Reduced operation and maintenance costs resulting from reduced complexity and improved reliability of the plant; – Added resilience to sabotage and other malevolent actions		IRIS
10	Natural convection of the coolant	Reduced operation and maintenance costs owing to design simplification and elimination of main coolant pumps	Increased specific cost of reactor pressure vessel; potentially increased complexity of reactor operation (startup, etc.)	CAREM-25
11	Increased reliance on natural convection of the coolant	Decrease in costs owing to simplified operation and maintenance	Increased specific cost of reactor pressure vessel; potentially increased complexity of reactor operation (startup, etc.)	SCOR
12	Relatively low core power density and coolant temperature facilitating the use of a passive emergency core cooling system with an infinite grace period, actuated upon flow rate decrease	Essential simplification of design, with cost savings	Increased plant costs owing to limited reactor power and energy conversion efficiency	MARS

[a] With a potential of being counteracted by modular construction of multiple units at a site.
[b] Counteracted by reduced containment size and reduced plant footprint.

Regarding solutions intended to eliminate certain types of accidents or prevent their consequences through design features, see numbers 1–6 of Table 46. The commonly mentioned expected benefits are:

- Decrease in plant capital costs due to compact primary circuit and compact containment (except for the MARS);
- Decrease in plant capital costs due to simplicity of operation and maintenance, specifically due to a reduction of the number of systems requiring maintenance;
- Decrease in plant capital costs due to elimination or reduction of off-site emergency planning;
- Decrease in plant capital costs via an enhanced option to build several plants at a site or to use twin or multiple unit plants, owing to decreased core damage frequency and large early release frequency;
- Less concern regarding human actions of a malevolent character and, potentially, cost reduction resulting from 'inherent security' of the plant.

At the same time, the same solutions are expected to result in the following negative implications:

- Increased plant capital costs owing to the limited power of a single module (potentially counteracted by modular construction of multiple units at a site);
- Increased cost of a larger reactor pressure vessel (or additional pressure vessel in the case of the MARS design);
- Certain deterioration of burnup cycle characteristics (for example, when the liquid boron system is abandoned) or maintainability (for the compact modular design of the KLT-40S and for the MARS design with an additional pressure vessel).

In nearly all cases, the above mentioned benefits and disadvantages have a potential to counteract each other; for example, increased specific capital costs for a single unit plant could possibly be counteracted by modular construction of multiple units at a site; increased vessel costs could be counteracted by reduced containment costs; and certain deterioration of maintainability could be counteracted by a reduced number of systems needing maintenance.

Regarding positive and negative impacts resulting from the application of passive safety systems, the opinions of SMR designers may vary. For example, designers of the KLT-40S see only negative cost implications with use of passive safety systems, such as increased construction and maintenance costs; see numbers 7–8 of Table 46. Designers of the IRIS see only positive cost implications with use of passive safety systems, such as reduced operation and maintenance costs and enhanced resilience to sabotage; see number 9 of Table 46. Other designers mention both positive and negative features. The opinion of designers may also be conditioned by a specific passive safety system type, i.e., expectations might be different for, say, a gravity driven passively actuated shutdown system and a natural convection based decay heat removal system.

4.2. PRESSURIZED LIGHT WATER COOLED HEAVY WATER MODERATED REACTORS

Table 47 summarizes the positive and negative implications of the inherent and passive safety design features of the AHWR in areas other that safety, based on inputs provided by the AHWR designers in Annex VI to this report.

As can be seen from Table 47, designers of the AHWR foresee both positive and negative impacts on plant economy resulting from core cooling by natural convection in all modes. Simplified design and maintenance and elimination of pumps, and the resulting reduced power requirements for a plant's own needs are positives regarding plant economy, while increased diameter and length of piping are on the negative side.

TABLE 47. SUMMARY OF POSITIVE AND NEGATIVE EFFECTS FROM INCORPORATION OF INHERENT AND PASSIVE SAFETY DESIGN FEATURES INTO THE AHWR — AREAS OTHER THAN SAFETY

#	Design feature	Positive effects	Negative effects
1	Core cooling by natural convection	– Simplifies design and maintenance, eliminates nuclear grade main circulating pumps, their drives and a control system, contributing to reduced plant cost; – Reduces the power requirement for plant operation, resulting in higher net plant efficiency and lower specific capital cost	Increased diameter and length of piping with associated increase in plant costs

4.3. HIGH TEMPERATURE GAS COOLED REACTORS

Table 48 summarizes the positive and negative effects of inherent and passive safety design features of the GT-MHR in areas other that safety, based on inputs provided by GT-MHR designers in Annex VII of this report.

Although it was not requested in the suggested format, designers of the GT-MHR apparently base their judgement on a comparison between typical light water reactors and the GT-MHR. The reason seems to be that all HTGR designs incorporate somewhat similar inherent and passive safety design features, with no active system based HTGR alternative being available for comparison [2]. Within the comparison as it was done, all major departures of a HTGR from a light water reactor (LWR) result in a plant cost increment. Such departures include the use of helium and graphite, annular design of the reactor core, the use of TRISO coated particle fuel, and use of the containment designed to retain helium-air fluid, as well as to withstand external loads; see Table 48. Positive impacts in plant costs are expected from the elimination of large diameter piping in the primary circuit and from the absence of steam generators.

In addition to what is suggested by the designers in Annex VII and in Table 1, it can be recalled that the above mentioned departures of the GT-MHR (and HTGRs in general) from LWRs could enable an increase in plant efficiency of up to ~50% against ~32% in LWRs, which is probably enough to counteract the cost penalties specified in Table 48. Also, it may be recalled that nearly all HTGRs provide for multimodule plant configurations [2], yet another factor capable of counteracting the above mentioned cost increases for a single module plant.

4.4. SODIUM COOLED AND LEAD COOLED FAST REACTORS

Table 49 summarizes the positive and negative effects of the inherent and passive safety design features of the sodium cooled and lead cooled fast SMRs in areas other that safety, based on inputs provided by the designers in Annex VIII and Annex IX of this report.

As seen in Table 49, designers of the 4S-LMR have provided no information regarding positive or negative effects of inherent and passive safety design features in areas other than safety, so that inputs to this table are limited to those for the lead cooled SSTAR and STAR-LM — the concepts that are still at a feasibility study stage. As in the case of HTGRs, the table incorporates an implicit comparison with present day LWRs, except for in cases when the SSTAR and STAR-LM incorporate features not typical of other lead or lead-bismuth cooled reactors, such as a CO_2 based Brayton cycle for electricity production.

Specifically, the CO_2 based Brayton cycle is viewed as a factor contributing to higher prototype plant costs via the high cost of the R&D still needed to prove the viability of such an option for the power circuit; see point 9 of Table 49. Being emplaced, such a cycle could, however, contribute to reduced costs via compact sizes of the turbo-machinery and via elimination of the intermediate circuit.[6]

[6] It should be noted that all known designs and concepts of lead cooled reactors foresee no intermediate heat transport system, even if a steam turbine cycle is used for power conversion, which is most common [18].

TABLE 48. SUMMARY OF POSITIVE AND NEGATIVE EFFECTS FROM INCORPORATION OF INHERENT AND PASSIVE SAFETY DESIGN FEATURES INTO THE GT-MHR — AREAS OTHER THAN SAFETY

#	Design feature	Positive effects	Negative effects
1	Helium coolant properties		Primary circuit and coolant costs increase, taking into account helium volatility
2	Graphite as a structural material for the reactor core		– Facilities should be constructed to produce graphite of specified properties; – Increase in reactor core cost; – Need to dispose of large volumes of graphite
3	Low core power density		Decrease in specific economic indices; increase in reactor costs
4	Annular reactor core with a high surface to volume ratio to facilitate core cooling		Increase of reactor vessel dimensions and cost
5	Central reflector		
6	Heat resistant steel used for the reactor internals and the reactor vessel		Increase in reactor costs
7	TRISO coated particle fuel capable of reliable operation at high temperatures and fuel burnups		– Increase in fuel costs; – Fuel production facilities need to be constructed
8	Design to limit fuel temperature in accidents by passively removing heat through the vessel wall, limiting total core power		Limited option to benefit from economy of scale, owing to limited unit capacity
9	Containment designed to retain helium-air fluid and to withstand external loads		Increase in NPP costs
10	No large diameter pipelines in the primary circuit and no steam generators		Decrease in reactor costs

For all other passive features of the SSTAR and STAR-LM, the expected effects in areas other than safety are specified as either positive or positive and negative; see points 1–7 of Table 49. Positive elements are:

- Lack of chemical interactions and elimination of intermediate heat transport systems;
- Increased reactor self-control and simplicity of operation, owing to natural convection cooling and optimum reactivity feedbacks, with a potential for lower operating costs;
- Self-sufficiency of fissile transuranic materials (a closed cycle is required to benefit from this) and intrinsic proliferation resistance features of transuranic fuel (high content of ^{238}Pu — an isotope which, due to α-decay, produces a significant amount of residual heat that would complicate or even make it practically impossible to create a nuclear weapon — and trans-plutonium isotopes, spoiling the effectiveness of fissile material for weapons purposes).

Negative elements are:

- Higher required thickness of the reactor vessel, owing to greater weight resulting from lead being used as a coolant, and resulting in higher vessel costs;

TABLE 49. SUMMARY OF POSITIVE AND NEGATIVE EFFECTS FROM INCORPORATION OF INHERENT AND PASSIVE SAFETY DESIGN FEATURES INTO SODIUM COOLED AND LEAD COOLED FAST SMRs — AREAS OTHER THAN SAFETY

#	Design feature	Positive effects	Negative effects	SMR designs
1	Positive and negative effects of passive safety design features on economics, physical protection, etc. have not been investigated yet.			4S-LMR
2	Use of lead (Pb) as a coolant	Lack of chemical interaction with working fluid enables elimination of intermediate heat transport circuit, reducing capital and operating costs	– Weight resulting from high Pb density may require greater vessel thicknesses, increasing capital costs; – Coolant chemistry control and filtering systems needed to prevent erosion/corrosion effects contribute to increased cost	SSTAR, STAR-LM
3	Use of transuranic nitride fuel	– Transuranics are self-protective in a safeguards sense; – Transuranic nitride fuel together with a fast spectrum core and a closed fuel cycle has the potential to reduce fuel costs		
4	Natural circulation heat transport	Natural circulation cooling enabled by Pb coolant properties eliminates main coolant pumps, contributing to reduced plant costs	Need for height separation of thermal centres between heat exchangers and core may require taller reactor and guard vessels, increasing capital costs	
5	Large reactivity feedbacks from fast spectrum core enabling passive load following and passive shutdown	Enhances reliability and reduces operator requirements, potentially reducing operating costs		
6	Low burnup reactivity swing over long core lifetime/ refuelling interval, reducing reactivity investment in each control rod	Core is fissile self-sufficient with conversion ratio near unity such that the spent core can be reprocessed to further utilize its energy content, positively influencing fuel economics		
7	Escape path for gas/void to reach free surface in the primary coolant system, provided by design		Requires slightly greater reactor and guard vessel diameters, increasing capital costs	
9	Supercritical carbon dioxide Brayton cycle energy conversion with CO_2 working fluid that does not react chemically with Pb primary coolant	– Lack of chemical reaction between primary Pb and CO_2 working fluids enables elimination of intermediate coolant circuit, reducing capital and operating costs; – Use of supercritical carbon dioxide Brayton cycle with smaller turbo-machinery components than Rankine saturated steam cycle reduces plant capital and operating costs	– Research and development costs will be required for supercritical CO_2 Brayton cycle; – Need to contain CO_2 with potential activity entrained from Pb coolant released from the reactor system following in-vessel heat exchanger tube rupture impacts upon containment requirements, potentially increasing containment building costs; – Need to preclude radiolytic decomposition of CO_2 may require additional shielding of in-vessel Pb to CO_2 heat exchangers, potentially increasing reactor system costs	

- Cost increases owing to required systems of coolant chemistry control and filtering, needed to prevent corrosion/erosion;
- Higher vessel costs owing to increased vessel height and diameter needed to assure natural convection core cooling and the escape path for gas/void to reach the free surface in the primary coolant system.

The above discussed indications of positive and negative effects of inherent and passive safety features of the SSTAR and STAR-LM in areas other that safety should be viewed as very preliminary, because of the pre-conceptual design stage of these reactor concepts.

4.5. NON-CONVENTIONAL DESIGNS

Table 50 summarizes the positive and negative implications of inherent and passive safety design features of CHTR — the only non-conventional SMR concept considered in this report — in areas other that safety, based on inputs provided by designers of the CHTR in Annex X.

For the CHTR, feasibility studies were completed in 2006. As in the case of the SSTAR and STAR-LM concepts, the design stage may be too early to assess positive and negative implications of inherent and passive safety design features in areas other than safety. However, as opposed to the SSTAR and STAR-LM, conceptual design development for the CHTR using an extensive testing programme showed noticeable progress in the Bhabha Atomic Research Centre (BARC) of India at the time this report was prepared.

According to Table 50 and Annex X, the positive implications of inherent and passive safety design features of the CHTR could be:

- Cost savings due to the absence of pumps and steam generators, with heat pipes being used for heat transfer to the secondary circuit;
- Cost savings due to simplified design and maintenance, owing to the passive power regulation system and passively actuated passive decay heat removal system based on gas gap filling with molten metal;

TABLE 50. SUMMARY OF POSITIVE AND NEGATIVE EFFECTS OF INCORPORATION OF INHERENT AND PASSIVE SAFETY DESIGN FEATURES INTO THE CHTR — AREAS OTHER THAN SAFETY

#	Design feature	Positive effects	Negative effects
1	Natural convection of heavy metal coolant	Cost saving due to the absence of pumps and associated components, and due to simplified design and maintenance	
2	Thorium fuel cycle with TRISO coating particle based fuel configuration; low core power density selected for the demonstration prototype	Increased proliferation resistance	Higher specific reactor costs due to lower core power density and because TRISO particles occupy a larger volume when compared to conventional fuel
3	Heat pipe based heat transfer to secondary system	Simplified design and maintenance, saving costs due to the absence of a heat exchanger and associated components	
4	Passive power regulation system	Simplified design and maintenance, saving costs with respect to a conventional complex mechanism based system	
5	Passive heat removal based on gas gap filling with molten metal in accident conditions	Simplified design and maintenance, and associated reduction in cost	

- Increased proliferation resistance owing to the use of TRISO fuel within the thorium fuel cycle, possibly resulting from the absence of a commercial technology of TRISO fuel reprocessing and from radiation barriers provided by the daughters of the ^{232}U in the thorium cycle (for more details see [2, 3]).

The anticipated negative implication is higher specific plant costs owing to low core power density, resulting from the use of TRISO fuel (similar to HTGRs).

5. APPROACHES TO SAFETY SYSTEM SELECTION: ACTIVE VERSUS PASSIVE SAFETY SYSTEMS

The enveloping design approach for SMR designs considered in the present report is meant to eliminate as many accident initiators and/or prevent as many accident consequences as possible by design, and then to deal with the remaining accidents/consequences using reasonable combinations of active and passive safety systems and consequence prevention measures.

To prevent accidents, inherent safety features are used in the design, making direct contributions to defence in depth Level 1. These features may be very different for different reactor lines, e.g., eliminated piping or internal location of control rod drives in pressurized water reactors; eliminated steam generators and steam power circuit in direct cycle HTGRs; optimum combinations of reactivity effects and negative void worth in sodium cooled and lead cooled fast reactors; they are summarized in more detail below.

When available, contributions of inherent safety features to subsequent levels of defence in depth can help reduce hazards associated with accidents by ensuring increased reactor self-control, by slowing down accident progression, or by limiting accident scope. Relatively high heat capacity of the primary circuit is typical here, for many reactor lines.

Certain inherent safety features, such as high temperature fission product confinement properties of fuel and high temperature margin to fuel failure contribute directly to defence in depth Levels 3 and 4.

In addition to inherent safety features, some reliable passive features, such as additional passive structures (containment, guard vessel, or additional pressure boundary around the primary circuit, or coaxial double pipes — categorized as Category A passive systems in [12] but often referred to as inherent or by-design safety features [2, 3]), or reliable mechanisms of heat transfer, such as heat transfer by conduction and radiation via reactor core and reactor internals, or ultimate heat sink based on natural draught of air outside of the reactor vessel, could contribute to various levels of defence in depth in a way similar to inherent safety features, i.e., help to prevent certain accidents or accident consequences or reduce their scope.

With maximum possible use of the inherent and passive safety features provided by design, the remaining accident sequences are then dealt with using dedicated active or passive safety systems.

There is no single approach in selecting an optimum combination of active and passive safety systems, even for a single reactor line. A balanced view is that passive safety systems that use natural mechanisms such as gravity or buoyancy, or spring force for their operation require no operator action to get actuated, and rely on no external power or working media supply, have a potential to make plant design, maintenance and operation more simple, to enhance plant safety under a variety of internal and external events and combinations thereof, to improve plant resilience to human actions of malevolent character (add ‘intrinsic security’), and to improve plant economy. At the same time, it is recognized that the incorporation of passive safety systems in reactor designs needs to be adequately validated and tested due to several issues highlighted in Appendix 1.

For a passive safety system, functional failure (i.e., a failure of the system to perform its function) may happen if the initial or boundary conditions deviate from a specified range of values on which the performance of the system depends. Mainly because the driving forces in passive systems are most often small, the overall balance of forces defining the functional operation of a system may easily get changed even with a small disturbance or change in operating parameters [19–28]. The difficulties in evaluation of a functional failure of passive safety systems may be related to:

- Lack of plant data and operating experience;
- The experimental data obtained from integral facilities or even from separate effect tests is insufficient to understand system performance characteristics in normal operation and in transients and accidents;
- Lack of a clear definition of failure mode for passive safety systems;
- Difficulties in modelling the physical performance of such systems; for example, for natural convection based systems, such difficulties may be related to:
  — Low flow rate of natural convection, under which the flow cannot be fully developed and which is multi-dimensional in its nature;
  — Flow instabilities, which include flashing, geysering, density waving, flow pattern transition instabilities, etc.;
  — Critical heat flux changes under oscillatory conditions;
  — Flow stratification with kettle type boiling, particularly in large diameter vessels;
  — Thermal stratification in large water pools;
  — Effects of non-condensable gases on condensation, etc.
- Unknown capability of the so-called 'best estimate codes' to simulate performance of passive safety systems, owing to the fact that such codes were mainly developed to model active safety systems.

Therefore, before incorporating passive safety systems into plant design, their capacity and reliability need to be validated and tested over a broad range of states, from normal power operation to transients and accidental conditions [22, 23].

In addition to what was mentioned above:

- Economics of advanced reactors with passive safety systems should be assessed, taking into account all related aspects of construction and decommissioning;
- Ageing of passive safety systems should be considered, especially for longer plant lifetimes; for example, corrosion and deposits on heat exchanger surfaces could impair the functional performance of passive safety systems;
- Passive safety systems should be designed with a provision for easy in-service inspection, testing and maintenance, and ensure that the dose rate to workers is within the limits prescribed by regulations.

With all these aspects in mind, selection of an optimum combination of active and passive safety systems depends on previous experience of their validation and testing, on the availability of a system prototype, on a function that the system is expected to perform, and on considerations of redundancy, diversity and independence as measures to cope with common cause failure [7], as well as on considerations of plant economy, operating complexity, applications, security, and other factors.

It should be noted that passive safety systems in the SMRs considered in this report are not limited to natural convection based systems for passive decay heat removal, such as emergency core cooling systems, or to passive safety injection systems, but also include passive shutdown systems, such as those based on gravity or spring-force driven insertion of control rods, actuated upon flow disruption or system de-energization; passive systems of gas gap filling with (liquid metal) coolant to boost conduction for heat removal to the outside of the reactor vessel; passive mechanisms of fuel carry over from the core in the case of a fuel element failure to avoid recriticality in fast reactors; and others.

A useful categorization of passive systems is provided in IAEA-TECDOC-626 [12]; for convenience, some definitions from this reference are reproduced in Appendix 1 of this report.

Particular approaches to application of passive versus active safety systems applied by the designers of the SMRs considered in the present report are highlighted in Section 3.2., in conjunction with Level 3 of defence in depth. A common feature of all SMRs considered in the present report is that they all use passive decay heat removal systems. In all cases these systems are redundant and safety grade. Regarding shutdown systems, they could be active or passive, safety grade or non-safety-grade, based on different principles and using different components — control rods, absorber balls, or safety injections. Where applicable, depressurization systems are provided, which in most cases are actuated passively, by safety relief valves (check valves).

All solutions with active and passive safety systems described in the present report follow the principles of redundancy, diversity and independence [7].

In the case of light water reactors, there are certain advantages regarding passive safety systems, because more experience in validation, testing, certification and operation of such systems has been accumulated [19]. Certain, although more limited, experience is available for HTGR type reactors [17]. For SMRs of other types, extensive R&D programmes are required; in some cases such programmes were already in progress during preparation of this report [2, 3].

Performance assessment issues for passive safety systems are highlighted in more detail in Appendices I and II.

6. SUMMARY AND CONCLUSIONS

This report presents a description of design features used to achieve defence in depth in eleven concepts of small and medium sized reactors (SMRs), representing different reactor lines. The descriptions are structured to follow the definitions and recommendations of IAEA safety standard Safety of Nuclear Power Plants: Design [7], with some references made to other IAEA safety standards and publications, such as [8, 12, 13].

The selected SMRs represent different reactor lines, intended for different applications, and targeting different deployment timeframes. The reactor lines considered are pressurized water reactors — the KLT-40S, the IRIS, the CAREM-25, the SCOR, and the MARS — targeted for cogeneration or electricity production; pressurized boiling light water cooled heavy water moderated reactors — the AHWR — targeted for electricity generation with potable water production; a high temperature gas cooled reactors — the GT-MHR — targeted for electricity generation and advanced non-electrical applications, including complex cogeneration with bottoming cycles; sodium cooled and lead cooled fast reactors — the 4S-LMR and the SSTAR and the STAR-LM — targeted for electricity production or cogeneration; and a non-conventional very high temperature design — the CHTR — targeted for hydrogen production and other advanced non-electrical applications. Design descriptions, design status, targeted deployment dates, and applications of the SMRs considered in this report are presented in more detail in Refs [2, 3, 4].

One of the reactors, the KLT-40S, to be used for a floating NPP, is under construction with deployment of the plant scheduled for 2010. The IRIS, the CAREM-25, and the AHWR are likely to be commercialized by 2012–2015. The SCOR, the MARS, and the 4S-LMR have the potential to be deployed as first of a kind or prototype plants by 2015. The GT-MHR, the SSTAR, the STAR-LM, and the CHTR are targeted for deployment by 2020—2025; they are still at pre-conceptual design stages.

An enveloping design approach for the SMR designs considered in this report is to eliminate as many accident initiators and/or to prevent as many accident consequences as possible through design, and to deal with the remaining accidents/consequences using plausible combinations of active and passive safety systems and consequence prevention measures. This approach is also targeted for Generation IV energy systems and, to a certain extent it is implemented in some near term light water reactor designs of larger capacity, such as the VVER-1000, the AP1000, and the ESBWR [4].

General features of SMRs that, in view of their designers, contribute to a particular effectiveness of the implementation of inherent and passive safety design features in smaller reactors are:

- Larger surface to volume ratio, which facilitates easier decay heat removal, especially with a single phase coolant;
- An option to achieve compact primary coolant system design, e.g. integral pool type primary coolant system, which could contribute to the effective suppression of certain initiating events;
- Reduced core power density, facilitating easy use of many passive features and systems;
- Lower potential hazard that generically results from lower source term owing to lower fuel inventory, lower non-nuclear energy stored in the reactor, and lower integral decay heat rate.

For pressurized water reactors, there are three distinct design approaches, including: designs with integral primary circuit, with the reactor vessel accommodating steam generators and internal control rod drives, as well as elimination of large diameter piping, and minimizing of reactor vessel penetrations; compact modular loop-type designs with reduced piping length, an integral reactor cooling system accommodating all main and auxiliary systems within a leaktight pressure boundary, and leak restriction devices; and a design which has the primary pressure boundary enclosed in an enveloping shell with low enthalpy slowly moving water.

All pressurized water small and medium sized reactors incorporate design features to prevent loss of coolant (LOCA) accidents or reduce their scope. In addition to this, the pressurized water SMRs also incorporate features for the prevention of certain reactivity initiated accidents (integral designs of the primary circuit with in-vessel location of the control rod drives), for the smooth and slow character of transients owing to internal or 'soft'[7] pressurization and a relatively large water inventory, and for the de-rating of events with steam generator tube rupture. Whether or not these features are unique to SMRs is an open question. For example, conceptual design studies performed for PWRs with the integral design of the primary circuit accommodating both steam generators and control rod drives, point to an option to realize such features in reactors of up to 1000 MW(e) capacity. However, such proposals are still at an early conceptual design stage [16]. Regarding compact modular loop-type designs, based on the experience of marine propulsion reactors, their maximum possible unit size (known from completed design studies) is around 400 MW(e) [2]. There are no known large capacity reactor proposals for a design which has the primary pressure boundary enclosed in an enveloping shell with slowly moving water of low enthalpy.

Advanced pressurized boiling light water cooled heavy water moderated reactors are represented by one design (the AHWR), with its principal feature being heat removal by natural circulation in all modes. Main circulation pumps are excluded, thus loss of flow accidents are prevented by design. Maximum unit size within which such a technical solution can be maintained has not been examined.

For high temperature gas cooled reactors (HTGRs), the concept considered (GT-MHR) corresponds to one of two known fuel design options — that with pin-in-block TRISO based fuel. HTGR concepts incorporating an alternative fuel design — pebble bed TRISO fuel — were not considered in the present report. Independent of fuel design, all HTGRs incorporate design provisions to reduce hazards in accident scenarios that are potentially severe in reactors of other types, including loss of coolant (LOCA), loss of flow (LOFA), and reactivity initiated accidents. These provisions are based on the proven fission product confinement capability of TRISO fuel at high temperatures and high fuel burnups, which also enables long term passive decay heat removal, even from a voided reactor core, via natural processes of conduction, radiation, and convection. For the known materials of reactor vessels and known HTGR core designs, passive decay heat removal is possible only when reactor unit power is below ~600 MW(th). Direct gas turbine cycle HTGRs also do not have steam generators and steam turbine power circuits, which could otherwise lead to initiating events.

For fast reactor lines, the sodium cooled 4S-LMR and the lead cooled SSTAR and STAR-LM concepts have been considered. Both designs incorporate optimum sets of reactivity feedbacks and other inherent safety features, provided by design, to effectively reduce the scope and hazard of certain accidents and combinations of accidents that are potentially severe in reactors of other types. This is specifically the case for transient overpower events.

In the 4S-LMR, corresponding features include a negative whole-core void reactivity effect, contributing to defence in depth Level 3, and the absence of control rods in the core, with power being controlled via a feedwater flow rate in the power circuit. Burnup reactivity compensation is then performed with an active system based on a very slow upward movement of pre-programmed radial reflectors, with no feedback control. Should a reflector get stuck, the reactor would operate safely for a certain time and then get 'passively shut down'[8] by the increasing negative reactivity. At the same time, the drop of axial reflectors is a standard reactor shutdown feature. Altogether, the features mentioned above are unique to small size reactors.

[7] The 'soft' pressurizer system is characterized by small changes in primary pressure under a primary coolant temperature increase.

[8] 'Passive shutdown' is used by designers to denote bringing the reactor to a safe low power state with balanced heat production and passive heat removal, with no failure to the barriers preventing radioactivity release to the environment; all relying on inherent and passive safety features only, with no operator intervention or active safety systems being involved, and no external power and water supplies being necessary, and with an infinite grace period for practical purpose.

For the lead cooled SSTAR and STAR-LM, the inherent safety features contributing to the prevention of possible accidents or to a reduction of their scope are generally typical of the lead cooled reactor line. They include the very high boiling point of lead; a pool type design with a free surface of lead to allow removal of gas bubbles from primary coolant before they enter the core; location of the guard vessel and reactor in the concrete shaft; optimum sets of reactivity effects, and; high heat capacity and small overall reactivity margin in the reactor core. Although some designers see it as capacity independent, the 'passive shutdown' option for larger sized lead cooled reactors needs to be further examined and proven. It should be noted that some designers mention the unit size of the lead and lead-bismuth cooled reactors is limited because of seismic considerations. According to studies performed in Japan, size cannot exceed ~750 MW(e), which is slightly above the SMR range boundary of 700 MW(e); see Annex XV in reference [2].

Finally, the CHTR, a non-conventional design lead-bismuth cooled very high temperature reactor, designed to operate with ^{233}U-Th based TRISO fuel, merges the technologies and inherent safety features of the lead cooled and HTGR type reactors, and also incorporates other features intended to prevent failures through increased temperature margins, to eliminate loss of flow accidents via natural circulation, to incorporate reliable heat pipe based systems for heat removal, and to reduce the scope and hazard of transient overpower accidents by limiting the reactivity margin in the core. The application of all these features is supported by the relatively small core power density typical of a TRISO type fuel. Although the CHTR is a very small reactor with 100 kW(e), similar technologies are planned for use in future reactors of larger capacity (up to 600 MW(th)).

The information on passive and active safety systems incorporated in the designs of the SMRs considered in this report indicates there is no single strategy; a variety of approaches are being applied in different SMRs even when they belong to the same reactor line. It is important to note that broad incorporation of inherent and passive safety features pursued by SMR designers to prevent certain accidents and accident consequences or reduce their scope and hazard is in several cases conditioned or facilitated by smaller reactor capacity and size. However, the design solutions used for active and passive safety systems are, in general, not capacity dependent. With smaller reactor capacity, it is possible to facilitate the application of passive safety features and systems, specifically, those based on the natural convection of a single phase coolant, or those incorporating mechanisms of heat transfer by conduction and radiation.

Selection of reasonable combinations of active and passive safety systems is based on specific design considerations, validation and testing experience, regulatory practice, plant economy and plant lifetime considerations, provisions for in-service inspection and other aspects, and may vary from case to case.

It should be noted that all SMRs addressed in the present report incorporate redundant passive systems or passive mechanisms of decay heat removal. Regarding reactor shutdown systems, a variety of approaches is proposed ranging from standard active mechanical control rods to gravity or spring force driven absorber insertion actuated upon de-energization or coolant flow disruption, to passively operated safety injections, to a 'passive shutdown' mechanism based on the inherent safety features of a reactor design, and to a mechanism of fuel carry over from the core in the case of a cladding failure (intended to prevent recriticality in fast sodium cooled reactors). Depressurization and isolation systems, where applicable, often use direct action devices, e.g., check valves, to become actuated. An approach that needs to be mentioned, as it is applied in several water cooled, gas cooled and liquid metal cooled SMRs, is to have all safety systems passive and safety grade. In this, it is assumed that certain non-safety-grade active systems/components of normal reactor operation are capable of making an (auxiliary) contribution to the execution of safety functions in accidents.

All SMRs considered in the present report incorporate a containment — in many cases a double containment — or a containment and a protective shell or enclosure. Compact containment design and plant embedment below ground level are commonly mentioned as factors contributing to enhanced protection against an aircraft crash.

The designers of SMRs mention that features of their reactors such as the capability to survive design basis accidents and combinations thereof relying only on inherent and passive safety features, with no operator or emergency team interventions, and without external supplies of energy and working media, could also contribute to plant protection against a variety of natural and human induced external events.

Altogether, passive safety systems are broadly applied in the SMR designs considered. At the same time, there are potential concerns related to passive safety systems, derived from a small amount of experience with reactor design using such systems. In particular, these concerns are the following:

- Reliability of passive safety systems may not be understood as well as that of active safety systems;
- There may be a potential for undesired interaction between active and passive safety systems;
- It may be more difficult to 'turn off' an activated passive safety system, if so desired, after it has been passively actuated;
- Implications of the incorporation of passive safety features and systems into advanced reactor designs to achieve targeted safety goals needs to be proven, and the supporting regulatory requirements need to be worked out and put in place.

To address these and other issues related to the performance assessment of passive safety systems, the IAEA recommended coordinating a research project called "Development of Methodologies for the Assessment of Passive Safety System Performance in Advanced Reactors" in 2008–2011. The objective is to determine a common analysis and test method for reliability assessment of passive safety system performance.

For all SMRs considered in this report, designers expect that prototype or first of a kind plants with their respective SMRs would be licensed according to currently emplaced regulatory norms and practices in Member States. Further advancement of regulatory norms could facilitate design improvements in the next generation of plants.

Further revisions of the IAEA safety standards toward a technology neutral approach[9] could be of value to facilitate design development and safety qualification of non-water-cooled SMRs, such as the GT-MHR, the 4S-LMR, the SSTAR and STAR-LM, and the CHTR.

The designers of most of the SMRs considered in the present report foresee that safety design features contributing to defence in depth Levels 1–4 [7] could be sufficient to meet the objective of the defence in depth Level 5 "Mitigation of radiological consequences of significant release of radioactive materials", i.e., that emergency planning measures outside the plant boundary might be reduced or even not needed at all. The design features of the SMRs indicated to make a contribution directly to Level 5 of defence in depth are lower fuel inventory, lower non-nuclear energy stored in the reactor, and lower integral decay heat rate of a smaller reactor as compared to a large capacity one.

As a desired or possible feature, reduced off-site emergency planning is mentioned in the Technology Goals of the Generation IV International Forum [15], in the user requirements of the IAEA's International Project on Innovative Reactors and Nuclear Fuel Cycles (INPRO) [14], and in the recommendations of the International Nuclear Safety Advisory Group (INSAG-12) [11], with the caution that full elimination of off-site emergency planning may be difficult to achieve or with the recommendation that Level 5 of defence in depth still needs to be kept, notwithstanding its possibly decreased role. Achieving the goal of reduced off-site emergency planning would require both development of a methodology to prove that such reduction is possible in the specific case of a plant design, and adjustment of existing regulations. A risk informed approach to reactor qualification and licensing could facilitate licensing with reduced off-site emergency planning for smaller reactors, once it gets established.[10] Within the deterministic safety approach it might be very difficult to justify reduced emergency planning in view of a prescribed consideration of a postulated severe accident with radioactivity release to the environment owing to a common cause failure. Probabilistic safety assessment (PSA), as a supplement to the deterministic approach, might help justify very low core damage frequency (CDF) or large early release frequency (LERF), but it does not address the consequences and, therefore, does not provide for assessment of the source terms. A risk-informed approach that introduces quantitative safety goals, based on the probability-consequences curve could help solve the dilemma by providing a quantitative measure for the consequences of severe accidents and by applying a rational technical and non-prescriptive basis to define a severe accident. An example of such an approach is in the recently published IAEA-TECDOC-1570 Proposal of a Technology-Neutral Safety Approach for New Reactor Designs [13]. When this report was prepared, such an approach had yet not been established as an IAEA safety standard.

[9] National regulations in some Member States are already technology neutral; examples are the United Kingdom or the Russian Federation.

[10] Risk informed regulations for beyond design basis accidents are already in place in some Member States, e.g., Argentina.

The report provides a review of the positive and negative effects of the incorporation of inherent and passive safety design features of the addressed SMRs in areas other than safety, based on inputs provided by SMR designers in Annexes I–X. Positive developments include:

- Simplicity of plant design, resulting from a reduction of the number of systems and components, and simplicity of plant operation and maintenance, resulting from a reduced number of systems and components requiring maintenance — both factors contribute to a reduction in plant costs;
- For many designs reduced plant costs, resulting from a compact primary circuit design and a compact containment design;
- Simplicity of plant operation and maintenance,[11] resulting from increased reactor self-control in accidents and a higher margin to fuel failure, has the potential to result in reduced requirements to operating personnel and reduced necessary plant staffing. Should this be accepted by regulators, it might contribute to reduced operating costs and facilitate deployments in countries with limited infrastructure;
- For nearly all designs, the potential to benefit from cost reduction resulting from reduced or eliminated off-site emergency planning; this still needs to be proven and accepted by regulators;
- Owing to increased reactor self-control in accidents and higher margin to fuel failure, less concern regarding human actions of a malevolent character and, potentially, a cost reduction owing to 'inherent security' of the plant.

On the other side, for all designs considered, the implementation of inherent and passive safety design features results in an increase in specific plant capital costs due to lower core power density or a larger required size of the reactor vessel to accommodate certain components of the primary circuit, etc. Elimination or reduction of liquid boron system (in PWR type reactors) or operation without on-site refuelling provided for in the sodium cooled and lead cooled SMRs results in certain deterioration of burnup cycle characteristics. Taller and broader reactor vessels or piping, necessary to enhance natural convection based heat removal, are also factors contributing to plant cost increase.

Designers expect that the above mentioned negative implications of passive safety design options could be counteracted by an enhanced option to build twin or multi unit plants at the same site (see Fig. 1 in Section 1.1.1), by enhanced pre-fabrication and, in some cases, by higher energy conversion efficiency, as well as by the positive implications highlighted earlier.

[11] Annex IV gives an example of how operation complexity of a plant could be quantified and used in comparative assessments of different design solutions.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Innovative Small and Medium Sized Reactors: Design Features, Safety Approaches and R&D Trends, IAEA-TECDOC-1451, IAEA, Vienna (2005).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Innovative Small and Medium Sized Reactor Designs 2005: Reactors with Conventional Refuelling Schemes, IAEA-TECDOC-1485, IAEA, Vienna (2006).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Small Reactor Designs Without On-site Refuelling, IAEA-TECDOC-1536, IAEA, Vienna (2007).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Advanced Light Water Reactor Designs 2004, IAEA-TECDOC-1391, IAEA, Vienna (2004).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Terms for Describing New, Advanced Nuclear Power Plants, IAEA-TECDOC-936, IAEA, Vienna (1997).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Advanced Nuclear Power Plant Design Options to Cope with External Events, IAEA-TECDOC-1487, IAEA, Vienna (2006).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of the Nuclear Power Plants: Design IAEA Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Evaluation of Seismic Hazard for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-3.3, IAEA, Vienna (2002).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.5, IAEA, Vienna (2004).

[10] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

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

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Terms for Advanced Nuclear Plants, IAEA-TECDOC-626, IAEA, Vienna (1991).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Proposal for a Technology-Neutral Safety Approach for New Reactor Designs, IAEA-TECDOC-1570, IAEA, Vienna (2007).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Methodology for the Assessment of Innovative Nuclear Reactors and Fuel Cycles — Report of Phase 1B (First Part) of the International Project on Innovative Reactors and Fuel Cycles (INPRO), IAEA-TECDOC-1434, IAEA, Vienna (2004).

[15] UNITED STATES DEPARTMENT OF ENERGY, A technology roadmap for Generation IV Nuclear Energy Systems, Nuclear Energy Research Advisory Committee, Washington, DC (2002).

[16] GAUTIER, G.M., CHENAUD, M.S., TOURNIAIRE, B. "SCOR 1000: An economic and innovative conceptual design PWR", paper 7417, Proc. ICAPP'07, Nice, France, 13–8 May 2007.

[17] SHOUYIN HU, RUIPIAN WANG, ZUYING GAO, "Safety demonstration tests on HTR-10", paper H06, Proc. 2nd Int. Topical Mtg. on High Temperature Reactor Technology, Beijing, China, 22–24 September 2004.

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Fast Reactor Database: 2006 Update, IAEA-TECDOC-1531, IAEA, Vienna (2006).

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Natural Circulation in Water Cooled Nuclear Power Plants. Phenomena, Models and Methodology for System Reliability Assessments, IAEA-TECDOC-1474, IAEA, Vienna (2005).

[20] AMERICAN SOCIETY OF MECHANICAL ENGINEERS, Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME RA-S-2002, ASME, New York (2002).

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level-1 PSA for Nuclear Power Plants, (2007).

[22] MARQUÈS, M., et al., Methodology for the reliability evaluation of a passive system and its integration into a Probabilistic Safety Assessment, Nucl. Eng. Des. **235** (2005) 2612–2631.

[23] NAYAK, A.K., et al., "Reliability analysis of a boiling two-phase natural circulation system using the APSRA methodology", paper 7074, Proc. of ICAPP'07, Nice, France, 13–18 May 2007.

[24] DELANEY, M.J., APOSTOLAKIS, G.E., DRISCOLL, M.J., Risk-informed design guidance for future reactor systems, Nucl. Eng. Des. **235** (2005) 1537–1556.

[25] BURGAZZI, L., State of the Art in Reliability of Thermal-Hydraulic Passive Systems, Reliab. Eng. Sys. Saf. **92** (2007) 671–675.

[26] CAHALAN J., et al., "Performance of metal and oxide fuels during accidents in a large liquid metal cooled reactor", Fast Reactor Safety (Proc. Top. Mtg. Snowbird, UT, 1990), American Nuclear Society (1990).

[27] ROYL P., et al., "Influence of metal and oxide fuel behavior on the ULOF accident in 3500 MWth heterogeneous LMR cores and comparison with other large cores", ibid.
[28] ROYL P. et al., "Performance of metal and oxide fuel cores during accidents in large liquid metal cooled reactor", Nucl. Technol. **97** (1992) 198–211.

Appendix I

PERFORMANCE ASSESSMENT OF PASSIVE SAFETY SYSTEMS

Background and experience

As already mentioned, broad incorporation of inherent and passive safety design features has become a 'trademark' of many advanced reactor designs, including several evolutionary designs and the majority of innovative SMR designs [1, 2, 3, 4, 5]. In addition to various possible combinations of inherent and passive safety features (sometimes referred to as by design safety approaches [2]), all SMRs addressed in this report incorporate passive safety systems. Passive safety systems may include moving liquids or expanding solid structures, direct action devices, or stored energy sources. As suggested in IAEA-TECDOC-626 [6], those may be classified as passive systems of categories B, C, and D, accordingly, see Appendix 1. Passive safety systems require validation and testing to demonstrate and prove their reliable operation and quantify their reliability and, if necessary, adjust their design accordingly.

While individual processes may be well understood, combinations of these processes, which determine the actual performance of passive safety systems, may vary depending on changes in conditions of state, boundary conditions, and failure or malfunctioning of other components within the system, the circuit or the plant. Passive safety systems of category A, or inherent safety features, incorporate no moving liquids or moving solid structures, direct action devices, or stored energy sources. There is a consensus that such systems have a strong advantage [2, 3, 6]. Therefore, the issue of process performance reliability is most important for passive safety systems of categories B, C, and D [6].

There are certain accomplishments regarding the testing, construction, licensing or validation of passive systems of categories B, C, or D [6], such as the more recent WWER-1000 reactors and the KLT-40S of the Russian Federation, or the AP600, the AP1000, and the ESBWR of the USA [4, 7]. Experiment based deterministic approaches to the validation of passive systems including separate-effect tests and integral tests of reactor models with subsequent qualification of analysis models and computer codes have been established and accepted by regulators in some countries, in line with the conventional safety requirements also applied to active safety systems. The indicated deterministic approaches are generally successful with regulators when the basic technology involved is evolutionary, e.g., that of water cooled reactors, and backed by years of validation and testing, as well as reactor operation experience, and when passive systems are reasonably conventional in their design. When the technology is innovative or a passive safety system has a distinctly non-conventional set of features, the application of established deterministic approaches may require a multi-year resource consuming effort to accomplish validation, testing and demonstration of the reliable operation of such a system, prior to licensing approval of the corresponding advanced NPP.

The regulations in Argentina, China, Japan, Germany, India, France, the Russian Federation, and the USA already incorporate provisions for accepting the results of probabilistic safety assessments (PSA) on a complementary basis. In order to ensure that the PSA used in the risk informed decision making (RIDM) process is of acceptable technical quality, efforts are being made in different countries to provide PSA standards that define inherent technical features of a PSA acceptable for a regulatory body. An example is the ASME probabilistic risk assessment (PRA) standard [8], recently endorsed by the United States Nuclear Regulatory Commission (US NRC). In line with worldwide trends, the IAEA is developing a series of publications for the safety standards series on PSA and RIDM. One of the latter, named the Safety Guide on Development and Application of Level-1 PSA for NPPs [9], planned to be published in 2008, would provide recommendations on the technical content of PSA studies to reliably support various PSA applications.

The general trend towards a more risk informed approach (e.g., see Refs [10, 11]) is pursued with a focus on what is really important from the safety perspective, in order to achieve a design that is more favourable from the cost-benefit perspective. A methodology for reliability assessment of passive safety systems would enable quantification of the reliability to treat both active and passive safety systems within a common PSA approach. Several such methodologies are under development in Europe, India, and the USA [12–14]. What is important from the perspective of overall risk assessment is that these methodologies take into account uncertainties associated with unforeseen physical phenomena that may affect the operation of passive safety systems,

worsening their reliability. All of the methodologies are at a preliminary stage of development and no consensus on a common approach had been established among their proponents at the time this report was being prepared. Two of these methodologies are described in brief below.

Examples of methodologies for reliability assessment of passive safety systems

RMPS methodology

In the late 1990s, a methodology known as REPAS was developed cooperatively by ENEA, the University of Pisa, the Polytechnic of Milan, and the University of Rome in Italy which was later incorporated into the European Commission's reliability methodology for passive systems (RMPS) project within the European Commission's 5th framework programme [12]. The RMPS methodology is based on evaluation of the failure probability of a system to carry out its desired function for a given set of scenarios, taking into account uncertainties of physical (epistemic) and geometric (aleatoric) parameters, deviations of which can lead to a failure of the system. The RMPS approach considers a probability distribution of failure to treat variations of the comparative parameters considered in the predictions of codes.

Schematics of the RMPS are shown in Fig. 1.

The RMPS methodology has been developed to evaluate reliability of passive systems incorporating a moving fluid and using natural convection as an operation mechanism. The reliability evaluation for such systems is based, in particular, on the results of thermal-hydraulic calculations. The RMPS methodology could be structured as follows:

— Identification and quantification of the sources of uncertainties;
— Reliability evaluation of a passive system;
— Integration of passive system reliability in PSA.

The methodology is applied to a specific accident scenario in which operation of a certain passive safety system is foreseen. When the scenario to be examined is specified, the first step — identification of the system — requires full characterization of the system under investigation be carried out. This step includes specifying the goals of the system, the modes via which it may fail, and providing the definition of a system failure, or more specifically the definition of success/failure criteria. Modelling of the system is also required, which is accomplished using best-estimate computer codes. Numerous sources of uncertainties present in the modelling process have to be identified. Such sources are related to approximations in modelling of physical processes and system geometry, and uncertainties in input variables, such as initial and boundary conditions. Identifying the most important thermal-hydraulic phenomena and parameters which have to be investigated for the system is an important part of the methodology. Such identification can be accomplished via a brainstorming session of experts with a good understanding of the system functions and best estimate code calculations, and through use of a method of the relative ranking of phenomena. The ranking technique implemented in the RMPS project is the analytical hierarchy process (AHP). After identifying important thermal-hydraulic parameters, the next step is to quantify their uncertainties. When experimental data are not available, expert judgement would be required to identify the range of uncertainties and select appropriate probability density functions for a given set of variables. The methodology incorporates a sensitivity analysis, which is to determine, among all uncertain parameters, the main contributors to the risk of a system failure.

The second part of the methodology requires evaluating uncertainty in the expected performance of the passive system as predicted by the thermal-hydraulic code and according to the studied scenario. Such uncertainty evaluation could be performed using confidence intervals or probability density functions. Within RMPS studies, it has been found that methods providing an uncertainty range of system performance are not very efficient for reliability estimation. Therefore, use of a probability density function was selected as an approach to be implemented. The probability density function of system performance can be directly used for reliability estimation once a failure criterion is given. The existing methods for such quantitative reliability evaluation are generally based on Monte Carlo simulations. Monte Carlo simulations consist of drawing samples of the basic variables according to their probabilistic density functions and then feeding them into the performance function evaluated by a thermal-hydraulic code. An estimate of the probability of failure can then

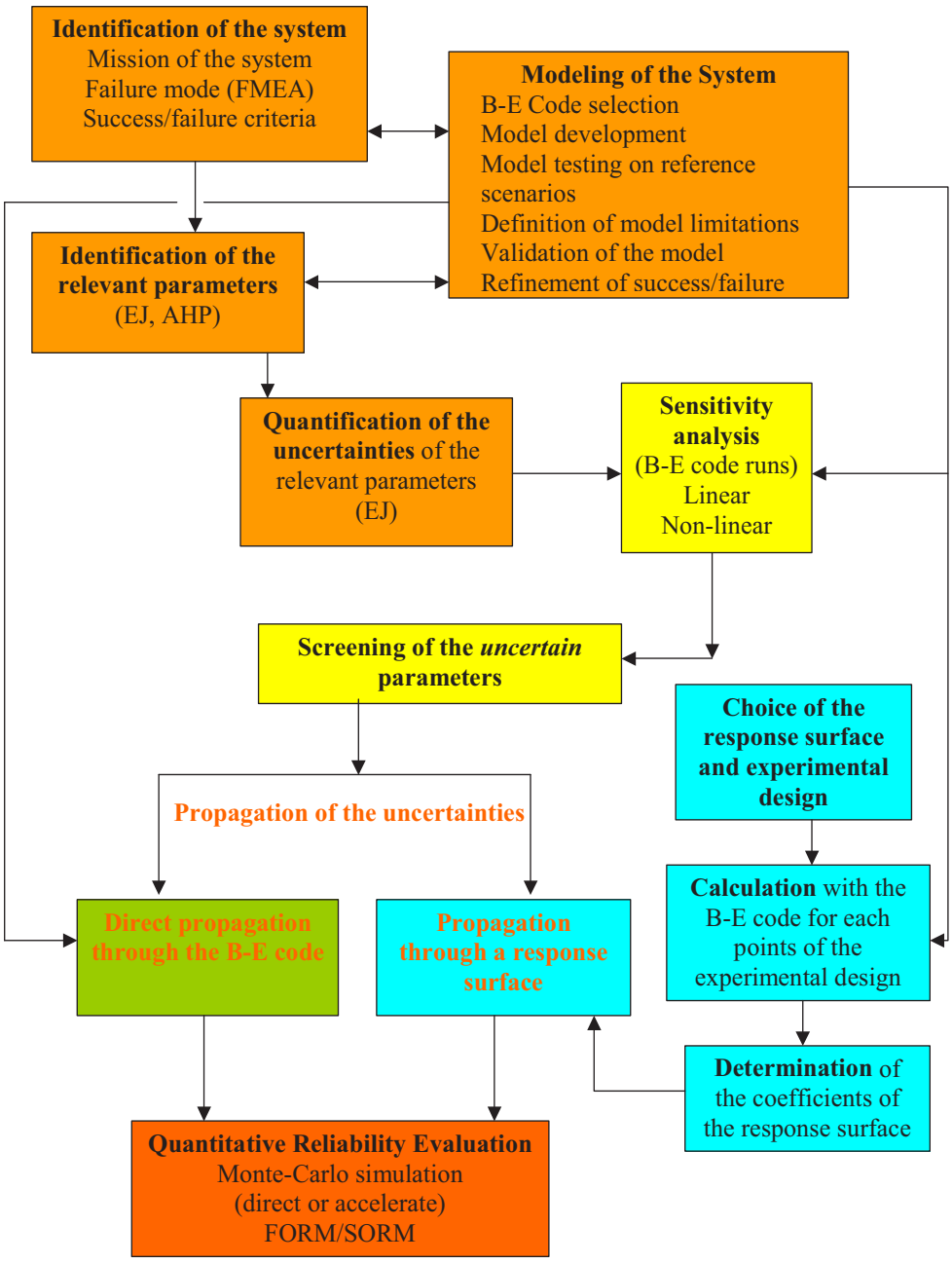


FIG. 1. Schematics of the RMPS methodology.

be determined by dividing the number of simulations leading to a failure of the system by the total number of simulation cycles. Monte-Carlo simulations require a large number of calculations; as a consequence, the technique can be prohibitively time consuming. To avoid this problem, two approaches are possible: (i) application of variance reduction techniques used in Monte-Carlo methods, or (ii) the use of response surfaces. It is also possible to use approximate methods, such as first and second order reliability methods (FORM/SORM).

The final part of the methodology focuses on the development of a consistent approach for quantitative reliability evaluations of passive systems, which would allow introducing such evaluations in the accident sequence of PSA. In the PSA of innovative reactor projects carried out until recently, only the failures of passive system components (valves, pipes, etc.) was taken into account and not failures of combinations of physical phenomena on which system performance is based. It is a difficult and challenging task to examine this aspect of passive system failure within PSA models, because there are no commonly accepted practices available.

Different options have been discussed within the framework of the RMPS project, but no real consensus between partners has been found. In line with the standards in place for Level 1 PSA models, the approach currently followed by the CEA and Technicatome of France is based on accident scenarios being presented in the form of static event trees. The event tree technique makes it possible to identify the whole variety of chains of accident sequences, deriving from initiating events and describing different basic events corresponding to a failure or a success of the safety systems. This method has been applied to a fictitious PWR type reactor equipped with two types of passive safety systems. The analyses of failures carried out for this reactor made it possible to characterize both technical failures (those of valves, heat exchanger pipes, etc.), and ranges of variation of uncertain parameters affecting the physical process. A simplified PSA has been performed starting from a single initiating event. The majority of sequences addressed by this event tree were analysed by deterministic evaluations, using enveloping values of the uncertain parameters. For some sequences, where definition of the enveloping cases was impossible, basic events corresponding to the failure of physical processes were added to the event tree, and quantitative reliability evaluations, based on Monte Carlo simulations and on thermal-hydraulic code analyses, were carried out to evaluate corresponding failure probability. Failure probabilities obtained by these reliability analyses were fed into the corresponding sequences. Such an approach allows for evaluation of the impact of a passive safety system on the accident scenario. In particular, for the example studied, a new design basis for the system has been proposed in order to meet in full the global safety objective assigned to the reactor.

The RMPS methodology has been applied to three types of passive safety systems, including the isolation condenser system of a boiling water (BWR) reactor, the residual heat removal system on the primary circuit of a PWR reactor, and the hydro-accumulator (HA) systems of PWR and WWER type reactors.

In RMPS applications performed by the CEA and Technicatome of France, the thermal-hydraulic passive system acts as an ultimate system in the management of an accident scenario. Under this assumption, characteristics of the current Level 1 PSA models remain adequate.

A test case using the RMPS methodology is currently underway for a CAREM like passive residual heat removal system within the ongoing IAEA coordinated research project “Natural circulation phenomena, modelling and reliability of passive systems that utilize natural convection”.

APSRA methodology

A different approach is the ‘APSRA’ methodology, developed at the Bhabha Atomic Research Centre (BARC) of India [13]. In this approach, the failure surface[12] is generated by considering the deviation of all those comparative parameters which influence system performance.

Schematics of the APSRA methodology are shown in Fig. 2.3.

Like the RMPS methodology described above, the APSRA methodology developed in BARC, India, is primarily intended to analyse reliability of passive systems employing natural convection. The smallness of the driving head means a natural convection based system is susceptible to deviation from the performance of an intended function by a small change in key parameters. Because of this, there has been growing concern about the reliability of natural convection based systems.

The methodology named assessment of passive system reliability (APSRA) starts with selection of the system, followed by the understanding of its operational mechanism. Using simple computer codes, key parameters causing functional failure of the system are identified. Failure criteria are determined. Best estimate codes, such as RELAP5, etc., are then used to determine key parameter ranges, a deviation from which may cause system failure. These ranges of parameters are then fine tuned based on data generated in test facilities. This is done by performing uncertainty analysis for predictions of a best estimate code using in-house experimental data obtained in integral and separate effect test facilities.

[12] Failure surface [23] is an experiment backed predicted boundary of reliable operation of a passive safety system defined against all variables that may affect performance of such a system; it is used to support subsequent root cause analysis (actually, the failure surface defined in [23] is of iterative nature, also supporting identification of those tests that are still missing).

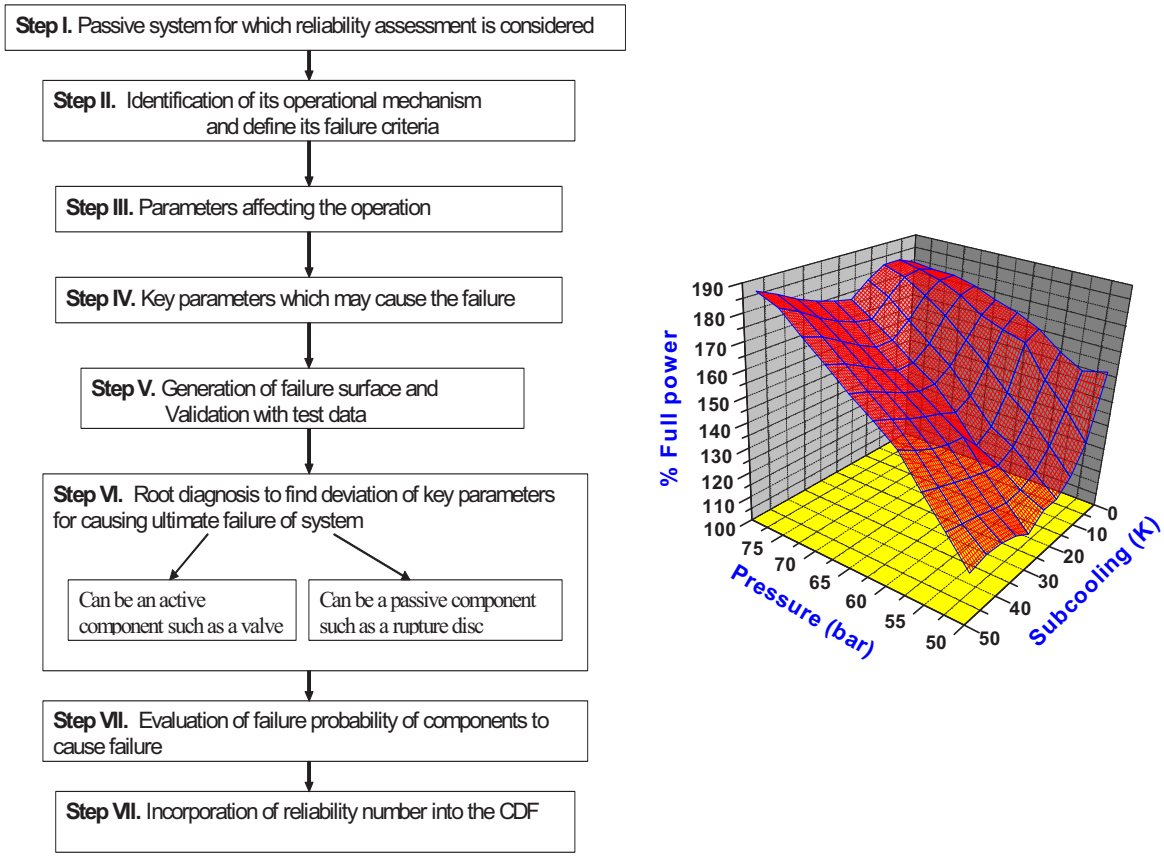


FIG .2. Flowchart of the APSRA methodology (left) and typical failure surface for natural circulation (right).

In the next step, the possible causes of deviation of these parameters are revealed through root diagnosis. It is assumed that the deviation of such physical parameters occurs only due to a failure of mechanical components, such as valves, control systems, etc. The probability of system failure is evaluated based on the failure probability of these mechanical components, through a classical PSA treatment.

To demonstrate the methodology in a test case, it has been applied to the main heat transport system of the AHWR reactor, described in Annex VI of this report. This system employs a boiling (two-phase) light water coolant in natural circulation. To find code uncertainties, code predictions were compared with data generated from experimental natural circulation facilities, and uncertainties were evaluated from the error distribution between code predictions and test data. The facilities mentioned for generation of the required experimental data were the integral test facility ITL, the high pressure natural circulation loop HPNCL, and the flow pattern transition instability loop FPTIL [13].

The effects of variation of key parameters on system performance were evaluated, and a multi-dimensional failure surface was generated. The probability of the system to reach the failure surface was elaborated using generic data for the failure of components.

The APSRA methodology is being applied to other passive systems of the AHWR, such as the decay heat removal system using isolation condensers, a passive containment cooling system, a passive containment isolation system, etc.

Common issues and recommended further R&D

The approaches presented in short in the previous section were discussed by their proponents and other experts at a dedicated IAEA technical meeting, convened on 12-16 June 2006 in Vienna (Austria) with experts from interested Member States and international organizations — Argentina, Brazil, China, France, India, Italy,

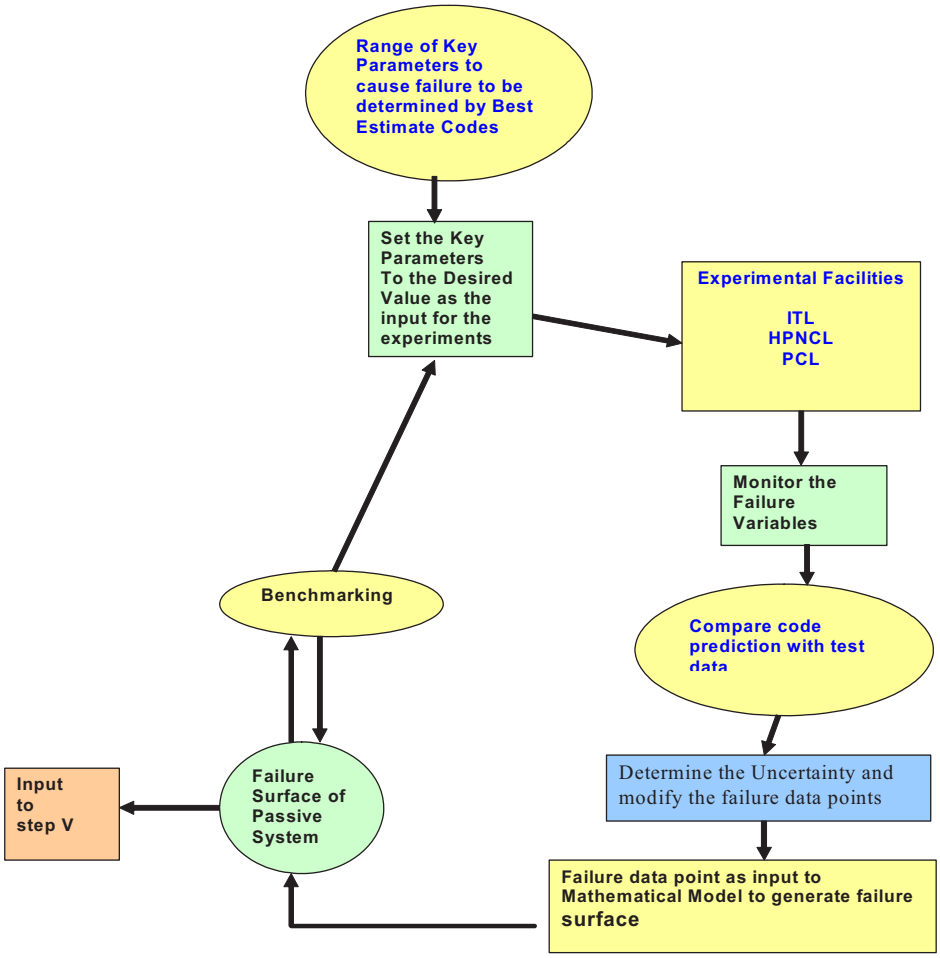


FIG. 3. APSRA methodology: programme flowchart for benchmarking of the failure surface based on experimental data.

Japan, the Russian Federation, the USA, and the European Commission as an observer. In the conclusions to this meeting, it was noted that the APSRA and the RMPS methodologies are complementary in the following:

- APSRA incorporates an important effort to qualify the model and use available experimental data. These aspects have not been studied in the RMPS, given the context of the RMPS project;
- APSRA includes, within the PSA model, failure of those components which cause a deviation of key parameters resulting in a system failure, but does not take into account the fact that the probability of success of a physical process could be different from unity;
- RMPS proposes to take into account, within the PSA model, failure of a physical process. It is possible to treat such data, e.g., the best estimate code plus the uncertainty approach is suitable for this purpose;
- In fact, two different philosophies or approaches have been used in the RMPS and in the APSRA and the two developed methodologies are, therefore, different. At the same time, proponents of the RMPS conclude that certain parts of the APSRA and the RMPS could be merged in order to obtain a more complete methodology.

During the IAEA technical meeting mentioned above — and after it — several other distinct approaches for reliability assessment of passive safety system performance were noted [14, 15], and the consensus was that a common analysis and test based approach would be helpful to the design and qualification of future advanced nuclear reactors. The inclusion of tests appears to be a must for new designs of passive systems and, especially, when non-water-cooled reactors are considered, for which validated codes and sufficient data for validation of the codes might be a priori not available. The approach itself is expected to streamline and speed up the process, and improve the quality of validation and testing of passive safety system performance.

Reflecting on these developments in Member States, the IAEA is implementing a CRP on Development of Methodologies for the Assessment of Passive Safety System Performance in Advanced Reactors in 2008–2012. The objective is to determine a common method for reliability assessment of passive safety system performance. Such a method would facilitate application of risk informed approaches in design optimization and safety qualification of future advanced reactors, contributing to their enhanced safety levels and improved economics.

In addition to the above discussed topics, it will likely be necessary to confirm that over a plant's lifetime passive safety systems retain the capability to perform safety functions as designed. As it has already been mentioned, such confirmation would be facilitated if possible ageing effects on passive safety systems are considered in plant design and if passive safety systems are designed with a provision for easy in-service inspection, testing, and maintenance. In addition to this, new approaches might be needed to perform this confirmation, different from those used with active safety systems. One possible approach to deal with this issue is outlined in a short paper contributed by D.C. Wade of the Argonne National Laboratory (USA), enclosed as Appendix II.

REFERENCES TO APPENDIX I

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Innovative Small and Medium Sized Reactors: Design Features, Safety Approaches and R&D Trends, IAEA-TECDOC-1451, IAEA, Vienna (2005).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Innovative Small and Medium Sized Reactor Designs 2005: Reactors with Conventional Refuelling Schemes, IAEA-TECDOC-1485, IAEA, Vienna, (2006).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Small Reactor Designs Without On-site Refuelling, IAEA-TECDOC-1536, IAEA, Vienna, (2007).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Advanced Light Water Reactor Designs, IAEA-TECDOC-1391, IAEA, Vienna (2004).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Advanced Nuclear Power Plant Design Options to Cope with External Events, IAEA-TECDOC-1487, IAEA, Vienna (2006).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Terms for Advanced Nuclear Plants, IAEA-TECDOC-626, IAEA, Vienna (1991).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Natural Circulation in Water Cooled Nuclear Power Plants. Phenomena, Models and Methodology for System Reliability Assessments, IAEA-TECDOC-1474, IAEA, Vienna (2005).

[8] AMERICAN SOCIETY OF MECHANICAL ENGINEERS, Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME RA-S-2002, ASME, New York (2002).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level-1 PSA for Nuclear Power Plants, IAEA, Vienna (2007).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Proposal for a Technology-Neutral Safety Approach for New Reactor Designs, IAEA-TECDOC-1570, IAEA, Vienna (2007).

[11] GENERATION-IV INTERNATIONAL FORUM, A technology roadmap for Generation-IV Nuclear Energy Systems, US Department of Energy, Nuclear Energy Research Advisory Committee, Washington, DC (2002).

[12] MARQUÈS, M. et al., Methodology for the reliability evaluation of a passive system and its integration into a Probabilistic Safety Assessment, Nucl. Eng. Des. **235** (2005) 2612–2631.

[13] NAYAK, A.K., et al., "Reliability analysis of a boiling two-phase natural circulation system using the APSRA methodology", paper 7074. Proc. ICAPP'07, Nice, France, 13–18.

[14] DELANEY, M.J., APOSTOLAKIS, G.E., DRISCOLL, M.J., Risk Informed Design Guidance for Future Reactor Systems, Nucl. Eng. Des. **235** (2005) 1537–1556.

[15] BURGAZZI, L., State of the Art in Reliability of Thermal-Hydraulic Passive Systems, Reliab. Eng. Sys. Saf. **92** (2007) 671–675.

Appendix II

PERIODIC CONFIRMATION OF PASSIVE SAFETY FEATURE EFFECTIVENESS

D. Wade
Argonne National Laboratory,
United States of America

Technical specifications that govern plant operations require that active safety systems be periodically validated and/or recalibrated as a means to assure that they continue to perform their required safety function. Passive safety features are subject to ageing phenomena over the multidecade life of the plant, and so a means is needed to periodically reconfirm that they also remain always capable of performing their required safety function.

The means to accomplish this reconfirmation is specific to the safety function being performed and to plant design, but the philosophy of periodic checking of passive safety features under technical specification requirements can be illustrated for the specific case of liquid metal cooled fast reactors that rely on a reactor vessel auxiliary cooling system (RVACS) for passive decay heat removal and thermo-structural reactivity feedbacks to self-regulate power output to match externally imposed heat removal rates.

First, in the case of the RVACS, performance degradation might occur due to partial clogging of ambient air circulation channels with dust, rodent nests, flooding of the lower regions of the ducting, etc.; additionally, changes of emittance properties of radiation surfaces due to oxidation or dust layers, etc., might increase heat transport impedance. Continuous heat balances on the always operating RVACS heat rejection rate can be performed in a completely straightforward manner by monitoring air flow rate and temperature rise versus reactor power level. The heat balance instrumentation will, of course, require periodic recalibration in its own right.

The thermo-structural reactivity feedbacks that govern power self-regulation are integral feedbacks which depend on temperature profiles in the reactor; they affect reactivity directly through Doppler and density coefficients of reactivity and indirectly through structural displacements which affect neutron leakage rates. Their components change versus burnup and age due to changing fuel composition and due to structural relaxations of core support structure, core clamping mechanisms, and creep of the fuel wrapper. Periodic reconfirmation to show that thermo-structural feedbacks remain in the range necessary to assure passive matching of power to external heat removal rate rests on the fact that such feedbacks are composite feedbacks with respect to externally controllable variables. These externally controllable variables are the inlet coolant temperature, the forced circulation flow rate, and the reactivity vested in control rods. Specifically, asymptotically — after transients die away — normalized power, P, depends on these external variables via a quasi reactivity balance as:

$$\Delta\rho \equiv 0 = (P-1)A + \left(\frac{P}{F} - 1\right)B + \delta T_{in} C + \Delta\rho_{ext}$$

where F is the normalized primary flow rate, and δT_{in} is change in coolant inlet temperature from its operating value.

Integral reactivity coefficients A, B, and C have the following physical interpretations:

— C is the reactivity vested in the deviation of core inlet temperature from its nominal value;
— B is the reactivity vested in the coolant average temperature rise above the coolant inlet temperature;
— A is the reactivity vested in the fuel average temperature rise above the coolant average temperature.

They are measurable in-situ on the operating power plant in a non-intrusive way by introducing step changes in flow rate, coolant inlet temperature and external (rod) reactivity and then measuring the asymptotic

value of the normalized power after the transient dies away [1]. For example, three measurements might be made wherein the external variables are changed one at a time:

- If $\Delta\rho_{ext}$ is changed while inlet temperature and flow remain fixed, the power will asymptotically self-adjust to:

$$P_1 = 1 + \frac{-\Delta\rho_{ext} / B}{1 + A/B}$$

- If flow rate is changed while inlet temperature and $\Delta\rho_{ext}$ remain fixed, the power will asymptotically self-adjust to:

$$P_2 = \frac{-(A+B)}{\left(A + \frac{B}{F_2}\right)}$$

- If inlet temperature is changed, δT, while $\Delta\rho_{ext}$ and flow rate remain fixed, the power will asymptotically self-adjust to:

$$P_3 = \frac{(A+B)}{\left(A + \frac{B}{F_o}\right)} - \left(\frac{C\,\delta T_{inlet}}{A + \frac{B}{F_o}}\right)$$

This procedure would yield three equations for the three unknowns, A, B and C, which would determine their current values on the operating reactor itself. The efficacy of such measurements in determining the values of A, B, and C on an operating reactor connected to the grid was demonstrated [2] at EBR-II.

Some small and medium sized reactors rely on natural circulation in which case flow, F, is not externally controllable, but instead is a function of power F= f(P). Assuming f(P), it could be represented as a quadratic:

$$F = a + bP + cP^{2.}$$

Several additional step changes in $\Delta\rho_{ext}$ and/or δT_{inlet} would be sufficient to determine the values of A, B, and C.

More elegant methods have been developed based on continuous monitoring and noise analysis techniques — taking advantage of spontaneous fluctuations or small purposeful power spectral density inputs to the externally controlled state variables.

These examples for liquid metal cooled fast reactors illustrate the approach that can be taken for periodic reconfirmation of the ability of passive safety features to perform their safety function. Other reactor types with different passive features may employ alternative approaches.

REFERENCES TO APPENDIX II

[1] D. C. WADE AND R. N. HILL, The design rationale of the IFR, Prog,. Nucl. Energy, **31** (1997) 13-42.

[2] PLANCHON, H.P., SACKETT, J.I., GOLDEN, G.H., SEVY, R.H., Implications of the EBR-II Inherent Safety Demonstration Test, Nucl. Eng. Des. **101**, (1987) 75.

Appendix III

TERMS USED

Small and medium sized reactors (SMRs)

According to the classification currently used by the IAEA, small reactors are reactors with an equivalent electrical power output of less than 300 MW, medium sized reactors have an equivalent electrical power output of between 300 and 700 MW [1].

Small reactors without on-site refuelling

According to the definition given in Ref. [1], small reactors without on-site refuelling are reactors designed for infrequent replacement of well-contained fuel cassette(s) in a manner that prohibits clandestine diversion of nuclear fuel material.

Safety related terms

Definitions from IAEA safety standards

The format used to describe passive safety design options for SMRs — provided in Appendix 3 and used in Annexes I–X — contributed by Member States, was developed reflecting definitions used in IAEA Safety Standards Series No. NS-R-1 Safety of Nuclear Power Plants: Design [2]:

ACTIVE COMPONENT: A component of which function depends on an external input such as actuation, mechanical movement or supply of power.

PASSIVE COMPONENT: A component of which function does not depend on an external input such as actuation, mechanical movement or supply of power.

PLANT EQUIPMENT: (see Fig. 1).

SAFETY SYSTEM: A system important to safety, provided to ensure safe shutdown of the reactor or residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents.

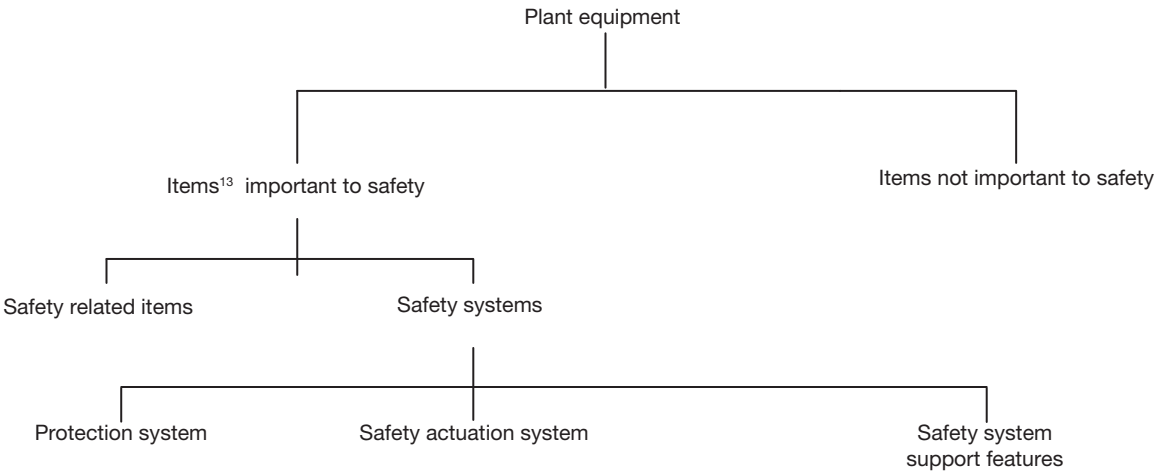
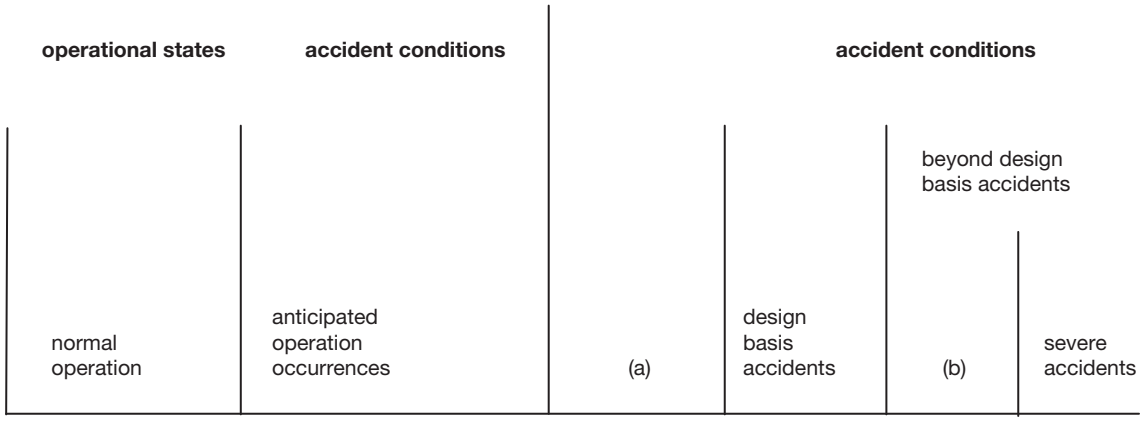


FIG. 1. Plant equipment [2].

[13] In this context, an 'item' is a structure, system or component [2].



(a) Accident conditions which are not explicitly considered design basis accidents but which they encompass;
(b) Beyond design basis accidents without significant core degradation.

FIG. 2. Plant states [2].

PROTECTION SYSTEM: A system which monitors the operation of a reactor and which, on sensing an abnormal condition, automatically initiates actions to prevent an unsafe or potentially unsafe condition.

PLANT STATES: (see Fig. 2).

NORMAL OPERATION: Operation within specified operational limits and conditions.

POSTULATED INITIATING EVENT: An event identified during design as capable of leading to anticipated operational occurrences or accident conditions.

ANTICIPATED OPERATIONAL OCCURRENCE: An operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility but which, with appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions.

ACCIDENT CONDITIONS: Deviations from normal operation more severe than anticipated operational occurrences, including design basis accidents and severe accidents.

DESIGN BASIS ACCIDENT: Accident conditions against which a nuclear power plant is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.

SEVERE ACCIDENTS: Accident conditions more severe than a design basis accident and involving significant core degradation.

ULTIMATE HEAT SINK: A medium to which residual heat can always be transferred, even if all other means of removing the heat have been lost or are insufficient.

SINGLE FAILURE: A failure which results in the loss of capability of a component to perform its intended safety function(s), and any consequential failure(s) which result from it.

COMMON CAUSE FAILURE: Failure of two or more structures, systems or components due to a single specific event or cause.

SAFETY FUNCTION: A specific purpose that must be accomplished for safety.

Non-consensus definitions from IAEA-TECDOCs

At the moment, the IAEA safety standards do not provide a complete set of definitions necessary for the description of safety features of NPPs with innovative reactors. In view of this, some missing definitions related to passive safety features could be taken from IAEA-TECDOC-626 [3]:

INHERENT SAFETY CHARACTERISTIC: Safety achieved by elimination of a specified hazard by means of the choice of material and design concept.

PASSIVE COMPONENT: A component which does not need any external input to operate.

PASSIVE SYSTEM: Either a system which is composed entirely of passive components and structures or a system which uses active components in a very limited way to initiate subsequent passive operation.

GRACE PERIOD: The grace period is the period of time during which a safety function is ensured without the necessity of personnel action in the event of an incident/accident.

Recommendations from the International Nuclear Safety Advisory Group (INSAG)

Although IAEA safety standard NS-R-1 [2] provides a consensus definition of defence in depth levels, the definitions suggested in INSAG-10 [4] may better suit for NPPs with innovative reactors. For future reactors, Ref. [3] envisages the following trends for different levels of defence in depth:

"— Level 1, for the prevention of abnormal operation and failures is to be extended by considering in the basic design a larger set of operating conditions based on general operating experience and the results of safety studies. The aims would be to reduce the expected frequencies of initiating failures and to deal with all operating conditions, including full power, low power and all relevant shutdown conditions.
— Level 2, for the control of abnormal operation and the detection of failures, is to be reinforced (for example by more systematic use of limitation systems, independent from control systems), with feedback of operating experience, an improved human-machine interface and extended diagnostic systems. This covers instrumentation and control capabilities over the necessary ranges and the use of digital technology of proven reliability.
— Level 3, for the control of accidents within the design basis, is to consider a larger set of incident and accident conditions including, as appropriate, some conditions initiated by multiple failures, for which best estimate assumptions and data are used. Probabilistic studies and other analytical means will contribute to the definition of the incidents and accidents to be dealt with; special care needs to be given to reducing the likelihood of containment bypass sequences.
— Level 4, for the prevention of accident progression, is to consider systematically the wide range of preventive strategies for accident management and to include means to control accidents resulting in severe core damage. This will include suitable devices to protect the containment function such as the capability of the containment building to withstand hydrogen deflagration, or improved protection of the basemat for the prevention of meltthrough.
— Level 5, for the mitigation of the radiological consequences of significant releases, could be reduced, owing to improvements at previous levels, and especially owing to reductions in source terms. Although less called upon, Level 5 is nonetheless to be maintained."

Terms to be avoided

The designers were not requested to adjust safety related terminology of their projects accordingly when preparing design descriptions for this report; they followed the definitions accepted in their respective Member States. However, in line with the recommendations of [6] and upon the approval from designers, terms such as 'revolutionary design', 'passive, simplified and forgiving design', 'inherently safe design', 'deterministically safe design', 'catastrophe free design' etc. were edited out from design descriptions, except for in cases when they appear in the names of certain reactor concepts.

Categorization of passive systems

At the moment, there is no consensus definition of a passive safety system.

In IAEA-TECDOC-626 [3], four different categories of passive safety features have been proposed, as described below.

Category A passive safety features are those which do not require external signal inputs of 'intelligence', or external power sources or forces, and have neither any moving mechanical parts nor any moving working fluid. Examples of safety features included in this category are:

- Physical barriers against the release of fission products, such as nuclear fuel cladding and pressure boundary components and systems;
- Hardened building structures for the protection of a plant against external event impacts;
- Core cooling systems relying only on heat radiation and/or convection and conduction from nuclear fuel to outer structural parts with the reactor in hot shutdown;

- Static components of safety related passive systems (e.g., tubes, pressurizers, accumulators, surge tanks), as well as structural parts (e.g., supports, restraints, anchors, shields).

Category B passive safety features are those which do not require external signal inputs of 'intelligence', or external power sources or forces, and have no moving mechanical parts. They do, however, have moving working fluid. Examples of safety features included in this category are:

- Reactor shutdown/emergency cooling systems based on injection of borated water produced by the disturbance of a hydrostatic equilibrium between the pressure boundary and an external water reservoir;
- Reactor emergency cooling systems based on air or water natural circulation in heat exchangers immersed in water reservoirs (inside containment) to which the decay heat is directly transferred;
- Containment cooling systems based on natural circulation of air flowing around the containment walls, with intake and exhaust through a stack or through tubes covering the inner walls of silos of underground reactors;
- Fluidic gates between process systems, such as 'surge lines' of PWRs.

Category C passive safety features are those which do not require external signal inputs of 'intelligence', or external power sources or forces. They do, however, have moving mechanical parts whether or not moving working fluids are present. Examples of safety features included in this category are:

- Emergency injection systems consisting of accumulators or storage tanks and discharge lines equipped with check valves;
- Overpressure protection and/or emergency cooling devices of pressure boundary systems based on fluid release through relief valves;
- Filtered venting systems of containments activated by rupture disks;
- Mechanical actuators, such as check valves and spring loaded relief valves, as well as some trip mechanisms (e.g., temperature, pressure and level actuators).

Category D passive safety features, referred to as 'passive execution /active initiation' type features, are those passive features where the execution of the safety function is made through passive methods as described in the previous categories except that internal intelligence is not available to initiate the process. In these cases an external signal is required to trigger the passive process. Since some desirable characteristics usually associated with passive systems (such as freedom from external sources of power, instrumentation and control and from required human actuation) are still to be ensured, additional criteria such as the following are generally imposed on the initiation process:

- Energy must only be obtained from stored sources such as batteries or compressed or elevated fluids, excluding continuously generated power such as normal AC power from continuously rotating or reciprocating machinery;
- Active components in passive systems are limited to controls, instrumentation and valves, but valves used to initiate safety system operation must be single action, relying on stored energy, and manual initiation is excluded.

Examples of safety systems which may be included in this category are:

- Emergency core cooling/injection systems, based on gravity driven or compressed nitrogen driven fluid circulation, initiated by fail safe logic actuating battery powered electric or electro-pneumatic valves;
- Emergency core cooling systems, based on gravity driven flow of water, activated by valves which break open on demand (if a suitable qualification process of the actuators can be identified);
- Emergency reactor shutdown systems based on gravity driven, or static pressure driven control rods, activated by fail-safe trip logic.

Some non-conventional terms used in this report

(1) The wording 'reactor line' is used to denote the totality of known designs of reactors of a given type, e.g., the reactor lines considered in the present report are pressurized water reactors, pressurized light water cooled heavy water moderated reactors, high temperature gas cooled reactors, sodium cooled and lead cooled fast reactors, and non-conventional reactor designs.

(2) Several designers of SMRs addressed in this report use the wording 'passive shutdown' to denote bringing the reactor to a safe low-power state with balanced heat production and passive heat removal, with no failure to the barriers preventing radioactivity release to the environment; all relying on inherent and passive safety features only, with no operator intervention, no active safety systems involved, and no external power and water supplies necessary, and with an infinite grace period for practical purposes.

(3) The wording 'reactor self-control' is used by the designers of SMRs to refer to the capability of an reactor to self-adjust reactivity and power levels in a way that prevents the progression of a abnormal operation occurrence or a design basis accident into a more severe stage, without the operation of active safety systems or operator intervention.

(4) Descriptions of the passive safety design features of SMRs, contributed by Member States and given in Annexes I–X of this report, may occasionally include the following terms that are not accepted internationally but are in use in certain Member States:
- In India they may use the term 'incident conditions' instead of 'accident conditions' defined in NS-R-1 [2];
- In France they may use the term 'intrinsic safety feature' with a meaning corresponding to 'inherent safety feature' used by the IAEA [2];
- In the Russian Federation, the term 'self-protection feature' is sometimes used to denote a capability of a reactor to bring itself in safe state in a certain unprotected transient without human intervention. It is used to denote a combination of inherent and passive safety features and also includes passively actuated or permanently operating passive safety systems;
- Also in the Russian Federation, the term 'self-defence principle' is sometimes used in application to innovative reactors to define use of reactor inherent and passive safety features and passive safety systems to ensure 'deterministic type' protection from more important severe accidents;
- In the USA, within I-NERI and Generation IV programmes, the term 'passive safety' is used in a meaning very close to what IAEA-TECDOC-626 defines as inherent safety characteristic. Specifically, 'passive safety' includes such phenomena: the core is always covered with coolant, or elimination of a possibility to lose the flow of a primary system;
- The IRIS team led by Westinghouse (USA) uses the term 'safety-by-design' to characterize an inherent safety feature where postulated accidents by design: 1) are outright eliminated, or 2) have reduced probability of occurring, and/or 3) have reduced consequences;
- Regarding passive design options not related to safety, the term 'passive load follow' is used in the USA to denote self-adjustment of a reactor power due to reactivity feedbacks following changes of heat removal;
- In the USA, the term 'pre-conceptual design' is used to denote the early design stage, referred to as 'feasibility study' in [7];
- Also in the USA, the term 'to design-out certain events' is used to denote essential suppression or elimination of certain events by design.

REFERENCES TO APPENDIX III

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Innovative Small and Medium Sized Reactors: Design Features, Safety Approaches and R&D Trends, IAEA-TECDOC-1451, IAEA Vienna (2005)

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design IAEA Safety Standards Series No. NS-R-1, IAEA, Vienna (2000)

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Terms for Advanced Nuclear Plants, IAEA-TECDOC-626, IAEA, Vienna (1991).

[4] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

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

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Terms for Describing New, Advanced Nuclear Power plants, IAEA-TECDOC-936, IAEA, Vienna (1997).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Innovative Small and Medium Sized Reactor Designs 2005: Reactors with Conventional Refuelling Schemes, IAEA-TECDOC-1485, IAEA, Vienna (2006).

Appendix IV

OUTLINE DESCRIBING SAFETY DESIGN FEATURES OF SMRs

1. Reactor full and abbreviated name

2. Brief description of the design and safety design concept with reference to previous publications

3. Description of inherent (by-design) and passive safety features, passive and active systems

- Inherent and passive safety features (Category A in IAEA-TECDOC-626)
- Passive systems (Categories B, C, D in IAEA-TECDOC-626)
- Active systems

IMPORTANT: For each passive and active system, please, indicate whether it is safety grade or a backup system

4. Role of inherent and passive safety features and passive and active systems in defence in depth (NS-R-1, with a reference to questionnaire Q4)

Level 1: Prevention of abnormal operation and failure
Level 2: Control of abnormal operation and detection of failure
Level 3: Control of accidents within the design basis
Level 4: Control of severe plant conditions, including prevention of accident progression and mitigation of consequences of severe accidents
Level 5: Mitigation of radiological consequences of significant release of radioactive materials

Note: Please try to follow this IAEA-supported DID structure, even if in your domestic practice the concept of DID is different.

5. Acceptance criteria for design basis accidents (DBA) and beyond design basis accidents (BDBA)

- List of DBA and BDBA (NS-R-1)
- Acceptance criteria for DBA and BDBA (deterministic and probabilistic, if applicable)
- Protection against the impacts of external events, and combinations of events considered in the design (NS-G-3.3, and NS-G-1.5)
- Probability of unacceptable radioactivity release beyond the plant boundaries
- Measures planned in response to severe accidents

6. Questionnaires

Q1. List of safety design features considered for/incorporated into a SMR design

#	SAFETY DESIGN FEATURES	WHAT IS TARGETED?

Q2. List of internal hazards

#	HAZARDS THAT ARE OF SPECIFIC CONCERN FOR A REACTOR LINE	EXPLAIN HOW THESE HAZARDS ARE ADDRESSED IN AN SMR

Q3. List of initiating events for safety analysis

#	LIST OF INITIATING EVENTS FOR SAFETY ANALYSIS (BOTH TYPICAL FOR THIS REACTOR LINE AND CHARACTERISTIC OF THIS INDIVIDUAL DESIGN) MARK INITIATING EVENTS THAT ARE SPECIFIC TO THIS PARTICULAR SMR	SPECIFY DESIGN FEATURES OF AN SMR USED TO PREVENT PROGRESSION OF INITIATING EVENTS TO AOO/DBA/BDBA, USED TO CONTROL DBA, USED TO MITIGATE BDBA CONSEQUENCES, ETC.

Q4. Safety design features attributed to defence in depth levels

#	SAFETY DESIGN FEATURE	(1) INDICATE AOO/DBA/BDBA OF RELEVANCE (2) INDICATE CATEGORY: A-D* (FOR PASSIVE SYSTEMS ONLY)	RELEVANT DID LEVEL ACCORDING TO NS-R-1**

* Categories A-D correspond to IAEA-TECDOC-626

** An outline of approaches to DID for advanced NPPs is provided in INSAG-10 and IAEA-TECDOC-1434

Q5. Positive/negative effects of passive safety design features in areas other that safety (if any)

PASSIVE SAFETY DESIGN FEATURES	POSITIVE EFFECTS ON ECONOMICS, ETC.	NEGATIVE EFFECTS ON ECONOMICS, ETC.

Annex I

SAFETY DESIGN FEATURES OF THE KLT-40S

OKBM,
Russian Federation

I–1. DESCRIPTION OF A NUCLEAR INSTALLATION WITH THE KLT-40S REACTOR

The KLT-40S is a modular reactor unit developed for a pilot floating nuclear cogeneration plant (PATES, in Russian), currently under construction in Severodvinsk, the Russian Federation. The KLT-40S nuclear installation belongs to a class of pressurized water reactors. The KLT-40S reactor unit is shown in Fig. I-1. Major specifications of the KLT-40S nuclear installation are given in Table I-1. A detailed design description of a floating NPP with KLT-40S reactor installations is provided in [I-1].

The main design features of the KLT-40S are the following:

- Modular design of reactor unit: the reactor, the steam generators (SGs) and the main coolant pumps (MCPs) are connected with short nozzles, without using long pipelines;
- Four-loop reactor cooling system with forced and natural convection of the coolant in the primary circuit;
- Leaktight primary circuit with canned motor pumps and leaktight bellows type valves;
- Once-through coil type SGs;
- Gas based pressurizer system in the primary circuit;
- Use of passive safety systems;
- Use of proven techniques for equipment assembly, repair and replacement; incorporation of proven diagnostics equipment and proven monitoring systems.

The KLT-40S core is based on marine reactor technologies and incorporates materials that are exempted from the IAEA definition of direct use material.

To increase uranium fraction, a closely packed assembly structure of the core is adopted, which provides maximum possible fuel volume in a given core volume. The core contains fuel rods with cylindrical claddings made of corrosion resistant zirconium alloy. The fuel rods are similar to those of the ice-breaker reactors but incorporate fuel with higher uranium fraction; such fuel is based on uranium dioxide granules in the inert matrix.

Each reactor unit of the floating nuclear power plant (NPP) is located in a containment that is a leaktight physical barrier designed to limit the propagation of radioactivity and to localize fission products in case of a loss of coolant accident (LOCA), using emergency containment cooling systems.

The containment is designed for internal pressure typical of design basis accidents and beyond design basis accidents, taking into account the emergency temperature conditions. The design value of the containment leakage rate ensures maximum possible limitation of the emergency planning area.

The containment, along with the barge structures, is designed for design basis external impacts including a floating NPP sink.

Protection of the systems important for safety from external impacts is provided by a protective enclosure. The protective enclosure is a waterproof and gas proof structure included in a ship hull; it covers the containment and the liquid and solid radioactive waste storage, and provides additional limitation of a leakage of radioactive products to other parts of the floating power plant and to the environment, in case of a severe accident.

The containment and the radioactive waste storage are placed in a power compartment located in the middle part of the floating power unit.

A general view of the floating power module is shown in Fig. I-2.

The floating power unit (FPU) is a flat deck non-self-propelled ship with a developed multilevel superstructure. An all-welded vessel of the floating power unit has ice reinforcements and special means for hauling and shoring. Nine waterproof bulkheads rising up to the top deck divide the FPU vessel into 10 impermeable compartments.

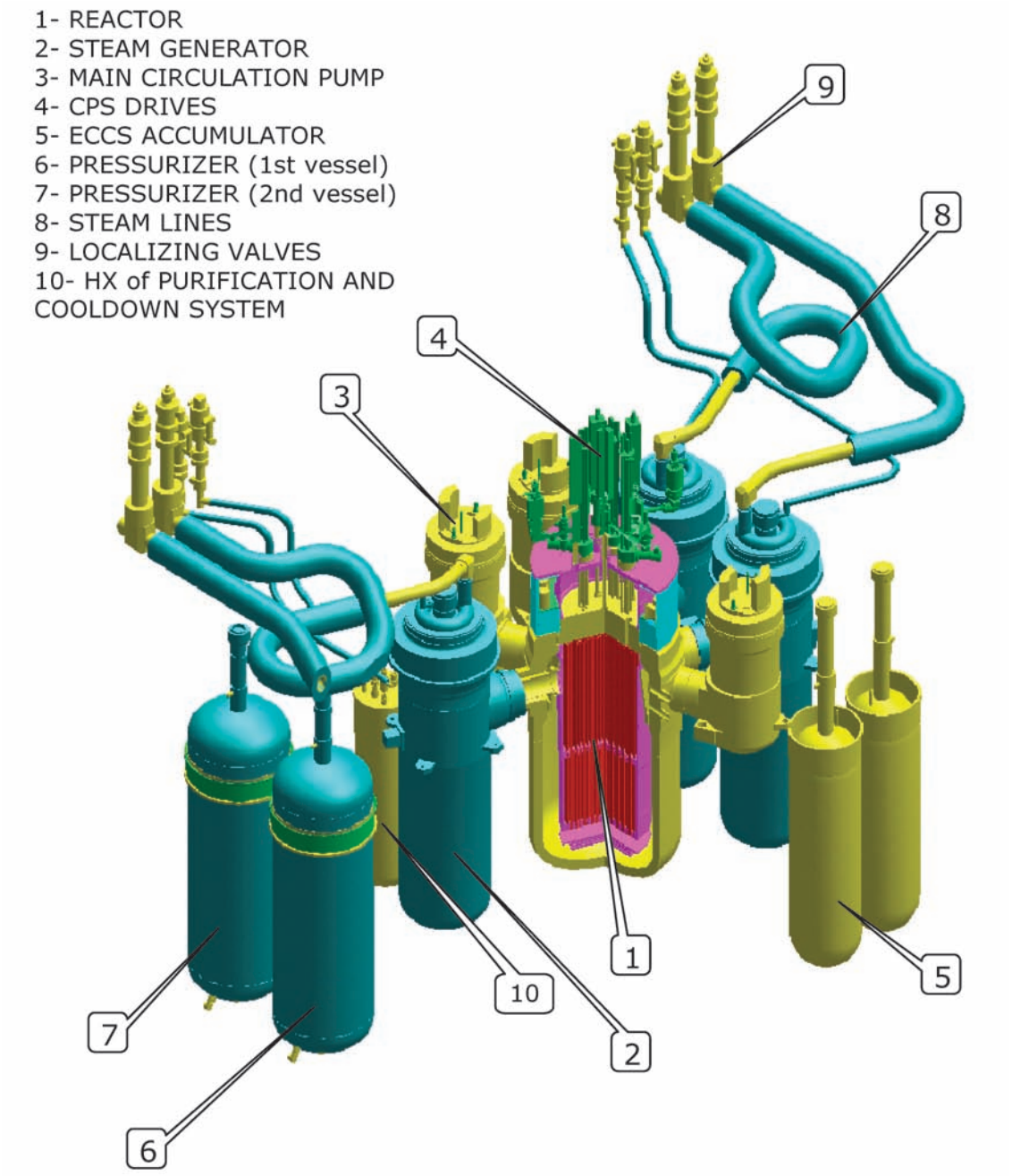


FIG. I–1. General view of the KLT-40S nuclear installation.

The floatability of the FPU is provided in case of flooding of any two adjacent compartments for all specification load cases satisfying the requirements of the Russian Marine Register.

I–2. PASSIVE SAFETY DESIGN FEATURES OF KLT-40S

Passive safety design features of the KTL-40S nuclear installation include both inherent safety features and dedicated passive (safety) systems.

TABLE I–1. MAJOR SPECIFICATIONS OF THE KLT-40S POWER PLANT

Characteristic	Value
Thermal power, MW	150
Primary circuit pressure, MPa	12.7
Coolant temperature, °C:	
—at core outlet	317
— at core inlet	279
Parameters of superheated steam downstream of the SG:	
— pressure, MPa	3.73
— temperature, °C.	290
Feedwater temperature, °C	170

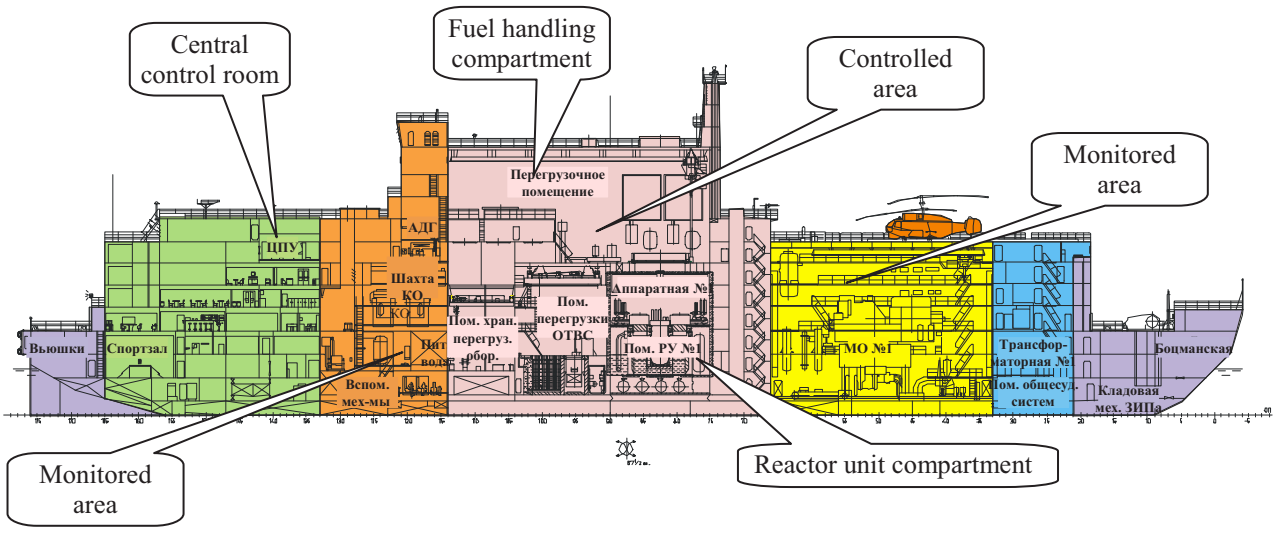


FIG. I-2. Floating power unit with two KLT-40S nuclear installations.

The so-called self-protection of a nuclear installation is expressed in its capability to prevent the occurrence and to limit the propagation and consequences of initiating events which could lead to accidents. Self-protection is, inter alia, achieved by reliance on natural feedbacks and processes that require no operator intervention, no external power, and no assistance from emergency teams for a certain period of time which could be used by personnel to evaluate the situation and to undertake necessary corrective actions.

The self-protection of the KLT-40S is provided by the following features:

(a) Negative reactivity coefficients on fuel and coolant temperature and on specific volume of the coolant; negative reactivity coefficients on steam density and integral power;
(b) High thermal conductivity of the fuel composition defining its relatively low temperature and, correspondingly, low stored non-nuclear energy;
(c) Adequate level of natural circulation flow in the primary system;
(d) High heat capacity of the nuclear installation as a whole, resulting from high heat capacity of the primary coolant and metal structures, from the use of a 'soft' pressurizer system[1], and from a safety margin

[1] A 'soft' pressurizer system is characterized by small changes of the primary pressure under a primary coolant temperature increase. This quality, due to a large volume of gas in the pressurizing system, results in an increased period of pressure increase up to the limit value under the total loss of heat removal from the primary circuit. For KLT-40S, the corresponding time is not less than 1.5 hours after the accident starts.

provided for by the design for the depressurization pressure of the primary system under emergency pressure increase;

(e) Compact design of the steam generating unit, with short nozzles between the main equipment items and with no large diameter primary pipelines;

(f) The use of restriction devices in nozzles connecting the primary circuit systems to the reactor, which limits the outflow rate in case of a break; the location of the connection nozzles is selected so that they provide a fast transition to the steam outflow of the primary coolant in case of a break in the corresponding pipeline;

(g) Favourable conditions for the realization of a 'leak before break' concept in application to structures of the primary circuit, provided by design;

(h) The use of once-through steam generators, which limits the rate of heat removal via the secondary circuit in case of a steam line break accident.

The active and passive safety systems (see Fig. I-3) are incorporated in the design of the KLT-40S to carry out the following safety functions:

— Emergency shutdown of the reactor;
— Emergency heat removal from the primary circuit;
— Emergency core cooling;
— Localization of released radioactive products.

Active safety systems

The KLT-40S nuclear installation incorporates the following active safety systems:

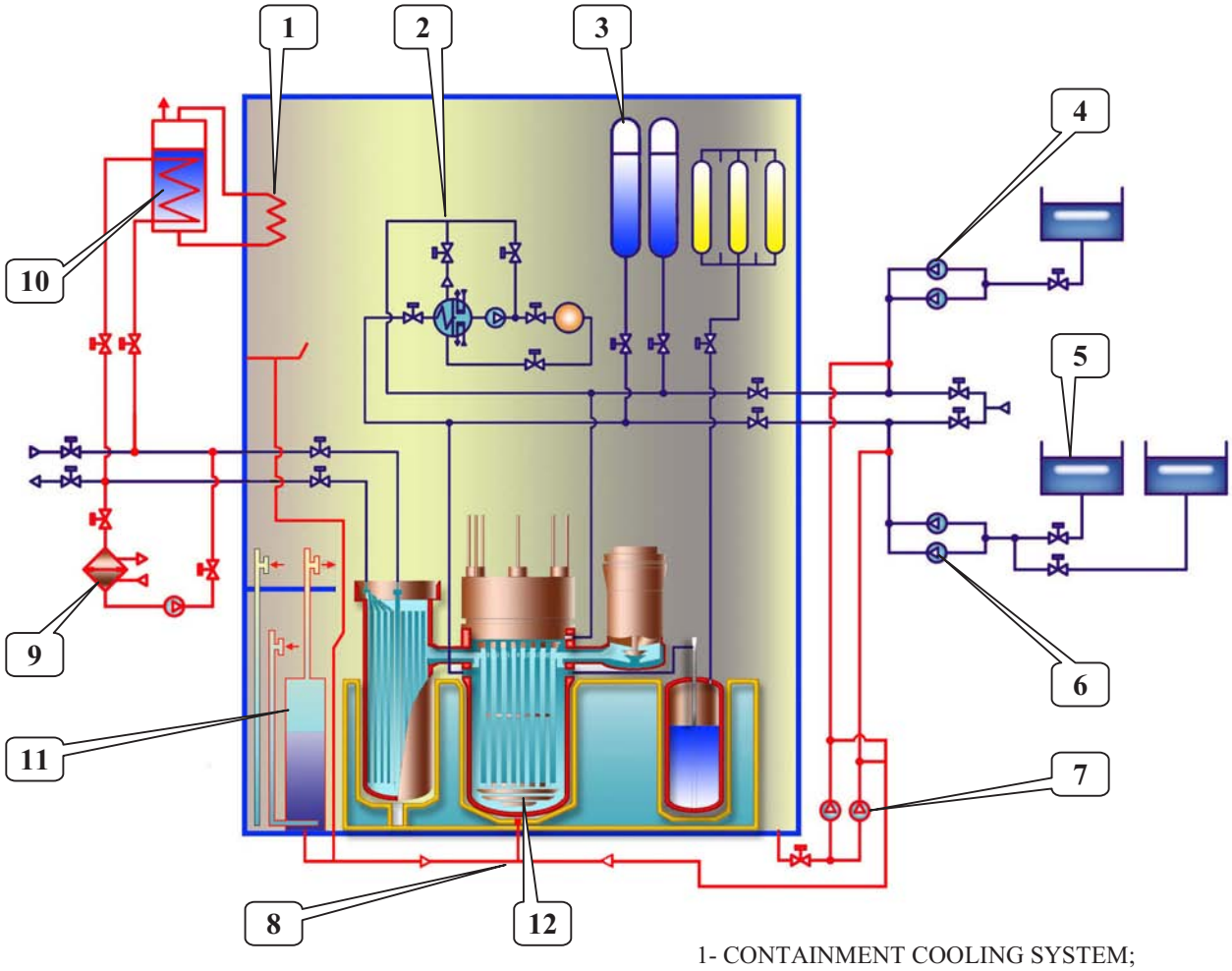
— System of reactor shutdown with shim control rod insertion in the electromotive mode;
— System of emergency reactor cooldown through the steam generator with steam dumping to a process condenser;
— System of emergency reactor cooldown through the heat exchanger of the purification and cooldown system;
— System of emergency water supply from the emergency core cooling system (ECCS) pumps and the recirculation pumps;
— Filtration system for releases from the protective enclosure.

Passive systems

The KLT-40S nuclear installation incorporates the following passive safety systems:

— System of reactor shutdown with insertion of control rods into the core under the force of springs (scram rods) or gravity (shim control rods), when holdup electromagnets from the control rod drives are de-energized;
— Passive system of emergency reactor cooldown through the steam generator;
— System of emergency water supply from the ECCS hydro-accumulators;
— Containment and stop valves, normally in a closed position, located at the auxiliary systems of the primary circuit and adjacent systems;
— Passive system of external cooldown of the reactor vessel;
— Self-actuated devices for startup of the safety systems;
— Emergency containment cooling system;
— Protective enclosure.

Passive safety systems operate with natural circulation of the coolant or use the energy of a compressed gas.



1- CONTAINMENT COOLING SYSTEM;
2-PURIFICATION AND COOLDOWN SYSTEM
3-ECCS ACCUMULATORS;
4, 6-ACTIVE ECCS;
5-ACTIVE ECCS TANK;
7-RECIRCULATION SYSTEM PUMPS;
8-RVCS;
9-ACTIVE EHRS;
10-PASSIVE EHRS;
11-CONTAINMENT BUBBLING SYSTEM;
12-REACTOR

ECCS – emergency core cooling system RVCS – reactor vessel cooling system
EHRS – emergency heat removal system

FIG. I-3. Safety systems of KLT-40S.

The emergency heat removal system (EHRS) is intended to remove residual heat from the reactor in beyond design basis accidents involving NPP blackout and failure of active channels. The system includes two channels, consisting of two heat exchange loops each. The capacity of a single EHRS loop (~1% of nominal reactor power) is sufficient to ensure reliable reactor cooldown and to maintain reactor pressure within design limits.

Residual heat is removed by natural convection of coolant in the primary and intermediate circuits and by the evaporation of water from the tank where heat exchanger-condensers (HXC) are located. Water reserve in EHRS tanks ensures heat removal from the reactor over 24 hours.

The prototypes of a passive EHRS are cooling systems used in propulsion reactors. The effectiveness of such systems has been confirmed both by experiments at test facilities and by tests at operating plants.

The majority of KLT-40S safety systems employ a two channel scheme with internal reservation of active elements such as valves and pumps. Using a two channel scheme for safety systems within the specific conditions of a floating structure (where it is necessary to save on space and equipment weight compared to land based NPPs) allows for a reduction in the amount of bulky equipment required, such as tanks and heat exchangers.

Elements of both active and passive safety systems belong to the second safety class, according to the top level Russian regulation OPB-88/97.

The requirements for manufacturing technologies of devices and equipment for active and passive safety systems correspond to regulatory requirements in the nuclear energy area.

For floating NPPs, specific regulations have been developed and adopted in the Russian Federation, in particular, "The rules of arrangement and safe operation of the equipment and items for light water reactors of the floating nuclear power plants (NP-062-05)".

I–3. ROLE OF PASSIVE SAFETY DESIGN FEATURES IN DEFENCE IN DEPTH

Safety of small sized heat and power plants with KLT-40S reactors is ensured by the incorporated defence in depth strategy. It includes a plan for accident prevention and mitigation, and envisages the use of a system of physical barriers on the possible pathways of propagation of the ionizing radiation and radioactive materials to the environment. The incorporated defence in depth strategy also provides for the use of a system of technical and organizational arrangements to protect the barriers and retain their effectiveness, and includes measures for protection of the personnel, population and environment.

The structure of the defence in depth system is based on the recommendations of IAEA [I-2, I-3], providing for the following levels:

Level 1 – Prevention of abnormal operation and failure;
Level 2 – Control of abnormal operation and detection of failure.;
Level 3 – Control of accidents within the design basis;
Level 4 – Control of severe plant conditions, including prevention of accident progression and mitigation of consequences of severe accidents;
Level 5 – Mitigation of radiological consequences of significant release of radioactive materials.

The role of inherent and passive safety features and of active and passive safety systems of the KLT-40S nuclear installation at certain levels of defence in depth is highlighted in brief below.

Level 1: Prevention of abnormal operation and failure

Inherent safety features contributing to this level are the following:

— Negative reactivity coefficients on fuel and coolant temperature and on specific volume of the coolant; negative reactivity coefficients on steam density and integral power in the whole range of reactor operation parameters;
— High thermal conductivity of fuel composition defining its relatively low temperature and, correspondingly, low stored non-nuclear energy;
— The use of compact modular design of the steam generating unit with short nozzles between the main equipment, and with no long or large diameter primary pipelines;
— The use of flow restriction devices to exclude large and medium break loss of coolant accidents (LOCAs), by design;
— Ultimately leaktight design of the primary circuit based on welded joints, packless canned pumps, and leaktight bellows sealed valves;
— Favourable conditions for the realization of a 'leak before break' concept in application to structures of the primary circuit, provided by design;
— The use of a gas pressurizer system that excludes failures of the electric pressurizer heaters;
— The use of a steam generator with lower pressure inside the tubes in normal operation mode, which reduces the probability of a steam generator tube rupture (SGTR) accident.

Level 2: Control of abnormal operation and detection of failure

The Level 2 contribution comes from active systems for the control, mitigation, protection and diagnostics used in the KLT-40S nuclear installation.

Level 3: Control of accidents within the design basis

The Level 3 contribution comes from the following inherent and passive safety features, provided by design:

— Limitation of an uncontrolled movement of the control rods (e.g., due to external impact loads or a break of the control and protection system (CPS) drive casing) by an overrunning clutch, or by movement limiters for an accident with the CPS drive bar break;
— The use of once-through steam generators, which limit the rate of heat removal via the secondary circuit in case of a steam line break accident.
— High heat capacity of the nuclear installation as a whole, resulting from high heat capacity of the primary coolant and metal structures, from the use of a 'soft' pressurizer system, and from a safety margin provided by design for the depressurization of the primary system under emergency pressure increase;
— Installation of restriction devices in the pipelines of the primary circuit systems and connection of these pipelines to the 'hot' part of the reactor.

Also for Level 3, the following passive safety systems of the KLT-40S provide a contribution:

— Insertion of scram control rods into the core by the force of accelerating springs;
— Insertion of shim control rods into the core by the force of gravity;
— The use of a passive emergency heat removal system (EHRS), using natural convection of coolant in all circuits and evaporation of water in the storage tanks;
— The level of natural convection flow in the primary circuit is adequate for core cooling in the case of all MCPs being switched off;
— The use of self-actuating devices in emergency reactor shutdown system and in the EHRS.

Level 4: Control of severe plant conditions, including prevention of accident progression and mitigation of consequences of severe accidents

The contribution for Level 4 comes from the following inherent and passive safety features, provided by design:

— The protective enclosure;

Also for Level 4, the following passive safety systems of the KLT-40S provide a contribution:

— The ESSC hydro-accumulators, which ensure a time margin for accident management in case of a failure of the active ECCS systems;
— Passive system of reactor vessel bottom cooling, which ensures in-vessel retention of core melt;
— Passive containment cooling system, provided to reduce containment pressure and limit radioactive release.

Level 5: Mitigation of radiological consequences of significant release of radioactive materials

The mitigation of radiological consequences in the case of a significant release of radioactive materials is assumed to be provided for mainly through administrative measures.

I–4. ACCEPTANCE CRITERIA FOR DESIGN BASIS AND BEYOND DESIGN BASIS ACCIDENTS

I–4.1. Lists of design basis accidents and beyond design basis accidents

The lists of initiating events, design basis and beyond design basis accidents for a floating NPP with KLT-40S nuclear installations have been developed on the basis of analysis of possible disturbances of normal operation caused by equipment failures, personnel errors, and internal and external impacts, also taking into account possible additional failures in the safety systems.

The basis for these lists was provided by corresponding lists of initiating events and accident scenarios for a prototype ice breaker reactor installation KLT-40; the KLT-40 lists were then modified, taking into account changes in structures and systems made during the transition to KLT-40S reactor installation, as well as experience in design and operation of relevant propulsion and land based NPPs.

The lists of initiating events and accidents adopted for the KLT-40S take into account typical lists given in the safety requirements of IAEA Safety Standards Series No. NS-R-1 [I-2].

Classification of the initiating events is adopted in accordance with the OPB-88/97 terminology, taking into account that initiating events associated with an independent single failure of a safety system element may lead to a pre-accident situation (abnormal plant state with disturbance of safe operation conditions that does not propagate into an accident) or to a design basis accident (abnormal plant operation with a release of radioactive materials beyond design barriers).

In safety substantiation of the nuclear installation, all operating conditions of the reactor unit and the floating NPP were taken into account, including startup, heatup, power operation, refuelling, repair and maintenance, hauling, etc.

The list of initiating events of pre-accident situations and design basis accidents is given in Table I-2. The list of beyond design basis accidents is presented in Table I-3.

TABLE I-2. CLASSIFICATION LIST OF INITIATING EVENTS OF PRE-ACCIDENT SITUATIONS AND DESIGN BASIS ACCIDENTS

Class of initiating events	Initiating event
	1. Faults in operation of reactor unit systems
1.1. Disruptions of reactivity and core power distribution	1.1.1. Uncontrolled change of shim control rod group position 1.1.2. Main coolant pump (MCP) switching on with deviation from instruction 1.1.3. Drop of one scram or shim control rod group 1.1.5. Faulty reactor shutdown 1.1.6. Faulty switching on of the standby cooldown pump 1.1.7. Disturbance of the design configuration of control rods of the control and protection system (CPS) at power operation
1.2. Increase of heat removal from the primary circuit	1.2.1. Decrease of feedwater temperature 1.2.2. Increase of feedwater flow 1.2.3. Increase of steam flow (opening of a dump valve and its failure to close, actuation of a safety valve on the steam line and its failure to close) 1.2.4. Guillotine break of the main steam line 1.2.5. Small break of the main steam line 1.2.6. Faulty switching on of the emergency heat removal system (EHRS) channels

TABLE I-2. CLASSIFICATION LIST OF INITIATING EVENTS OF PRE-ACCIDENT SITUATIONS AND DESIGN BASIS ACCIDENTS (cont.)

Class of initiating events	Initiating event
1.3. Decrease of heat removal from the primary circuit	1.3.1. Decrease of steam flow (one or two of the SGs switching off; malfunctions in control system; turbo-generator failure; failure of the main condenser) 1.3.3. Decrease of feedwater flow (closure of a feedwater valve; stop of the feedwater pumps) 1.3.4. Termination of a feedwater flow 1.3.5. Guillotine break of the feedwater pipeline 1.3.6. Small break of the feedwater pipeline 1.3.7. Malfunction of equipment cooling by the third circuit 1.3.8. Disruption of heat removal to the outboard water (stop of the fourth circuit pump, break of the fourth circuit pipeline) 1.3.9. Disconnection of high pressure gas reservoirs (balloons) from the pressurizer in normal operation mode 1.3.10. Drop of compressed air pressure in the valve driving system 1.3.11. Faulty disconnection of the purification and cooldown system 1.3.12. Faulty disconnection of the cogeneration bleed-off
1.4. Loss of electric power sources	1.4.1. Partial loss of auxiliary power 1.4.2. Total loss of auxiliary power (blackout of the two switchboards)
1.5. Decrease of the reactor coolant system flow rate	1.5.1. Transition of one or two of the MCPs from high speed to low speed (high speed 'blackout') 1.5.2. Stopping of one or two of the MCPs running at low speed 1.5.3. Stopping of one or two of the MCPs running at high speed 1.5.4. Transition of four MCPs from high speed to low speed 1.5.5. Stopping of four MCPs 1.5.6. Seizure of one MCP
1.6. Increase of the reactor primary coolant system inventory	1.6.1. Inadvertent operation of the make-up system
1.7. Loss of coolant accidents (LOCAs)	1.7.1. Guillotine break of the pressurizer surge line 1.7.2. Guillotine break of the purification and cooldown system pipeline 1.7.3. Guillotine break of the emergency core cooling system (ECCS) pipeline in a section which cannot be cut off 1.7.4. Break of the CPS drive support (bar) 1.7.5. Steam generator tube rupture 1.7.6. Tube rupture in the heat exchanger of purification and cooldown system 1.7.7. Tube rupture of the MCP cooler 1.7.8. Leak of a cooler for the supports of the CPS drives 1.7.9. Small primary circuit LOCA 1.7.10. Faults in sampling and draining of the reactor coolant 1.7.11. Rupture of the sampling pipeline outside the containment
	2. Internal impacts
2.1. Fires	2.1.1. Fires in the floating power unit (FPU) compartments
2.2. Flooding, steaming of the compartments	
2.3. Explosion of the gas balloons	

TABLE I-2. CLASSIFICATION LIST OF INITIATING EVENTS OF PRE-ACCIDENT SITUATIONS AND DESIGN BASIS ACCIDENTS (cont.)

Class of initiating events	Initiating event
	3. Accidents in a shutdown state
3.1. Disruptions of reactivity & core power distribution	3.1.1. Drop of a 'fresh' fuel assembly to the wrong place during refuelling
3.2. Disruptions in heat removal	3.2.1. Total blackout during long term cooling of the reactor unit 3.2.2. Total blackout during refuelling 3.2.3. Total blackout during equipment maintenance 3.2.4. Termination of heat removal during refuelling 3.2.5. Termination of heat removal during equipment maintenance
3.3. LOCAs	3.3.1. Guillotine break of the pressurizer surge line in reactor hot shutdown state 3.3.2. Faults in sampling and draining of the reactor coolant
3.4. Disruption of water and gas chemistry in an opened reactor	
3.5. Fire in the reactor equipment compartment during refuelling or maintenance	
	4. Disruptions in nuclear fuel and radioactive waste handling
4.1. Disruptions at refuelling	4.1.1. Hang-up of a spent fuel assembly during refuelling 4.1.2. Hang-up of a container with spent fuel assemblies 4.1.3. Drop of a spent fuel assembly 4.1.4. Drop of a case with a spent fuel assembly 4.1.5. Blackout of refuelling equipment
4.2. Disruptions in nuclear fuel storage systems	4.2.1. Depressurization of a cooling circuit and gas system for spent fuel and solid waste storage 4.2.2. Blackout of the cooling system for spent fuel assembly storage tanks or decrease of heat removal from the tanks 4.2.3. Termination of heat removal from the spent fuel assembly storage tank 4.2.4. Leak of a case in the spent fuel assembly storage tank 4.2.5. Flooding or steaming of the storage tank and of the case with spent fuel assemblies 4.2.6. Disruption of gas content conditions in the spent fuel storage
4.3. Release of radioactive fluids from equipment and systems	4.3.1. Leaks in pipelines and equipment sealing: Leak in the gas removal system; Leak in the drainage and sampling system; Leak in the zero-discharge technology system 4.3.2. Disruptions during reloading of the reactor coolant system filter, resulting in the release of radioactive substances
	5. External impacts on the FPU
5.1. Taking place on site, as a result of natural events	5.1.1.Break of the rigid mooring bars due to formation of an ice plug with subsequent FPU grounding under the impact of wind and rough water 5.1.2. Earthquake
5.2. Taking place on site, as a result of human induced events	5.2.1. Explosion of an external source on the shore 5.2.2. Explosion on a moored tanker 5.2.3. Pressing of a mooring ship 5.2.4. Break of shore communication pipelines 5.2.5. Helicopter crash-landing on the FPU
5.3. Taking place at hauling	5.3.1. Collision of the FPU with another ship 5.3.2. Grounding

TABLE I-3. LIST OF BEYOND DESIGN BASIS ACCIDENTS

Groups of beyond design basis accidents	Representative scenarios of beyond design basis accidents
	1. Accidents in leaktight reactor coolant system
1.1. Accidents with disruption of reactivity	1.1.1. Inadvertent withdrawal of shim control rod groups driven simultaneously with normal or emergency speed 1.1.2. Inadvertent withdrawal of any of the two shim control rod groups accompanied by a failure of the system of detection and termination of control rod inadvertent movement, and a failure of the control system of reactor shutdown on power and/or doubling period signal 1.1.3. Drop of one control rod group with failures in the CPS: failures of interlocks, failures of control rod movement algorithms, failure of emergency reactor shutdown 1.1.4. Erroneous loading and operation of a fuel assembly in a wrong position 1.1.5. Break of a steam line inside the containment
1.2. Anticipated Transients Without Scram (ATWS)	1.2.1. 'Hang up' of all shim or scram control rod groups or failures of the control system of emergency reactor shutdown on all protection signals, incited by the following initiating events: (1) Termination of steam flow to the turbine (closure of valves on the main steam lines); (2) Maximum increase of steam flow in the secondary system (full opening of the safety valve and its seizure in this position); (3) Termination of the feedwater flow (full closure of the feedwater valve); (4) Switch off of all MCPs; (5) Total blackout of the two auxiliary power switchboards; (6) Inadvertent withdrawal of simultaneously driven control rod groups (at reactor startup or during power operation)
1.3. Disruption of heat removal with failures in the emergency heat removal system (EHRS)	1.3.1. Break of the feedwater line with a failure of the fourth circuit and a failure of the system of outboard water supply to process condenser 1.3.2. Break of the feedwater line with EHRS failure to start on automatic signals 1.3.3. Total blackout with failure of all emergency and backup alternate current (AC) sources 1.3.4. Termination of heat removal by the secondary circuit with inadvertent cut off of the high pressure gas balloons 1.3.5. Break of the feedwater line with complete failure of the reactor shutdown system 1.3.6. Partial blockage of the reactor coolant circuit or of the fuel assembly inlet
	2. Loss of coolant accidents
2.1. LOCAs inside the containment	2.1.1. Guillotine break of the reactor coolant system pipeline with failure of the active ECCS subsystem 2.1.2. Guillotine break of the reactor coolant system pipeline with failure of the passive ECCS subsystem (hydro-accumulators) 2.1.3. Guillotine break of an ECCS pipeline of one of the channels with a pump failure at the second channel 2.1.4. Guillotine break of a reactor coolant system pipeline with a double end leak (failure of the cut-off valves of the purification system) and a failure of the active ECCS subsystem 2.1.5. Guillotine break of a reactor coolant system pipeline with failure to cut off the high pressure gas balloons 2.1.6. Small LOCA with total blackout, due to the loss of all AC sources 2.1.7. Guillotine break of a reactor coolant system pipeline with total blackout, due to the loss of all AC sources 2.1.8. Guillotine break of a reactor coolant system pipeline with failure to close the cut-off valves in the containment ventilation system on automatic signals 2.1.9. Rupture of a CPS drive support

TABLE I-3. LIST OF BEYOND DESIGN BASIS ACCIDENTS (cont.)

Groups of beyond design basis accidents	Representative scenarios of beyond design basis accidents
2.2. Accidents with bypassing of the containment	2.2.1. SG tube rupture with a failure of the cut-off valves to close 2.2.2. Break of a steam line – SG collector with a failure of the cut-off valves to close 2.2.3. Leak of a cooler supporting the CPS drives with a failure of the cut-off valves to close 2.2.4. Rupture of an MCP cooler tube with a failure of the cut-off valves to close 2.2.5. Rupture of an MCP cooler tube with a failure to cut off the high pressure gas balloons 2.2.6. Rupture of a tube in the heat exchanger of the purification and cooldown system with a failure to close the cut-off valves 2.2.7. Break of a cooling water outlet pipeline in the heat exchanger of the purification and cooldown system with failure to close the cut-off valves 2.2.8. Rupture of a pipeline of the sampling system with failure to close cut-off valves located on the lines of the sampling systems and the purification and cooldown system
2.3. Accumulation of a potentially explosive gas mixture in the reactor in an accident with diluent gas release outside the reactor primary coolant system	
3. Accidents in a shut down reactor; accidents during fuel handling	
3.1. Insertion of a positive reactivity	3.1.1. Inadvertent withdrawal of one shim control rod group during dismantling operations in the reactor
3.2. Disruption in heat removal from the reactor	3.2.1. Total blackout with a failure of all AC sources during refuelling 3.2.2. Total blackout with a failure of all AC sources during equipment maintenance (maintenance of the SG, MCP, cooldown system pumps, valves)
3.3. Depressurization of the primary circuit	3.3.1. Guillotine break of the pressurizer surge line in a hot shutdown state of the reactor with a failure of the ECCS active subsystem
3.4. Accidents during refuelling	3.4.1. Drop of a spent fuel assembly container: (1) Onto the reactor (2) Onto the spent fuel storage 3.4.2. Destruction of spent fuel assemblies as a result of an inadvertent closure of the container gate or an inadvertent turn of the aiming mechanism 3.4.3. Drop of a container with the case loaded by spent fuel assemblies 3.4.4. Drop of a container with the reactor coolant system filter
3.5. Accidents in spent fuel storage	3.5.1. Failure of a cooling system of the spent fuel storage tanks (all channels)
3.6. Release of radiolysis products from the opened reactor in an accident with loss of heat removal from the reactor (during refuelling, during equipment maintenance)	
4. External impacts on the FPU	
4.1. Collisions of the FPU with other ships having a speed above critical value	
4.2. Fall of an aircraft onto the FPU from high altitude	
4.3. Sinking of the FPU	
4.4. Grounding of the FPU, including on rocky ground	

I–4.2. Acceptance criteria for design basis accidents and beyond design basis accidents

Substantiation of the KLT-40S NPP safety in design basis and beyond design basis accidents has been performed on the basis of safety assessment criteria (acceptance criteria) presented in Tables I-4 and I-5.

Table I-6 establishes a correspondence between safety assessment criteria (acceptance criteria) and design basis accidents.

Table I-7 establishes similar correspondence for beyond design basis accidents.

I–5. PROVISIONS FOR SAFETY UNDER EXTERNAL EVENT IMPACTS

Structures, systems and components of a floating NPP with KLT-40S nuclear installations are developed taking into account possible impacts of natural and human induced external events, typical of a floating NPP location site and transportation routes, and meet the currently adopted regulatory requirements. NPP safety is ensured at the specific values of the parameters of natural impacts on the NPP and reactor unit, determined in the design, that have a frequency of 10^{-2} year^{-1}; including the impacts of design (10^{-2} year^{-1} frequency) and maximum design (10^{-4} year^{-1} frequency) earthquakes.

For the FPU location in Severodvinsk (the Russian Federation), design earthquake magnitude is taken to mean equal to 7, and maximum design earthquake magnitude is equal to 8 on the MSK scale.

Equipment, machinery, and systems important for safety, and their mounting, are designed to withstand shock loads corresponding to a peak ground acceleration (PGA) of 3g in all directions. Also, they remain operable under inclination and heaving, typical of FPU operating conditions.

TABLE I-4. SAFETY ASSESSMENT CRITERIA FOR DESIGN BASIS ACCIDENTS

Criterion number	Criterion formulation
1.	Maximum fuel temperature shall be below melting point
2.	Specific threshold enthalpy of fuel rod destruction shall not be exceeded
3.	Minimum value of the departure from nucleate boiling (DNBR) in the core shall be ≥1.0, taking into account the most unfavourable deviation of parameters, the maximum non-uniformity of power distribution, and the uncertainties of local power and critical heat flux calculations
4.	The core shall be covered by the coolant
5.	Maximum temperature of the fuel element claddings shall not exceed 500°C
6.	Primary circuit pressure shall not exceed 1.15 of the design pressure value
7.	Containment pressure shall not exceed 1.1 of the design pressure value
8.	Radiation doses for the population (critical group) at the control area* boundary and beyond this area shall not exceed the values requiring a decision on measures for population protection in the case of a radiation accident (the values that shall not be exceeded are specified in Tables 6.3 and 6.4 of the NRB-99 [I-4])
9.	Radiation dose to personnel shall not exceed the dose value planned for liquidation of accident consequences; 100mSv, as established by the NRB-99 [I-4]
10.	Effective neutron multiplication factor (K_{eff}) of fresh or spent fuel storage shall not exceed 0.95 in normal operation and in design basis accidents
11.	Maximum temperature of the fuel element claddings in spent fuel assemblies during a refuelling process or in storage shall not exceed 650°C
12.	Pressure in the fuel storage tanks shall not exceed the limiting value of 1.4 MPa

* The control area boundary coincides with the FPU boards, to the bow and stern directions it coincides with the monitored area boundaries, see Fig. I-2.

TABLE I-5. SAFETY ASSESSMENT CRITERIA FOR BEYOND DESIGN BASIS ACCIDENTS

Criterion number	Criterion formulation
1.	Radiation doses for the critical population group at the boundary of the area of emergency action planning and beyond this area shall not exceed values requiring a decision on measures for population protection in the case of a radiation accident (the values that shall not be exceeded are specified in Tables 6.3 and 6.4 of the NRB-99 [I-4]; beyond area of emergency planning, temporary restrictions may be established on consumption of local agricultural products)
2.	Radiation dose to personnel shall not exceed the dose value planned for liquidation of accident consequences; 100mSv, as established by the NRB-99 [I-4]
3.*	Pressure in the primary circuit shall not exceed the value that ensures the elastic deformation of the primary system components is preserved
4.*	Containment pressure shall not exceed the value that ensures the elastic deformation of the containment system components is preserved
5.*	Time margin to core uncovery shall be sufficient for personnel to take accident management actions (not less than 1 hour)
6.*	Maximum temperature of fuel element claddings shall not exceed the value corresponding to cladding rupture (taking into account fuel burnup)

* Additional criteria for beyond design basis accidents not resulting in core damage

I–6. PROBABILITY OF UNACCEPTABLE RADIOACTIVE RELEASE BEYOND THE PLANT BOUNDARY

Probabilistic safety parameters determined in the probabilistic risk assessment (PRA) of a floating NPP with KLT-40S reactors are prescribed by a top level Russian regulatory document, the OPB-88/97 [I-5]. The parameters include core damage frequency and the probability of a large (limited) radioactivity release in accidents.

According to OPB-88/97, the PRA goal is to demonstrate that cumulative core damage frequency does not exceed 10^{-5} per reactor year, and the probability of a large radioactivity release is not higher than 10^{-7} per reactor year.

Level 1 PRA has been performed for a floating NPP with KLT-40S nuclear installations. According to its results, point estimate of the resulting core damage frequency of the KLT-40S under internal initiating events is about 10^{-7} per reactor year for initial reactor conditions, corresponding to normal power operation. Uncertainty analysis of probabilistic safety attributes, performed using a method of statistical testing (Monte Carlo method), has shown an upper confidence boundary (95% quantile) that core damage frequency will not be higher than 10^{-6} per reactor-year.

Low probability of a severe accident with core damage is conditioned by inherent safety features (self-protection) and other design features of this modular reactor design, as well as by redundancy and diversity of safety systems in the NPP. Both active and passive safety systems are incorporated in the KLT-40S; these systems are based on components with high reliability proven by multi-year operating experience of prototype (marine) reactors.

I–7. MEASURES PLANNED IN RESPONSE TO SEVERE ACCIDENTS

In line with the state of the art trends, an approach to severe accident management is based on a combination of two categories of accident management measures:

— Those aimed at the prevention of core damage (decrease of core damage probability);
— Those aimed at the limitation of severe accident consequences (accident mitigation).

TABLE I-6. CORRESPONDENCE BETWEEN SAFETY ASSESSMENT CRITERIA AND DESIGN BASIS ACCIDENTS

Design basis accident number according to table I-2	Criterion number according to table I-4											
	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.
1.1.1.	+	+	+		+	+						
1.1.2.	+	+	+									
1.1.3.			+									
1.1.4.			+									
1.1.5.	+		+									
1.1.6.			+									
1.1.7.	+		+		+							
1.2.1.–1.2.4.	+		+		+							
1.2.5.			+									
1.2.6.			+									
1.3.1.–1.3.12.			+			+						
1.4.1.–1.4.2.			+			+						
1.5.1.–1.5.6.			+									
1.6.1.						+						
1.7.1.–1.7.11.			+	+	+		+	+	+			
2.1.1.	+	+	+			+	+					
2.2.	+	+	+			+	+					
2.3.						+	+					
3.1.1.			+									
3.2.1.			+			+						
3.2.2.–3.3.2.				+	+			+	+			
3.4.								+	+			
3.5.				+	+			+	+			
4.1.1.–4.1.5.								+	+		+	
4.2.1.								+	+		+	
4.2.2.											+	+
4.2.3.											+	
4.2.4.											+	
4.2.5.										+		
4.2.6.												+
4.3.1., 4.3.2.								+	+			
5.1.1.–5.3.2								+	+			

TABLE I-7. CORRESPONDENCE BETWEEN SAFETY ASSESSMENT CRITERIA AND BEYOND DESIGN BASIS ACCIDENTS

Beyond design basis accident number according to table I-3	Criterion number according to table I-5					
	1.	2.	3.	4.	5.	6.
1.1.1.			+			+
1.1.2.			+			+
1.1.3.						+
1.1.4.	+	+				+
1.1.5.						+
1.2.1. 1)-6)			+			+
1.3.1.-1.3.6.			+			+
2.1.1.-2.1.9.	+	+		+	+	+
2.2.1.-2.2.8.	+	+			+	+
2.3.	+	+		+		
3.1.1.	+	+				+
3.2.1.	+	+			+	+
3.2.2.	+	+			+	+
3.3.1.	+	+			+	+
3.4.1.	+	+				+
3.4.2.	+	+				+
3.4.3.	+	+				+
3.4.4.	+	+				+
3.5.1.	+	+			+	+
3.6.	+	+				
4.1.-4.4.	+	+				

Measures on the prevention of core damage

The analyses of more probable scenarios of accidents with a loss of core cooling, potentially resulting in core damage, and PRA results show that the most critical LOCA scenario is that accompanied by a failure of 'normal' ECCS channels, caused by the failure of active elements (pumps or connecting valves of the same type).

To cope with such situation, the KLT-40S design provides for an option to supply water to the reactor via the pipelines of the purification system, using the turbine plant pumps.

Measures on accident mitigation include measures on limitation of the core damage fraction, measures on in-vessel retention of the corium, and measures on limitation of radiological consequences.

Measures on limitation of core damage fraction

Core damage process in the KLT-40S nuclear installation is relatively slow due to the injection of water from the hydro-accumulator that cools overheated and partially degraded core elements. Successful realization of the measures on water supply to the reactor at this stage of an accident will lead to the flooding and cooling of core materials, and would allow prevention of a molten pool formation on the reactor bottom head and exclude an impact of the corium on the reactor vessel.

Measures on in-vessel retention of corium

For retention of the molten core inside the reactor vessel, a special system is provided for in the reactor unit design that secures external cooling of the reactor vessel in accidents with core damage and core melt relocated to the reactor vessel bottom. In-vessel retention of the corium allows for exclusion of negative phenomena associated with corium release to the containment.

Measures on limitation of radiological consequences

To exclude irradiation of the personnel and population in case of a severe accident, the following protective measures need to be implemented:

(1) To ensure protection of the personnel, it is necessary to exclude staff presence in the compartments adjacent to the containment and in other compartments with high radiation levels;
(2) To limit radiation dose to the population living within a 1 km radius from the floating NPP, it may be required (depending on the actual radiation situation) that some protective measures, such as iodine prophylaxis or sheltering, are implemented. As a protective measure, a temporary limitation should be established on the consumption of separate agricultural products grown within a radius of up to 5 km from the floating NPP and contaminated by radioactive release.

Evacuation of the population is not required at any distance from the floating NPP.

I–8. SUMMARY OF PASSIVE SAFETY DESIGN FEATURES FOR THE KLT-40S

Tables I-8 to I-12 below provide the designer's response to questionnaires developed at an IAEA technical meeting "Review of passive safety design options for SMRs" held in Vienna on 13–17 June 2005. These questionnaires were developed to summarize passive safety design options for different SMRs according to a common format, based on the provisions of IAEA Safety Standards [I-2] and other IAEA publications [I-3, I-6]. The information presented in Tables I-8 to I-13 provided a basis for conclusions and recommendations of the main part of this report.

TABLE I-8. QUESTIONNAIRE 1 — LIST OF SAFETY DESIGN FEATURES CONSIDERED FOR/ INCORPORATED INTO THE KLT-40S DESIGN

#	Safety design features	What is targeted?
1.	Negative reactivity coefficients on specific volume of the coolant, on fuel and coolant temperature and on reactor power in the whole range of variation of reactor parameters	In reactivity initiated accidents: limitation of reactor power increase, ensuring reliable core cooling, prevention of pressure and temperature increase in the primary circuit
2.	Absence of liquid boron reactivity control system	Exclusion of inadvertent reactivity insertion as a result of boron dilution
3.	High thermal conductivity of the fuel composition (uranium dioxide granules in the inert matrix)	Prevention of the fuel element cladding temperature increase in loss of flow accidents; prevention of the primary pressure and temperature increase in accidents with disruption of heat removal
4.	Use of a gas pressurizer system	Exclusion of electric heaters — a potentially unreliable component
5.	Insertion of scram control rods into the core by force of accelerating springs	Increased reliability of a reactor shutdown
6.	Insertion of shim control rods into the core by gravity force (under their own weight)	Increased reliability of a reactor shutdown

TABLE I-8. QUESTIONNAIRE 1 — LIST OF SAFETY DESIGN FEATURES CONSIDERED FOR/ INCORPORATED INTO THE KLT-40S DESIGN (cont.)

#	Safety design features	What is targeted?
7.	Use of a passive emergency heat removal system	Increased reliability of emergency heat removal
8.	Adequate level of natural circulation flow in the primary system	Reliable core cooling
9.	Limitation of uncontrolled movement of the control rods by an overrunning clutch and by movement limiters, for an accident with a break in the CPS drive support bar	Decrease of a positive reactivity inserted under impact loads or under a break of the CPS drive casing, or under a break of the CPS drive support bar
10.	Use of self-actuating devices in safety systems	Increased reliability of an emergency reactor shutdown; increased reliability of a startup of emergency heat removal systems
11.	Use of once-through steam generators	Limited increase of heat power removed by the secondary circuit in case of a steam line break accident
12.	Use of a 'soft' pressurizer system	Damping of the transients; increased time margins for measures on accident management
13.	Provision of a mechanical strength margin on the primary pressure	Increased time margin for measures on management of accidents with heat removal disruption
14.	High thermal capacity of primary system components	Increased time margin for measures on management of accidents with heat removal disruption
15.	Modular design of the reactor unit	Elimination of long pipelines in the reactor coolant system
16.	Leaktight reactor coolant system	Decreased probability of loss of coolant accidents
17.	Favourable conditions for the realization of a 'leak before break' concept in application to the structures of the primary circuit, provided by design	Reduced probability of a guillotine break for the primary pipelines
18.	Use of restriction devices in the pipelines of the primary circuit systems	Limitation of the break flow in case of a pipeline guillotine rupture; less strict requirements to the ECCS
19.	Connection of primary coolant systems to a 'hot' part of the reactor	Ensuring fast transition to a steam flow through a break in case of a pipeline rupture; limitation of break flow; less strict requirements to the ECCS
20.	Use of hydro-accumulators in the ECCS	Providing a time margin for personnel to take actions on accident management in case of a failure of the active means of emergency water supply (pump failure)
21.	Use of a steam generator with lower pressure inside the tubes in normal operation mode	Reduced probability of a steam generator tube rupture
22.	Use of secondary system pipelines designed for primary pressure, up to the cut-off valves	Absence of coolant release in the case of a steam generator leak
23.	Use of a passive reactor vessel cooling system	In-vessel retention of the corium
24.	Use of a passive containment heat removal system	Reliable decrease of containment pressure and limitation of radioactive release in accidents
25.	Use of the protective enclosure	Limitation of radioactive release in accidents; additional protection from the impacts of external events

TABLE I-9. QUESTIONNAIRE 2 — LIST OF INTERNAL HAZARDS

#	Hazards (safety functions) that are of concern (relevant) for a reactor line	How these hazards (safety functions) are addressed (performed) in the KLT-40S
1.	Prevent unacceptable reactivity transients	– Negative values of reactivity coefficients; – Absence of liquid boron system; – Low velocity of control rod movement; minimized number of simultaneously driven control rod groups; – Limitation of uncontrolled movement of the control rods by an overrunning clutch or by movement limiters, for an accident with a break of the CPS drive support bar.
2.	Avoid loss of coolant	– Modular design of the reactor unit; elimination of long pipelines in the reactor coolant system; – Installation of restriction devices in the pipelines of the primary circuit systems; – Connection of primary coolant systems to a 'hot' part of the reactor; – Use of hydro-accumulators within the ECCS; – Use of coolant recirculation system.
3.	Avoid loss of heat removal	– Use of passive emergency heat removal system; – Redundancy of the active systems.
4.	Avoid loss of flow	– Adequate natural circulation flow in the primary system; – Redundancy of the circulation pumps; – Use of two coils in the MCP electric motor.
5.	Avoid exothermic chemical reactions	– It is ensured that thermal state of the fuel rods in emergency conditions excludes the exothermic reaction of zirconium oxidation by steam.

TABLE I-10. QUESTIONNAIRE 3 — LIST OF INITIATING EVENTS FOR ABNORMAL OPERATION OCCURRENCES (AOO)/DESIGN BASIS ACCIDENTS (DBA)/BEYOND DESIGN BASIS ACCIDENTS (BDBA)

#	List of initiating events for AOO/DBA/BDBA typical for a reactor line (PWRs)	Design features of the KLT-40S used to prevent progression of the initiating events to AOO/DBA/BDBA, to control DBA, to mitigate BDBA consequences, etc.	Initiating events specific to this particular SMR
1.	Disruptions of reactivity due to control rod malfunctioning	– Negative values of reactivity coefficients; – Low velocity of control rod movement; minimized number of simultaneously driven control rod groups; – Two independent systems of reactivity control — shim and scram control rods; – Use of self-actuating devices — drive circuit breakers, self-actuated on primary pressure; – Mechanical strength margin on the primary pressure.	
2.	Reactivity disruption due to boron dilution	– Boric acid is not used for excess reactivity compensation.	
3.	Loss of flow due to pump coastdown	– Adequate (sufficient) natural circulation flow in the primary system; – Use of two coils in the MCP electric motor.	

TABLE I-10. QUESTIONNAIRE 3 — LIST OF INITIATING EVENTS FOR ABNORMAL OPERATION OCCURRENCES (AOO)/DESIGN BASIS ACCIDENTS (DBA)/BEYOND DESIGN BASIS ACCIDENTS (BDBA) (cont.)

#	List of initiating events for AOO/DBA/BDBA typical for a reactor line (PWRs)	Design features of the KLT-40S used to prevent progression of the initiating events to AOO/DBA/BDBA, to control DBA, to mitigate BDBA consequences, etc.	Initiating events specific to this particular SMR
4.	Loss of primary system integrity (LOCAs)	– Modular design of the reactor unit; elimination of long pipelines in the reactor coolant system; – Connection of the primary coolant systems to a 'hot' part of the reactor; – Installation of restriction devices in pipelines of the primary circuit systems.	
		See Table I-11	Specific initiating event for the KLT-40S is a break of the connection pipeline between the pressurizer and the gas balloons; Specific beyond design basis accident for the KLT-40S is a break of the primary circuit pipeline with a failure to cut off the gas balloons.
5.	Interfacing systems LOCA	– Up to the cut-off valves, the interfacing systems are designed for primary pressure.	
6.	Loss of power supply	– Use of a passive emergency heat removal system providing the removal of heat over 24 hours.	
7.	Accidents due to external events	– Structures, systems and components of the floating NPP are designed taking into account possible impacts of natural and human induced external events typical of a floating NPP location site and transportation routes, and meet the regulatory requirements.	
8.		See Table I-11	Disconnection of gas balloons from the pressurizer during power operation.
9.		See Table I-11	Explosion of gas balloons.
10.		See Table I-11	Accidents connected to reactor placement on a non-self-propelled ship: – For DBA see item 5 in Table I-2; – For BDBA see item 4 in Table I-3.

TABLE I-11. QUESTIONNAIRE 3 (PART 2) — DESIGN FEATURES OF THE KLT-40S THAT PREVENT PROGRESSION OF SPECIFIC INITIATING EVENTS TO A MORE SEVERE PHASE

Specific initiating event for the KLT-40S (see Table I-10)	Design features that prevent progression of the initiating events to a more severe phase
Disconnection of the gas balloons from the pressurizer during power operation	– Gas already present in the pressurizer ensures the absence of unacceptable pressure increase; – Availability of warning and protection emergency signals on primary pressure increase (active systems); – Availability of self-actuating devices providing a reactor shutdown and startup of the passive EHRS.
Rupture of a pipeline connecting the gas balloons to the pressurizer	– A flow limiter is installed in the pressurizer surge line; – Availability of the cut-off valves ensuring a disconnection of the gas balloons and leak termination in the case of a break after the cut-off valves.
Explosion of the gas balloons	– Fire-extinguishing systems available in the protective enclosure and in the containment; – Pressure sources that have pressure head higher than the design pressure of the balloons do not exist.
Collision with another ship	– On-board protection structures available, including reinforced sheets of outer clothing and deck planking sheets adjacent to the board, as well as longitudinal stiffening ribs of the board.
Sinking of the FPU	– System of containment flooding is available that prevents containment destruction by external hydrostatic pressure; this system is provided to protect the environment from possible radioactive contamination in the case of a FPU sink
Grounding of the FPU, including onto rocky ground	– The bottom ceiling is isolated from the containment structures by horizontal crimps in the bulkheads.
Helicopter crash-landing	– Protective structures consisting of steel planking and other structures of appropriate dimensions and strength are provided.

TABLE I-12. QUESTIONNAIRE 4 — SAFETY DESIGN FEATURES ATTRIBUTED TO DEFENCE IN DEPTH LEVELS

#	Safety design features	Category: A-D (for passive systems only), according to IAEA-TECDOC-626 [I-6]	Relevant DID level, according to NS-R-1 [I-2] and INSAG-10 [I-3]
1.	Negative reactivity coefficients on specific volume of the coolant, on fuel and coolant temperature and on reactor power in the whole range of variation of the reactor parameters	A	1
2.	Absence of a liquid boron reactivity control system (excess reactivity is compensated for by a heterogeneous absorber in the burnable poison rods and by the CPS control rods)	A	1
3.	High thermal conductivity of the fuel composition (uranium dioxide granules in the inert matrix)	A	3
4.	Insertion of scram control rods into the core by force of accelerating springs	D (by automatic system) C (by self-actuating devices)	3
5.	Insertion of shim control rods into the core by gravity force (under their own weight)	D (by automatic system) C (by self-actuating devices)	3
6.	Use of a passive emergency heat removal system	D (by automatic system) C (by self-actuating devices)	3
7.	Adequate level of natural circulation flow in the primary system	B	1
8.	Limitation of uncontrolled movement of the control rods by an overrunning clutch or by movement limiters, in case of an accident with a break in the CPS drive support bar	C	3
9.	Self-actuating devices in the safety systems	C	3
10.	Steam generators of a once-through design	A	1
11.	‘Soft’ pressurizer system	A	1, 3
12.	Provision of a mechanical strength margin on the primary pressure	A	1, 3
13.	Modular design of the reactor unit, eliminating long pipelines in the reactor coolant system	A	1
14.	Totally leaktight reactor coolant system	A	1
15.	Installation of restriction devices in the pipelines of the primary circuit systems	A	3
16.	Connection of the primary coolant systems to a ‘hot’ part of the reactor	B	3
17.	Hydro-accumulators in the ECCS	C	3
18.	Steam generator with lower pressure inside the tubes in a normal operation mode	A	1
19.	Passive reactor vessel cooling system	D	4
20.	Containment	A	3, 4
21.	Passive containment heat removal system	D	4
22.	Availability of the protective enclosure	A	4

TABLE I-13. QUESTIONNAIRE 5 — POSITIVE/NEGATIVE EFFECTS OF PASSIVE SAFETY DESIGN FEATURES IN AREAS OTHER THAN SAFETY

Passive safety design features	Positive effects on economics, physical protection, etc.	Negative effects on economics, physical protection, etc.
Absence of liquid boron reactivity control system	Decrease in plant costs and operation simplification	Certain deterioration of fuel cycle characteristics
Use of passive systems		Increase of plant construction and maintenance costs
Use of self-actuating devices in safety systems		Increase of plant construction and maintenance costs
Modular design of the reactor unit	Compactness of the reactor unit, decrease in containment dimensions, decrease in plant costs	Certain deterioration of maintainability as compared to loop type plants
Totally leaktight reactor coolant system	Decrease of the amount of radioactive waste, reduction in operation costs	

REFERENCES TO ANNEX I

[I–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Advanced Light Water Reactor Designs 2004, IAEA-TECDOC-1391, IAEA, Vienna (2004).

[I–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[I–3] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, Vienna (1996).

[I–4] Radiation Safety Regulations (NRB-99): Hygiene Regulations, Ministry of Health (Minzdrav) of the Russian Federation, Moscow, (1999) (in Russian).

[I–5] General Principles of Safety Provision for NPPs, OPB-88/97. NP-001-97 (PNAE G-01-011-97). Moscow, Gosatomnadzor RF (1997).

[I–6] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Terms for Advanced Nuclear Plants, IAEA-TECDOC-626, IAEA, Vienna (1991).

Annex II

SAFETY DESIGN FEATURES OF THE IRIS

International Team Led by Westinghouse,
United States of America

II–1. DESCRIPTION OF THE IRIS DESIGN

The International Reactor Innovative and Secure (IRIS) is an advanced, integral, light water cooled reactor of medium generating capacity (335 MW(e)), that features an integral reactor vessel containing all the reactor primary system components, including steam generators, coolant pumps, pressurizer and heaters, and control rod drive mechanisms; in addition to the typical core, internals, control rods and neutron reflector [II-1, II-2]. This integral configuration allows for the use of a small, high design pressure, spherical steel containment which results in a significant reduction in the size of the nuclear island. Other IRIS innovations include a simplified passive safety system concept and equipment features that derive from the 'safety-by-design'™ philosophy [II-3]. This design approach allows for elimination of certain accident initiators at the design stage, or when outright elimination is not possible, decreases accident consequences and/or their probability of occurrence. Major design characteristics of the IRIS are given in Table II-1. As part of the IRIS pre-application licensing review by the U.S. Nuclear Regulatory Commission (NRC), the IRIS design team has developed a test plan that will provide the necessary data for safety analysis computer model verification, as well as for verifying the manufacturing feasibility, operability, and durability of new component designs.

TABLE II-1. MAJOR DESIGN FEATURES OF THE IRIS

Parameters	Features
Core thermal power	1000 MW
Mode of operation	Base load operation standard. Enhanced load follow mode with control rods ('mechanical shim' or M-SHIM strategy)
Plant design life	Over 60 years
Fuel	Sintered ceramic UO_2/MOX fuel
Enrichment	Up to 4.95% U fuel readily available, enabling extended cycle of up to four years. Option for infrequent refuelling (8-10 years) requires 7~10% fissile content
Coolant and moderator	Light water, sub-cooled
Number of coolant pumps	Integral primary system; forced circulation with eight in-vessel fully immersed pumps
Containment	Pressure suppression, spherical steel
Reactivity feedback	Moderator temperature coefficient (MTC) negative over the whole cycle and power operating range
Power flattening approach	Burnable absorbers
Reactivity control	Soluble boron, burnable absorber, control rods
Shut down system	Control rods, emergency boron system
Fuel cycle options	Near term deployment — fuel licensable today; Mid term deployment with extended refuelling interval — requires fuel irradiation testing
Average discharge burnup	Up to 60 GW·day/t U (immediately available); Increased discharge burnup option (expected available by ~2020)

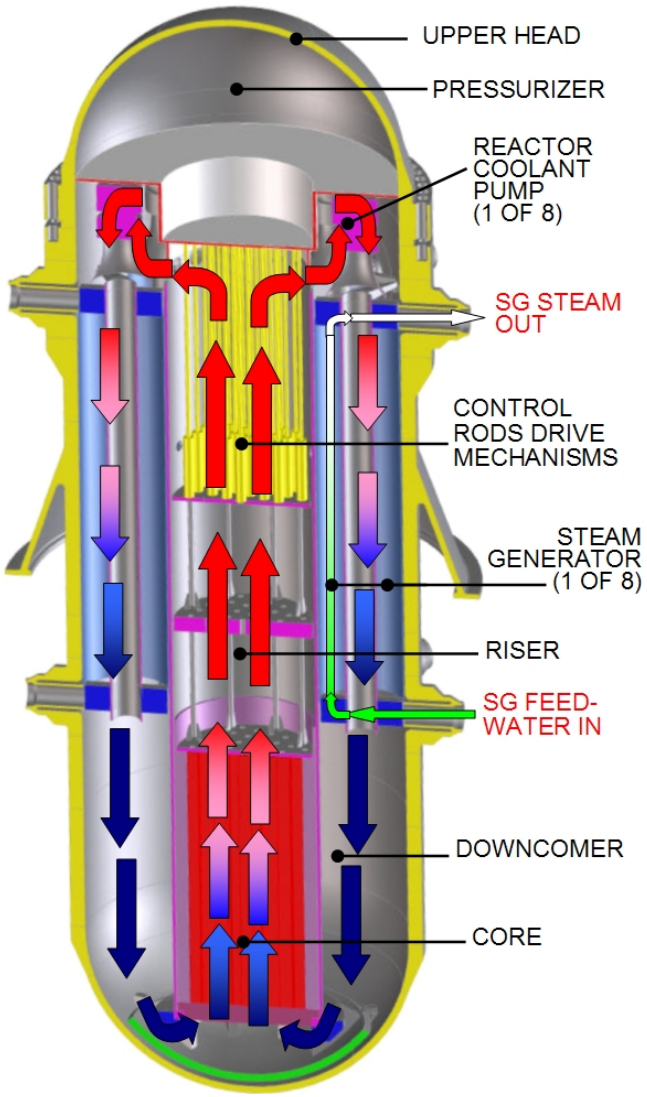


FIG. II-1. Integral primary system of IRIS.

IRIS is innovative in design – employing an integrated primary system that incorporates all the main primary circuit components within a single vessel, i.e., the core with control rods and their drive mechanisms, eight helical coil steam generators with eight associated fully immersed axial flow pumps, and a pressurizer, see Fig. II-1.

The integral configuration offers intrinsic design improvements as briefly discussed below:

- *Steam generators:* With the primary coolant outside, tubes are in compression, and tensile stress corrosion cracking is eliminated;
- *Primary coolant pumps:* The axial fully immersed pumps result in no seal leak concerns, no possibility for shaft breaks, and no required maintenance;
- *Internal control rod drive mechanisms (CRDMs):* This solution eliminates head penetrations and the possibility of penetration failures as well as the need for any future head replacements, and eliminates rod ejection accidents;
- *Pressurizer:* A much larger volume/power ratio provides better control of pressure transients. Additionally, no sprays are required;

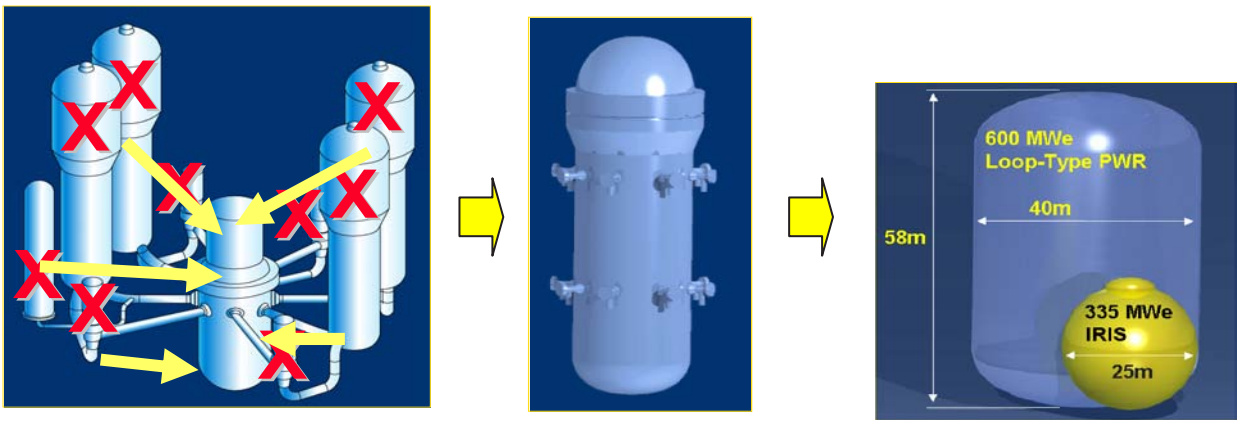


FIG. II-2. Compact integral layout of IRIS.

- *Large downcomer:* The 1.7 m wide downcomer reduces the fast neutron flux on the reactor vessel by 5 orders of magnitude. This leads to a 'cold' (i.e., not activated) vessel with almost no outside dose, no vessel embrittlement, and no need for surveillance. The vessel is essentially 'eternal', and decommissioning is simplified;
- *Fuel assembly:* The same assembly as in standard Westinghouse PWRs is used, but it can provide an extended cycle up to 48 months;
- *Maintenance:* Intervals between maintenance outages can also be extended up to 48 months, thus enabling uninterrupted operation for up to 4 years.

While leading to a larger reactor vessel, the integral layout results in a smaller containment (as illustrated in Fig. II-2) and overall a more compact site, with a positive impact on safety and economics.

IRIS new design features and components

The integral reactor coolant system (Integral RCS) is characterized by:

- Entire RCS located in a single pressure vessel;
- No additional pressure vessels, connecting loop piping, or supports.

The integral reactor vessel includes:

- Axial flow, fully immersed coolant pumps with high temperature bearings and high temperature sealed rotor and stator windings;
- Helical-coil, once through steam generators (SGs);
- Internal control rod drive mechanisms (I-CRDMs) designed for in-vessel environment;
- Pressurizer and related heaters.

IRIS three tier safety concept

The overall approach to safety in the IRIS is represented by the following three tier approach:

(1) The first tier is safety-by-design™ [II-3], which aims at eliminating by design the possibility for an accident to occur, rather than dealing with its consequences. By eliminating some accidents, the corresponding safety systems (passive or active) become unnecessary as well;
(2) The second tier is provided by simplified passive safety systems, which protect against the accident possibilities still remaining and mitigate their consequences;

(3) The third tier is provided by active systems which are not required to perform safety functions (i.e., are not safety grade) and are not considered in deterministic safety analyses, but do contribute to reducing core damage frequency (CDF).

First Tier

The first tier is embodied in the IRIS 'safety-by-design'™ philosophy [II-3]. Nuclear power plants consider a range of hypothetical accident scenarios. The IRIS 'safety-by-design'™ philosophy is a systematic approach that aims — by design — to eliminate altogether the possibility for an accident to occur, i.e., to eliminate accident initiators, rather than having to design and implement systems to deal with the consequences of an accident. It should be noted that integral configuration is inherently more amenable to this approach than a loop type configuration, thus enabling safety improvements not possible in a loop reactor. To consider only the most obvious example, loss of coolant accidents caused by a large break of external primary piping (large break loss of coolant accidents – large break LOCAs) are eliminated by design since no large external piping exists in IRIS. Additionally, in cases where it is not possible or practical to completely eliminate potential initiators of an accident, safety-by-design™ aims at reducing the severity of the accident's consequences and the probability of its occurrence. As a result of this systematic approach, the eight Class IV design basis events [II-3] (potentially leading to the most severe accidents) that are usually considered in light water reactors (LWRs), are reduced to only one in the IRIS, with the remaining seven either completely eliminated by design, or their consequences (as well as probability) reduced to a degree that they are no longer considered Class IV events [II-1, II-2].

Second Tier

The second tier consists of passive safety systems needed to cope with remaining potential accidents. Because of safety-by-design™, they are fewer and simpler than in typical passive loop type LWRs [II-1]. Notably, the elimination of the possibility for some accidents to occur enables simplifications of the IRIS design and passive safety systems, resulting simultaneously in enhanced safety, reliability, and economics. In other words, increased safety and improved economics support each other in the IRIS design.

Third Tier

The third tier has been addressed within the probabilistic risk assessment/probabilistic safety assessment (PRA/PSA) framework. In fact, PRA was initiated early in the IRIS design, and was used iteratively to guide and improve the design safety and reliability (thus adding 'reliability by design'). The PRA has suggested modifications to reactor system designs, resulting in reduction of the predicted core damage frequency (CDF). After these modifications, the preliminary PRA level 1 analysis [II-4] estimated the CDF due to internal events (including anticipated transients without scram, ATWS) to be about 2×10^{-8}, more than one order of magnitude lower than in typical advanced LWRs [II-1]. A subsequent evaluation [II-5] of the large early release frequency (LERF) also produced a very low value, of the order of 6×10^{-10}, which is more than one order of magnitude lower than in typical advanced loop LWRs [II-1], and several orders of magnitude lower than in present LWRs.

II–2. PASSIVE SAFETY DESIGN FEATURES OF IRIS

Inherent safety features

The IRIS design significantly increases defence in depth by adding as the first layer of safety an inherent elimination of as many accidents as practical through the safety-by-design™ philosophy [II-3], as previously described. The postulated accident scenarios eliminated include:

- Large break LOCAs;
- Control rod ejection;
- Reactor coolant pump shaft break.

The postulated accidents whose severity or consequences are reduced include:

- Small/medium break LOCAs;
- Steam generator tube rupture;
- Steam line break;
- Feed line break;
- Reactor coolant pump seizure.

Passive safety systems

The passive safety systems in IRIS are fewer and simpler than in typical passive LWRs [II-1]. Their function is to protect against remaining possible accidents and mitigate their consequences.

When compared with typical passive LWRs, the IRIS's safety systems are not novel. Most of them are similar to those in the AP600/AP1000 but simplified and fewer in number, while the pressure suppression system is similar to that of a BWR [II-1].

Active systems

In IRIS, no active safety grade systems are required. However, active non-safety-grade systems, while not assumed available in deterministic safety analysis, may be used (if available) to help mitigate accidents, and thus enhance defence in depth (DID) and contribute to reducing the probability of core damage in the PRA analysis. The active, non-safety related features include:

(1) Standby diesel generators which provide power to DID systems in the event that normal plant alternate current (AC) power supplies are not available[1];
(2) A startup feedwater system that can provide feedwater to the steam generators in order to remove core decay heat, in the event that the normal feedwater system is unavailable;
(3) Functioning of the normal plant cooling water systems (service water and component cooling water) can provide support for other DID components as well as remove core decay heat;
(4) The chemical and volume control system normal make-up pumps with their boric acid tank as suction source can provide high pressure make-up water to the RCS in the event of a small loss of coolant accident;
(5) The normal residual heat removal pumps with their in-containment water source can provide low pressure make-up water to the RCS and heat removal capability when RCS pressure is reduced;
(6) Diverse means of containment cooling are provided to significantly reduce the chance of containment failure.

Design and functions of the passive safety systems

IRIS employs simplified passive safety systems to mitigate the effects of all postulated design basis events. Shown schematically in Fig. II-3, these systems include the following innovative features:

- *Pressure suppression system (PSS):* located within the containment vessel, acts to condense steam released into the small spherical steel containment due to any postulated design basis LOCA or steam/feed line break. The IRIS PSS is designed to limit containment pressure to ~1.0 MPa, or only 65% of the containment vessel design pressure. The PSS also provides an elevated source of water that is available for gravity injection into the reactor vessel through the direct vessel injection (DVI) lines in the event of a LOCA;
- *Emergency heat removal system:* consists of four independent subsystems, each of which has a horizontal, U-tube heat exchanger connected to one of the four IRIS SG steam lines. These heat exchangers are immersed in the refuelling water storage tank (RWST) located outside the containment structure and act

[1] Note that batteries are used as emergency backup for safety grade equipment and functions.

as the heat sink for emergency heat removal system (EHRS) heat exchangers. The EHRS operates on natural circulation, removing heat from the primary system via the steam generators' heat transfer surface, transferring the heat to the RWST water and condensing the steam, and returning the condensate back to the SG via the feedwater line. Following a LOCA, the EHRS heat removal function acts to depressurize the RCS by cooling the SGs, thus condensing the steam produced by the core directly inside the reactor vessel. The EHRS is designed so that only one of the four independent subsystems is needed to remove the decay heat, thus providing a very high degree of redundancy, important for both safety and security concerns;

- *Long term gravity make-up system:* combined with a small RCS depressurization system and containment layout, provides gravity driven make-up water to the reactor vessel to assure that the core remains covered indefinitely following a LOCA;
- *Emergency boration system (EBT):* Two full emergency boration systems provide a diverse means of reactor shutdown by delivering borated water to the reactor vessel (RV) through the DVI lines. By their operation, these tanks also provide limited gravity feed make-up water to the primary system;
- *Automatic depressurization system (ADS):* A small ADS from the pressurizer steam space assists the EHRS in depressurizing the reactor vessel if reactor vessel coolant inventory drops below a specified level. The ADS consists of two parallel lines, each with two normally closed valves. The ADS discharges into a quench tank through a sparger. This ADS function ensures that the reactor vessel and containment pressure are equalized in a timely manner, thus limiting the loss of coolant and preventing core uncovery following a postulated LOCA even at low reactor vessel elevation;
- S*pecially constructed lower containment volume:* collects the liquid break flow, as well as any condensate from the containment, in a cavity where the reactor vessel is located. Following a LOCA, the cavity is flooded above core level, creating a gravity head of water sufficient to provide coolant make-up to the reactor vessel through the DVI lines. This cavity also assures that the lower outside portion of the reactor vessel surface is or can be wetted following postulated core damage events;
- S*afety strategy of IRIS:* provides a diverse means of core shutdown through make-up of borated water from the EBT in addition to the control rods; also, the EHRS provides a means of core cooling and heat removal to the environment in the event that normally available active systems are not available. In the event of a significant loss of primary-side water inventory, the primary line of defence for IRIS is represented by the large coolant inventory in the reactor vessel and the fact that EHRS operation limits the loss of mass, thus maintaining a sufficient inventory in the primary system and guaranteeing that the core will remain covered for all postulated events. The EBT is actually capable of providing some primary system injection at high pressure, but this is not necessary, since the IRIS strategy relies on 'maintaining' coolant inventory, rather than 'injecting' make-up water. This strategy is sufficient to ensure that the core remains covered with water for an extended period of time (days and possibly weeks). Thus, IRIS does not require and does not have the high capacity, safety grade, high pressure safety injection system characteristic of typical loop reactors.

Passive safety features supporting management of severe accidents

The IRIS containment is inerted with nitrogen gas during operation so that the control of hydrogen concentration following postulated events and severe accident scenarios cannot cause containment pressurization due to hydrogen burn.

The IRIS is designed to provide in-vessel retention of core debris following severe accidents by assuring that the vessel is depressurized, and by cooling the outside vessel surface. The reactor vessel is cooled by containing the lower part of the vessel within a cavity that always will be flooded following any event that jeopardizes core cooling. Also, like in AP1000 [II-1], the vessel is covered with stand-off insulation, which forms an annular flow path between the insulation and the vessel outer surface. Following an accident, water from the flooded cavity fills the annular space and submerges and cools the bottom head and lower sidewalls of the vessel. A natural circulation flow path is established, with heated water and steam flowing upwards along the vessel surface, and single phase water returning downward along the outside of the vessel insulation, to the bottom of the flood-up cavity. AP1000 testing has demonstrated that this natural circulation flow is sufficient to prevent corium melt-through. Application of AP1000 conditions to the IRIS is conservative, due to the IRIS having a

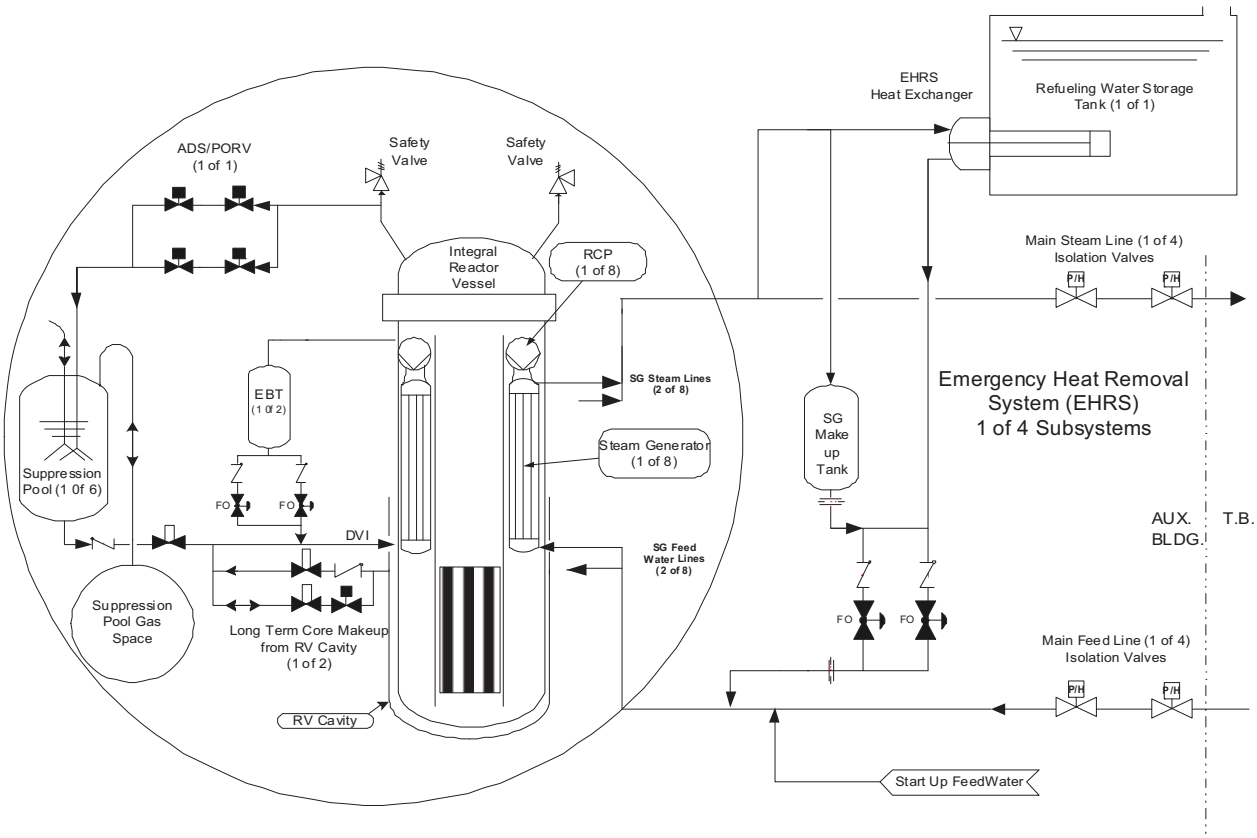


FIG. II-3. Schematic view of the IRIS's passive safety systems.

much lower core power to vessel surface ratio. The design features of the containment ensure flooding of the vessel cavity region during accidents and submerging of the reactor vessel lower head in water, since the liquid effluent released through the break during a LOCA event is directed to the reactor cavity. The IRIS design also includes a provision for draining part of the water present in the PSS water tanks directly into the reactor cavity.

A diverse, passive containment cooling system is employed as part of the severe accidents management strategy, to significantly reduce the chance of containment failure.

II–3. ROLE OF PASSIVE SAFETY DESIGN FEATURES IN DEFENCE IN DEPTH

Some major highlights of the passive safety design features in the IRIS design, structured in accordance with the various levels of defence in depth [II-6, II-7], are shown below.

Level 1: Prevention of abnormal operation and failure

The IRIS safety-by-design™ systematic approach is the basis for effective Level 1 prevention of many initiating events; correspondence between design features and initiating events prevented is the following:

(A) Integral design of primary circuit with no large diameter piping:

- Elimination of large break LOCAs;
- Elimination of loss of seal (head, pump) LOCAs;
- Elimination of control rod ejection accidents;
- Elimination of concerns related to high pressure safety injection (HPSI) systems;

(B) Increased natural circulation due to large, tall vessel:

- Reduced severity of loss of flow (LOFA) accidents;

(C) Large thermal inertia due to increased water inventory:

- Prevention of core uncovery in small and medium break LOCAs;
- Reduced requirements for heat removal systems;
- Reduced concerns related to loss of feedwater;

(D) Other specific design solutions:

- Elimination of the possibility of a reactor coolant pump shaft break.

Level 2: Control of abnormal operation and detection of failure

IRIS will use state of the art plant control and protection systems to monitor and control plant operations; it will also incorporate advanced diagnostics/prognostics systems. The contribution of passive systems at this level would be as follows:

- Slower progression of a loss of heat sink accident (LOHS) due to large thermal inertia.

Level 3: Control of accidents within the design basis

Level 3 safety functions are contributed to by the following passive safety features/systems:

(A) Passive emergency heat removal system (EHRS):

- Control of LOHS;

(B) Increased natural circulation due to large, tall vessel:

- Control of loss of flow accidents (LOFA);

(C) Steam generator system designed for full primary pressure:

- Significantly reduced severity and simple mitigation of steam generator tube rupture (SGTR) accident.

Level 4: Control of severe plant conditions, including prevention of accident progression and mitigation of consequences of severe accidents

The following passive safety features/systems of IRIS contribute to achieving the objective at this DID level:

- Prevention of LOFA progression into a more severe accident sequence, achieved via increased natural circulation due to large, tall vessel;
- Passive flooding of the reactor cavity following a LOCA;
- Secondary means of core cooling via containment cooling;
- Passive in-vessel retention of core debris following severe accidents;
- Inerted containment;
- Passive EHRS;
- Very low leakage containment; elimination/reduction of containment vessel penetrations.

Level 5: Mitigation of radiological consequences of significant release of radioactive materials

Level 5 safety functions are contributed to by the following passive safety features/systems:

(A) Small fuel inventory:

- Reduced radioactivity release;

(B) High design pressure containment plus pressure suppression system plus reduced core power density plus increased thermal inertia:

- Slower progression of accidents and increased retention of fission products;
- Low leakage rate containment;
- Deposition of radionuclides in auxiliary building.

II–4. ACCEPTANCE CRITERIA FOR DESIGN BASIS AND BEYOND DESIGN BASIS ACCIDENTS

II–4.1. List of design basis and beyond design basis accidents

Table II-2 summarizes the main inherent safety features of IRIS, stemming from its safety-by-design™ approach [II-3], together with their implication on design basis events (listed in the fourth column) typically considered by the US NRC for PWRs.

Preliminary list of initiating events for beyond design basis accidents:

- Hypothetical reactor pressure vessel break;
- A transient with failure of all safety systems.

II–4.2. Acceptance criteria

The deterministic acceptance criteria for design basis accidents (DBAs) are assumed to be the same as for conventional PWRs with a note, that de facto most of the DBAs in IRIS would be either eliminated or downgraded via a safety-by-design™ approach [II-3], see Table II-2.

The deterministic acceptance criteria for beyond design basis accidents (BDBA) in IRIS, defined on a preliminary basis, include in-vessel retention by passive means.

The probabilistic acceptance criteria for BDBA in the IRIS are summarized in Table II-3.

II–5. PROVISIONS FOR SAFETY UNDER EXTERNAL EVENTS

The safety design features of IRIS intended to cope with external events and external/internal event combinations are described in detail in [II-8].

The reactor, containment, passive safety systems, fuel storage, power source, control room and backup control are all located within the reinforced concrete auxiliary building and are protected from on-site explosions. The reactor unit appears as a very low profile, minimum sized target to an aircraft. The IRIS containment is completely within the reinforced concrete auxiliary building and one-half of it (13 m) is actually underground, since the containment is only 25m in diameter. The external, surrounding building target profile is only about 30 m high, and can easily be hardened and/or placed further underground. Also, the IRIS's safety features are passive and are contained within the auxiliary building.

TABLE II-2. SAFETY-BY-DESIGN™ IRIS PHILOSOPHY AND ITS IMPLICATIONS ON DESIGN BASIS EVENTS

IRIS Design Characteristic	Safety Implication	Accidents Affected	Design Basis Events	Effect on Design Basis Events by IRIS Safety-by-Design™
Integral layout	No large primary piping	• Large break loss of coolant accidents (LOCAs)	Large break LOCA	Eliminated
Large, tall vessel	Increased water inventory Increased natural circulation Accommodates internal control rod drive mechanisms (CRDMs)	• Other LOCAs • Decrease in heat removal various events • Control rod ejection, head penetrations failure	Spectrum of control rod ejection accidents	Eliminated
Heat removal from inside the vessel	Depressurizes primary system by condensation and not by loss of mass Effective heat removal by steam generators (SG)/ emergency high removal system (EHRS)	• LOCAs • LOCAs • All events for which effective cooldown is required • Anticipated transients without scram (ATWS)		
Reduced size, higher design pressure containment	Reduced driving force through primary opening	• LOCAs		
Multiple, integral, shaftless coolant pumps	Decreased importance of single pump failure No shaft	• Locked rotor, shaft seizure/ break • Loss of flow accidents (LOFAs)	Reactor coolant pump shaft break Reactor coolant pump seizure	Eliminated Downgraded
High design pressure steam generator system	No SG safety valves Primary system cannot over-pressure secondary system Feed/Steam System Piping designed for full reactor coolant system (RCS) pressure reduces piping failure probability	• Steam generator tube rupture • Steam line break • Feed line break	Steam generator tube rupture Steam system piping failure	Downgraded Downgraded
Once through steam generators	Limited water inventory	• Feed line break • Steam line break	Feedwater system pipe break	Downgraded
Integral pressurizer	Large pressurizer volume/reactor power	• Overheating events, including feed line break • ATWS		
			Fuel handling accidents	Unaffected

TABLE II-3. PROBABILISTIC ACCEPTANCE CRITERIA FOR BDBA IN IRIS

Core damage frequency (CDF)	$<10^{-7}$
Large early release frequency (LERF)	$\sim10^{-9}$

The IRIS is designed to survive a hypothetical flood called the probable maximal flood (PMF), which combines the worst possible values of all factors that contribute to producing a flood. This and other capabilities of the IRIS design are connected to use of the passive features, which are all contained within the auxiliary building and do not require external water or power supplies for at least 7 days.

As an example, the plant ultimate heat sink is provided by water stored in the auxiliary building in the refuelling water storage tank (RWST). This water is heated and boiled and steam is vented to the atmosphere. This safety grade ultimate heat sink provides for the removal of sensible heat of the reactor coolant system and core decay heat for at least one week, without credit for any water make-up. The design objective of IRIS is to apply both the safety-by-design™ philosophy [II-3] and the PRA guided design approach to design the plant in such a way as to minimize the contribution of external events to core damage frequency (CDF) to a level lower or at most comparable to that of internal events, which is currently estimated to be $\sim2 \times 10^{-8}$.

II–6. PROBABILITY OF UNACCEPTABLE RADIOACTIVITY RELEASE BEYOND PLANT BOUNDARY

See Table II-3.

II–7. MEASURES PLANNED IN RESPONSE TO SEVERE ACCIDENTS

The passive safety design features of the IRIS aimed at prevention of core damage (decrease of core damage probability) are described in section II-2; those aimed at mitigation of severe accident consequences are listed in section II-3 (DID Level 5).

Regarding measures for population evacuation/relocation in the vicinity of a plant, the designers are considering an option to license IRIS with the off-site emergency planning zone being drastically reduced in area or even essentially eliminated by reducing it to the site boundary.

II–8. SUMMARY OF PASSIVE SAFETY DESIGN FEATURES FOR IRIS

Tables II-4 to II-8 below provide the designer's response to questionnaires developed at an IAEA technical meeting, "Review of passive safety design options for SMRs", held in Vienna on 13-17 June 2005. These questionnaires were developed to summarize passive safety design options for different SMRs according to a common format, based on provisions of IAEA Safety Standards [II-6] and other IAEA publications [II-7, II-9]. The information presented in Tables II-4 to II-8 provided a basis for the conclusions and recommendations of the main part of this report.

TABLE II-4. QUESTIONNAIRE 1 — LIST OF SAFETY DESIGN FEATURES CONSIDERED FOR/ INCORPORATED INTO THE IRIS DESIGN

#	Safety design features	What is targeted?
1	Integral primary circuit	Elimination of large break LOCA
2	Integral primary circuit	Increased coolant inventory/thermal inertia
3	Internal CRDMs	Elimination of rod ejection
4	Internal CRDMs	Elimination of vessel head penetrations
5	Increased natural circulation	Downgraded LOFA
6	Reduced size, high design pressure containment	Small break LOCA mitigation
7	Pressure suppression containment	Fission product retention improvement
8	Inerted containment	Prevention of hydrogen explosion
9	Reduced core power density	Slower progression of accidents
10	Integral steam generators, designed for full system pressure and with tubes in compression	Prevention or downgrading of: – SG tube rupture – Steam line break – Feed line break Elimination of tensile stress induced cracking
11	Internal (fully immersed) axial design pumps	Elimination of: – Shaft seizure – Locked rotor
12	Thick downcomer acting as internal neutron shield	No vessel embrittlement, and no need for surveillance resulting from a reduction of fast neutron fluence on the reactor vessel
13	Large volume integral pressurizer	Prevention of overheating events, elimination of sprays

TABLE II-5. QUESTIONNAIRE 2 — LIST OF INTERNAL HAZARDS

#	Specific hazards that are of concern for a reactor line	Explanation of how these hazards are addressed in an SMR
1	Prevent unacceptable reactivity transients	Internal CRDMs (no rod ejection); limited negative moderator reactivity coefficient
2	Avoid loss of coolant	– Integral design of the primary circuit (no large break LOCA) – Increased coolant inventory extends grace period – Coupled response of reactor vessel and containment to small break LOCA limits loss of coolant and prevents core uncovery
3	Avoid loss of heat removal	– Large thermal inertia due to increased water inventory – Passive EHRS – Passive containment cooling – Passive in-vessel retention
4	Avoid loss of flow	– Increased natural circulation due to a large, tall vessel
5	Avoid exothermic chemical reactions	– It is ensured that the thermal state of the fuel rods in accident conditions excludes the exothermic reaction of zirconium oxidation by steam – Hydrogen production due to zirconium-water interaction is coped with by inerted containment

TABLE II-6. QUESTIONNAIRE 3 — LIST OF INITIATING EVENTS FOR ABNORMAL OPERATION OCCURRENCES (AOO)/DESIGN BASIS ACCIDENTS (DBA)/BEYOND DESIGN BASIS ACCIDENTS (BDBA)

#	List of initiating events for AOO/ DBA/BDBA typical for a reactor line (PWRs)	Design features of IRIS used to prevent progression of initiating events to AOO/DBA/BDBA, to control DBA, to mitigate BDBA consequences, etc.	Initiating events specific to this particular SMR
1	Large break LOCA	– Integral primary circuit eliminates large break LOCA	Nothing in particular specified here
2	Small break LOCA	Coupled response of reactor vessel and containment to small break LOCA limits loss of coolant and prevents core uncovery	
3	LOCA	– Integral primary system – High design pressure containment – Increased coolant inventory extends grace period – Pressure suppression system	
4	Steam generator tube rupture	– Because the primary coolant is on the shell side of the steam generators, the tubes are compressed and the possibility of a steam generator tube rupture (e.g., by stress corrosion cracking) is greatly reduced – SG designed for full primary system pressure, up to main isolation valves (MIV)	
5	Rod ejection	Internal CRDMs	
6	LOFA	– Multiple (8) main circulating pumps (MCPs) – Increased natural circulation fraction because of a large, tall vessel	

TABLE II-7. QUESTIONNAIRE 4 — SAFETY DESIGN FEATURES ATTRIBUTED TO DEFENCE IN DEPTH LEVELS

#	Safety design features	Category: A-D (for passive systems only), according to IAEA-TECDOC-626 [II-9]	Relevant DID level, according to NS-R-1 [II-6] and INSAG-10 [II-7]
1	Safety-by-design™ approach	– Several DBAs eliminated by design – Reduced severity/progression of several other DBAs	1 3,4,5
2	Integral primary circuit	Elimination of large break LOCA – A	1
3	Internal CRDMs	Prevention of rod ejection – A	1
4	Passive EHRS	Downgrading loss of heat sink – D	3
5	Steam generator system designed for full system pressure up to MIV	A	3
6	Increased natural circulation fraction	Downgrading LOFA – B	1, 3, 4
7	Large thermal inertia	B, C, D (depending on the accident)	1, 2
8	Inerted containment	A	4
9	Containment cavity and design ensuring in-vessel retention	A, B	4
10	Low leakage containment	Limiting radioactivity release – A	5
11	Small fuel inventory (relative to large NPPs)	Limiting radioactivity release – A	5
12	Slower progression of accidents and increased retention of fission products due to high design pressure containment + pressure suppression system + reduced power density + increased thermal inertia	Limiting radioactivity release – A, B, C, D	5

TABLE II-8. QUESTIONNAIRE 5 — POSITIVE/NEGATIVE EFFECTS OF PASSIVE SAFETY DESIGN FEATURES IN AREAS OTHER THAN SAFETY.

Passive safety design features	Positive effects on economics, physical protection, etc.	Negative effects on economics, physical protection, etc.
Integral primary circuit with safety-by-design™	– Core damage frequency (CDF) and large early release frequency (LERF) are reduced, allowing for twin unit or multiunit power plants; potential economic benefits from reduced or eliminated emergency planning – Allows use of a compact steel containment, minimizing the siting area and improving protection from external events, such as aircraft crash – Safety-by-design™ results in a reduced complexity of the plant and its safety systems, contributing to reduced costs – Intrinsic security ('security by design') contributes to reduced costs	– Limits power of a single module (counteracted by modular construction of multiple units at site) – Increases reactor pressure vessel size (however, containment and overall footprint are decreased)
All safety grade systems are passive	– Results in reduced complexity and improved reliability of the plant, contributing to reduced capital and maintenance costs – Added resilience to sabotage and other malevolent acts	None identified

REFERENCES TO ANNEX II

[II–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Advanced Light Water Reactor Designs 2004, IAEA-TECDOC-1391, IAEA, Vienna (2004).

[II–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Innovative Small and Medium Sized Reactor Designs 2005: Reactors with Conventional Refuelling Schemes, IAEA-TECDOC-1485, IAEA, Vienna (2006).

[II–3] CARELLI, M.D., et al., The design and safety features of the IRIS reactor, Nucl. Eng. Des. **230** (2004) 151-167.

[II–4] FINNICUM, D., et al., "IRIS preliminary PRA analysis", GLOBAL 2003, paper 2069 (Proc. Int. Mtg., New Orleans, LA, 2003), American Nuclear Society/European Nuclear Society (2003).

[II–5] MAIOLI, A., FINNICUM, D. J., KUMAGAI, Y., "IRIS simplified LERF model", ANES 2004 (Proc. Int. Conf., Miami, FL, 2004).

[II–6] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA, Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[II–7] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

[II–8] INTERNATIONAL ATOMIC ENERGY AGENCY, Advanced Nuclear Power Plant Design Options to Cope with External Events, IAEA-TECDOC-1487, IAEA, Vienna (2006).

[II–9] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Terms for Advanced Nuclear Plants, IAEA-TECDOC-626, IAEA, Vienna (1991).

Annex III

SAFETY DESIGN FEATURES OF CAREM

CNEA,
Argentina

III–1. DESCRIPTION OF THE CAREM DESIGN

CAREM is an Argentine project for design and technology development and construction of an innovative, simple and small nuclear power plant (NPP). This nuclear power plant is based on an indirect cycle nuclear reactor with some distinctive and characteristic features which simplify design, and contribute to enhanced safety. A detailed description of the CAREM design and features is presented in [III-1, III-2].

The first step of this project is the construction of a prototype of about 27 MW(e) (CAREM-25) [III-2]. Main features of the CAREM approach and, specifically, the CAREM-25 design, are the following; see Fig. III-1:

- Integrated primary coolant system;
- Primary cooling by natural circulation (for CAREM-25 and CAREM designs below 150 MW(e));
- Self-pressurization (active pressurizer is eliminated);
- Safety systems relying on passive features.

Main characteristics of the CAREM nuclear power plant are given in Table III-1.

In order to simplify design, the whole high energy primary system, including the core, the steam generators, primary coolant and the steam dome, is contained inside a single reactor pressure vessel. This considerably reduces the number of pressure vessels and simplifies the layout.

The absence of large diameter piping associated with the primary system, removes the possibility of large break loss of coolant accidents (LOCA). The elimination of large break LOCA substantially reduces the necessity for emergency core cooling system (ECCSA) components, alternate current (AC) supply systems, etc.

Large coolant inventory in the primary circuit results in large thermal inertia and long response time in the case of transients or accidents.

The reactor primary coolant system operates on natural convection. Water enters the core from the lower plenum. After being heated, the coolant exits the core and flows up through the riser to the upper dome. In the upper part, water leaves the riser through lateral windows, going to the periphery region of the in-vessel space. Then it flows down through the modular steam generators, with decreased enthalpy. Finally, the coolant exits the steam generators and flows down through the down-comer to the lower plenum, closing the circuit.

The CAREM primary coolant system is self-pressurized.

Due to the innovative design of the reactor core cooling system (RCCS), an extensive experimental plan has been developed and is being implemented [III-2, III-3].

RCCS modelling and qualification are supported by tests performed in a high pressure natural circulation rig (CAPCN), covering thermal hydraulics and techniques of reactor control and operation. The CAPCN rig reproduces all dynamic phenomena of the RCCS, except for 3D effects.

The fuel is enriched UO_2. Core reactivity is controlled by the use of Gd_2O_3 as a burnable poison in special fuel rods and moveable absorbing elements belonging to the reactor control and adjustment system. Liquid chemical compositions (like boric acid solution) are not used for reactivity control during normal operation.

Each absorbing element (AE) consists of a cluster of rods linked by a structural element (namely, 'spider'), so that the cluster moves as a single unit. Absorber rods fit into guide tubes. The absorber material is the commonly used Ag-In-Cd alloy. Absorbing elements (AE) are used for reactivity control during normal operation (control and adjustment system) and to interrupt nuclear chain reaction promptly when required (fast shutdown system).

The shutdown system is diversified to fulfil the requirements of the Argentine regulatory authority.

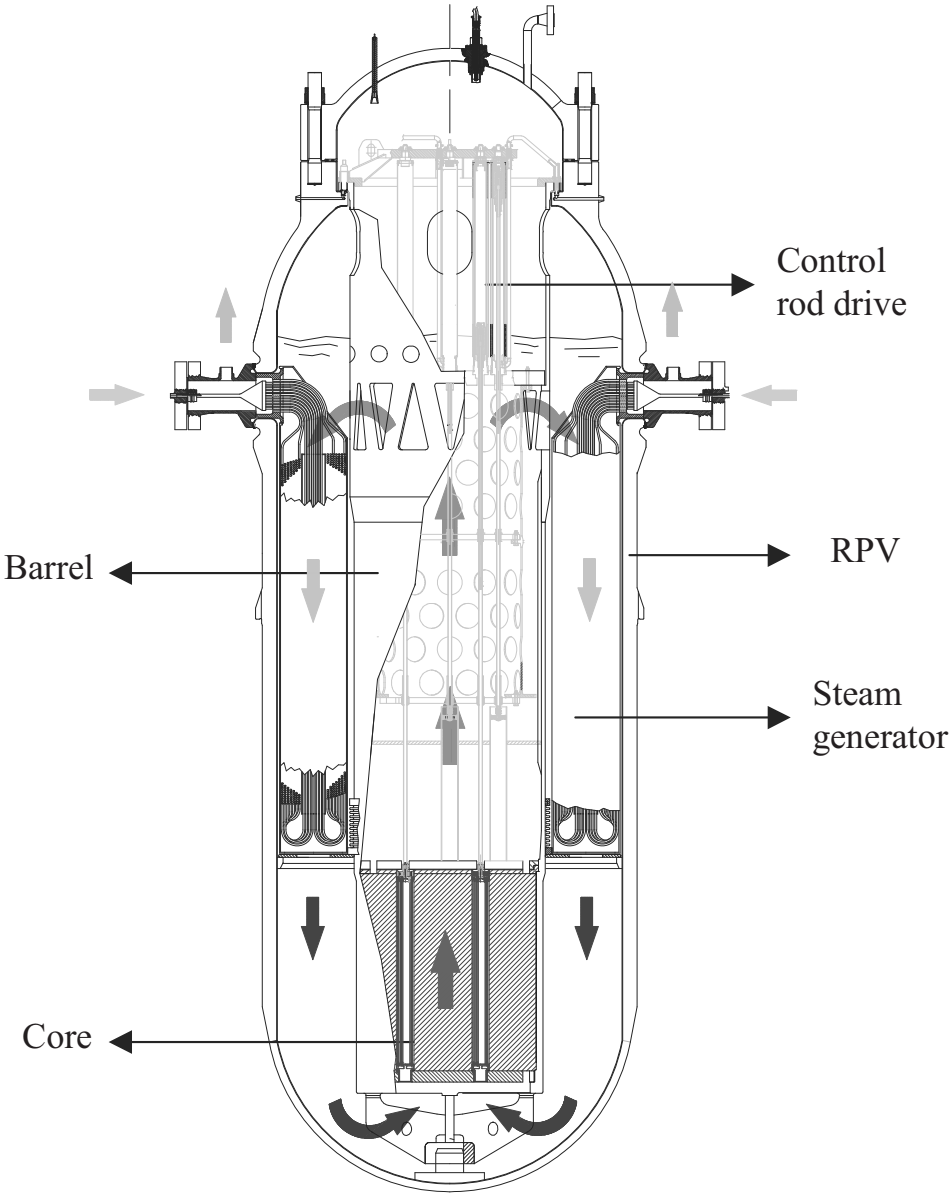


FIG. III-1. CAREM primary system.

The first shutdown system (FSS) consists of gravity driven neutron-absorbing elements. In CAREM-25, this system provides a total negative reactivity of 6880 pcm in a cold shutdown state, with all rods inserted.

During normal operation, elements of the FSS are kept in the upper position. They are designed to provide a minimal dropping time, so it takes only a few seconds to completely insert the absorbing rods into the core. In CAREM-25, this system has a minimum worth of 3500 pcm, with one rod unavailable.

The second shutdown system (SSS) is a gravity driven injection device based on high pressure borated water. In CAREM-25, this system provides a total negative reactivity of 5980 pcm in a cold shutdown state, assuming a single rod failure.

Twelve identical 'mini-helical' vertical steam generators (see Fig. III-2) of the once-through type are placed equidistant from each other along the inner surface of the reactor pressure vessel (RPV) [III-1, III-2]. They are used to transfer heat from the primary to the secondary circuit, producing superheated dry steam at 47 bar. The secondary system circulates upwards within the tubes, while the primary is in counter current flow. An external shell surrounding the outer coil layer and adequate seal form the flow separation system. It guarantees that the entire stream of the primary system flows through the steam generators.

TABLE III-1. MAIN CHARACTERISTICS OF CAREM PLANT [III-2]

Characteristics	Design Particulars
Installed capacity	900 MW(th)/300 MW(e) for CAREM-300 100 MW(th)/27 MW(e) for CAREM-25 (prototype)
Type of fuel	PWR type fuel assembly with low enriched UO_2
Fuel enrichment	About 3.5%
Moderator	Light water
Coolant	Light water
Structural materials	Barrel: SS-304L Core grids and envelope: SS-304 Steam generator shell: SS-304L Steam generator tubes: Inconel 690 (SB 163 N06690)
Core	Fuel assemblies of hexagonal cross section. Each fuel assembly contains 108 fuel rods of 9 mm outer diameter, 18 guide thimbles and 1 instrumentation thimble. The core of CAREM-300 has 199 fuel assemblies with about 2.85 m active length. The core of CAREM-25 has 61 fuel assemblies with about 1.40 m active length.
Reactor vessel	Vessel material: SA508 Grade 3 Class 1 Lining material: SS-304L For the CAREM-25 vessel the main dimensions are: Height: 11 m Inner diameter: 3.16 m Wall thickness: 0.135 m

To achieve rather uniform pressure-loss and superheating on the secondary side, the length of all tubes is equalized. For safety reasons, steam generators are designed to withstand the primary pressure without pressure in the secondary side and the live steam system is designed to withstand primary pressure up to the isolation valves (including the steam outlet/water inlet headers) in case of SG tube breakage.

III–2. PASSIVE SAFETY DESIGN FEATURES OF CAREM

Inherent safety features

The inherent safety features of CAREM are:

- Integrated primary coolant system, eliminating large break LOCA;
- Long characteristic times in the event of a transient or severe accident, due to large coolant inventory and the use of passive safety systems;
- Natural convection core cooling in lower power modules (e.g., CAREM-25) eliminates loss of flow accidents (LOFA);
- Hydraulic control rod drive mechanisms located completely inside the RPV eliminate control rod ejection accidents;
- Negative reactivity effects and coefficients, see Table III-2.

Passive safety systems

The CAREM safety systems are based on passive features obviating the need for accident management over a long period [III-1, III-2]; see Fig. III-2. Systems are duplicated to fulfil redundancy criteria. According to Argentine regulations, the shutdown system is diversified.

Natural circulation and self-pressurization properties

Flow rate in the reactor's primary systems is achieved by natural circulation. The driving forces resulting from differences in density along the circuit are balanced by friction and shape change losses, producing an adequate flow rate in the core and securing a sufficient thermal margin to critical phenomena. Natural convection of reactor coolant is due to the location of the steam generators above the reactor core.

Self-pressurization of the primary system in the steam dome results from liquid-vapour equilibrium. The large volume of the integral pressurizer also contributes to damping of eventual pressure perturbations. Heaters and sprinkles typical of conventional pressurized water reactors (PWRs) are, therefore, eliminated.

Eliminating primary pumps and the pressurizer results in added inherent safety features (loss of flow accident elimination), and in advantages for maintenance and availability.

First shutdown system (FSS)

The FSS is designed to shut down the core when an abnormality or a deviation from normal operation occurs and to maintain the core in a subcritical condition during all shutdown states. This function is achieved by dropping neutron absorbing elements into the core, driven by gravity. Each neutron absorbing element is a cluster composed of a maximum of 18 individual rods coupled together in a single unit. Each unit fits into the guide tubes of a fuel assembly.

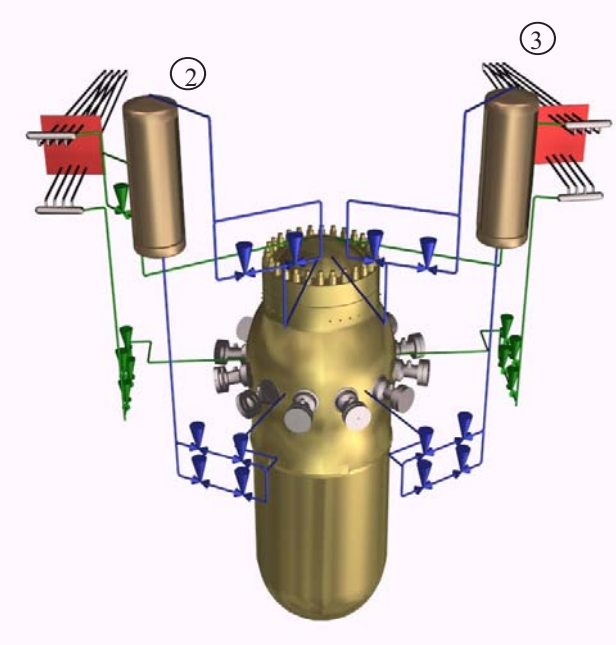
The internal hydraulic control rod drive (CRD) eliminates the mechanical shafts passing through the reactor pressure vessel (RPV) or through the extension of the primary pressure boundary and, as the whole device is located inside the RPV, contributes to the elimination of large break LOCAs. This design is an important element in the CAREM concept. Many of the control rods belong to a fast shutdown system. A simplified diagram of the fast shutdown system hydraulic CRD is shown in Fig. III- 3. During normal operation, fast shutdown system control rods are kept in the upper position, where the piston partially closes the outlet orifice and reduces water flow leaking into the RPV dome.

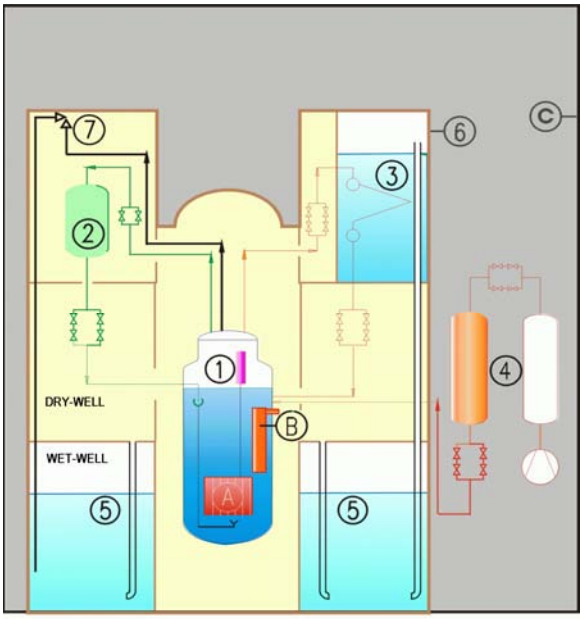
The CRD of the control and adjustment system is a hinged device controlled in steps and fixed in position by pulses over a base flow, designed so that each pulse produces only one step.

Both types of devices perform the reactor scram function by using the same principle: 'rods are dropped driven by gravity when the flow is interrupted', so that the malfunction of any powered part of the hydraulic circuit (i.e., a valve or a pump failure) causes immediate shutdown of the reactor. CRD of the fast shutdown system is designed with a large gap between piston and cylinder to obtain a minimum dropping time (of a few seconds) to insert absorbing rods completely into the core. CRD manufacturing and assembling allowances are stricter, and clearances are narrower for rods of the control and adjustment system, but there is no stringent requirement on dropping time.

TABLE III-2. REACTIVITY EFFECTS OF CAREM

Characteristic	Value
Fuel temperature reactivity coefficient	<–2.1 pcm/°C
Coolant temperature reactivity coefficient	<–40 pcm/°C in normal operation <–4 pcm/°C in cold shutdown
Coolant void coefficient	<–147 pcm/% in normal operation <–43 pcm/% in a cold shutdown state
Burnup reactivity swing	3600 pcm
Maximum power peaking factor	2.7





1: First shutdown system
2: Second shutdown system
3: Residual heat removal system
4: Emergency injection system
5: Pressure suppression pool
6: Containment
7: Safety valves
A: Core
B: Steam generators
C: Reactor building

FIG. III-2. Containment and safety systems of CAREM.

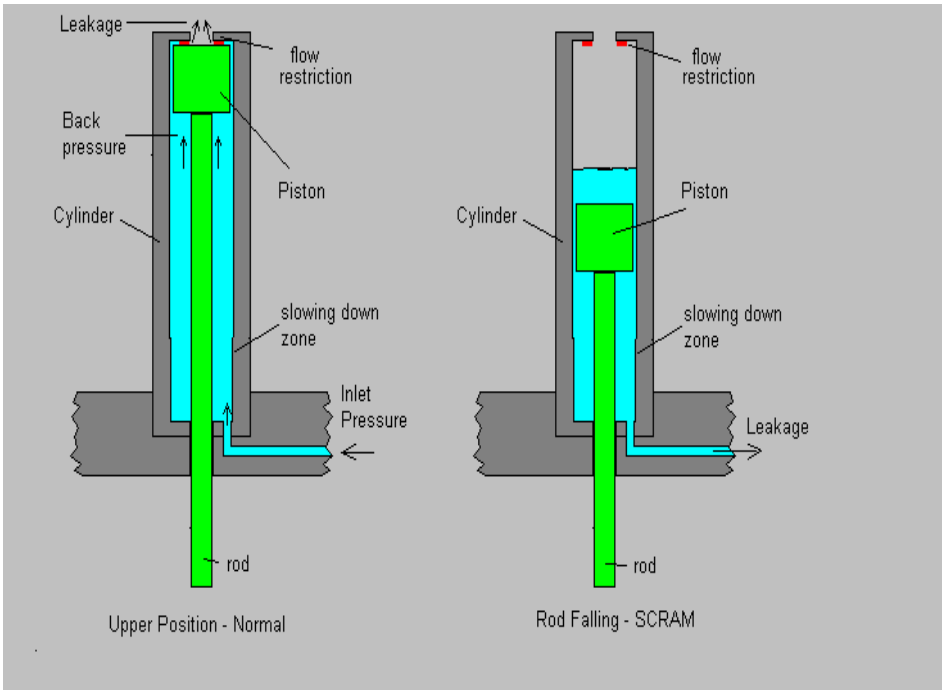


FIG. III-3. Simplified operating diagram of a hydraulic control rod drive (fast shutdown system).

Second shutdown system (SSS)

The SSS is a gravity driven injection device using borated water at high pressure. It acts automatically when the reactor protection system detects a failure of the FSS or in the case of a LOCA. This system consists of two tanks located in the upper part of the containment. Each of them is connected to the reactor vessel by two pipelines; one is from the steam dome to the upper part of the tank, and the other is from a position below the reactor water level to the lower part of the tank. When the system is triggered, the valves open automatically and the borated water drains into the primary system, driven by gravity. The discharge of a single tank produces the complete shutdown of the reactor.

Residual heat removal system (RHRS)

The RHRS is a simple and reliable system that operates by condensing steam from the primary system in the emergency condensers. The emergency condensers are heat exchangers consisting of an arrangement of parallel horizontal U tubes located between the two common headers. The top header is connected to the reactor vessel steam dome, while the lower header is connected to the reactor vessel at a position below the reactor water level. The condensers are located in a pool filled with cold water inside the containment building. The inlet valves of the steam line are always open, while the outlet valves are normally closed (the tube bundles are filled with condensate). When the system is triggered, the outlet valves open automatically. Water drains from the tubes and steam from the primary system enters the tube bundles and condenses on the cold surface of the tubes. The condensate is returned to the reactor vessel forming a natural circulation circuit. In this way, heat is removed from the reactor coolant. During the condensation, heat is transferred to water of the pool by a process of boiling. The evaporated water is then condensed in the suppression pool of the containment.

Emergency injection system

This system prevents core uncovery in the case of a LOCA. The system consists of two redundant accumulators with borated water connected to the RPV. The tanks are pressurized, so that during a LOCA,

when pressure in the reactor vessel becomes relatively low, rupture disks break and flooding of the RPV starts, preventing core uncovery over a long period. The RHRS is also triggered to help depressurize the primary system when the area of a break is small.

Safety relief valves

Three safety relief valves protect the reactor pressure vessel against over-pressurization in the case of strong differences between core power and the power removed from the RPV. Each valve is capable of 100% of the necessary relief. Blow-down pipes are routed from the safety valves to the suppression pool.

Active safety systems

All safety systems of the CAREM are passive systems. All safety systems are safety grade.

For long term water inventory control and to maintain the reactor in a hot shutdown state, auxiliary active systems are used. These are class III safety grade systems [III-4].

III–3. ROLE OF PASSIVE SAFETY DESIGN FEATURES IN DEFENCE IN DEPTH

Some major highlights of passive safety design features in the CAREM design, structured in accordance with the various levels of defence in depth [III-5, III-6], are below.

Level 1: Prevention of abnormal operation and failure

Contributions of CAREM inherent and passive safety features at this level are as follows:

- Due to the absence of large diameter piping in the primary system, large break LOCAs are eliminated;
- Natural convection core cooling in lower power CAREM modules eliminates loss of flow accidents.
- Hydraulic CRDs located completely inside the reactor pressure vessel eliminate control rod ejection accidents and contribute to downgrading of LOCA by minimizing necessary vessel penetrations;
- Soluble boron free core design eliminates boron dilution accidents.

Level 2: Control of abnormal operation and detection of failure

The CAREM passive safety feature for this level is as follows:

- A large coolant inventory in the primary circuit results in a larger thermal inertia and in longer response times in the case of transients or accidents.

Level 3: Control of accidents within the design basis

CAREM's safety systems are based on passive features obviating the need for actions related to accident management over a long period, see Section III-2.

Level 4: Control of severe plant conditions, including prevention of accident progression and mitigation of consequences of severe accidents

Contributions of inherent and passive features of CAREM at this defence in depth level are as follows:

- When core uncovery is assumed, only for analytic purposes, low heat-up rates of fuel elements in the exposed part of the core are predicted, if the geometry is still intact. The characteristic time of core melting is long, eventually preventing temperature excursion due to a metal-water reaction, which in turn limits the hydrogen generation rate;

- Reduction of the hydrogen concentration in the containment by catalytic recombiners and, if necessary, selectively located igniters;
- Sufficient floor space for cooling of molten debris;
- Extra layers of concrete to avoid direct exposure of the containment basement to debris.

Level 5: Mitigation of radiological consequences of significant release of radioactive materials

The following passive features of CAREM make a contribution to this defence in depth level:

- Suppression pool type containment provides a physical mechanism for the retention of fission products by water;
- Relatively small fuel inventory, when compared to larger NPPs;
- Slower progression of accidents and increased retention of fission products (facilitated by such features as reduced power density, increased thermal inertia, a pressure suppression system, etc.);
- The containment is located inside the nuclear module building, which reduces the release of fission products due to local deposition.

The CAREM concept provides for extended accident prevention and mitigation by relying on the principles of simplicity, reliability, redundancy, and passivity. Nevertheless, in the very low probability case of failure of all redundant passive safety systems or in the case of no recovery action after the design period by the safety systems (a grace period of several days), a severe accident could be postulated to occur. Several passive features are incorporated to address hypothetical severe accidents and to secure confinement of the resulting radioactivity. These features provide for the optimum use of all available process systems to achieve primary cooling and containment recovery after the grace period. Some passive features are mentioned above, in the sections on Levels 4 and 5 of defence in depth. In addition to these, the following active features are also possibilities:

- The suppression pool cooling and purification system could cool and refill, if necessary, the suppression pool and the cooling pool for the residual heat removal system, and could also feed spray in the dry well and the wet well to depressurise the containment. In the event of a LOCA, this system is capable of feeding pure water into the RPV;
- Provisions are made for the injection of water to the reactor cavity from the refuelling water storage tank to cool the RPV from the outside in order to enhance retention of core debris, taking advantage of the high ratio of the RPV lower bottom head area to the core mass, characteristic of integral type reactors.

III–4. ACCEPTANCE CRITERIA FOR DESIGN BASIS AND BEYOND DESIGN BASIS ACCIDENTS

III–4.1. Design basis accidents (DBA) and acceptance criteria

The DBA considered for CAREM are listed and commented upon below. In these accidents, proper actuation of related safety systems is provided for and deterministic acceptance criteria (such as sufficient thermal margin or no core uncovery) are applied [III-1, III-2].

Reactivity initiated accident (RIA)

As the hydraulic control rod drive (CRD) for the first shutdown system (FSS) and the control and adjustment system are located inside the RPV, accidents with control rod ejection are eliminated. Therefore, only inadvertent control rod withdrawal transients are postulated. Two scenarios involving an FSS success and an FSS failure with actuation of the second shutdown system (SSS) have been simulated, based on conservative assumptions. The results of these simulations show that safety margins (such as departure from the nucleate boiling ratio (DNBR) and the critical power ratio (CPR)) are well above critical values and, therefore, no core

damage is expected. Moreover, as there is no liquid boron in the coolant, boron dilution as a reactivity initiated event is precluded.

Loss of heat sink

In case of a total loss of feedwater to the steam generators, the residual heat removal system is actuated, cooling the primary system and reducing reactor pressure to values below those of a reactor hot shutdown state. In case of a hypothetical failure of the FSS, reactor power is reduced due to negative reactivity coefficients, without compromising the integrity of fuel elements. The SSS would then guarantee medium and long term reactor shutdown.

Total loss of flow

In the CAREM modules using natural convection in the primary coolant system (CAREM designs with a unit power of less than 150 MW(e)), there are no primary pumps, thus this initiating event is excluded. In higher power modules with forced circulation, natural convection is enhanced intrinsically by the integral type layout of the primary circuit.

Loss of coolant

The diameter of RPV penetrations is limited by design (there are no large diameter penetrations). Therefore, no large LOCA is possible and there is no need for a high pressure injection system. In case of a LOCA, the FSS, SSS, and RHRS are actuated and, when the pressure is decreased, the emergency injection system discharges water to keep the core covered for several days. As the CAREM design obviates active systems, in safety evaluations the secondary coolant system is not assumed to cool and depressurize the primary system. However, once it is available and when needed, it could be used as part of the accident management strategy.

The inherent response of the reactor to LOCA has been analyzed considering a FSS success and the failure of all safety systems related to core cooling. Due to a large water inventory over the core and small diameters of RPV penetrations, the core is uncovered only after several hours.

Steam generator tube rupture

This accident is mitigated by isolating the group of steam generators affected via closing their steam and feedwater lines. The secondary side of the steam generators then reaches thermal equilibrium with the primary circuit, with the pressure also being equalized. Eventually, the reactor could continue its operation at reduced power.

Steam line break

Sudden depressurization of the secondary side of the steam generators increases heat removal from the primary system, resulting in a consequent core overpower. Reactor shutdown (FSS and SSS) and the residual heat removal system are actuated, and the reactor then reaches a safe state. In the case of a hypothetical failure of both shutdown systems, reactor overpower does not compromise critical safety values (DNBR and CPR) because the total primary heat removal by the steam generators is intrinsically limited by the reduced tube-side water inventory.

NPP blackout

This is an event with a major contribution to core meltdown probability in a conventional light water reactor. In CAREM, extinction and cooling of the core and decay heat removal are secured without external electric power, by the passive safety systems. Loss of electric power causes the interruption of feedwater supply to the hydraulically driven CRDs and results in the insertion of absorbing elements into the core. Nevertheless,

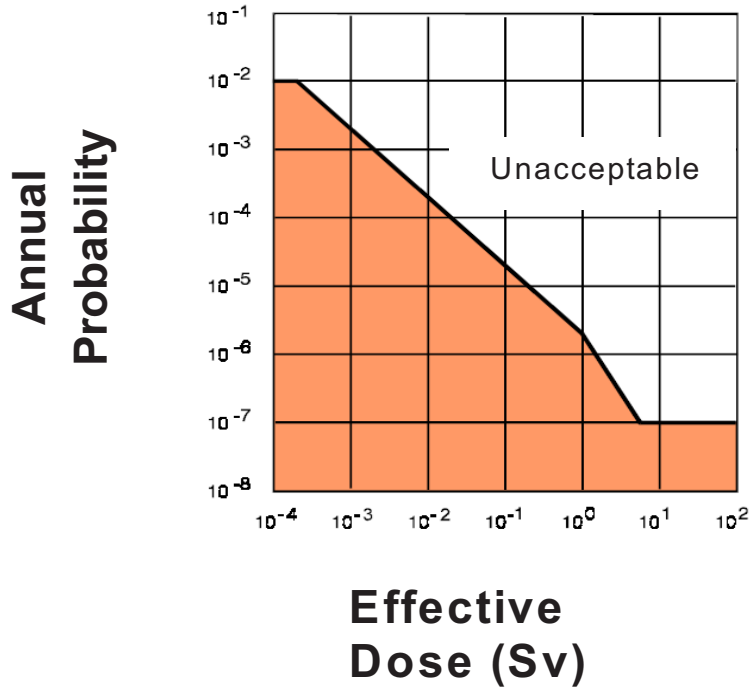


FIG. III-4. Acceptance criterion for BDBA.

in the case of a failure of the first and the second shutdown systems (both passive), feedback coefficients cause a self-shutdown of the fission chain reaction without compromising safety related variables. The decay heat is then removed by the RHRS with an autonomy of several days.

III–4.2. Beyond design basis accidents (BDBA) and acceptance criteria

To fulfil Argentina's regulations, a set of accidental sequences associated with potential exposure of the personnel and population has been identified. The annual probability of occurrence of each identified sequence is calculated using event trees and fault trees. Failure analysis systematically covers all failures and accidental sequences that can be foreseen, including combinations of failures. In these analyses, an assumption is being made that safety functions are not operable.

The dose to the critical group that would result from the release and dispersion of radioactive nuclides is calculated using accepted methods. Meteorological conditions and their probabilities are being considered. No credit is taken for any countermeasure, such as evacuation.

According to Argentina's regulations, no accidental sequence with radiological consequences for the public shall have an annual probability of occurrence that, when plotted against the calculated effective dose, results in a point located in the unacceptable region shown in Fig. III-4 [III-7].

If the number N of accidental sequences is greater than 10, the allowed annual probability shall be divided by N/10, in order to keep the overall risk below 10^{-6} per reactor per year.

III–5. PROVISIONS FOR SAFETY UNDER EXTERNAL EVENTS

The safety design features of CAREM intended to cope with external events and external/internal event combinations are described in detail in [III-8].

Seismic considerations for the CAREM have been developed at the basic engineering level, with the objective of achieving an enveloping design that could qualify for a variety of possible siting conditions.

The philosophy and terminology of the Argentine regulations have been adopted for seismic design. The applicable regulation is AR 3.10.1 "Protección contra terremotos en reactores nucleares de potencia" [III-9]. This norm defines two seismic levels for design purposes:

(1) ‘Severe earthquake’, similar to the safe shutdown earthquake defined by the US NRC and to the L-S2 earthquake level of the IAEA guides [III-10];
(2) ‘Probable earthquake’, similar to the operating basis earthquake defined by the US NRC and to the L-S1 earthquake level of the IAEA guides.

As the targeted sites are located in a moderate seismic zone, the effective peak ground acceleration (PGA) of a severe earthquake was defined as 0.4g.

The IAEA Safety Standards and Guides regarding seismic design have been adopted [III-10]. Combinations with internal events are also considered. For example, a combination of DBA (LOCA with the break of a primary pipe of maximum diameter) with NPP blackout and probable earthquake is considered in the CAREM design.

III–6. PROBABILITY OF UNACCEPTABLE RADIOACTIVITY RELEASE BEYOND PLANT BOUNDARY

The large release probability of the CAREM-25 (a prototype reactor) has been evaluated at 5.2×10^{-8}/year. Reflecting on this very low value, the designers consider an option to license the reactor with simplified or abandoned off-site emergency planning requirements.

III–7. SUMMARY OF PASSIVE SAFETY DESIGN FEATURES FOR CAREM

Tables III-3 to III-7 below provide the designer’s response to the questionnaires developed at the IAEA technical meeting “Review of passive safety design options for SMRs” held in Vienna on 13-17 June 2005[1]. The questionnaires were developed to summarize passive safety design options for different SMRs according to a common format, based on provisions of the IAEA Safety Standards [III-5] and other IAEA publications [III-6, III-11].

The information presented in Tables III-3 to III-7 provided a basis for the conclusions and recommendations in the main part of this report.

TABLE III-3. QUESTIONNAIRE 1 — LIST OF SAFETY DESIGN FEATURES CONSIDERED FOR/INCORPORATED INTO THE CAREM DESIGN

#	Safety design features	What is targeted?
1	Integral primary circuit	Large-break LOCA
2	Integral primary circuit	Increased coolant inventory/increased thermal inertia
3	Internal CRDMs	Rod ejection
4	Internal CRDMs	Reduced number and size of reactor vessel head penetrations
5	Soluble boron free core	Boron dilution
6	Natural circulation	Loss of flow accident
7	Pressure suppression containment	Fission product retention improvement
8	Large thermal inertia	Slower progression of accidents

[1] Some features of the integral design PWRs — CAREM, IRIS (see ANNEX II) and SCOR (see ANNEX V) — may be described using the same or similar words, because their designers have undertaken a collective effort to describe such features at the IAEA technical meeting “Review of passive safety design options for SMRs” held in Vienna on 13–17 June 2005.

TABLE III-4. QUESTIONNAIRE 2 — LIST OF INTERNAL HAZARDS

#	Specific hazards that are of concern for a reactor line	Explain how these hazards are addressed in a SMR
1	Prevent unacceptable reactivity transients	Internal CRDMS (no rod ejection); boron-free core (no boron dilution); limited negative moderator reactivity coefficient
2	Avoid loss of coolant	• Integral primary circuit • Increased coolant inventory per unit of power (high thermal inertia)
3	Avoid loss of heat removal	• Large thermal inertia due to increased specific water inventory • Passive heat removal systems
4	Avoid loss of flow	• Natural circulation of primary coolant
5	Avoid exothermic chemical reactions	• Large thermal inertia

TABLE III-5. QUESTIONNAIRE 3 — LIST OF INITIATING EVENTS FOR ABNORMAL OPERATION OCCURRENCES (AOO)/DESIGN BASIS ACCIDENTS (DBA)/BEYOND DESIGN BASIS ACCIDENTS (BDBA)

#	List of initiating events for AOO/DBA/BDBA typical for a reactor line (PWRs)	Design features of CAREM used to prevent progression of initiating events to AOO/DBA/BDBA, to control DBA, to mitigate BDBA consequences, etc.	Initiating events specific to this particular SMR
1	LOCA	• Integral primary circuit eliminates large break LOCA • Increased coolant inventory extends grace period • Pressure suppression system maintains integrity of the containment	Nothing specified here
2	Steam generator tube rupture	• Steam generators designed for full primary system pressure	
3	Rod ejection	• Internal CRDMs	
4	Boron dilution	– Soluble boron free core design	
5	Loss of flow accident	– Natural circulation	
6	Loss of heat sink	– Passive heat removal systems	

TABLE III-6. QUESTIONNAIRE 4 — SAFETY DESIGN FEATURES ATTRIBUTED TO DEFENCE IN DEPTH LEVELS

#	Safety design features	Category: A-D (for passive systems only), according to IAEA-TECDOC-626 [III-11]	Relevant DID level, according to NS-R-1 [III-5] and INSAG-10 [III-6]
1	Integral primary circuit	Large break LOCA – A	1
2	Internal CRDMs	Rod ejection – A	1
3	Soluble boron free core design	Boron dilution – A	1
4	Natural circulation	Loss of flow (LOFA) – B	1
5	Large thermal inertia	B	2
6	Passive shutdown systems	D	3
7	Passive EHRS	Loss of heat sink – D	3
8	Passive low pressure injection system	LOCA – D	3
9	Large thermal inertia	– When core uncovery is assumed, only for analytic purposes, low heat-up rates of fuel elements in the exposed part are predicted as long as the geometry is still intact. Therefore, core melt characteristic time is long, eventually preventing temperature excursion due to a metal-water reaction, which in turns limits the hydrogen generation rate – B	4
10	Containment located inside the nuclear building	Reduction of fission product release due to deposition – A	5
11	Small fuel inventory (relative to large NPPs)	Radioactivity release – A	5
12	Slower progression of accidents and increased retention of fission products (pressure suppression system + reduced power density + increased thermal inertia, etc.)	Radioactivity release – A, B, C, D	5

TABLE III-7. QUESTIONNAIRE 5 — POSITIVE/NEGATIVE EFFECTS OF PASSIVE SAFETY DESIGN FEATURES IN AREAS OTHER THAN SAFETY.

Passive safety design features	Positive effects on economics, physical protection, etc.	Negative effects on economics, physical protection, etc.
Integral primary circuit	– Longer RPV lifetime due to reduced fast neutron fluence; – Elimination of certain accident initiators and relevant safety systems, reducing plant costs	Limits total power
Natural circulation	– Simplified design and maintenance, reduced costs due to the absence of main coolant pumps	Increased specific RPV cost; potentially increased complexity of reactor operation (startup, etc.)
Self-pressurization	– The elimination of an active pressurizer (with heaters and sprinklers) results in lower plant costs and advantages for maintenance and availability	

REFERENCES TO ANNEX III

[III–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Advanced Light Water Reactor Designs 2004, IAEA-TECDOC-1391, IAEA, Vienna (2004).

[III–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Innovative Small and Medium Sized Reactor Designs 2005: Reactors with Conventional Refuelling Schemes, IAEA-TECDOC-1485, IAEA, Vienna (2006).

[III–3] INTERNATIONAL ATOMIC ENERGY AGENCY, Innovative Small and Medium Sized Reactors: Design Features, Safety Approaches and R&D Trends, IAEA-TECDOC-1451, IAEA, Vienna (2005).

[III–4] ANSI/ANS 51.1, Nuclear Safety Criteria for the Design of Stationary PWR Plants, American Nuclear Society, Standards Committee Report of Activities (2005): http://www.ans.org/standards/resources/downloads/docs/comactivitiesreport.pdf

[III–5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[III–6] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

[III–7] AUTORIDAD REGULATORIA NUCLEAR, Criterios radiológicos relativos a accidentes en reactores nucleares de potencia, Norma 3.1.3., Revisión 2, Argentina (2002).

[III–8] INTERNATIONAL ATOMIC ENERGY AGENCY, Advanced Nuclear Power Plant Design Options to Cope with External Events, IAEA-TECDOC-1487, IAEA, Vienna (2006).

[III–9] AUTORIDAD REGULATORIA NUCLEAR, 1 Protección contra terremotos en reactores nucleares de potencia, Norma 3.10.1, Revisión 2, Argentina (2002).

[III–10] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.6, IAEA, Vienna (2004).

[III–11] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Terms for Advanced Nuclear Plants, IAEA-TECDOC-626, IAEA, Vienna (1991).

Annex IV

SAFETY DESIGN FEATURES OF THE SCOR

CEA,
France

IV–1. DESCRIPTION OF THE SCOR DESIGN

The Simple Compact Reactor (SCOR) is a 2000 MW(th) integral design pressurized light water reactor (PWR). The design for the reactor was developed at the Nuclear Energy Division of the Commissariat à l'Energie Atomique in Cadarache, France. A detailed description of SCOR design and features is provided in [IV-1].

The SCOR is mainly being developed for electricity generation, providing competitive costs, when compared to large sized reactors, through system simplification and compactness in plant layout. However, the SCOR could be used in cogeneration schemes, such as seawater desalination using low temperature processes, as well as thermo-compression or multi-effect distillation.

The SCOR is an integral design reactor having new features with respect to the designs of typical integral type reactors, which usually contain several modular steam generators inside the vessel. Such architecture has led to the design of a large vessel, limiting the output of the reactor to a maximum of 1000 MW(th). In the SCOR concept, the steam generator is located above the vessel and acts as the vessel head. This layout component provides space inside the vessel to increase core size and therefore, has the same safety advantages (elimination of a large break loss of coolant accident); the SCOR unit power is twice as high as the maximum power of a typical integral design reactor [IV-1, IV-2].

Passive safety features allow the SCOR to respond safely to all initiating events within the design basis, with few operator actions required. Except for loss of coolant accidents (LOCA), where low electric power is needed in the mid term (a low pressure safety injection with a power of about a few tens of kW is required for less than one day), no alternative current (AC) power is needed for accident management. Most of the design extension[1] conditions are eliminated or passively managed as accidents within the design basis. This simplifies the scope of operator training, equipment qualification and surveillance to meet safety requirements.

The main characteristics of a nuclear power plant (NPP) with a SCOR reactor are given in Table IV-1. A schematic view of the SCOR plant is shown in Fig. IV-1.

The plant control scheme will be specifically designed for operation with a single steam generator and will be based on a 'reactor follows the plant load' strategy.

The SCOR is an integral type PWR with a compact primary circuit. The reactor pressure vessel houses the main primary system components including the core, the pressurizer, the reactor coolant pumps, the control rod drive mechanism (CRDM), and the heat exchangers of the decay heat removal system. Such design configuration eliminates large penetrations through the reactor vessel, excluding the possibility of large break loss of coolant accidents. A single steam generator acts as the reactor vessel head; see Fig. IV-2 (this figure also illustrates the flow path of the coolant).

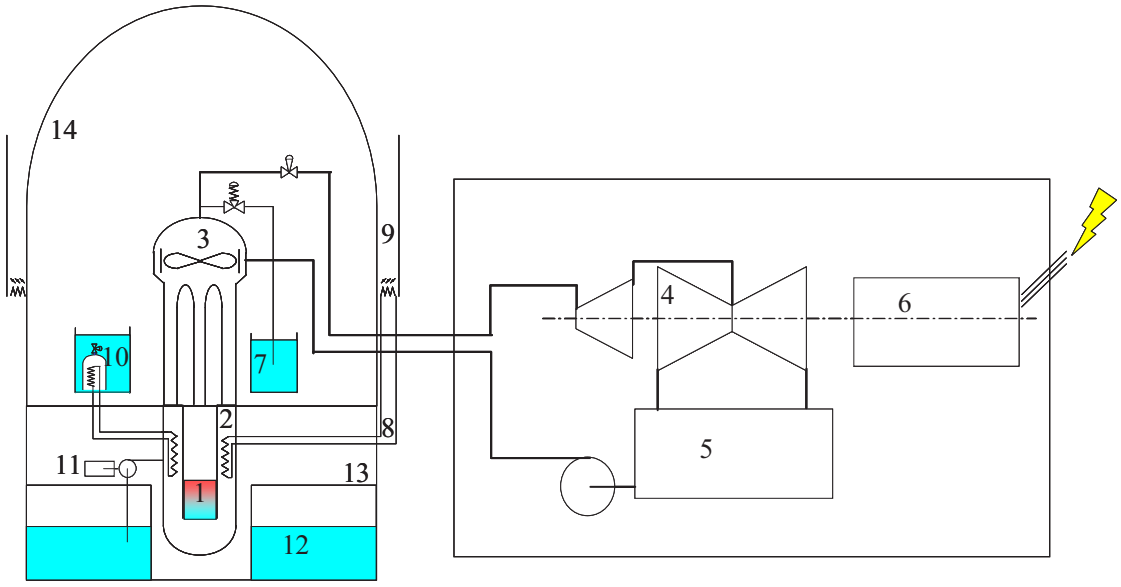
From the lower plenum, water flows upward through the core and the riser and through the centre of the pressurizer. At the top of the vessel, fluid flows upward and downward through the U shaped tubes of the steam generator. Then, the fluid is collected in an annular plenum and passes to the inlet of the reactor coolant pumps. From the pump outlet, the coolant flows through a venturi and then across the tubes of the decay heat exchangers to the lower plenum.

A design with integrated pumps eliminates large diameter loops typical of a standard PWR and substantially eliminates large break LOCA events. The number of smaller diameter pipes is also reduced, limiting the probability of occurrence of small breaks and small break loss of coolant events.

[1] In IAEA terminology, beyond design basis accident conditions.

TABLE IV-1. MAJOR DESIGN AND OPERATING CHARACTERISTICS OF THE SCOR [IV-1]

Characteristic	Value
Installed capacity	
Power plant output, net	630 MW(e)
Reactor thermal output	2000 MW(th)
Reactor core	
Active core height	3.66 m
Equivalent core diameter	3.04 m
Average linear heat rate	12.9 kW/m
Average fuel power density	24 kW/kg UO_2
Average core power density (volumetric)	75.3 kW/l
Thermal heat flux	430 kW/m²
Reactor pressure vessel (RPV)	
Cylindrical shell inner diameter	4983 mm
Wall thickness of cylindrical shell	141 mm
Total height	14813 mm
RPV head	No (steam generator)
Base material: cylindrical shell	Carbon steel
Liner	Stainless steel
Design pressure/temperature	9.78/309 MPa/°C
Transport weight (lower part)	280 t



1	Core	8	Residual heat Removal system on Primary circuit (RRP)
2	Reactor vessel	9	Air-cooling tower of the RRP
3	Steam generator	10	Heat sink pool of the RRP
4	Turbine	11	Low Pressure Safety Injection system
5	Condenser	12	Pool of the wetwell
6	Generator	13	Primary containment (drywell)
7	Steam dump pool	14	Containment building

FIG. IV-1. Schematics of the SCOR plant [IV-1].

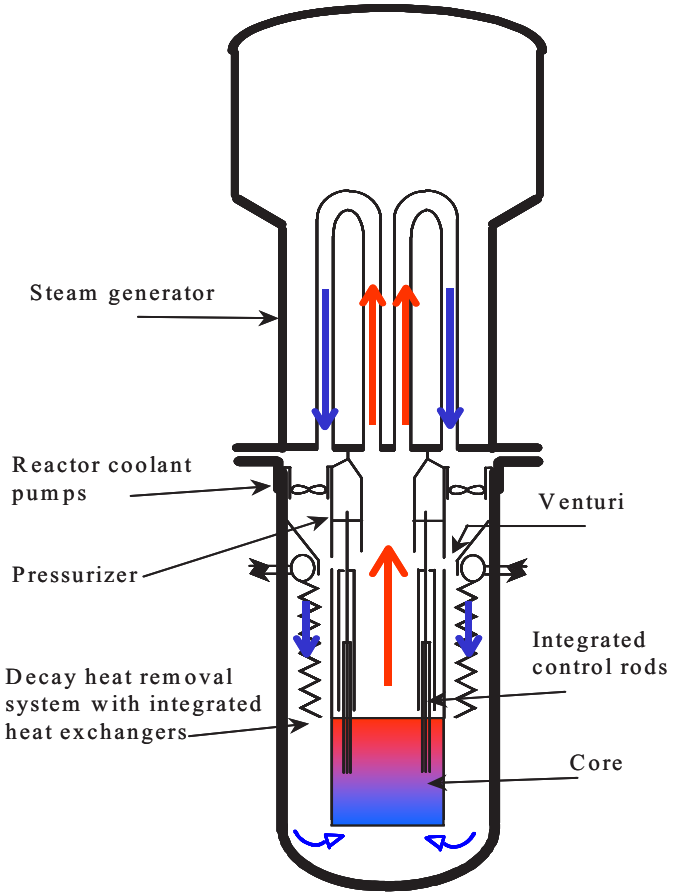


FIG. IV-2. Primary coolant system [IV-1].

The SCOR concept is based on well-proven nuclear reactor technologies; its major innovations are related to safety design and the design of auxiliary systems. The innovative features of SCOR are as follows:

- Elimination of large diameter penetrations through the reactor pressure vessel;
- Integrated passive emergency core cooling systems based only on natural convection and using external air as the ultimate heat sink;
- A soluble boron free core with control rod drive mechanisms located inside the reactor pressure vessel;
- Relatively low core power density, enabling a large margin (i.e., departure from the nucleate boiling ratio (DNBR)) within the whole range of operating parameters;
- Reduction of reactor building maximum pressurization;
- Reduction of human factors affecting safety systems;
- Easy testing and maintenance of all safety systems.

Reactivity control is achieved through the use of control rods with in-vessel drives; no soluble boron system is foreseen. To reduce reactivity at the beginning of the cycle, the loaded portion of fuel contains burnable poison. As in standard pressurized water reactors (PWRs), the clusters of control rods are moved in guide thimbles but, as the steam generator acts as a vessel head, there is no possibility of using an external mechanism to move the control rod clusters. The control rod drive mechanism (CRDM) appears as an integrated hydraulic system. There is around one control rod cluster per two fuel assemblies; such selection is sufficient to control reactivity from a full power to a cold shut down state. In accident conditions, redundancy is achieved by another device, called the MP98 system [IV-3]; this system enables the movement of a liquid neutron absorber in dedicated tubes in the guide thimbles of the assemblies without control rod clusters. Main characteristics of the reactivity control system are summarized in Table IV-2.

TABLE IV-2. REACTIVITY CONTROL SYSTEMS OF SCOR

System type/characterization	Availability/value
Burnable absorbers	Yes
Number of control rods	78
Absorber rods per control assembly	24
Drive mechanism	Hydraulic
Soluble neutron absorber	No
2nd system for accidental conditions	Yes

The SCOR design philosophy is based on finding an optimum between economic and safety approach issues:

- SCOR is a larger size integral design PWR, compatible with the option of industrial manufacturing in series and also offering a compact plant layout;
- The safety approach is based on architecture with which as many as possible accident initiators are eliminated or reduced, or the possible consequences of accidents are limited, by relying upon both inherent safety features and active and passive systems.

The design options of SCOR were selected to facilitate safety demonstration:

- The integral design eliminates large primary penetrations of the reactor vessel; therefore, large break loss of coolant accidents (LOCAs) are practically eliminated;
- The integrated control rod drive mechanisms eliminate the risk of rapid reactivity insertion through control rod ejection;
- The residual heat removal system on the primary circuit (RRP) with heat exchangers located in the vessel, very close to the core, eliminates an additional loop with the primary water typical of a standard residual heat removal system.

The design philosophy of SCOR results from reactor studies conducted in the 1990s, based on such PWR designs as the AP600, SIR, PIUS, low pressure PWRs, and the EPR, and incorporates the results of CEA (France) studies of safety systems and several PWR core types [IV-1, IV-2].

The SCOR design concept provides for a simplification of the main systems. Such selection contributes to simplified plant operability and reduced plant costs and also improves safety and reduces machine-human interactions.

Low primary operating pressure enables a reduction of the wall thicknesses of pressure bearing components and reduces the required pressurizer volume.

The elimination of alternate current (AC) powered safety systems[2] contributes to a reduced complexity of the active systems, which otherwise would need sensors, actuators, etc. that must be qualified for reliable operation over the full range of conditions which might be encountered (e.g., fire, seismic events, etc.).

Another important implication of the design simplification targeted for SCOR may be related to improved human reliability [IV-4], as discussed in more detail below.

Most human reliability assessment (HRA) models acknowledge the fact that human performance in operating a system (especially in performing cognitive, demanding tasks) is largely influenced by complexity characteristics of the system. Although this notion of complexity may appear somewhat subjective at a certain level (the perceived complexity of a system is highly dependent on the knowledge and skills that the operators have developed), it still exhibits an objective component directly correlated to the intrinsic complexity of the features of a system. For example, minimizing the intrinsic complexity of a system, particularly in the early

[2] Except for the safety injection system, which operates at low pressure and with a low flow rate.

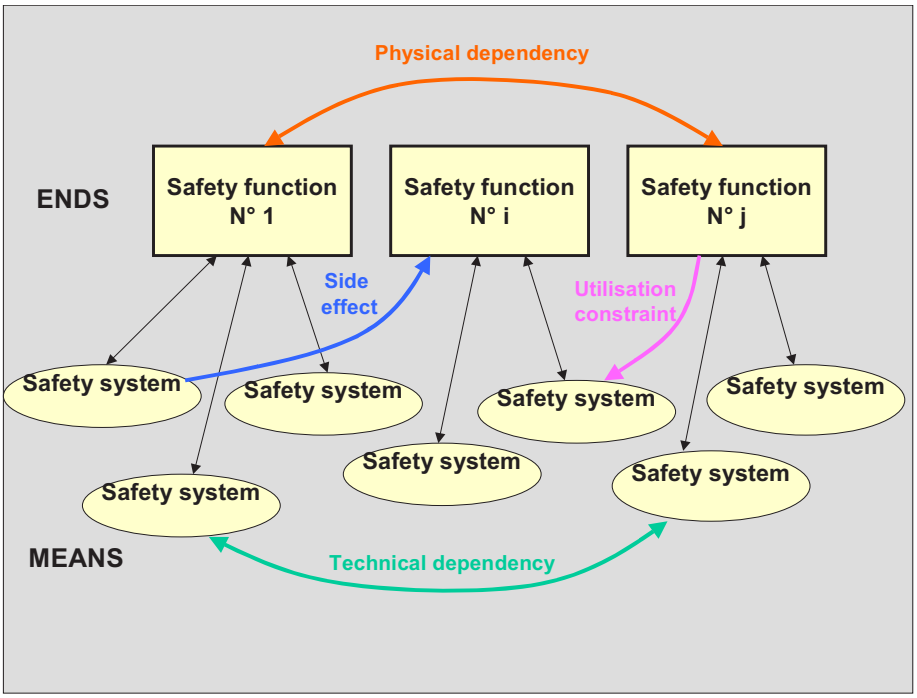


FIG. IV-3. Characterization of the complexity features (illustration) [IV-1].

phases of its design, appears to be an attractive way of improving the system operation taking into account human factors.

The abovementioned considerations form a basis for the approach proposed by the CEA (France) to assess the relevance of human factors in advanced nuclear reactor concepts, particularly during the very early phases of the design, that is, when it is still possible to propose alternative solutions at a limited cost. Such an approach was followed in the SCOR design.

The method consists of characterizing design features, especially within safety system architecture, that are likely to pose problems in operation, notably during degraded situations in which plant safety strongly depends on human reliability. The characterization of the intrinsic physical behaviour of plant processes (safety functions), of the operating constraints of the safety systems, and, finally, of the interrelations between these entities[3] (most of the complexity theories consider these interrelations to be the main contributors to the complexity of a system), lead to the definition of an operational complexity index and to the identification of sources of operational constraints bearing on operation crews. Figure IV-3 illustrates such complexity features, as defined by the relationships between safety functions and safety systems.

Figure IV-4 illustrates the principles applied for quantification of complexity (operational complexity index (OC)), on the basis of functional architecture shown in Fig. IV-3.

Each parameter used in the expression of Fig. IV-4 is evaluated on the basis of a discrete scale, considering the potential human factor impact of a certain feature. For example, in the case of the reversibility (REV_J) of an engineered safety system, a 3-level scale has been defined:

REV = 1 — for a system in which the effects are totally reversible (easily achieved by making a reverse action);
REV = 2 — for a system in which the reverse action requires more effort than a normal action;
REV = 3 — for a system in which the consequences of an action are irreversible (the worst case).

[3] Most of the complexity theories consider these interrelations to be the main contributors to the complexity of a system [IV-4].

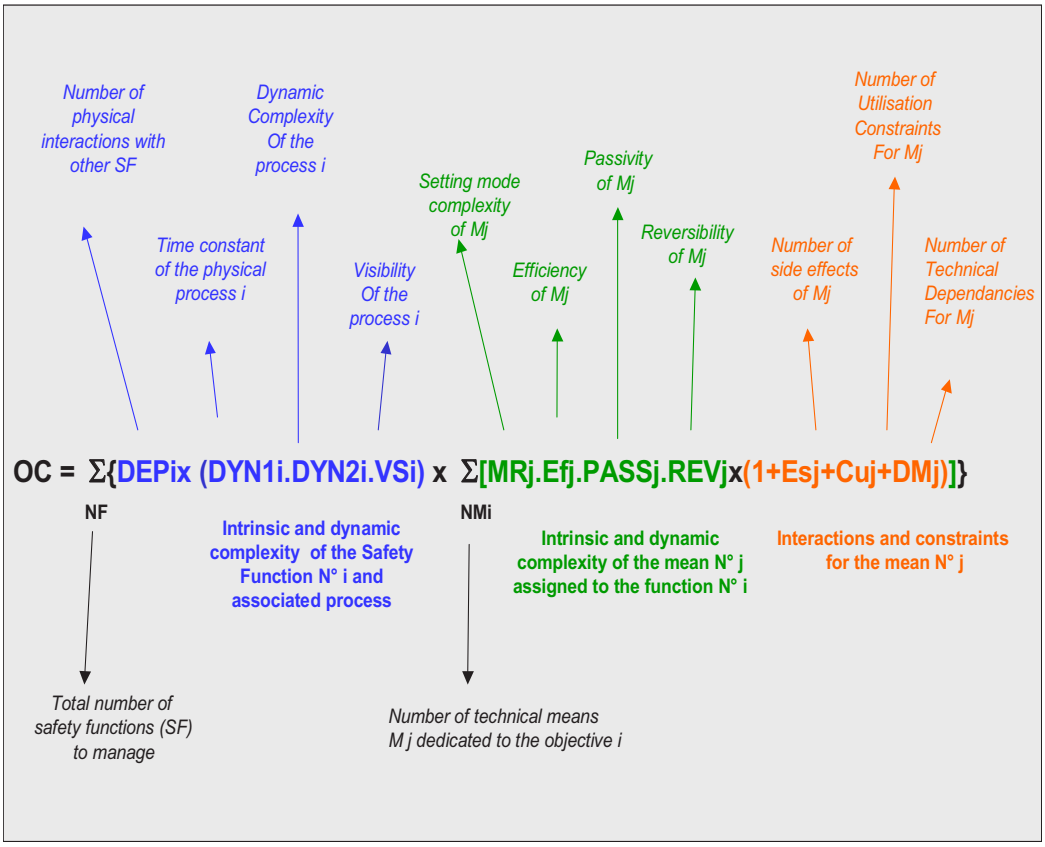


FIG. IV-4. Quantification of complexity — Operational complexity index (OC).

The basic idea behind this quantification is the notion that it is possible to undo the effects of a (potentially erroneous) action, which is a definitive factor in human decision making. If such a possibility is not understood, operators may be reluctant to take an action, even though it might be vital for plant safety. This characteristic has a strong link to what is called the 'forgiving features' of a design. On its basis, comparative studies among various designs are possible, outlining a new approach to design optimization which considers human factors at a very early phase in the conceptual design, whereas customary approaches only consider these aspects during instrumentation and control (I&C) and man-machine interface (MMI) design phases.

Even though the SCOR design is still at an early conceptual phase, the present knowledge of its safety design options is sufficient for a preliminary assessment of the operational complexity. Figure IV-5 presents the first results of such an assessment, performed in comparison with a standard loop-type PWR.

The presented results point to a potential decrease in the operational complexity of the SCOR as compared to a standard loop-type PWR. The reasons behind this expected simplification are twofold [IV-1]:

- First, it may originate from a modification of the physical processes of the plant, as defined by the specific selected design options. For example, this is the case for the SCOR coolant inventory function (INV), where the choice of an integral design of the primary system limits the flow rate in possible LOCAs and increases the grace period for managing such events. This is also true for steam generator integrity management (SGINT), where the absence of a direct evacuation of the steam to the atmosphere in the SCOR obviates the need to explicitly manage the steam generator tube rupture, while it appears to be a major source of operational complexity in standard PWRs;
- Second, this simplification may originate from the performance features of engineered safety systems. This is the case for systems dedicated to reactor cooling (RCO), which, in case of SCOR, use passive and closed loop cooling configurations instead of active and open loop ones and, therefore, exhibit much fewer operating constraints than in standard PWRs. This is also true for sub-criticality (S/K) management —

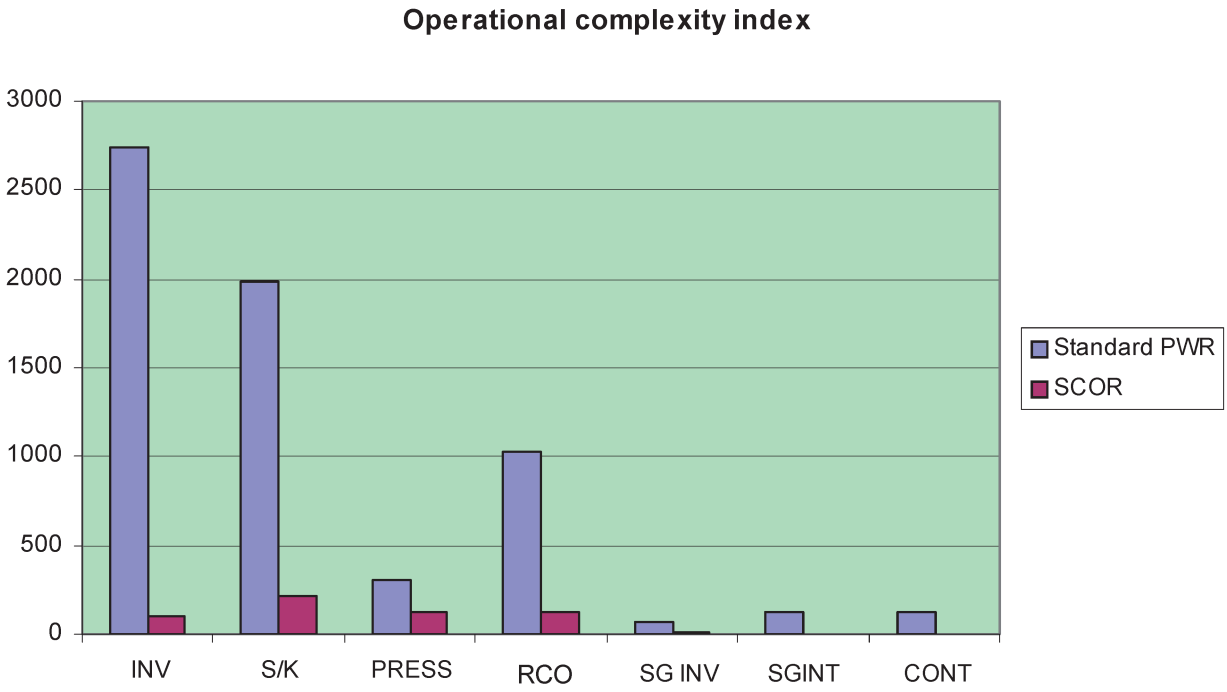


FIG. IV-5. Operational complexity vs. safety functions for the SCOR and a standard PWR [IV-1].

elimination of soluble boron in the SCOR, and for the coolant inventory control (INV) systems — simplification of the configuration of a low pressure safety injection in the SCOR.

Even though the assessment of human factors for the SCOR concept is preliminary (it focuses on degraded operation, but similar analysis is required for normal operation, maintenance and testing), results confirm that the design options for SCOR may lead to a considerable simplification of operation and to a possible improvement of human reliability in operation. This conclusion appears particularly valuable as probabilistic safety assessments (PSA) indicate that human failures make a major contribution to the global risk in existing nuclear power plants.

IV–2. PASSIVE SAFETY DESIGN FEATURES OF SCOR

The occurrence and consequences of a significant number of accidents are either eliminated outright or reduced by the SCOR concept at the design level. The major safety systems are passive; they require no operator action or off-site assistance for a long period after an accident. Moreover, core and containment cooling is provided during a long period without AC power.

The inherent safety features incorporated in the SCOR design are:

- Integral primary circuit layout with no option for a large break in the primary circuit; the maximum possibility is a double rupture of the pressurizer line (50 mm);
- Large thermal inertia of the primary circuit;
- A relatively low core power density, resulting in larger thermal-hydraulic margins;
- In-vessel location of CRDMs, eliminating reactivity insertion accidents due to control rod ejection;
- No soluble boron system, eliminating reactivity insertion that might otherwise occur in the case of water dilution;
- Substantially negative moderator temperature reactivity coefficient throughout the whole burnup cycle.

The SCOR design incorporates the following passive safety systems:

- Passive residual heat removal system on the primary circuit (RRP). Passive operation of this system is ensured simultaneously in the primary circuit, in the RRP loop, and in the ultimate heat sink; the RRP system has two types of heat sinks: water pool and air-cooling tower;
- No action regarding the steam line of the steam generator is needed to ensure decay heat removal[4];
- In the case of a blackout, natural convection in the primary circuit with 4 operating RRPs is sufficient to remove the decay heat (and to achieve zero reactivity via feedback due to the moderator reactivity coefficient in the case of a anticipated transient without scram (ATWS));
- A dedicated steam dump pool, located in the containment building, prevents radioactivity release into the atmosphere in the case of a steam generator tube rupture;
- Passive control of the containment pressure by pressure suppression in the case of a LOCA;
- In-vessel retention of corium achieved via reactor cavity flooding in the case of a hypothetical severe accident;
- Infinite autonomy with the air cooling tower heat sink;
- Prevention of hydrogen combustion by maintaining an inert atmosphere in the reactor vessel compartment;
- One of the shutdown systems is based on insertion of gravity driven control rods to the core (the actuation of this system is the same as in a standard PWR), see [IV-1].

More details about passive safety systems incorporated in the SCOR design are given below.

Decay heat removal systems

As the reactor has only one steam generator, passive decay heat removal systems are diversified by being included in both the primary and the secondary circuit.

Secondary circuit

A decay heat removal system should not release steam to the atmosphere under a steam generator tube rupture (SGTR). In the case of an overpressure transient in SCOR, the released steam is condensed in a dedicated pool. The steam generator is not considered as a main system for decay heat removal. It acts as a thermal buffer until the safety systems on the primary side are fully operational.

Primary circuit

The primary coolant system is after cooled by means of heat exchangers located in the downcomer, see Fig. IV-6. Each heat exchanger has a dedicated heat sink. There are 16 independent loops used for this purpose, altogether forming the RRP system (an abbreviated 'residual heat removal on primary circuit'). There are two types of heat sinks:

- Four RRP loops are cooled by heat exchangers immerged in a pool (RRPp);
- The other twelve RRP loops are cooled by heat exchangers located in an air cooling tower (RRPa).

All RRP loops are designed to operate on natural convection both in the loop and in the heat sink.

The RRP design is very simple. RRP loops are designed to resist the primary pressure. Isolating valves are placed in RRP circuits to minimize the risk of the primary water passing outside the containment in the event of a heat exchanger tube rupture. A surge tank compensating for water dilation from a cold shutdown to a full power operating state carries out pressure control of the RRP circuit.

[4] This line incorporates the safety isolation valves; these valves are automatically closed on a SCRAM signal (as in a standard PWR).

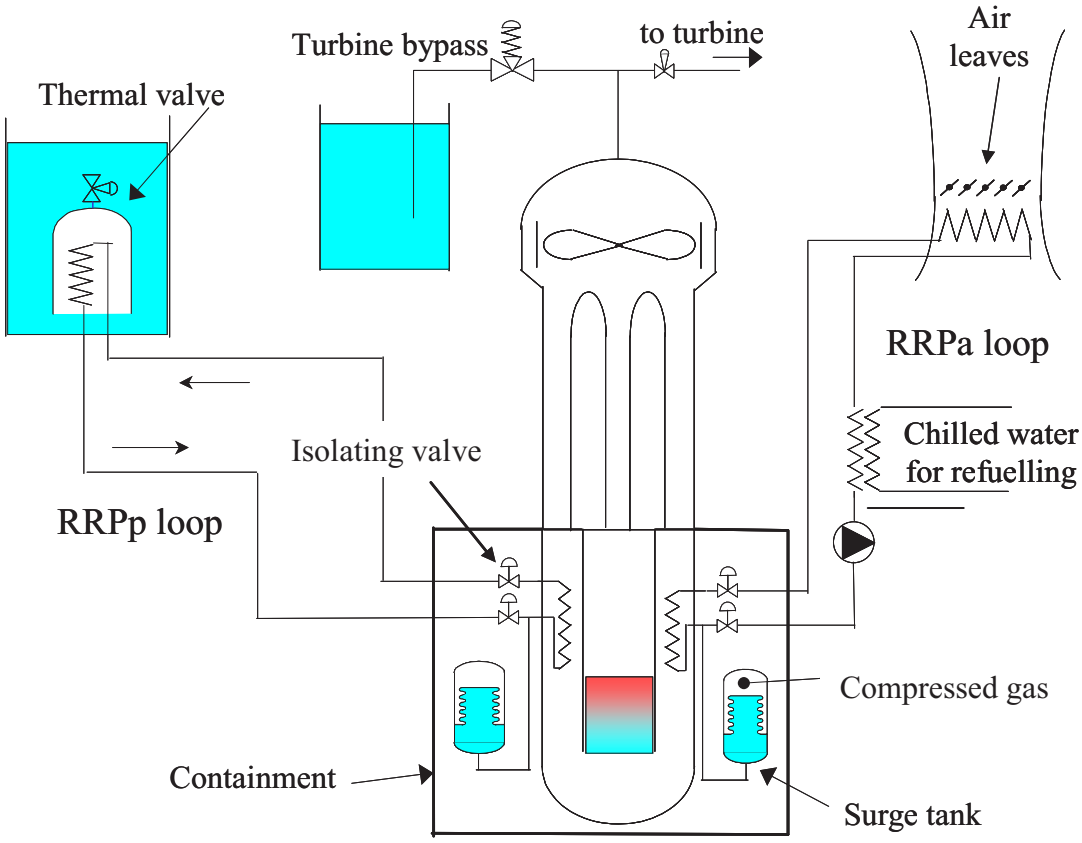


FIG. IV-6. Residual heat removal system on the primary circuit [IV-1].

The control valves are placed on the level of the heat sink: thermal valves or air leaves function so that the temperature of the RRP loop remains high when the reactor is in power [IV-1]. In the case of an accident, the RRPs operate passively by opening the air leaves in the RRP air coolers or by opening the thermal valves in the RRP pools. These valves are automatically opened on a SCRAM signal.

Forced convection is only required when the chilled water cooling is requested for core refuelling. The 12 RRPa are able to cool the primary system down to a cold shutdown state. They replace the normal heat removal system of the reactor.

Safety features of the passive heat removal system

The maximum power removed by each RRP loop is about 5 to 7 MW(th), depending on operating conditions. The low amount of removed power ensures that, whatever the reactor power, it is possible to test the heat removal system while the reactor is in operation without significantly disturbing operating conditions. The abovementioned testing procedure is a significant element in validation of the reliability of such passive heat removal systems.

The RRPp are safety grade. The RRPa are safety grade, except for the chilled water loop and pumps.

Normal residual heat removal system

In the reactor hot state, residual heat is removed through the steam generator. The steam is discharged to the atmosphere, and the steam generator is fed by the startup shutdown system (SSS). This system is not safety grade. At low temperatures, the RRP with the air-cooling tower (RRPa) removes decay heat.

When the reactor vessel is open, especially during refuelling operations, decay heat is removed by the twelve RRPa cooled by chilled water to secure a very low primary water temperature, compatible with the

maintenance action conditions. The primary circuit operates on natural convection and the RRPa loops operate in an active mode (with forced circulation in the chilled water loop).

The safety injection system is the only active safety system of the SCOR; it is safety grade. A short description of this system is provided below.

Safety injection system

As large break LOCAs are eliminated by design, and as the primary system thermal inertia is larger than that of a loop type PWR, the safety injection system requires devices with a small flow rate. With the selected low pressure for the reactor, there is safety injection of only one with a pressure of about 20 bars. The pump power required for the safety injection is very small, about 35 kW(e).

IV–3. ROLE OF PASSIVE SAFETY DESIGN FEATURES FOR DEFENCE IN DEPTH

Some major highlights of the passive safety design features in the SCOR, structured in accordance with the various levels of defence in depth [IV-5, IV-6], are brought out below.

Level 1: Prevention of abnormal operation and failure

- Integral design of the primary circuit;
- Internal CRDMs;
- Relatively low core power density;
- Elimination of soluble boron reactivity control system;
- Substantially negative moderator temperature reactivity coefficient throughout the whole burnup cycle.

Level 2: Control of abnormal operation and detection of failure

- Large coolant inventory in the main coolant system, large thermal inertia of the primary circuit;
- Substantially negative moderator temperature reactivity coefficient throughout the whole burnup cycle.

Level 3: Control of accidents within the design basis

- For a steam line rupture, no possibility of return to criticality and no need for safety injection;
- Large inventory of water inside the RPV; long term cooling by the RRP systems in a passive mode during LOCA;
- For a steam generator tube rupture, no steam release to the atmosphere (steam is condensed in a dedicated pool);
- Primary circuit has no soluble boron; therefore, no risk of dilution by water of the secondary circuit;
- Natural circulation heat removal during a loss of flow accident (LOFA);
- Increased reliability of decay heat removal system achieved through the use of natural convection.

Level 4: Control of severe plant conditions, including prevention of accident progression and mitigation of severe accident consequences

- For total loss of heat sink, the decay heat removal of the SCOR is based on several independent loops (RRP) ready to operate in a passive mode with a heat sink either in pools with a limited autonomy of several hours or in an air cooling tower in which the autonomy is infinite;
- In-vessel retention of corium achieved by flooding of the reactor cavity with water and heat removal based on natural convection.

Level 5: Mitigation of radiological consequences of significant release of radioactive materials

The following features help in passively bringing down the containment pressure and in minimizing any releases from the containment following a LOCA:

- As large break LOCAs are eliminated by design, the maximum break size in LOCA is limited by 2 × 50 mm;
- Relatively small, inerted, pressure suppression containment;
- Relatively small fuel inventory;
- Increased retention of fission products (flooding of reactor cavity, dedicated pool for steam condensation under a steam generator tube rupture, etc.).

IV–4. ACCEPTANCE CRITERIA FOR DESIGN BASIS AND BEYOND DESIGN BASIS ACCIDENTS

IV–4.1. List of design basis and beyond design basis accidents

Design basis accidents

Basic design basis accidents, such as NPP blackout, steam line rupture, steam generator tube rupture, and LOCA, were studied with the CEA's CATHARE code. All calculations have been performed with 4 out of the 16 available RRP loops. The scenarios of design basis accidents are summarized below.

NPP blackout

For this transient, power is first removed by the steam generator and then by the RRP system. The RRP system reaches full operation at about 1000 seconds after the accident starts. After an hour and a half, the power removed by the RRP becomes sufficient to cool the reactor adequately in the long term.

Steam line rupture

Under a steam line rupture, the amplitude of cold shock is 22°C at the core inlet. The control rods incorporated in the SCOR design are sufficient to prevent reactivity increase until the cold shutdown state is reached. After the trip is set off, residual power is first removed by the steam released from the steam generator and then stored courtesy of large thermal inertia of the primary circuit. The RRP loops reach their full power in 1000 seconds. One hour after the beginning of the transient, the RRP are able to remove all residual power. In this transient, no water is released through the safety valve of the pressurizer.

Loss of coolant

The largest LOCA which can occur is a break in the line between the vessel and the boiler of the pressurizer (2×50 mm). At the beginning, power is removed through the break and by the steam generator. As for the blackout, the RRP reach their full power in 1000 seconds. After being stabilized at the pressure of the secondary safety valve, the primary pressure reaches the threshold pressure of the safety injection system in 4000 seconds.

Steam generator tube rupture

During the first 1000 seconds, residual power is removed by the steam generator and by the RRP system. To prevent steam release into the atmosphere, the steam is condensed in a dedicated pool. With four RRP loops in operation and five steam generator tubes ruptured, the mass of the released steam is around 40–50 tons, depending on the RRP heat sink capacity; with 8 RRP loops in operation, the mass of the released steam is

20 tons. After 6000 seconds, the RRP system becomes sufficient to cool the reactor adequately, and steam release from the steam generator is stopped.

Summary of performance in design basis accidents

Table IV-3 gives a comparison of the progression of typical design basis accidents between a standard PWR and the SCOR.

The calculations performed for the SCOR show that all transients could be adequately managed in a passive way (in the vessel, in the RRP loop, and in the heat sink) with only 4 out of 16 RRP loops, no matter what the heat sink is: a pool or an air cooling tower. This represents a redundancy of 16 times 25%. RRP operation is compatible with an active or passive mode, whatever the primary pressure or temperature. As the in-vessel heat exchangers of the RRP loop are located very close to the core, and thanks to the flow bypass of the venturi, the RRP are operational in a two phase flow mode (primary side), in the case of a small primary water inventory. Long term cooling may be ensured in a totally passive mode due to the RRP with an air cooling tower. A safety injection at 2.0 MPa with a small flow rate is needed only one hour after the beginning of the biggest possible LOCA, that is, a double break of the pressurizer line (2×50 mm). In the event of a steam generator tube rupture, the steam released from the safety valves of the secondary circuit is condensed in a dedicated pool. No steam is released to the atmosphere.

TABLE IV-3. DESIGN BASIS ACCIDENTS IN STANDARD PWRS AND IN SCOR [IV-1]

Initiating event	Transient progress in standard PWRs	Transient progress in SCOR
NPP blackout	– Natural convection in the primary circuit – An external electricity source (diesel) is required for the systems involved (seal pump, safety injection, etc.) – Heat sink effective for a few hours	– Natural convection in the primary circuit – Very few systems involved (diesels with a reduced power or a battery) – Infinite autonomy of the RRP systems with an air heat sink
Steam line rupture	– Risk of recriticality – High pressure safety injection (HPSI) with borated water required	– No risk of recriticality – Not need for safety injection
LOCA	– Possible early core exposure, depending on the break size – Demand for safety injection systems of three types: HPSI, hydro-accumulators, and low pressure safety injection (LPSI) – Possible demand for a fast safety injection (depending on the break size) – Long term cooling by LPSI (active system) required	– No early core dewatering (at least for 1.5 hours after the transient start with no RRP operation) – Safety injection of only one type – LPSI – is needed, with a small flow rate – No demand for immediate LPSI operation – Long term cooling provided by the RRP systems in a passive mode
Steam generator tube rupture	– Risk of a primary water release through the broken steam generator – Request for safety injection disturbs the transient management – Delicate management of the decreasing pressure is required to prevent the secondary water without boron from flowing into the primary circuit through broken tubes of the steam generator	– No steam release to the atmosphere (steam is condensed in a pool) – Cooling by RRP systems; no need for safety injection – Primary coolant has no soluble boron; therefore, no risk of dilution by the secondary coolant

Beyond design basis accidents (BDBA)

For the SCOR, transients leading to an extension of design basis conditions are either eliminated by design or managed using the following passive provisions:

- H1 (total loss of the heat sink): the SCOR concept is based on several independent decay heat removal (RRP) loops ready to operate in a passive mode with a heat sink either in the pools with a limited autonomy of several hours or in an air cooling tower in which autonomy is infinite;
- H2 (total loss of feedwater supply to the steam generator): decay heat is removed by systems of the primary circuit with a redundancy of 16 × 25%. There is no need for a safety grade auxiliary feedwater system;
- H3 (total loss of all power supplies): natural convection is possible in all decay heat removal systems with integrated exchangers, from the primary circuit to the heat sink;
- H4 (loss of the containment spray or the low pressure safety injection): the SCOR has no containment spray system, because it uses a pressure suppression type containment. The low pressure safety injection plays a less significant role than in standard PWRs because of large thermal inertia of the primary circuit; large break LOCAs are eliminated by design; the decay heat removal systems are sufficiently effective and redundant;
- ATWS (anticipated transient without scram): the SCOR has two independent shutdown systems so that the overlapping transients will be treated individually as in standard PWRs. Accident management would be simplified due to the permanently negative and higher moderator temperature reactivity coefficient, as compared to standard PWRs. In the case of a LOFA, power is removed by 4 RRP and the primary temperature is stabilized at a value below the saturation temperature, corresponding to the opening of the pressure safety valve;
- Multiple rupture of steam generator tubes and loss of containment isolation: steam from the steam generator is discharged to a dedicated pool;
- Failure of HPSI: no HPSI is provided for in the SCOR.

The hypothetical case of a core meltdown is managed through the following measures:

- In-vessel retention: corium cooling can be ensured by natural convection of water in the flooded reactor cavity, because power density in the core is relatively low and the grace period before a hypothetical core meltdown is long, which altogether reduces decay heat by the time the corium enters the lower plenum;
- Hydrogen risk: the atmosphere of the reactor vessel compartment is inerted to prevent hydrogen combustion (similar to boiling water reactors).

IV–4.2. Acceptance criteria

The qualitative and quantitative objectives of radiological protection of the population and the environment developed for generation III reactors, e.g., for the EPR [IV-2], are already very strict and guarantee a very high level of protection [IV-7]. They apply to a set of situations with which the plant has to cope. Such situations are defined taking into account the specific features of the plant and the design of its systems, similar to how it was done in the past. Different from past systems, the factor of system simplification is taken into account more accurately. Situations of which the consequences are potentially intolerable should be practically eliminated; if they cannot be made physically impossible, design provisions must be adopted to rule out either initiating events or potential consequences [IV-7].

The abovementioned objectives could be effectively applied to the SCOR design and, more generally, to future generation IV systems.

No further details regarding the acceptance criteria have been provided.

IV–5. SUMMARY OF PASSIVE SAFETY DESIGN FEATURES FOR SCOR

Tables IV-4 to IV-8 below provide the designer's response to questionnaires developed at the IAEA technical meeting "Review of passive safety design options for SMRs" held in Vienna on 13-17 June 2005. These questionnaires were developed to summarize passive safety design options for different SMRs according to a common format, based on the provisions of IAEA Safety Standards [IV-5] and other IAEA publications [IV-6, IV-8]. The information presented in Tables IV-4 to IV-8 provided a basis for the conclusions and recommendations of the main part of this report.

TABLE IV-4. QUESTIONNAIRE 1 — LIST OF SAFETY DESIGN FEATURES CONSIDERED FOR/ INCORPORATED INTO THE SCOR DESIGN

#	Safety design features	What is targeted?
1	Integral primary circuit	Elimination of large break LOCA
2	Integral primary circuit	Increased coolant inventory/larger thermal inertia
3	Internal CRDMs	Elimination of rod ejection
4	Internal CRDMs	Elimination of vessel head penetrations or reduction of their size
5	Soluble boron free core	Elimination of boron dilution
6	Increased level of natural circulation	Passive decay heat removal in LOFA
7	Pressure suppression containment	Fission product retention increase
8	Inerted containment	Prevention of hydrogen explosion
9	Reduced core power density	Slower progression of accidents
10	Soluble boron free core and reduced core power density	Mitigation of ATWS

TABLE IV-5. QUESTIONNAIRE 2 — LIST OF INTERNAL HAZARDS

#	Specific hazards that are of concern for a reactor line	Explain how these hazards are addressed in an SMR
1	Prevent unacceptable reactivity transients	Internal CRDMs (no control rod ejection); boron-free core (no boron dilution); (limited) negative moderator reactivity coefficient
2	Avoid loss of coolant	– Integral design of the primary circuit (no large break LOCA, minimized vessel penetrations due to internal CRDMs) – Grace period increased due to large coolant inventory and reduced core power density
3	Avoid loss of heat removal	– Diverse and redundant passive decay heat removal systems with heat exchanges integrated in the primary coolant system – Diverse ultimate heat sinks with the air cooling tower having infinite autonomy – In-vessel retention achieved via RPV cooling by natural convection of water in the reactor cavity – Large heat capacity of the primary circuit
4	Avoid loss of flow	– Increased level of natural circulation in the primary coolant system; reduced power density in the core
5	Avoid exothermic chemical reactions	– Inerted containment – Reduced core power density, providing an increased margin to Zr-steam reaction

TABLE IV-6. QUESTIONNAIRE 3 — LIST OF INITIATING EVENTS FOR ABNORMAL OPERATION OCCURRENCES (AOO)/DESIGN BASIS ACCIDENTS (DBA)/BEYOND DESIGN BASIS ACCIDENTS (BDBA)

#	List of initiating events for AOO/DBA/BDBA typical for a reactor line (PWRs)	Design features of SCOR used to prevent progression of the initiating events to AOO/DBA/BDBA, to control DBA, to mitigate BDBA consequences, etc.	Initiating events specific to this particular SMR
1	LOCA	– Integral primary circuit eliminates large break LOCA – Increased coolant inventory extends grace period – Containment with high design pressure – Pressure suppression system	Nothing specified here
2	Steam generator tube rupture	– Steam generator designed for full system pressure	
3	Steam line rupture	– Steam is discharged to a dedicated water pool	
4	Control rod ejection	Internal CRDMs eliminate an option of control rod ejection	
5	Boron dilution by the ingress of boron free water from the secondary circuit	– Soluble boron free core design	
6	LOFA	– Increased level of natural circulation – Reduced core power density	

TABLE IV-7. QUESTIONNAIRE 4 — SAFETY DESIGN FEATURES ATTRIBUTED TO DEFENCE IN DEPTH LEVELS

#	Safety design features	Category: A-D (for passive systems only), according to IAEA-TECDOC-626 [IV-8]	Relevant DID level, according to NS-R-1 [IV-5] and INSAG-10 [IV-6]
1	Integral design primary circuit	Large break LOCA – A	1
2	Internal CRDMs	Rod ejection – A	1
3	Diverse and redundant passive decay heat removal systems with increased heat sink autonomy	Loss of heat sink – D In-vessel retention – D	3 4
4	Increased natural circulation, reduced core power density	LOFA – B	1, 3, 4
5	Large thermal inertia	B, C, D (depending on the accident)	1, 2
6	Small fuel inventory (relative to large NPPs)	Radioactivity release – A	5
7	Slower progression of accidents and increased retention of fission products (due to high design pressure containment + pressure suppression system + reduced core power density + increased thermal inertia + cavity flooding system + dedicated pool for steam discharge)	Radioactivity release – A, B, C, D	5
8	Inerted containment	Hydrogen combustion – A	4

TABLE IV-8. QUESTIONNAIRE 5 — POSITIVE/NEGATIVE EFFECTS OF PASSIVE SAFETY DESIGN FEATURES IN AREAS OTHER THAN SAFETY

Passive safety design features	Positive effects on economics, physical protection, etc.	Negative effects on economics, physical protection, etc.
Integrated primary circuit	Allows for a reduction in containment volume (see below)	Increased RPV cost per unit of energy produced; unit power limited by 2000 MW(th) for the original SCOR steam generator concept
Increased reliance on natural circulation	Simplifies design and maintenance, contributing to reduced costs	RPV cost increased due to larger vessel size; may increase complexity of reactor operation (startup phase, etc.)
Compact primary circuit	Containment volume could be reduced with a positive effect on plant economy	
Soluble boron free core	Relaxes concerns related to human actions of malevolent character	

REFERENCES TO ANNEX IV

[IV–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Innovative Small and Medium Sized Reactor Designs 2005: Reactors with Conventional Refuelling Schemes, IAEA-TECDOC-1485, IAEA, Vienna (2006).

[IV–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Advanced Light Water Reactor Designs 2004, IAEA-TECDOC-1391, IAEA, Vienna (2004).

[IV–3] EMIN, M. MP98, New passive control rod system for a full and extended reactivity control on LWR, paper 3163, ICAPP'03, Cordoba (2003).

[IV–4] PAPIN, B., QUELLIEN P., The operational complexity index: A new method for the global assessment of the human factor impact on the safety of advanced reactors concepts, Nucl. Eng. Des. **236** (2006) 1113-1121.

[IV–5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[IV–6] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

[IV–7] Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors, GPR/German experts, (19th and 26th October, 2000), Germany (2000).

[IV–8] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Terms for Advanced Nuclear Plants, IAEA-TECDOC-626, IAEA, Vienna (1991).

Annex V

SAFETY DESIGN FEATURES OF MARS

The University of Rome 'La Sapienza'
Italy

V–1. DESCRIPTION OF THE MARS DESIGN

The Multipurpose Advanced Reactor, inherently Safe (MARS) is a 600 MW(th), single loop, pressurized light water reactor (PWR); its design was developed at the Department of Nuclear Engineering and Energy Conversion of the University of Rome "La Sapienza". The design was conceived in 1984 as a nuclear power plant able to conciliate well proven PWR nuclear technology with special safety features intended to facilitate plant location in the immediate proximity of highly populated areas in fast growing countries, to meet their energy and potable water needs. The plant has to guarantee a high and easily understandable safety level, has to be inexpensive and easy to build, operate, maintain and, eventually, repair; and has to ensure low production of radioactive wastes. The objective of the design effort was to find those (suitably supported by tests) plant solutions that could keep the features of a 'traditional' PWR in an essentially simplified design. A detailed description of the MARS design is presented in [V-1].

The core cooling system includes only one loop with a recirculation type steam generator. During normal operation, forced circulation of the primary coolant is applied, based on the use of a pump while, in emergency conditions, the necessary coolant flow rate in the core is maintained by an independent cooling system, which transfers heat to the external atmosphere through natural convection and relies only on static components and on one non-static, direct action component (a check valve, 400% redundant).

The MARS reactor module is enclosed in a pressurized containment filled with cold water; the complete nuclear power plant (NPP) also incorporates a containment building needed to cope with external events (such as aircraft crash) in accordance with Italian and European regulations. The containment building is able to withstand any internal pressurization, also in the hypothetical event of complete destruction of the core coolant boundary.

Loss of coolant accidents (LOCAs), loss of flow accidents (LOFAs), and anticipated transients without scram (ATWSs) are eliminated in the MARS concept by design, which is intended to make the plant reliable, safe, and easy to operate. With major accidents being eliminated, the plant incorporates a substantially reduced number of safety related structures, systems, and components, and provides for maximum possible pre-fabrication and easy assembly/disassembly, particularly by allowing easy component substitution in the case of a failure or consumption, instead of requiring a local repair.

Major design specifications of the MARS are shown in Table V-1. The reactor cooling system and some of its components are shown in Fig. V-1, V-2 and V-3.

Some features of the MARS concept are similar to well known features of standard PWRs (loop type primary circuit design, similar core geometry and materials, similar means of reactor control, etc.) [V-1, V-2]. For example, the core is cooled and moderated by pressurized light water containing a boron solution. Boron and burnable poisons compensate for excess reactivity during the irradiation cycle[1].

Different from many other PWR designs, the MARS primary coolant system includes only one loop with 25 inch internal diameter pipes, one vertical axis U-tube type steam generator, and one canned rotor pump connected to the steam generator outlet nozzle (see Fig. V-1).

The safety core cooling system (SCCS) is connected to the reactor vessel. A vapour-bubble type pressurizer controls the pressure inside the primary coolant system.

On/off valves in the primary loop main isolation system (MIS) are installed in the primary cooling loop to isolate, if necessary, the steam generator and the primary pump (i.e., in the event of a steam generator tube rupture).

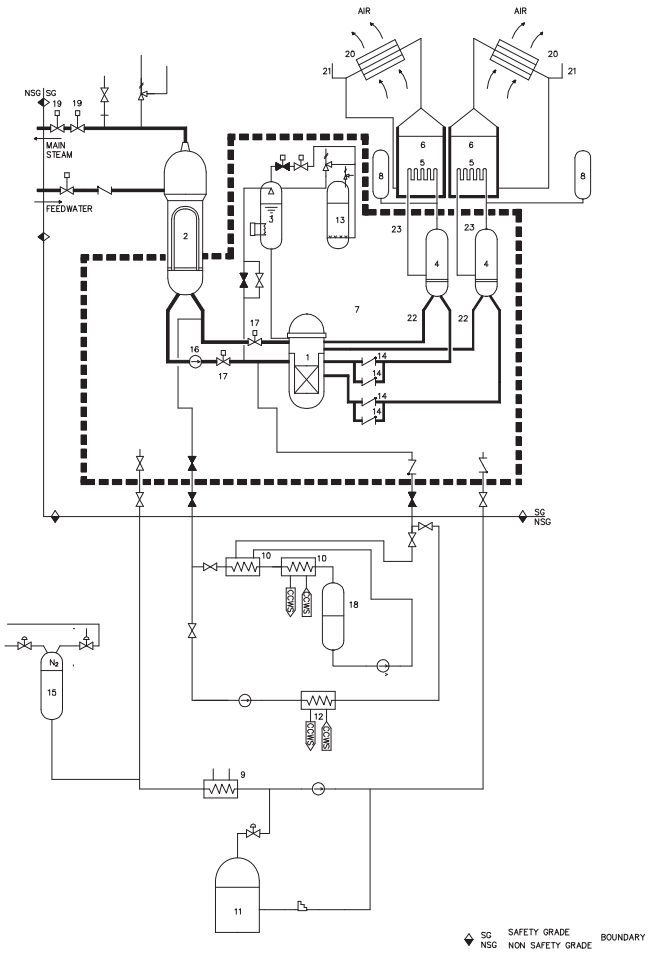
[1] Another design version of the MARS provides for total elimination of a liquid boron reactivity control system.

TABLE V-1. MAJOR SPECIFICATIONS OF MARS NPP [V-1]

Characteristic	Value
Power rating	
Reactor rated thermal power, MW	600
Rated electric power (one module), MW	150
Rated electric power (suggested cluster of 3 modules), MW	450
Suggested rated electric power in cogeneration configuration (electricity + desalinated water/district heating)	300
Core average volumetric power density (kW/litre)	56.5
Thermal-hydraulic characteristics	
Primary coolant flow rate (forced flow) (kg/s)	3327
Operating pressure, bar	75
Total RCS internal volume (m^3)	130
Pressurizer heaters power (kW)	800
Steam flow rate (kg/s)	277
SG steam pressure (bar)	18.8
Temperatures (°C)	
Reactor vessel outlet	254
Reactor vessel inlet	214
Steam generator steam outlet	209
Steam generator feedwater inlet	150
Reactor vessel data	
Internal diameter of the shell, mm	3000
Internal design pressure, bar	83
Length of the cylindrical shell, mm	8056
Upper head thickness, mm	80
Bottom head thickness, mm	80
Overall length of the assembled vessel, mm	11 091
Shell thickness, mm	120
Total weight (approximate; dry), kg	88 000

The design incorporates the primary safety cooling loop (PSC), the intermediate safety cooling loop (ISC), and the pool and condenser loop (a.k.a. the third safety cooling loop or TSC) in a cascading operation chain, providing redundant barriers for potentially activated primary coolant on the way of to the environment, see Fig. V-3.

The SCCS operation is actuated by special check valves that open automatically when conditions require additional core cooling, without operator intervention and without the operation of any energized system. These valves are of innovative design. They are kept in the closed position by a pressure difference between the reactor vessel inlet and outlet (which is roughly proportional to the square of the coolant flow rate); when a flow rate through the core goes to zero, the pressure difference decreases, and when it is no longer sufficient to sustain the weight of the valve plug, this falls and a complete flow area is opened with very low hydraulic resistance. Two valves, each of 100% capacity, are inserted in each SCCS train. To increase system reliability to values that make a failure incredible, two additional valves, different in type and mechanical design, are incorporated in each loop (the second valve in each loop is of conventional design).



Legend

1. Reactor
2. Steam generator
3. Pressurizer
4. Heat exchanger (reactor coolant/intermediate coolant)
5. Heat exchanger (intermediate coolant/ final heat sink
6. Water reservoir
7. Pressurized containment for primary loop protection (CPP)
8. Intermediate loop pressurizer
9. Heat exchanger (primary containment water cooling system)
10. Chemical and volumetric control system heat exchangers
11. Water storage tank
12. Residual heat removal system heat exchanger
13. Pressurizer relief tank
14. Safety core cooling system check valve
15. Primary containment pressure control system pressurizer
16. Main coolant pump
17. Primary loop on/off valve
18. Volumetric control system (VCS) tank
19. Steam line on/off valve
20. Ultimate heat sink condenser
21. Communication path with the atmosphere
22. Safety core cooling system primary loop
23. Safety core cooling system intermediate loop

FIG. V-1. Reactor cooling system (RCS) and main auxiliaries [V-1].

When any of the four check valves is opened, after a short transient phase, flow in the PSC is assured by a difference in level of about 7 m between the vessel outlet nozzle and the primary heat exchanger and by the difference between vessel inlet and outlet temperatures. A horizontal axis, U-tube type heat exchanger transfers heat from the PSC to the ISC.

Pressure in the ISC loop is slightly higher than 75 bar (thanks to a dedicated pressurizer); this value guarantees sub-cooled water conditions of the fluid during any accidental situation or transient; the difference in level for natural circulation in the ISC loop is about 10 m. The second heat exchanger transfers heat from the ISC circuit to the water of a reservoir; see Fig. V-3.

Steam produced in the reservoir is mixed with air initially present in the dome over the pool; pressure in the dome rises and this causes a flow of the air-steam mixture towards a small connection path with the atmosphere. An inclined tube heat exchanger is placed between the pool dome and the connection path to the atmosphere, where steam is partially condensed due to passive draught of external air, drawn by a chimney.

The above listed design features introduced some constraints to plant design. In particular, with the selected safety core cooling system (SCCS) and its functional requirements, reactor thermal power cannot exceed approximately 1000 MW(th). The MARS design version described in this paper has a thermal output of about 600 MW(th). Another characterizing parameter is primary system pressure. It was selected to equal 75 bar, which is different from the pressure values typical of standard PWRs (150-170 bar) [V-2]. Such selection leads to a loss in the thermodynamic efficiency of the plant because of the resulting limitation of a higher isotherm in the steam cycle. At the same time, it allows for adoption of a pressurized primary containment for protection of the primary loop (CPP, the pressurized boundary that envelopes the primary coolant system and

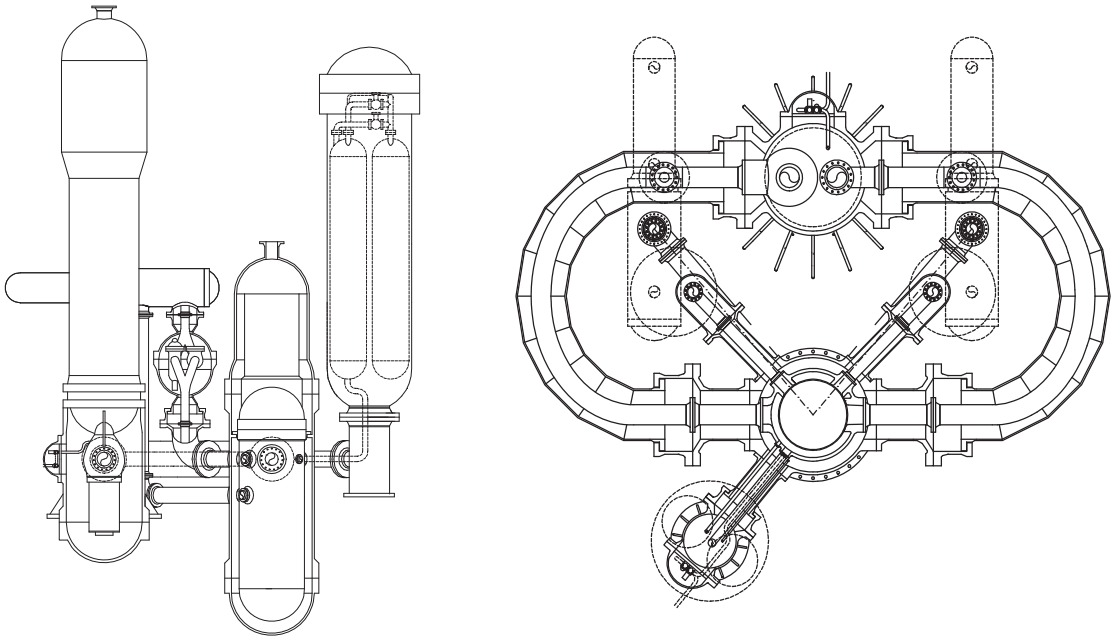


FIG. V-2. Pressurized containment for primary loop protection (CPP) [V-1].

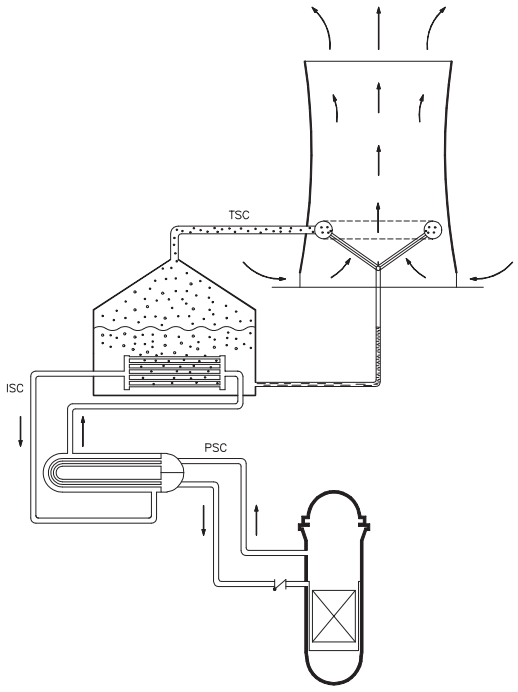


FIG. V-3. Scheme of the safety core cooling system (SCCS) [V-1].

emergency core cooling system, see Fig. V-2), substantially eliminating the possibility of LOCA of any type and of a control rod ejection.

Inclusion of the primary coolant system (with an average operating temperature of 234°C) inside the low enthalpy water filled pressurized containment (CPP, at a temperature of 70°C) requires thermal insulation to reduce heat losses from the primary coolant system. An insulating system has been designed on the external side of the primary coolant boundary, with only the lower head of the reactor vessel being thermally insulated in the internal part through the use of matrices of stainless steel wiring that cause the presence of semi-stagnant water which resists high pressure and fast pressure gradients with acceptable flow shape modifications. This system limits heat losses to about 0.3% of the reactor's thermal power.

It should be noted that the special design of the passive emergency decay heat removal system (SCCS) avoids thermal stratifications of any type, contributing to increased reliability of this system.

V–2. PASSIVE SAFETY DESIGN FEATURES OF MARS

Inherent safety features of the MARS design are the following:

- The same set of inherent safety features that are typical of conventional PWRs (negative reactivity coefficients in all power and coolant temperature ranges; all nuclear components of the reactor core are safety grade; etc.) [V-1, V-2];
- The primary coolant system and all components of the emergency core cooling system (SCCS) are located inside a pressurized primary containment which is filled with water at the same pressure as the primary coolant, but at a lower temperature (70°C). This pressurised containment, called CPP (pressurized containment for primary loop protection, see Fig. V-2), allows for a substantial reduction (up to total elimination) of primary stresses on the primary coolant boundary and provides for an intrinsic protection from coolant loss; the CPP does not need to be safety grade;
- Complete hydraulic isolation of the primary coolant within the primary coolant pressure boundary during most of the operation time (coolant outflow and inflow for purification purposes operate only periodically, over short periods); hydraulic connections to the primary coolant boundary are safety grade;
- Low maximum fuel temperature, which is due to coolant temperature being lower than 250°C, relatively low core power density, and elimination of fast fuel enthalpy increase accidents (due to the elimination of control rod ejection accidents). Altogether, this provides for substantially increased margin to fuel melting and, additionally, limits the potential release of radioactive isotopes into the coolant during any plant condition;
- Low fuel temperature gradients, due to relatively low core power density; slow thermal transients in fuel (no accident resulting in rapid fuel enthalpy increase is possible because the core is always adequately cooled); which limits possible fuel failure;
- Relatively low coolant temperature, below threshold values for a steam generator tube rupture; the steam generator tubes are safety grade;
- Very high values of minimum departure from the nucleate boiling ratio (DNBR), both in normal operation and as anticipated in the most severe design basis accidents;
- A substantial reduction in the number of physical connections between the primary coolant loop and auxiliary circuits (in total two small diameter lines, generally intercepted, for the chemical and volumetric control system (CVCS), and two small diameter lines, normally intercepted, connected to the safety/relief valve discharge tank, enclosed within the containment for primary loop protection (CPP)); the interconnection lines are safety grade up to the fourth interception valve on each line;
- The containment building, designed to withstand external events such as aircraft impact, provides additional protection against a potential release of radioactive products to the environment during postulated accidents (it may resist up to several bars of internal pressurization; even in the incredible event of a severe accident, the maximum internal overpressure is of the order of fractions of a bar); the containment building is safety grade;
- By design, human factors cannot affect the safety systems;
- All of the few MARS safety systems can be easily and rapidly tested for full operation at any time during plant operation.

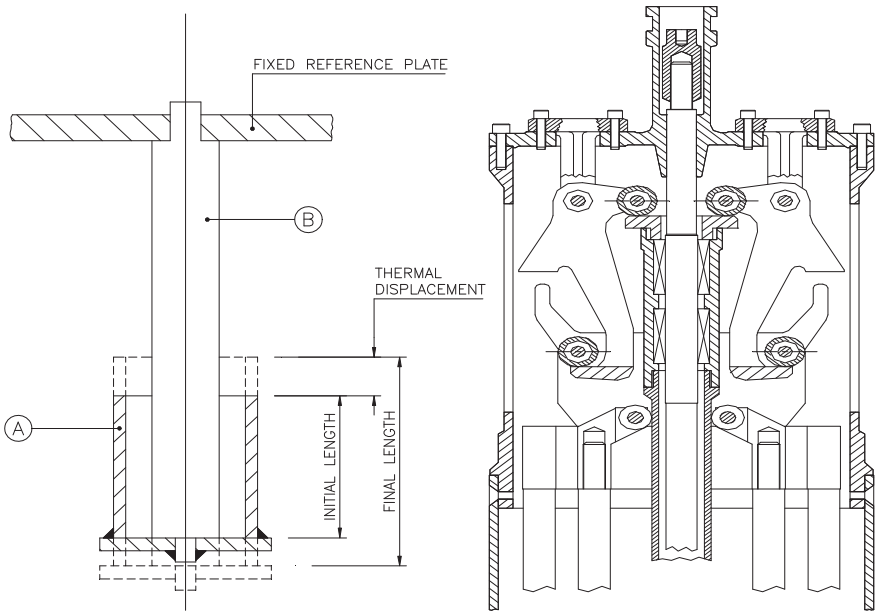


FIG. V-4. Operating scheme (left) and self-releasing head (right) of the ATSS [V-1].

The ***passive safety systems*** incorporated in the MARS design are the following:

- A passive emergency core cooling system (SCCS), based only on natural convection of cooling fluids and using external air as the ultimate heat sink, Fig. V-3. The SCCS is designed to transfer core decay heat directly from the reactor pressure vessel to the external air, without the intervention of any energized system or component. The system operating principle relies on fluid density differences, due to temperature differences between vertical fluid columns, for fluid circulation. The SCCS includes two trains; each train can remove 100% of the core decay heat power. In an accident causing a reduction of core coolant flow (such as a station blackout or primary pump trip), system activation is automatic, requiring no intervention either by the operator or by the control and monitoring system, because the primary coolant system interception valves are kept in a closed position by the force of primary coolant flow and start opening when this flow decreases below a set point value. The SCCS includes only one non-static mechanical component – check valves of an innovative design [V-1] – which is 400% redundant; the SCCS is safety grade;
- An additional (optional) passive scram system actuated by a bimetallic core temperature sensor and operated by gravity (ATSS – additional, temperature-actuated scram system). This system provides for the insertion of additional control rods to the core when the core coolant temperature reaches a preset value. The operation of this system (Fig.V-4) is based on the differential thermal expansion of the bimetallic sensor located inside the fuel assembly; the differential displacement, due to coolant temperature increase, causes the release of a conventional type control rod cluster. This system is safety grade;
- Special connections of components in the primary coolant system, including bolted flanges for load transmission and welded gaskets for leakage prevention; they may be safety grade.

The main scram system in the MARS plant is an active type scram system based on control rods, similar to that used in conventional PWRs. The control rods in this system are divided into four different banks. This system is safety grade.

V–3. ROLE OF PASSIVE SAFETY DESIGN FEATURES IN DEFENCE IN DEPTH

Some major highlights of passive safety design features in the MARS, structured in accordance with the various levels of defence in depth [V-3, V-4], are listed below.

Level 1: Prevention of abnormal operation and failure

- Primary coolant pressure boundary enclosed in a pressurized water filled containment;
- Primary coolant isolation for most of the operating time;
- Low fuel temperature and small temperature gradients in fuel, provided by design;
- High DNBR, provided by design;
- Small diameter physical connections between the primary coolant boundary and the auxiliary systems.

Level 2: Control of abnormal operation and detection of failure

- Additional (optional) passive scram system actuated by a bimetallic core temperature sensor and operated by gravity (ATSS).

Level 3: Control of accidents within the design basis

- Passive emergency core cooling system (SCCS) with a 400% redundant check valve of innovative design;
- Additional (optional) passive scram system actuated by a bimetallic core temperature sensor and operated by gravity (ATSS).

Level 4: Control of severe plant conditions, including prevention of accident progression and mitigation of consequences of severe accidents

- Passive emergency core cooling system (SCCS) with a 400% redundant check valve of innovative design;
- Additional barrier to possible radioactivity release to the environment provided by pressurized water filled primary containment;
- Containment building designed to withstand a variety of internal and external events, capable of resisting internal pressure.

Level 5: Mitigation of radiological consequences of significant release of radioactive materials

As a consequence of the extremely low probability of core damage and the capability of the MARS concept to experience severe accidents while maintaining reactor vessel integrity, the licensing of a MARS NPP does not require any off-site emergency planning [V-1].

V–4. ACCEPTANCE CRITERIA FOR DESIGN BASIS AND BEYOND DESIGN BASIS ACCIDENTS

V–4.1. List of design basis and beyond design basis accidents

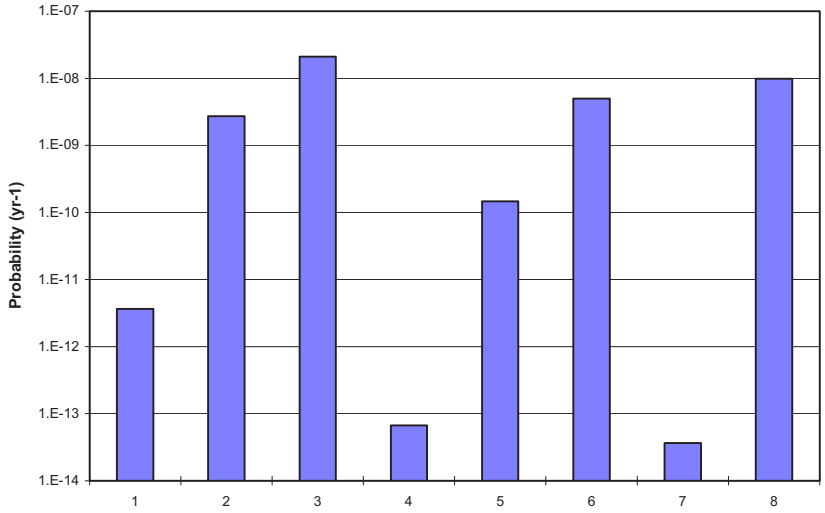
A complete safety analysis of the MARS nuclear plant has been performed to verify the capability of the plant to meet safety objectives and to confront any accidental condition with a frequency of occurrence higher than 1×10^{-7} year^{-1} [V-5].

This analysis was extended to ascertain the ability of the plant to handle accidental conditions with an even lower frequency but involving severe consequences (severe accidents).

The MARS design is intended to prevent the harmful release of radioactive products from fuel to the environment; as such a release is possible only if fuel is damaged and fuel damage is possible only if core cooling is jeopardized. All possible situations (accidental sequences) leading to a failure of core cooling were identified.

An analysis was performed of possible transients of thermal hydraulic parameters in the reactor core by first identifying initiating events leading to variations from standard operating values and then analyzing possible sequences of events resulting from the initiating events, up to identification of the combinations of those events finally leading to fuel damage.

This approach considered the unique aspects of the MARS reactor plant with respect to traditional PWRs. The HAZOP method was used to identify initiating events; the ‘fault tree’ technique was used to evaluate the



1: Primary pump stop
2: Relief/safety valves stuck open
3: SG exchanged power degradation (loss of SG feedwater)
4: Loss of on/off site power
5: Loss of coolant from auxiliary systems
6: SG tube rupture
7: Primary pump trip
8: Steam line break

FIG. V-5. Results of probabilistic safety analysis [V-1].

probability of failure of novel components or systems and the 'event tree' method was used to identify possible evolutions of accidental sequences [V-1, V-5]. Twenty-eight different initiating events, grouped into eight main categories, were identified and their evolutions were analyzed. The results of the probabilistic safety analysis are summarized in Fig. V-5, which also lists the initiating events of design basis accidents (DBA). Accident sequences that may lead to core damage, stemming from the initiating events of DBA, i.e., the sequences that could be categorized as beyond design basis accidents, are reviewed in brief below. The probability of core damage corresponding to each such sequence is also shown in Fig.V-5.

The highest probability of core damage is 2.1×10^{-8} year^{-1}. This number is lower than the probability of ultra-catastrophic natural events such as, for example, a meteorite striking a large city (such as New York) causing 1 million deaths, which was evaluated as 1×10^{-7} year^{-1}. For this reason, as a common cause failure depending on ultra-catastrophic natural events is recognized, the core damage probability for the MARS plant was assumed to be 1×10^{-7} year^{-1} [V-1].

The sequence group related to the loss of electric supply to primary pumps, causing core damage, has a probability of 3.65×10^{-12} year^{-1}, provided the initiating event is followed by a failure of both the automatic and the additional scram systems.

The sequence group related to LOCAs through the pressurizer safety/relief valves, causing core damage, has a probability of 2.73×10^{-9} year^{-1}, provided the initiating event is followed by a failure of the safety core cooling system through failure of the primary loop interception and the primary pump stops.

The sequence group mainly related to the loss of steam generator feedwater as the initiating event and causing core damage has a probability of 2.1×10^{-8} year^{-1}, if the initiating event is followed by a failure of the safety core cooling system through a failure of the primary loop interception and the primary pump stops.

The sequence group related to the loss of on/off site power, causing core damage, has a maximum probability of 6.67×10^{-14} year^{-1}, if the initiating event is followed by a failure of the safety core cooling system through a failure of the check valves or by a simultaneous failure of the automatic and additional scram systems.

The sequence group related to loss of coolant from connections with auxiliary systems, causing core damage, has a probability of 1.46×10^{-10} year^{-1}, if the initiating event is followed by a failure of the primary loop isolation valves and the primary loop interception system.

The sequence group related to a steam generator tube rupture, causing core damage, has a probability of 5×10^{-9} year^{-1}, if the initiating event is followed by a failure of the safety core cooling system, through a failure of the special check valves.

The sequence group related to the primary pump trip, causing core damage, has a probability of 3.65×10^{-14} year^{-1}, if the initiating event is followed by a failure of both the automatic and additional scram systems.

V–4.2. Acceptance criteria

The acceptance criteria for DBA can be deterministic, similar to those used for conventional PWRs. For beyond design basis accidents (accident sequences stemming from certain initiating events of DBA), probabilistic acceptance criteria could be applied, as outlined in Section V-4.1.

V–5. PROVISIONS FOR SAFETY UNDER EXTERNAL EVENTS

Safety related components are designed to resist seismic loads under reference site conditions. Initiating events for relevant accident scenarios include the crash of military aircraft at the site.

V–6. PROBABILITY OF UNACCEPTABLE RADIOACTIVITY RELEASE BEYOND PLANT BOUNDARY

Results of the PRA analysis are described above; the evaluated core fuel melting probability is lower than 1×10^{-7}.

V–7. MEASURES PLANNED IN RESPONSE TO SEVERE ACCIDENTS

Even if the probabilistic safety assessment of the MARS plant shows a core damage probability lower than the probability of ultra-catastrophic natural events, core melting has been considered as a hypothetical event to evaluate the capability of the plant to confront it [V-1].

In particular, thermal mechanical analyses show that the reactor vessel of the MARS plant can guarantee the in-vessel retention and cooling of corium produced by the melting of 60% of the core and vessel internals if the following conditions are met:

– Water is present in the CPP with pressure equal to 1 bar and temperatures lower than 100°C;

– The heat transfer coefficient between the external wall of the vessel and water in the CPP is higher than 1800 W/m^2 K (to avoid partial melting of the vessel wall itself).

The first condition may be met simply by using a depressurizing system for the containment of the primary loop protection (CPP), which is already foreseen to follow primary loop pressure in case of a depressurization.

The second condition is guaranteed if boiling conditions are reached, because heat transfer coefficients of the order of 10 000 W/m^2 K may be then reached. Boiling conditions are surely achieved if the pressure is reduced to 1 bar, with an acceptable temperature of the external vessel wall. Ad hoc high thermal resistance within the core vessel keeps the temperature of metal below harmful values even for lower values of a heat transfer coefficient with CPP water; in turn, should the metal temperature increase during a transient without boiling, boiling conditions would rapidly be reached because of increased metal temperature, and an increased cooling capacity by the CPP water.

Therefore, the two abovementioned requirements could be actually reduced to the first one; and fulfilling it requires the adoption of a reliable, possibly passive depressurization system for the CPP.

As a consequence of the very low probability of core damage and the capability of the MARS concept to confront severe accidents while maintaining reactor vessel integrity, licensing of a MARS NPP may not require any off-site emergency planning.

V–8. SUMMARY OF PASSIVE SAFETY DESIGN FEATURES FOR MARS

Tables V-2 to V-6 below provide the designer's response to questionnaires developed at the IAEA technical meeting "Review of passive safety design options for SMRs", held in Vienna on 13-17 June 2005. These questionnaires were developed to summarize passive safety design options for different SMRs according to a common format, based on the provisions of IAEA Safety Standards [V-3] and other IAEA publications [V-4, V-6]. The information presented in Tables V-2 to V-6 provided a basis for the conclusions and recommendations in the main part of this report.

TABLE V-2. QUESTIONNAIRE 1 — LIST OF SAFETY DESIGN FEATURES CONSIDERED FOR/ INCORPORATED INTO THE MARS DESIGN

#	Safety design features	What is targeted?
1.	Primary coolant boundary enclosed in a pressurized, low enthalpy water containment	–No primary stress on the primary coolant pressure boundary (which is also surrounded by cold water) –Elimination of large break and small break LOCA from the primary coolant pressure boundary –Elimination of control rod ejection accidents
2.	Reactor vessel enclosed in a low temperature pressurized water containment	In-vessel retention of corium (reactor vessel integrity maintained by external cooling even under unforeseen but postulated core melting)
3.	Small coolant flow rate in the low temperature pressurized water containment	Enables early detection of unforeseen but postulated leakages from the primary coolant pressure boundary
4.	Passive, natural convection based emergency core cooling system (with only one non-static mechanical component check valve, 400% redundant)	Decay heat removal never jeopardized in any accidental condition, nor by human failure
5.	Only one small diameter, double connecting line between the primary coolant pressure boundary and the auxiliary systems, with four isolation valves in a series operating intermittently	Limitation of the probability of a failure that may potentially result in the slow drainage of fluid from the reactor coolant pressure boundary (the only initiating event which, coupled with a steam generator tube rupture, may result in core damage from a probabilistic view)
6.	Dedicated atmospheric condenser releasing decay heat to the external air in a natural draft cooling tower	Cooling capacity relying on an infinite medium, with infinite capability in time
7.	Maximum temperature of reactor coolant is below 250°C	–Enables effective use of a passive ECCS with a single, redundant direct action device –Prevents the corrosion experienced in steam generator tubes of PWRs
8.	Steam generator shell, steam piping and feedwater piping designed to withstand primary pressure, with four check valves in series on the steam line and check valves on the feedwater line	Together with a low temperature of the primary coolant, reduces steam generator tube rupture accident probability to negligible values
9.	Reduced number of components requiring maintenance; within the primary coolant pressure boundary only three components need maintenance	Reduction of failure probability in a potentially contaminated fluid boundary; limitation of doses to personnel
10.	All components of the primary coolant pressure boundary are designed for full factory fabrication and testing; only requiring assembly at the site	–Quality improvement with respect to on-site construction –Reduction in construction time and possible errors in the construction phase –Easy replacement of faulty components
11.	Additional passive scram system (ATSS)	–Temperature increase in the core facilitates not only detection, but actuation of the safety function –The additional scram system guarantees sub-criticality in the case of anticipated transients without scram (ATWSs)
12.	Lower core power density, with respect to conventional PWRs	Increase in DNBR (4.6 in the worst transient conditions, for category 2 events)

TABLE V-2. QUESTIONNAIRE 1 — LIST OF SAFETY DESIGN FEATURES CONSIDERED FOR/ INCORPORATED INTO THE MARS DESIGN (cont.)

#	Safety design features	What is targeted?
13.	All components of the nuclear steam supply system (NSSS) are easy to remove and replace	Limitation of doses to personnel during repair/ maintenance/replacement/decommissioning operations
14.	The relief tank of the steam generator safety/relief valve is enclosed in a low temperature pressurized water containment, also enclosing the primary coolant pressure boundary	No loss of coolant is possible because of a steam generator relief/safety valve being stuck open
15.	Presence of a large water inventory in the reactor building (primary coolant + cold pressurized water containment)	Limitation of temperature and pressure in the reactor building in an unforeseen but postulated LOCA/severe accident
16.	Reasonably oversized reactor building, with respect to unforeseen LOCAs and severe accidents	Withstands severe external events, such as military aircraft falling on the plant, tornado, maximum earthquake, acts of sabotage

TABLE V-3. QUESTIONNAIRE 2 — LIST OF INTERNAL HAZARDS

#	Specific hazards that are of concern for a reactor line	Explain how these hazards are addressed in an SMR
1.	Prevent unacceptable reactivity transients	–Control rod ejection is eliminated by enclosing the whole reactor coolant pressure boundary in a low temperature pressurized water containment –Other reactivity transients result only in slow thermal transients, easily controlled by the reactor control system, due to low liquid boron content + primary coolant inertia + low core power and fuel temperature + passive decay heat removal (SCCS) + additional passive scram system (ATSS) –The additional, passive reactor scram system (ATSS) essentially prevents ATWS
2.	Avoid loss of coolant	–Independent of break size, LOCAs are eliminated by enclosure of the whole reactor coolant pressure boundary in a low temperature pressurized water containment –Steam generator tube rupture is avoided due to relatively low primary coolant temperature and pressure –The secondary coolant pressure boundary is designed to withstand the same pressure as that in the primary coolant system, with redundant isolation valves –'Leak before break' concept; low flow rate of cold water in the low temperature pressurized water containment (CPP) enclosing the primary coolant pressure boundary facilitates detection of a leak, with continuous monitoring being carried out
3.	Avoid loss of heat removal	Passive ECCS with an infinite grace period, using natural draught of air as the ultimate heat sink, actuated upon flow rate decrease: –Secures effective decay heat removal –Prevents excessive nuclear fuel heating/core melting In-vessel retention is secured by passive external cooling of the reactor vessel by water
4.	Avoid loss of flow	The consequences of loss of flow accidents are prevented by: –The additional, passive reactor scram system (ATSS), actuated by flow rate decrease –The passive ECCS with an infinite grace period, actuated by flow rate decrease
5.	Avoid exothermic chemical reactions	Nothing in particular specified here

TABLE V-4. QUESTIONNAIRE 3 — LIST OF INITIATING EVENTS FOR ABNORMAL OPERATION OCCURRENCES (AOO)/DESIGN BASIS ACCIDENTS (DBA)/BEYOND DESIGN BASIS ACCIDENTS (BDBA)

#	List of initiating events for AOO/DBA/BDBA typical for a reactor line (PWRs)	Design features of MARS used to prevent progression of the initiating events to AOO/DBA/BDBA, to control DBA, to mitigate BDBA consequences, etc.	Initiating events specific to this particular SMR
1.	Reactivity anomalies due to control rod malfunctions	–Use of well proven conventional control rod system (as in PWRs) –The additional, passive reactor scram system (ATSS), actuated by flow rate decrease	
2.	Reactivity anomalies due to boron dilution	Core design (A): –Reduced boron inventory during the whole irradiation period (maximum ~500 ppm at BOC), and intermittent operation of the chemical and volume control system (CVCS) Core design (B): –No liquid boron in the core	
3.	Reactivity anomalies due to cold water injection	There is no system capable of injecting cold water into the primary coolant system (the ECCS is innovative, relying on natural circulation)	
4.	Coast-down of the main circulation pumps	The innovative ECCS 'substitutes' primary coolant pumped by the primary pump with primary coolant driven by natural convection (infinite grace period)	
5.	Loss of primary system integrity (LOCAs)	Independent of break size, LOCAs are eliminated by enclosing the whole reactor coolant pressure boundary in a low temperature pressurized water containment	
6.	LOCA in the interfacing systems	The only two systems having physical interface with the primary coolant system are: the secondary system and the CVCS; the CVCS is connected through a special small diameter line with check valves, and operates intermittently	
7.	Loss of integrity of the secondary system	The only two systems having physical interface with the primary coolant system are: the secondary system and the CVCS; the secondary system is designed for the same pressure as the primary one, as comes to the steam generator shell and the steam and feedwater lines, which include appropriate isolation valves	
8.	Loss of power supply	Will cause primary coolant pump coast-down, with a 'normal' startup of passive ECCS. No energized component relevant to safety is employed	
9.	Malfunctions in the primary system	Only three components with mechanical movement are included in the primary coolant system; their malfunctioning does not affect the capability of the ECCS to intervene. The pressurizer relief/safety valves of the reactor coolant system cannot initiate hazardous primary coolant system depressurization	
10.	Malfunctions in the secondary system	Owing to large inventory of the primary coolant and to low design power, any malfunctioning of the secondary system leads to normal slow transients in the primary coolant system that are typical of normal plant operation	
11.	ATWSs	The additional, passive reactor scram system (ATSS) essentially prevents ATWSs	
12.	Accidents in fuel handling	No improvement over state of the art PWR designs	
13.	Accidents in auxiliary systems	They do not affect the operation and safety of the primary coolant system, because the only system connected to the primary coolant boundary is the CVCS, which operates intermittently	
14.	Accidents due to external events	The plant has been designed to withstand severe external events of both natural and human induced origin, such as military aircraft falling on the plant, tornado, maximum earthquake, acts of sabotage, etc.	

TABLE V-5. QUESTIONNAIRE 4 — SAFETY DESIGN FEATURES ATTRIBUTED TO DEFENCE IN DEPTH LEVELS

#	Safety design features	Category: A-D (for passive systems only), according to IAEA-TECDOC-626 [V-6]	Relevant DID level, according to NS-R-1 [V-3] and INSAG-10 [V-4]
1.	Primary coolant pressure boundary enclosed in a pressurized, low enthalpy water containment	A	1
2.	Only one small diameter, double connecting line between the primary coolant pressure boundary and auxiliary systems, with four isolation valves in series and intermittent operation	A	1
3.	Reduced number of components requiring maintenance; within the primary coolant pressure boundary only three components need maintenance	A	1
4.	All components of the primary coolant pressure boundary are designed for full factory fabrication and testing; to be assembled at the site	A	1
5.	The relief tank of the steam generator safety/relief valve is enclosed in a low-temperature pressurized water containment, also enclosing the primary coolant pressure boundary	A	1, 2, 3
6.	Maximum temperature of reactor coolant below 250°C	A	1, 2, 3, 4
7.	Relatively low core power density and higher thermal inertia	A	1, 2, 3, 4
8.	Reasonably oversized reactor building, with respect to unforeseen LOCAs and severe accidents	A	3, 4, 5
9.	Small coolant flow in the low temperature pressurized water containment	A, B	2 (facilitates leak before break concept)
10.	Dedicated atmospheric condenser releasing decay heat to the external air in a natural draft cooling tower, acting as a heat sink with infinite in time capacity	B, A	2, 3, 4
11.	Steam generator shell, steam piping and feedwater piping designed to withstand primary pressure, with four check valves in series on the steam line and check valves on the feedwater line	A, C	1
12.	Passive ECCS with an infinite grace period, using natural draught of air as the ultimate heat sink and actuated upon flow rate decrease (check valve, 400% redundant)	C	1, 2, 3, 4
13.	Additional passive scram system ATSS	C	1, 2, 3

TABLE V-6. QUESTIONNAIRE 5 — POSITIVE/NEGATIVE EFFECTS OF PASSIVE SAFETY DESIGN FEATURES IN AREAS OTHER THAN SAFETY.

Passive safety design features	Positive effects on economics, physical protection, etc.	Negative effects on economics, physical protection, etc.
Passive ECCS with an infinite grace period, using natural draught of air as the ultimate heat sink and actuated upon flow rate decrease (check valve, 400% redundant)	Improved plant reliability	Limits reactor power and energy conversion efficiency (via lower primary coolant pressure)
Primary coolant pressure boundary enclosed in a pressurized, low enthalpy water containment	–May facilitate licensing without off-site emergency planning –Complicated unauthorized access to fuel	Negatively affects plant cost: –Additional pressure vessel –Control rod drive mechanisms able to operate in cold water –Complicates plant maintenance through lower accessibility of the primary pressure boundary
The main scram system is the only safety grade system; within the primary coolant pressure boundary, only three components aimed at fluid flow (one pump, two valves) need maintenance	–Improved plant economy and simplified maintenance –Contributes to a reduction in radioactive waste	
Full factory fabrication and testing of all components, requiring only assembly on-site; all components are easily replaceable	–Improved plant reliability –Reduced construction time and costs –Simplified maintenance –May allow plant lifetime extension of up to 80 years and beyond (similar to hydroelectric plants)	
Relatively low core power density and coolant temperature	Reduction of waste production	Increase of specific capital costs

REFERENCES TO ANNEX V

[V–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Innovative Small and Medium Sized Reactor Designs 2005: Reactors with Conventional Refuelling Schemes, IAEA-TECDOC-1485, IAEA, Vienna (2006).

[V–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Advanced Light Water Reactor Designs 2004, IAEA-TECDOC-1391, IAEA, Vienna (2004).

[V–3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA, Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[V–4] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAGH10, IAEA, Vienna (1996).

[V–5] DEPARTMENT OF NUCLEAR ENGINEERING AND ENERGY CONVERSION, 600 MW(th) MARS Nuclear Power Plant - Design Progress Report, 2003, University of Rome “La Sapienza”, Rome (2003).

[V–6] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Terms for Advanced Nuclear Plants, IAEA-TECDOC-626, IAEA, Vienna (1991).

Annex VI

SAFETY DESIGN FEATURES OF THE AHWR

Bhabha Atomic Research Centre,
India

VI–1. DESCRIPTION OF THE AHWR DESIGN

The Advanced Heavy Water Reactor (AHWR) is a concept for a 300 MW(e), vertical pressure tube type reactor cooled by boiling light water and moderated by heavy water. The AHWR design is being developed by the Bhabha Atomic Research Centre (BARC, India). The reactor is designed to be fuelled with $(U^{233}\text{-Th})O_2$, together with $(\text{Pu-Th})O_2$. In this, the AHWR would be nearly self-sustaining in U^{233}. The design of the AHWR is fine tuned to derive most of its power from thorium based fuel, while achieving a negative void coefficient of reactivity. A detailed description of the AHWR concept and its design status can be found in [VI-1].

The general arrangement of the AHWR is shown in Fig. VI-1. Heat removal from the core is achieved by natural circulation of the coolant. The core consists of vertical fuel channels housed in a calandria containing the heavy water moderator.

The calandria is located in a water filled reactor cavity. The core is connected to four steam drums. A large water pool, called the gravity driven water pool (GDWP), is located near the top of the containment. Moderator heat is utilized for feedwater heating. As shown in Fig. VI-2, double containment is provided to prevent any release of radioactivity to the environment.

The fuel assembly is suspended from the top into the coolant channel of the reactor. The assembly consists of a single, long fuel cluster (see Fig. VI-2) and two shield sub-assemblies. The cluster has 54 fuel pins arranged in three concentric rings, 12 pins in the inner ring, 18 pins in the intermediate ring, and 24 pins in the outer ring

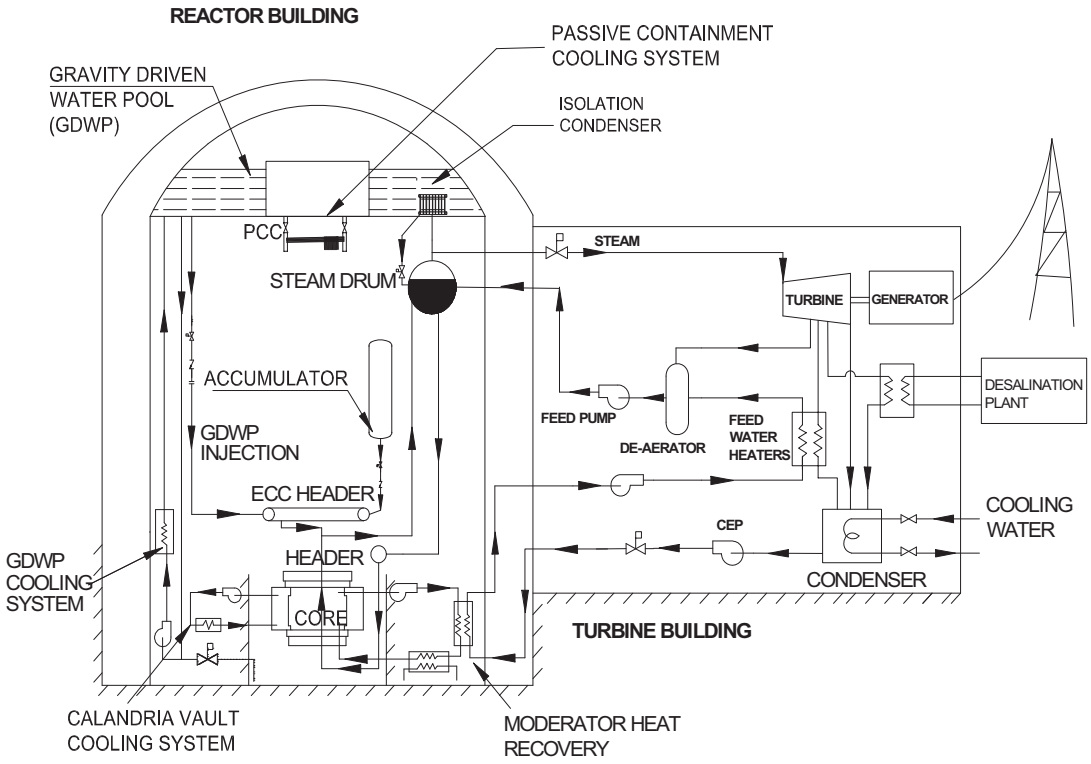


FIG. VI-1. General arrangement of AHWR [VI-1].

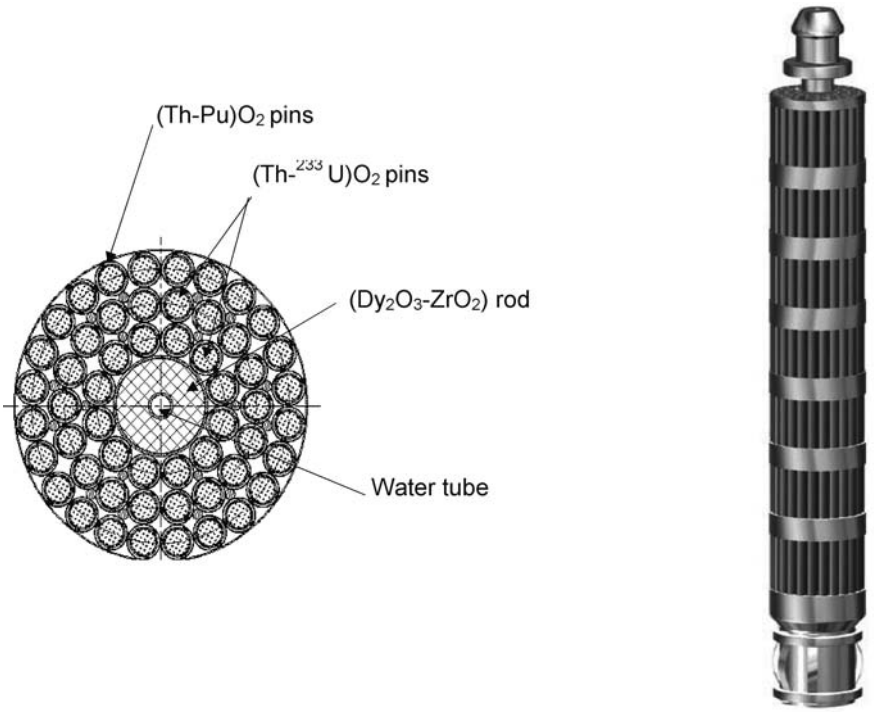


FIG. VI-2. AHWR fuel cluster arrangement.

around a central rod containing the burnable absorber dysprosium as Dy_2O_3-ZrO_2. The 24 fuel pins of the outer ring incorporate (Th-Pu)O_2 fuel and the 30 fuel pins in the inner and intermediate rings are based on (Th-^{233}U)O_2 fuel. Like other pressurized heavy water reactor designs, the AHWR provides for on-line refuelling.

The AHWR incorporates several passive safety systems to facilitate the execution of safety functions related to normal reactor operation, residual heat removal, emergency core cooling, confinement of radioactivity, etc. Passive shutdown during a high pressure transient due to a failure of wired (sensors, signal carriers and actuators) shutdown systems and high temperature protection of the concrete by passive cooling are some of the additional features of the AHWR. A 6000 m^3 capacity GDWP, located at higher elevation inside the containment, serves as a heat sink for the residual heat removal system and several other passive systems; in addition to this, it acts as a suppression pool.

Major design specifications of the AHWR are given in Table VI-1.

VI–2. PASSIVE SAFETY DESIGN FEATURES OF AHWR

The main ***inherent safety features*** of AHWR are:

- Negative void coefficient of reactivity;
- Negative fuel temperature coefficient of reactivity;
- Negative power coefficient of reactivity;
- Double containment system;
- Absence of main circulating pumps;
- High pressure and low pressure independent emergency core cooling system (ECCS) trains;
- Direct injection of ECCS water into the fuel cluster.

The important ***passive safety features and systems*** in AHWR are:

TABLE VI-1. MAJOR DESIGN CHARACTERISTICS OF AHWR [VI-1]

Attributes	Design particulars
Major design specifications	
Core configuration	Vertical, pressure tube type
Fuel	Pu-ThO_2 MOX, and $^{233}UO_2$-ThO_2 MOX
Moderator	Heavy water
Coolant	Boiling light water
Number of coolant channels	452
Pressure tube inner diameter	120 mm
Pressure tube material	20% Cold worked Zr-2.5% Nb alloy
Lattice pitch	245 mm
Active fuel length	3.5 m
Calandria diameter	7.4 m
Calandria material	Stainless steel grade 304L
Steam pressure	7 MPa
Mode of core heat removal	Natural circulation
MHT loop height	39 m
Shutdown system-1 (SDS-1)	40 mechanical shut off rods
Shutdown system-2 (SDS-2)	Liquid poison injection in moderator
Thermal hydraulic characteristics	
Circulation Type	Natural for normal operating as well as hot shutdown conditions
Coolant Conditions	Core inlet: 532 K, 2237 kg/s; Core outlet: 558 K, average exit quality 18.2%
Steam and feed water conditions	Steam at outlet from steam drum: 7 MPa, 558 K, 407.6 kg/s Feed water at inlet to steam drum: 403 K
Fuel temperatures during normal operation	For maximum rated channel: Fuel centre line: 1213 K, Clad surface: 572 K The maximum permissible clad temperature is 673 K.
Reactivity feedbacks	
Condition	Reactivity change (mk)
Temperature and void effects	
Channel temperature (300 K at cold critical to 558 K at hot standby)	+2.5
Moderator temperature (300 K to 353 K)	+3.0
Reactivity feedbacks (continued)	
Fuel temperature (558 K at hot standby to 898 K at full power)	–6.5
Coolant void (density from 0.74 at hot standby to 0.55 g/cc at full power)	–2.0
LOCA at full power (density change from 0.55 to 0.0 g/cc)	–4.0
Xenon load	
Equilibrium load	–21.0
Transient load 30 min. after shutdown from full power	< –1.0
Peak load 300 min. after shutdown from full power	–7.0
Other neutron physical parameters	
Delayed neutron fraction, β (without photon neutrons)	0.003
Prompt neutron lifetime, l, sec.	0.00022

- Core heat removal by natural convection of the coolant during normal operation and in shutdown conditions;
- Decay heat removal by isolation condensers (ICs) immersed in a large pool of water in a gravity driven water pool (GDWP);
- Direct injection of ECCS water into the fuel cluster in a passive mode during postulated accident conditions, such as loss of coolant accidents (LOCAs), initially from the accumulators and later from the GDWP;
- Containment cooling by passive containment coolers during LOCA;
- Passive containment isolation via formation of a water seal in the ventilation ducts, following a large break LOCA;
- Passive shutdown through injection of poison to the moderator, using high pressure steam, in case of the low probability event of failure of the wired (sensors, signal carriers and actuators) mechanical shutdown system (SDS-1) and the liquid poison injection system (SDS-2);
- Passive concrete cooling system to protect the concrete structure in a high temperature zone.

The availability of a large inventory of water in the GDWP at higher elevation inside the containment facilitates sustainable core decay heat removal, ECCS injection, and containment cooling for at least 72 hours without invoking any active systems or operator actions.

Passive safety features/systems of the AHWR are described in brief below.

Passive core heat removal by natural convection during normal operation and in shutdown conditions

In the AHWR, natural convection is the mode of coolant circulation to remove heat from the reactor core under both normal and shutdown conditions. Figure VI-3 shows the main heat transport (MHT) system and the passive decay heat removal system of the AHWR. A two phase steam water mixture generated in the core flows through the tail pipes to the steam drum, where steam gets separated from water. The separated water flows down through the downcomers to the reactor inlet header (RIH). From the header it flows back to the core through inlet feeders.

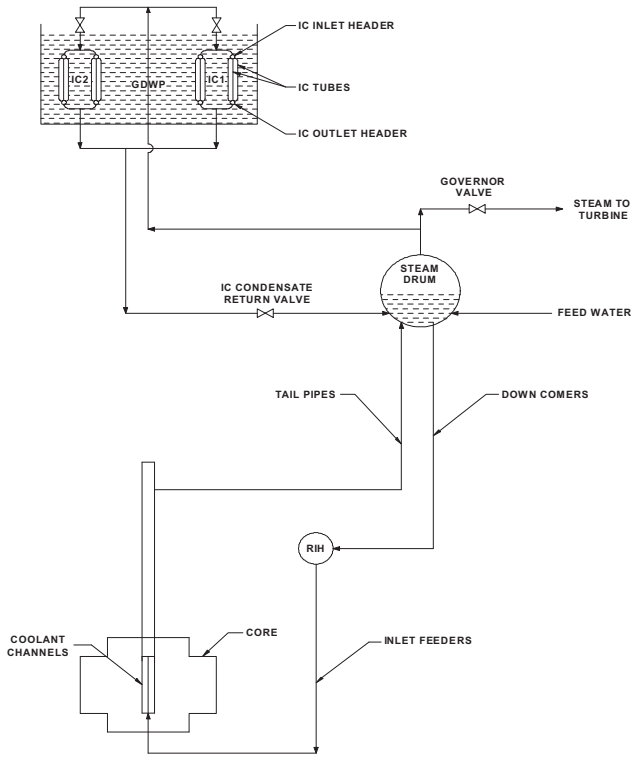


FIG. VI-3. MHT and decay heat removal system.

During a shutdown, core decay heat is removed by isolation condensers (ICs) submerged in a 6000 m^3 capacity GDWP. Passive valves are provided downstream from the ICs. These valves operate on steam drum pressure and establish an interaction between steam drums and the ICs in hot shutdown conditions. The steam, brought to the ICs by natural convection, condenses inside the IC pipes immersed in the GDWP. The condensate is then returned to the core by gravity.

The ICs are designed to bring MHT temperature down from 558 K to 423 K. The water inventory in GDWP is adequate to cool the core for more than three days without any operator intervention and without boiling of the GDWP water.

During normal shutdown, when the main condenser is available, decay heat is removed by natural convection in the main heat transport circuit and heat is transferred to the ultimate heat sink through the main condenser. The IC system removes heat when the main condenser is not available. In the case of unavailability of both the IC and the main condenser, decay heat can be removed by an active system making use of MHT purification coolers.

Emergency core cooling system

This system provides for the injection of water directly into the reactor core in three stages. In the first stage, injection from the accumulator takes place, see Fig. VI-4. In the second stage, water flows from the GDWP under gravity, providing core cooling for three days. In the third stage, water accumulated in the reactor cavity is pumped back to the GDWP, from which it eventually enters the core. The first and the second stages of ECCS are passively actuated and do not depend on any active component. The important components of the ECCS are the GDWP, which has been discussed in Section VI-1, and an advanced accumulator equipped with a fluidic device as shown in the right part of Fig. VI-4.

The FFCD consists of a vortex chamber with one outlet, a tall vertical stand pipe and a small tangential side connection with two inlets. With the incorporation of a fluidic flow control device (FFCD) at the bottom of the accumulators, the large amount of water which is flowing directly into the core in the early stage of a LOCA is reduced to a relatively small amount and continues to flow for a longer time into the core, removing the decay heat. The FFCD is a simple passive device which reduces flow automatically after some time because of an increase in the pressure drop due to the formation of vortex. This passive feature provides many safety benefits suc as design simplicity and high reliability, and cools the core for a longer time.

Passive containment cooling system

Passive containment coolers (PCCs) are used to provide post-accident primary containment cooling in a passive mode, as well as to limit post-accident primary containment pressure. The PCCs are located below the GDWP and are connected to the GDWP inventory, see Fig. VI-5. During a LOCA, condensation of steam and cooling of hot air are achieved via cooling provided by natural convection of GDWP water through the PCC tubes. This design feature ensures long term containment cooling after an accident.

Passive containment isolation system

The reactor has a double containment, i.e., incorporates primary and secondary containment. Between the two containments, a negative pressure in relation to the atmosphere is maintained to ensure that there is no release of radioactivity to the atmosphere. The primary containment envelops the high enthalpy and the low enthalpy zones designated as volume V1 and volume V2, respectively. Volume V2 is normally ventilated to the atmosphere through a ventilation duct, as shown in Fig. VI-6.

There is a very remote possibility of a release of radioactivity along with steam into the containment under accidental conditions. Under such accidental conditions, it is of paramount importance to isolate the containment from the atmosphere within a minimum possible time. The AHWR incorporates a scheme of containment isolation requiring no actuation by active means. This passive scheme is based on isolation of the containment atmosphere by establishing a liquid U-seal in the ventilation duct. A theoretical model is formulated to determine the time required for the formation of such a liquid seal.

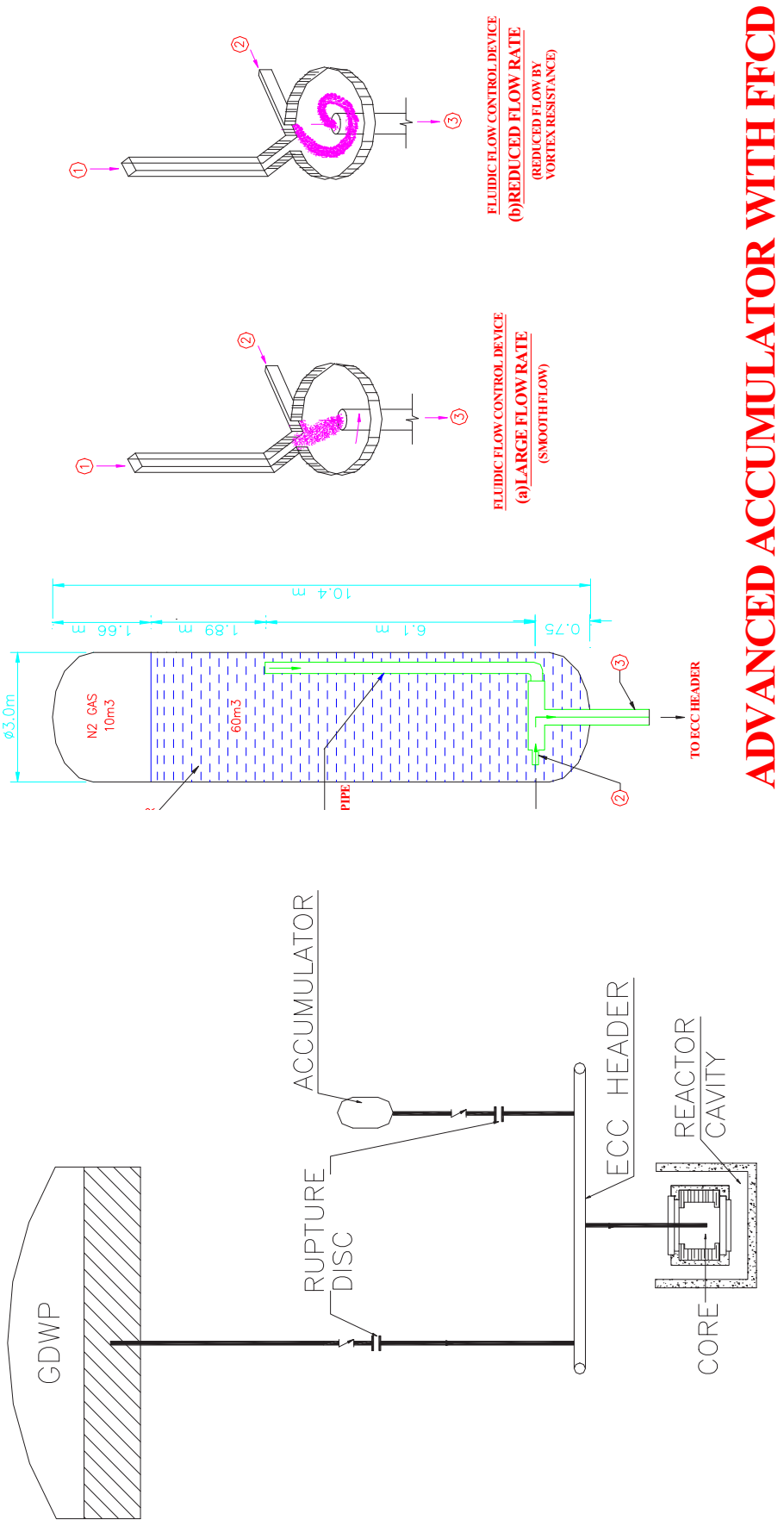


FIG. VI-4. Emergency core cooling system.

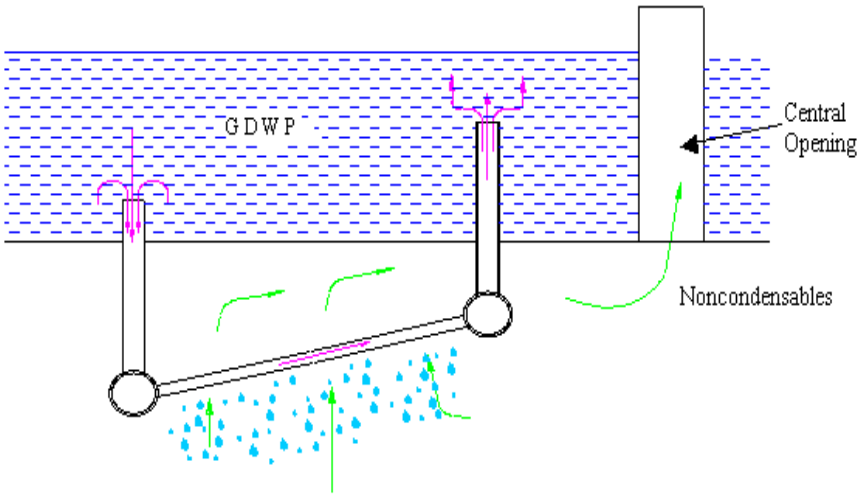


FIG. VI-5. Passive containment cooling system.

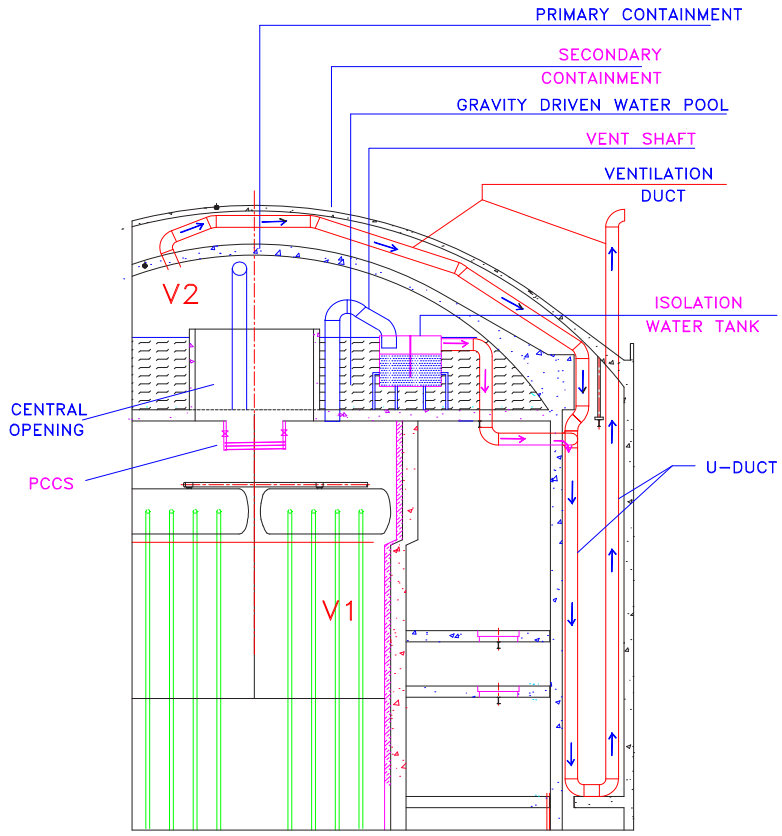


FIG. VI-6. Passive containment isolation system.

The scheme consists of an isolation water tank comprising the two compartments, one having a connection with volume V1 through a vent shaft, and the other having a connection with volume V2 via the normal ventilation duct, as shown in Fig. VI-6. A vertical baffle plate, running from the top of the tank, separates the two compartments. The baffle plate, however, does not run through the full height of the tank. The bottom portion of the tank allows the two compartments to communicate. It should be noted that volume V2 is normally ventilated to the atmosphere through a 'U' duct, which has a branched connection to the isolation water tank outlet. In the event of volume V1 reaching a certain preset pressure, the water level in another compartment of

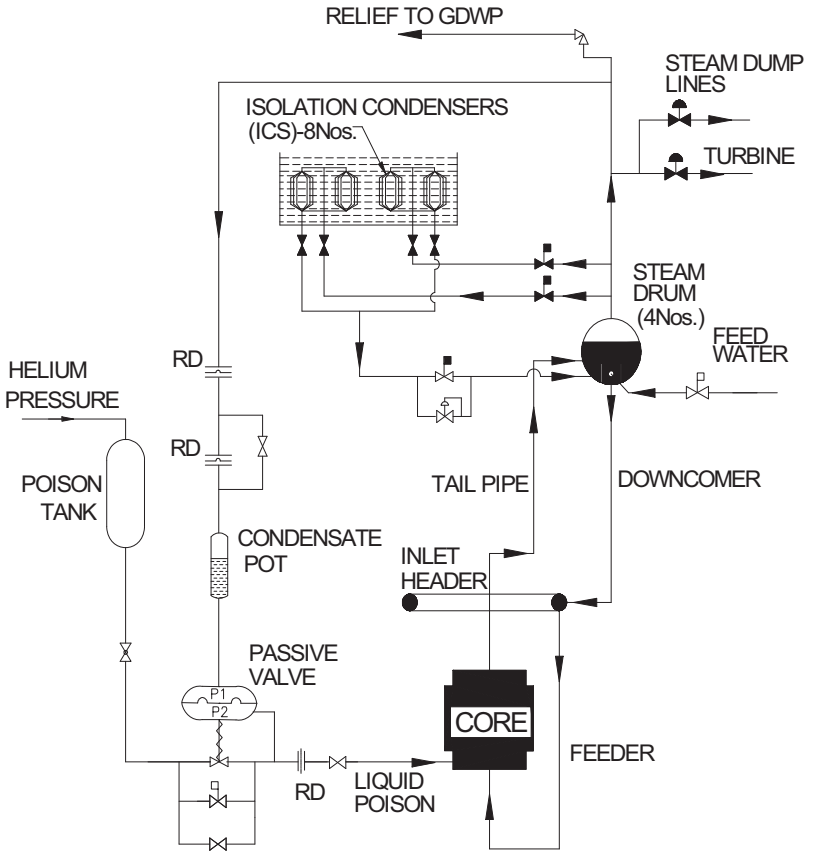


FIG. VI-7. Passive shutdown by MHT high pressure (RD is for rupture disc).

the tank rises to spill the water into the 'U' duct. Thus, the isolation of volumes V1 and V2 from the atmosphere is ensured by securing a water seal at the base of the U duct. The seal must form in a minimum possible time, typically in the order of a few seconds, to ensure that the isolation is effective. Tests are to be conducted to identify degrading factors which could adversely affect the performance of this system. A probable degrading factor could be incomplete venting of air from the U tube.

Passive shutdown on MHT high pressure

This shutdown system passively injects poison into the moderator by using the increased system steam pressure in the case of a low probability event of failure of the wired (sensors, signal carriers and actuators) shutdown systems. The AHWR has two independent shutdown systems, one comprising mechanical shut off rods (SDS-1) and the other employing the injection of a liquid poison into the low pressure moderator (SDS-2). Both these shutdown systems require the actuation of active signals for a reactor shutdown to occur. The proposed scheme of a passive shutdown is actuated by high steam pressure due to the unavailability of a heat sink, following a failure of the SDS-1 and the SDS-2. The schematics of a passive shutdown by MHT high pressure are shown in Fig. VI-7.

In the event of a pressure rise, high steam pressure opens a rupture disc and steam pressure is transmitted to open a passive valve connected to the pressurized poison tank; the reactor is shutdown by passive poison injection into the moderator. Following a reactor shutdown, the system reaches a hot shutdown condition due to effective passive decay heat removal by the ICs. Inadvertent poison injection is avoided by keeping the margin on a rupture disc with burst pressure above the expected pressure gradient after a reactor shutdown by the SDS-1 or the SDS-2.

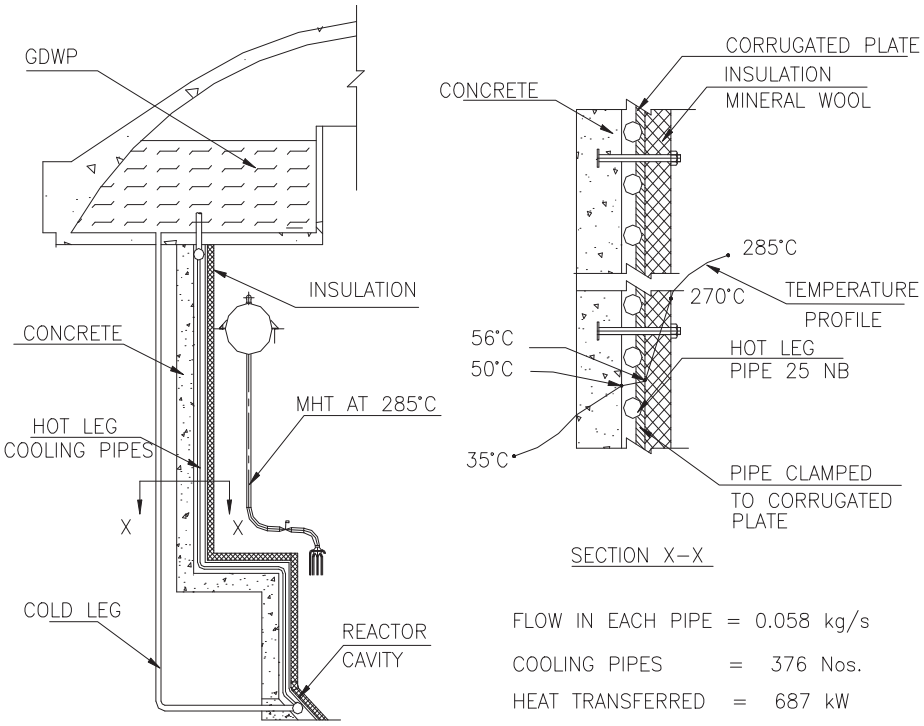


FIG. VI-8. Schematic view of passive concrete cooling system.

Passive concrete cooling system

A passive concrete cooling system is designed to protect the concrete structure of the reactor in a high temperature zone (volume V1). A schematic of the passive concrete cooling system is shown in Fig. VI-8. Cooling is achieved by the circulation of a coolant from the GDWP in natural convection mode through cooling pipes located between the concrete structure and the insulation panel surrounding the MHT system hot piping. Heat loss from the high temperature MHT piping is reduced by the insulation panel. Heat transferred through the insulation panel is removed in a natural convection mode by GDWP water through pipes fixed on a corrugated plate on the outer surface of the insulation panel. This passive design maintains the concrete temperature at below 55°C. It also eliminates the need for high capacity blowers and prevents consequences that otherwise may result from equipment or power supply failures which might lead to a temperature increase in the concrete structure.

The AHWR incorporates two independent fast acting wired (sensors, signal carriers and actuators) shutdown systems, which could be categorized as category D passive systems [VI-2]; they are:

- Shutdown system–1 (SDS–1), based on mechanical shut-off rods with boron carbide absorbers in 40 lattice positions. In case of a signal requiring rector trip, shut-off rods fall under gravity into the core in less than two seconds to achieve required reactivity worth;
- Shutdown system–2 (SDS–2), based on liquid poison injection into the moderator. On a trip signal, a quick opening valve located between the helium gas tank and the poison tank opens, letting high pressure helium gas communicate with the poison tank. As a result, the liquid poison is driven out from the poison tank into the moderator by helium gas pressure.

The AHWR incorporates no dedicated active safety systems. As was already mentioned above, when both the IC and the main condenser are unavailable, decay heat can be removed in an *active mode*, using MHT purification coolers.

The passive systems are safety grade.

VI–3. ROLE OF PASSIVE SAFETY DESIGN FEATURES IN DEFENCE IN DEPTH

Some major highlights of passive safety design features in the MARS, structured in accordance with the various levels of defence in depth [VI-3, VI-4], are described below.

Level 1: Prevention of abnormal operation and failure

(a) Elimination of the hazard of loss of coolant flow:

- Heat removal from the core under both normal full power operating conditions and shutdown conditions is performed by natural convection of the coolant; this eliminates the hazard of a loss of coolant flow;

(b) Reduction of the extent of overpower transient:

- Slightly negative void coefficient of reactivity;
- Low core power density;
- Negative fuel temperature coefficient of reactivity;
- Low excess reactivity.

Level 2: Control of abnormal operation and detection of failure

- An increased reliability of the control system achieved with the use of high reliability digital control using advanced information technology;
- Increased operator reliability achieved with the use of advanced displays and diagnostics using artificial intelligence and expert systems;
- Large coolant inventory in the main coolant system.

Level 3: Control of accidents within the design basis

- Increased reliability of the emergency core cooling system, achieved through passive injection of cooling water (initially from an accumulator and later from the overhead GDWP) directly into a fuel cluster through four independent parallel trains;
- Increased reliability of a shutdown, achieved by providing two independent shutdown systems, one comprising the mechanical shut off rods and the other employing injection of a liquid poison into the low pressure moderator. Each of the systems is capable of shutting down the reactor independently. Further enhanced reliability of the shutdown is achieved by providing an additional passive shutdown device operated by steam pressure for the injection of a poison in the case of a extremely low probability failure of both the mechanical shut-off rods and the liquid poison shutdown system;
- Increased reliability of decay heat removal, achieved through a passive decay heat removal system, which transfers decay heat to the GDWP by natural convection;
- Large inventory of water inside the containment (about 6000 m^3 of water in the GDWP) provides prolonged core cooling, meeting the requirement of an increased grace period.

Level 4: Control of severe plant conditions, including prevention of accident progression and mitigation of consequences of severe accidents

- Use of the moderator as a heat sink;
- Flooding of the reactor cavity following a LOCA.

Level 5: Mitigation of radiological consequences of significant release of radioactive materials

The following features help in passively bringing down the containment pressure and in minimizing any releases from the containment following a large break LOCA:

- Double containment;
- Passive containment isolation;
- Vapour suppression in GDWP;
- Passive containment cooling.

VI–4. ACCEPTANCE CRITERIA FOR DESIGN BASIS AND BEYOND DESIGN BASIS ACCIDENTS

VI–4.1. List of design basis and beyond design basis accidents

Safety analysis of AHWR has identified an exhaustive list of 43 postulated initiating events [VI-1]. Events considered within the design basis are categorized as follows:

- Decrease in coolant inventory (Loss of coolant accidents);
- Increase in coolant inventory;
- Increase in heat removal;
- Increase in system pressure/Decrease in heat removal;
- Decrease in coolant flow;
- Reactivity anomalies;
- Start-up and shutdown transients;
- AHWR specific events (defuelling, refuelling of AHWR channel).

Events considered beyond the design basis are categorized as follows:

- Multiple failure events;
- Failure of wired shutdown systems and other BDBAs.

Specifically, safety analyses included the analysis of four transients due to failure of the wired (sensors, signal carriers and actuators) systems of the SDS-1 and the SDS-2, with reactor shutdown executed passively, through injection of a poison into the moderator by usage of the system steam pressure.

VI–4.2. Acceptance criteria

The acceptance criteria for all design basis accidents are as follows:

(a) Coolability criteria:

- Clad temperature to be less than 1473 K;
- Oxidation of clad surface should be less than 17%;
- Maximum energy deposition in fuel for fuel shattering shall not exceed 200 Cal/g;
- Maximum fuel temperature anywhere in the core shall not exceed UO_2 melting temperature throughout a transient;

(b) Fuel failure criteria:

- Maximum energy deposition in fuel for fuel failure shall not exceed 140 Cal/g;
- Maximum clad surface temperature shall be 1073 K;
- The radially averaged fuel enthalpy, anywhere in the core, shall not exceed 586 J/g.

Actual calculations indicate that fuel clad temperatures do not exceed 1073 K in any design basis accident sequences mentioned above.

For the purpose of containment design, a double ended guillotine rupture of the 600 mm diameter inlet header has been considered a design basis accident. A large number of other accident scenarios would

conventionally fall within the category of beyond design basis accidents (BDBA). However, even in these cases, including the case of an NPP blackout accompanied by failures of both independent fast acting shutdown systems (SDS–1 and SDS–2), it has been demonstrated that none of the acceptance criteria for design basis accidents as indicated above has been violated.

VI–5. PROVISIONS FOR SAFETY UNDER EXTERNAL EVENTS

The safety design features of the AHWR intended to cope with external events and external/internal event combinations are described in detail in [VI-5].

The reactor is provided with an inner pre-stressed concrete containment designed to provide leaktightness in the case of a large break LOCA, and an outer secondary containment that protects the inner containment from external events including aircraft impacts.

Location at a high elevation counters the effects of flood related events as well as probable maximum precipitation, maximum possible sea level etc. in extreme environmental conditions.

AHWR structures, systems and equipment are being designed for high level and low probability seismic events such as an operating basis earthquake (OBE) and safe shutdown earthquake (SSE). These are also called S1 and S2 level earthquakes respectively. Seismic instrumentation is also planned in accordance with national and international standards.

Safety related buildings are protected from turbine generated low trajectory missiles.

Fire protection measures comprise physical separation, barriers, and the use of fire resistant materials at potential systems, and also minimize the inventory of combustible material.

Closing dampers in the ventilation systems provide for detection of poisonous gases and minimize their ingress into structures and air intakes. Air bottles with a capacity of 30 minutes are provided to supply fresh air to operating personnel.

Important nuclear auxiliary systems are located inside the reactor building and in the basement, to the extent possible.

As outlined in previous sections, the AHWR incorporates many inherent safety features (e.g., negative void coefficient of reactivity, and passive systems that require no external power and no operator actions to accomplish certain safety functions. The design provides for several heat sinks that remain available with loss of external coolant supply, such as the gravity driven water pool (GDWP) with 6000 m^3 of storage capacity, ensuring a three day grace period for decay heat removal; fire water storage, providing cooling of the important auxiliary systems for eight hours; the moderator, which in AHWR acts as an ultimate heat sink; and the emergency water reservoir. All of these features/systems are intended to secure plant safety in the case of both internal and external events and their combinations.

VI–6. PROBABILITY OF UNACCEPTABLE RADIOACTIVITY RELEASE BEYOND PLANT BOUNDARY

It is expected that the probability of unacceptable radioactivity release beyond the plant boundary would be less than 1×10^{-7}/year.

VI–7. MEASURES PLANNED IN RESPONSE TO SEVERE ACCIDENTS

One of the important design objectives of the AHWR is to eliminate the need for any intervention in the public domain beyond plant boundaries as a consequence of any postulated accident condition within the plant [VI-1].

VI–8. SUMMARY OF PASSIVE SAFETY DESIGN FEATURES FOR AHWR

Tables VI-2 to VI-6 below provide the designer's response to the questionnaires developed at the IAEA technical meeting "Review of passive safety design options for SMRs" held in Vienna on 13-17 June 2005. These questionnaires were developed to summarize passive safety design options for different SMRs according to a common format, based on the provisions of IAEA Safety Standards [VI-3] and other IAEA publications [VI-2, VI-4]. The information presented in Tables VI-2 to VI-6 provided a basis for the conclusions and recommendations of the main part of this report.

TABLE VI-2. QUESTIONNAIRE 1 — LIST OF SAFETY DESIGN FEATURES CONSIDERED FOR/ INCORPORATED INTO THE MARS DESIGN

#	Safety design features	What is targeted?
1.	Heat removal by natural convection of the coolant	Elimination of postulated initiating events associated with pump failure
2.	Slightly negative void coefficient of reactivity	Reduction of the extent of an overpower transient
3.	Negative fuel temperature coefficient of reactivity	
4.	Low core power density	
5.	Low excess reactivity	
6.	Large coolant inventory in the main coolant system	Thermal inertia securing a reduced rate of temperature rise under certain transients
7.	Two fast acting shutdown systems (mechanical shut off rods and liquid poison injection system)	Safe termination of abnormal operational conditions and accidental conditions
8.	Passive emergency injection of cooling water (initially from the accumulators and later from the overhead gravity driven water pool - GDWP) directly into the fuel cluster through four independent trains	Core heat removal during loss of coolant accidents (LOCA); including a prolonged core cooling for 3 days via GDWP water injection. Direct injection reduces the time for ECCS water to reach fuel
9.	Passive decay heat removal by isolation condensers	Core decay heat removal under non-availability of the main condenser, by transferring heat to the GDWP water without any operator action or active signal
10.	Passive injection of poison into the moderator, by using high pressure steam	– Effective reactor shutdown in the case of a failure of the wired (sensors, signal carriers and actuators) mechanical shutdown system and the liquid poison injection system – Elimination of the possibility of radioactive steam release through safety relief valves, by performing an effective reactor shutdown and bringing the system back to a condition with restored heat removal capability of the isolation condensers
11.	Large inventory of water in the GDWP inside the containment	– Provides a heat sink/working fluid for decay heat removal by passive systems, containment cooling and containment isolation during a LOCA, as well as passive concrete cooling – Provides prolonged core cooling during LOCAs, meeting the requirement of a three day grace period
12.	Use of the moderator as a heat sink	Impedes accident propagation in the case of a failure of the ECC injection during a LOCA
13.	Flooding of the reactor cavity following a LOCA	Facilitates eventual submerging of the core after a LOCA
14.	Double containment	Minimization of radioactivity release from the reactor building during accident conditions, such as a LOCA
15.	Passive containment isolation through the formation of a water seal in the ventilation ducts	Prevention of radioactivity release from the reactor building through the ventilation ducts following a large break LOCA

TABLE VI-2. QUESTIONNAIRE 1 — LIST OF SAFETY DESIGN FEATURES CONSIDERED FOR/ INCORPORATED INTO THE MARS DESIGN (cont.)

#	Safety design features	What is targeted?
16.	Vapour suppression in the GDWP	Minimization of containment pressurization by the absorption of energy released immediately following a LOCA
17.	Containment cooling by passive containment coolers	Limit post-LOCA primary containment pressure. Condensation of steam and cooling of hot air in the containment by natural convection of the GDWP water, to ensure long-term containment cooling after an accident

TABLE VI-3. QUESTIONNAIRE 2 — LIST OF INTERNAL HAZARDS

#	Specific hazards that are of concern for a reactor line	Explain how these hazards are addressed in a SMR
1.	Prevent unacceptable reactivity transients	– Slightly negative void coefficient of reactivity – Small overall reactivity margin – Increased reliability of the control system achieved through the use of high reliability digital control using advanced information technology – Reactor protection system comprised of two independent fast acting shutdown systems – Provision of passive injection of poison to the moderator using system high steam pressure in the case of a failure of both wired shutdown systems
2.	Avoid loss of coolant	– Large coolant inventory in the main coolant system – Presence of water in the calandria vault – Core cooling by passive injection of ECC water using high pressure accumulators and low pressure injection from the GDWP – Filling of the reactor cavity with GDWP water
3.	Avoid loss of heat removal	– Low core power density – Large coolant inventory in the main coolant system – A 6000 m^3 capacity GDWP, located at higher elevation inside the containment, serves as a heat sink for the passive residual heat removal system, ensuring a grace period of not less than three days – Use of the moderator as a heat sink
4.	Avoid loss of flow	Core heat is removed by natural convection of the coolant; the design incorporates no main circulation pumps
5.	Avoid exothermic chemical reactions:	
	–Zirconium-steam reaction	– Passive systems adopted in design for core heat removal during all operational modes, transients, and accidental conditions – Under any transient or accident conditions, the clad temperature is maintained lower than the threshold temperature at which a zirconium-steam reaction of a significant rate may occur
	–Deuterium concentration in cover gas system of the moderator reaching the deflagration limit	Recombination units are provided for recombining deuterium and oxygen, limiting the deuterium concentration in cover gas well below the deflagration limit

TABLE VI-4. QUESTIONNAIRE 3 — LIST OF INITIATING EVENTS FOR ABNORMAL OPERATION OCCURRENCES (AOO)/DESIGN BASIS ACCIDENTS (DBA)/BEYOND DESIGN BASIS ACCIDENTS (BDBA)

#	List of initiating events for AOO/DBA/BDBA typical for a reactor line (PHWRs)	Design features of AHWR used to prevent progression of the initiating events to AOO/DBA/BDBA, to control DBA, to mitigate BDBA consequences, etc.	Initiating events specific to this particular SMR
1.	Reactivity anomalies due to control rod malfunctions	Two independent fast acting shutdown systems	
2.	Reactivity anomalies due to boron dilution	Boron-free equilibrium core configuration. Boron is injected into the moderator, not into the primary coolant. During a prolonged shutdown, the boron removal ion exchange columns of the moderator purification circuit are isolated	
3.	Reactivity anomalies due to cold water injection	– Slightly negative void coefficient of reactivity, which prevents large variations in reactor power – Emergency core cooling water cannot enter the main heat transport (MHT) circuit, because there is a certain differential pressure requirement for the injection to start	
4.	Coastdown of the main circulation pumps	Core heat is removed by natural convection of the coolant; there are no main circulation pumps in the AHWR	
5.	LOCA	– Two independent fast acting reactor shutdown systems provided for shutting down the reactor upon a LOCA signal, such as high containment pressure or low primary pressure – Core cooling by passive injection of ECC water using high pressure accumulators and low pressure injection from the GDWP – Minimization of containment pressurization by vapour suppression in the GDWP and by condensation of the steam and cooling of the air by the passive containment coolers – Prevention of radioactivity release by passive formation of a water seal in the ventilation duct, in addition to closure of the mechanical dampers – Prevention of accident propagation, facilitated by a large inventory of the moderator surrounding the fuel channels, by the presence of water in the calandria vault, and by filling of the reactor cavity with GDWP water	
6.	Loss of integrity in the secondary system	Shutdown of the reactor in the case of non-availability of the secondary circuit and decay heat removal by the isolation condensers in a passive mode	
7.	Loss of power supply	Reactor shutdown on power supply failure and passive decay heat removal by the isolation condensers	
8.	Malfunctions in the primary systems	– Large coolant inventory in the primary circuit provides thermal inertia to limit the rate of temperature rise – Low excess reactivity, achieved through the types of fuel used – Negative void coefficient of reactivity and low core power density reduce the extent of possible overpower transients – Reliable reactor control and protection system – Passive circulation of the coolant that transfers heat from the source to a sink – Annulus gas monitoring system to detect leakage from a pressure tube or calandria tube – Rupture discs installed before the safety relief valves, to prevent inadvertent coolant leakage	

TABLE VI-4. QUESTIONNAIRE 3 — LIST OF INITIATING EVENTS FOR ABNORMAL OPERATION OCCURRENCES (AOO)/DESIGN BASIS ACCIDENTS (DBA)/BEYOND DESIGN BASIS ACCIDENTS (BDBA) (cont.)

#	List of initiating events for AOO/DBA/BDBA typical for a reactor line (PHWRs)	Design features of AHWR used to prevent progression of the initiating events to AOO/DBA/BDBA, to control DBA, to mitigate BDBA consequences, etc.	Initiating events specific to this particular SMR
9.	Malfunctions in the secondary systems	– Due to a large coolant inventory in the main heat transport circuit and low power, any malfunctioning of the secondary system leads to slow transients in the main heat transport circuit – Redundancy is provided for the feedwater pumps – In the case of non-availability of the secondary circuit, the reactor is shut down and the decay heat is removed by the isolation condensers	
10.	Anticipated transient without scram (ATWS)	ATWS is not included in the accident list for the AHWR because two independent, diverse shutdown systems are being incorporated, backed up by a passive shutdown system in which poison is passively injected into the moderator using the system high pressure steam in the case of a failure of both wired shutdown systems	
11.	Accidents in fuel handling	– Fuel insertion and withdrawal rate controlled by on-line fuelling machine, for reactivity considerations – Control system capable of arresting the reactivity increase due to a sudden fall of the fuel assembly	
12.	Accidents due to external events	– Core cooling function for decay heat removal is fulfilled without any external energy or water supply for at least three days, due to natural convection of the coolant in the heat transport circuit and decay heat removal by the isolation condensers immersed in a large pool of water in the GDWP inside the containment – Safety related components, systems, and structures are designed for an operating basis earthquake (OBE) and for a safe shutdown earthquake (SSE); sites having unacceptable seismic potential are excluded – The effects of flood related events are avoided by providing a high grade elevation level to take care of maximum probable precipitation, maximum possible sea level, etc. – Double containment provides protection against aircraft crash or missile attack – Damages related to lightning are avoided by grounding – Detection of toxic gases is provided for; minimization of ingress of toxic gases into the structures and air intakes is achieved by closing the dampers in the ventilation systems. Air bottles with a 30-minute capacity are provided to supply fresh air to operating personnel – Chemical explosions and toxic gas release from off-site facilities are excluded by executing control of hazardous industrial facilities located within a 5 km radius	
13.		Appropriate startup procedure backed up by analysis and experiments	Instability during a startup

TABLE VI-5. QUESTIONNAIRE 4 — SAFETY DESIGN FEATURES ATTRIBUTED TO DEFENCE IN DEPTH LEVELS

#	Safety design features	Category: A-D (for passive systems only), according to IAEA-TECDOC-626 [VI-2]	Relevant DID level, according to NS-R-1 [VI-3] and INSAG-10 [VI-4]
1.	Natural convection of the coolant	B	1, 2, 3
2.	Slightly negative void coefficient of reactivity	A	1
3.	Negative fuel temperature coefficient of reactivity	A	1
4.	Low core power density	A	1
5.	Low excess reactivity	A	1
6.	Large coolant inventory in the main coolant system	A	1, 2, 3
7.	Two independent fast acting shutdown systems	D	2, 3
8.	Passive injection of the emergency coolant water (initially from the accumulators and later from the overhead GDWP) directly into the fuel cluster through four independent trains	C	3
9.	Passive decay heat removal by isolation condensers	C, D	2, 3
10.	Passive shutdown through injection of a poison into the moderator, done by high pressure steam	C	2, 3
11.	Large inventory of water in the GDWP inside the containment	A	3, 4
12.	Use of the moderator as a heat sink	A	4
13.	Presence of water in the calandria vault	A	4
14.	Flooding of the reactor cavity following a LOCA	B, C	4
15.	Double containment	A	3, 4, 5
16.	Passive containment isolation by formation of a water seal in the ventilation ducts	B	3, 4, 5
17.	Vapour suppression in the GDWP	B	3, 4, 5
18.	Containment cooling by the passive containment coolers	B	3, 4, 5

TABLE VI-6. QUESTIONNAIRE 5 — POSITIVE/NEGATIVE EFFECTS OF PASSIVE SAFETY DESIGN FEATURES IN AREAS OTHER THAN SAFETY

Passive safety design features	Positive effects on economics, physical protection, etc.	Negative effects on economics, physical protection, etc.
Core cooling by natural convection	Simplifies design and maintenance, eliminates nuclear grade main circulating pumps, their drives and control systems, contributing to reduced plant cost Reduces the power requirements for plant operation, resulting in higher net plant efficiency and lower specific capital cost	Increased diameter and length of the piping; with associated increase in plant cost

REFERENCES TO ANNEX VI

[VI–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Innovative Small and Medium Sized Reactor Designs 2005: Reactors with Conventional Refuelling Schemes, IAEA-TECDOC-1485, IAEA, Vienna (2006).

[VI–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Terms for Advanced Nuclear Plants, IAEA-TECDOC-626, IAEA, Vienna (1991).

[VI–3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[VI–4] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

[VI–5] INTERNATIONAL ATOMIC ENERGY AGENCY, Advanced Nuclear Power Plant Design Options to Cope with External Events, IAEA-TECDOC-1487, IAEA, Vienna (2006).

Annex VII

SAFETY DESIGN FEATURES OF THE GT-MHR

Experimental Design Bureau of Machine Building (OKBM),
Russian Federation

VII–1. DESCRIPTION OF THE GT-MHR CONCEPT

An international project for the GT-MHR was launched in 1995 by the Russian Ministry for Atomic Energy and the General Atomics Company of the USA. Later, the project was joined by the Framatome[1] (France) and Fuji Electric (Japan). At present, the preliminary design is completed, and the technology demonstration phase is underway. The goal of technology demonstration is experimental validation of key design solutions, mainly for fuel, for turbomachine, for structural materials, vessels, and for computer codes. A detailed description of the GT-MHR concept is presented in [VII-1].

The GT-MHR is a high temperature gas cooled reactor based on the following state of the art technologies:

— Technologies of modular helium cooled reactors using inherently safe micro fuel with several layers of ceramic coating;
— Highly efficient gas turbines designed for aviation and power applications;
— Electromagnetic bearings;
— Effective compact plate heat exchangers.

The helium cooled modular GT-MHR, capable of generating high temperature heat, is coupled with a gas turbomachine consisting of a turbine, an electric generator, and compressors, and implements the direct Brayton gas-turbine cycle for electricity generation (see Fig. VII-1).

Figure VII-2 shows a flow diagram of the cooling system of the GT-MHR reactor plant. Main characteristics of the reactor plant are given in Table VII-1.

The reactor, the power conversion unit (PCU), and all associated primary circuit systems are located in an underground silo of the reactor building (see Fig.VII-3).

The reactor includes an annular core consisting of 1020 hexahedral fuel assemblies similar to those of the Fort Saint Vrain reactor. The core is surrounded by a graphite reflector. The lower part of the reactor vessel houses the shutdown cooling system (SCS).

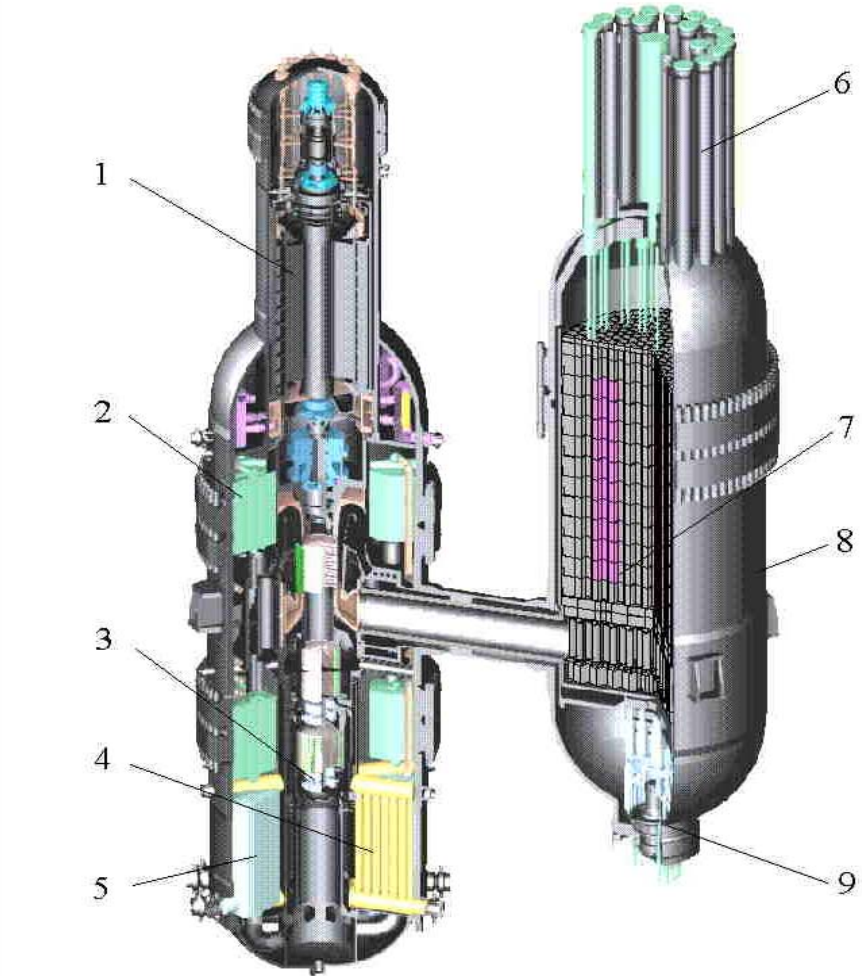
The reactor vessel is surrounded by the surface cooler of the passive reactor cavity cooling system (RCCS). The RCCS removes heat from the reactor vessel in all accidents, including complete loss of coolant (LOCA).

The power conversion system is arranged in the PCU vessel and includes a turbomachine, a recuperator, and water cooled pre-cooler and intercooler. The single shaft turbomachine consists of a generator, a gas turbine, and two compressor sections with fully electromagnetic suspension systems.

Reactor design characteristics and the direct closed gas-turbine power conversion cycle are major advantages of the GT-MHR nuclear power plant (NPP) compared to other plants with steam cycles, because they allow for simplification and reduce the number of required equipment items and systems (including safety systems), by completely eliminating a steam turbine power circuit from the plant.

The GT-MHR can achieve a high safety standard through inherent safety features of the plant and via the use of passive safety systems that rule out the possibility of a reactor core meltdown in any accident, including LOCA.

[1] Currently within the AREVA Group.



1 – Generator; 2 –Recuperator; 3 – Turbocompressor; 4 – Intercooler;
5 – Precooler; 6 – Control and protection assembly; 7 – Reactor core; 8 – Vessel system;
9 – Reactor shutdown cooling system

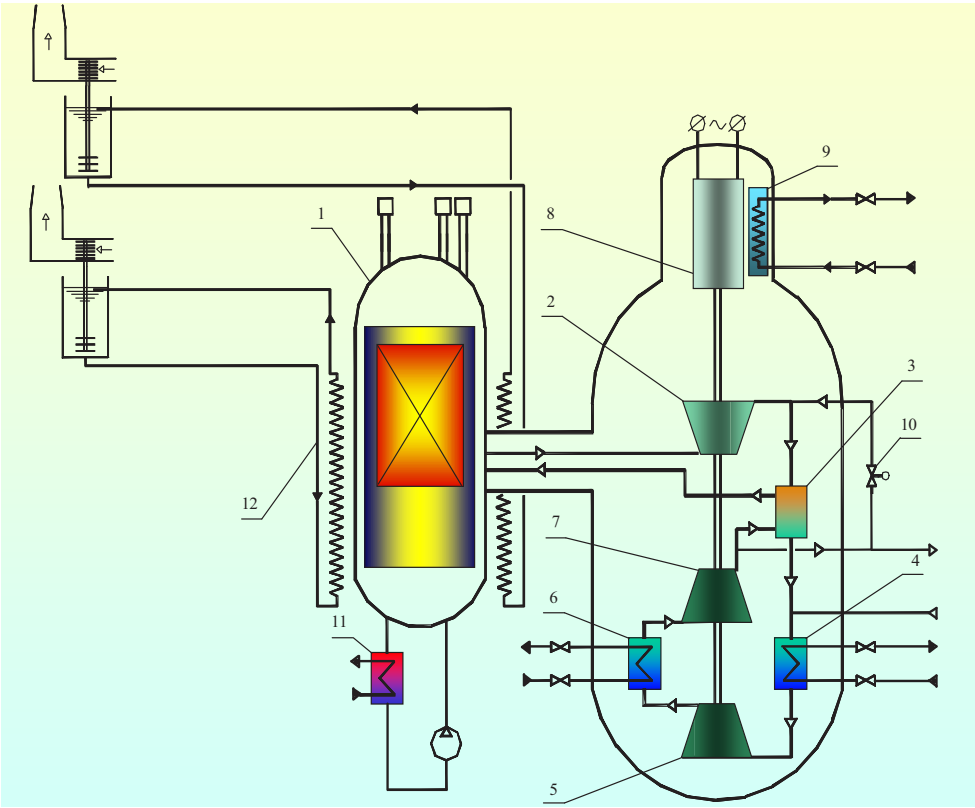
FIG. VII-1. Reactor plant.

VII–2. PASSIVE SAFETY DESIGN FEATURES OF THE GT-MHR

Safety objectives

The top level safety objective is to provide protection for the personnel, public, and environment against radiation and radioactive contamination. This main objective must be fulfilled at every stage of the reactor plant lifecycle and in all operating conditions; more specifically it is defined by the radiation and technical safety objectives.

The radiation safety objective is aimed at restricting radiation doses to personnel and the public and at limiting radioactive releases to the environment. The radiation impact of the GT-MHR NPP on personnel, the public, and the environment in normal operation and in design basis and beyond design basis accidents should be lower than the limits specified in regulatory documents and, in fact, as low as possible, taking into account economic and social factors. No emergency response measures should be necessary for the public or the environment beyond the buffer area.



1–Reactor; 2–Turbine; 3–Recuperator; 4, 6–Precooler and intercooler;
5, 7–Low and high pressure compressors; 8–Generator; 9–Cooler; 10–Bypass valve;
11–Reactor shutdown cooling system; 12–Reactor cavity cooling system

FIG.VII-2. Flow diagram of the reactor cooling system.

The technical safety objective is targeted at the prevention of accidents and at mitigation of accident consequences. This objective is met via a system of physical barriers and through a complex of measures aimed to protect these barriers and maintain their effectiveness. Effectiveness of physical barriers in accidents can be maintained through inherent reactor safety features (based on the negative feedback and natural processes), and passive safety systems.

Inherent safety features

Safety objectives for the GT-MHR are first achieved by relying on the *inherent safety features* incorporated into plant design, which are described below.

Thermal stability of the reactor core

Thermal stability of the reactor core is ensured by the use of:

— Fuel in the form of small particles with several coating layers, which can effectively retain fission products at high temperatures (up to 1600°C) and high fuel burnups (up to 70% of fissile materials for Pu fuel);
— Graphite as the structural material for the core. Graphite has a sublimation temperature of about 3000°C and, therefore, can withstand high temperatures. Graphite structures maintain their strength even at temperatures higher than those possible in accidents. This feature ensures stability of the reactor core configuration and prevents fuel redistribution over the core volume in accidents;
— Annular reactor core with a relatively low power density (6.5 MW/m^3).

TABLE VII-1. MAIN DESIGN CHARACTERISTICS

Characteristic	Value	
Thermal power	600 MW(th)	
Efficiency	47%	
Electric power	287.5 MW(e)	
Fuel	Ceramic coated particles forming compacts, loaded into prismatic blocks	
Fuel type[a]	$PuO_{1.65}$	
Fuel enrichment	~92%	
Coolant	Helium	
Moderator	Graphite	
In-vessel structures	Prismatic fuel blocks, reflectors, and core support structure are made of graphite	
	Metallic structures are made of chromium-nickel alloy	
	Service life is 60 years	
Reactor core	Annular core (hexahedral graphite blocks)	
	Core height is 8.0 m	
	Core inner diameter is ~3 m	
	Core outer diameter is ~4.8 m	
Reactor vessel	Material: chromium-molybdenum steel	
	Height is 29 m	
	Outer diameter (across flanges) is 8.2 m	
	Service life is 60 years	
Cycle	Direct closed gas turbine cycle (Brayton cycle)	
Number of circuits	1	
Neutronic characteristics	Temperature reactivity coefficient is negative	
	Burnup margin (with burnable poison rods) is 2.0 %	
	Burnable poison is erbium oxide	
Reactivity control and reactor safety systems	Control rods with boron carbide absorbing elements are located in the reflector; they are used during normal operation and hot shutdown	
	Control rods with boron carbide absorbing elements are located in the core; they are used for scram	
	Reactor safety system based on boron carbide spheres	
Thermal-hydraulic characteristics	Core inlet/outlet temperature, °C	490 / 850
	Core inlet/outlet pressure, MPa	7.15 / 7.1
	Coolant flow rate through the core, kg/s	318.1
	Cycle total compression ratio	2.86
	Turbine inlet/outlet temperature, °C	848 / 518
	Turbine inlet/outlet pressure, MPa	7.02 / 2.66
	Inlet/outlet temperature of the recuperator hot side, °C	506 / 126
	Inlet/outlet temperature of the recuperator cold side, °C	105 / 490
	Fuel temperature during normal operation, °C	1250
	Fuel temperature in design basis accidents, °C	Up to 1600

[a] Fuel characteristics presented in this table correspond to the GT-MHR design developed in the Russian Federation for plutonium utilization (for more details about fuel designs see Annex XV of [VII-1])

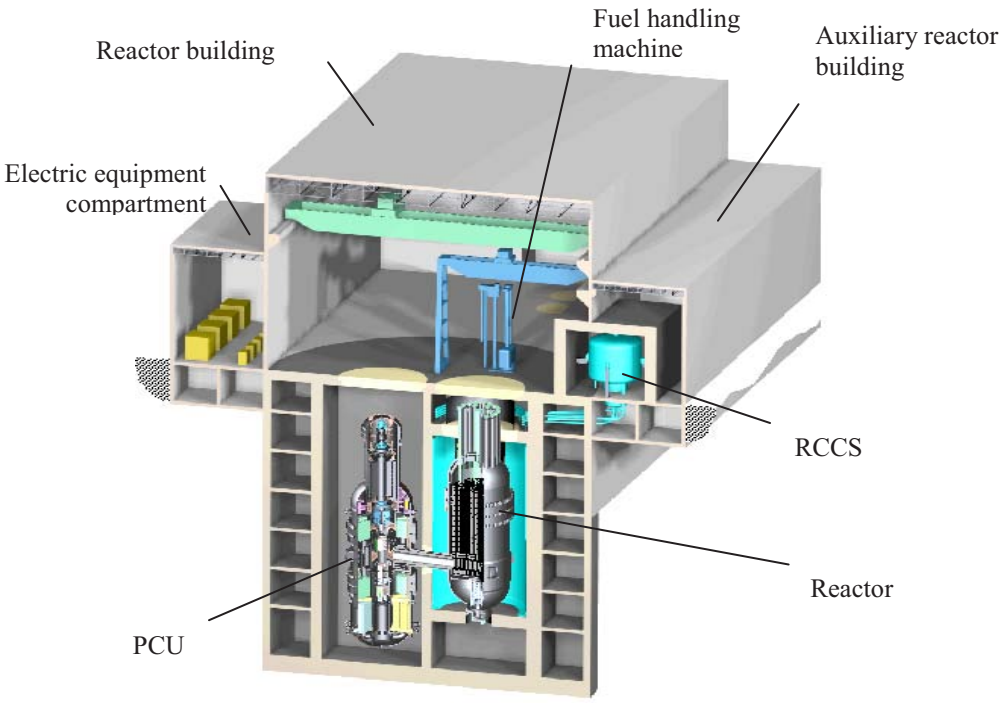


FIG. VII-3. Reactor building.

Neutronic stability of the reactor core

Neutronic stability of the reactor core is ensured by:

— High degree of reactor power self-control and self-limitation owing to negative feedback on reactor core temperature and reactor power;
— Self-shutdown capability of the reactor core at temperatures below the minimum level allowable from the viewpoint of reliable operation of the fuel particles;
— The fact that the coolant has no impact on the neutron balance because of 'zero' neutron absorption and scattering cross-sections. The latter prevents an uncontrolled increase of reactor power during variations in coolant density as well as under coolant loss in accidents.

Chemical stability

Chemical stability of the plant is ensured by the helium coolant being:

— Chemically inert;
— Not prone to phase changes, which rules out sharp variations of heat removal conditions in the core.

Structural stability

Structural stability of the plant is attributed to:

— No large diameter pipelines used in the primary circuit;
— No steam generator (with associated complexities related to operation using a two phase coolant); no large diameter steam lines, and no steam condensing circuit existing in the plant;
— By-design prevention of large scale depressurization of vessel system components.

Dynamic stability

Dynamic stability of the reactor core is secured by:

— Core cooling by natural processes; prevention of a core meltdown in all credible accidents including primary circuit depressurization without compensation for coolant loss;
— Plant capability to switch to a safe state without control actions if all power supply sources are lost;
— Plant capability to maintain such a safe state over a long time period (dozens of hours) in hypothetical critical situations without emergency protection (EP) actuation and with no organized heat removal from the reactor.

Activity localization

Passive localization or radioactivity is provided mainly by containment designed for the retention of helium-air fluid during accidents with primary circuit depressurization. The containment is also designed for external loads, which may apply to seismic impacts, aircraft crash, air shock waves, etc. Radioactivity release from the containment into the environment is determined by the containment leakage level, which is about 1% of the volume per day at an emergency pressure of 0.5 MPa. Results of safety analyses carried out at the preliminary design stage are being used to elaborate technical measures in an effort to reduce the requirements of containment characteristics.

General approach for safety system design

In addition to the inherent (self-protection) features of the reactor, the GT-MHR plant incorporates safety systems based on the following principles:

(1) Simplicity of both system operation algorithm and design;
(2) Usage of natural processes for safety system operation under accident conditions;
(3) Redundancy, physical separation and independence of system channels;
(4) Stability in the case of internal and external impacts and malfunctions caused by accident conditions;
(5) Continuous or periodical diagnosis of system conditions;
(6) Conservative approach used in design, applied to the list of initiating events, to accident scenarios, and for the selection of definitive parameters and design margins.

All safety systems are designed with two channels. Regulatory safety requirements are met through compliance with both deterministic and probabilistic criteria, and are secured by exclusion of active elements in a channel or by applying the required redundancy of such active elements inside a channel, as well as via the use of the normal operation systems to prevent design basis accidents.

Passive safety systems

A summary of passive systems in the GT-MHR is given below, in line with the classification suggested by IAEA-TECDOC-626 [VII-2].

Category A systems

Category A passive systems [VII-2], which are certain static structures with no moveable mechanical parts, liquids or energy sources are as follows:

— Fuel particles with multilayer coatings;
— Annular graphite reactor core and reflector;
— Reactor vessel system and power conversion unit (PCU) vessel;
— Leaktight primary circuit;
— The containment.

Certain attributes of the Category A passive systems could also be classified as inherent or 'by-design' safety features. Their role in the overall safety design of the GT-MHR is highlighted at the beginning of this section.

Category B systems

Category B passive systems [VII-2], which incorporate natural convection driven liquids but no actuation devices and no moving mechanical parts or energy sources, are represented by the reactor cavity cooling system (RCCS), see Fig. VII-1.

If it is impossible to use systems that remove heat through the PCU and the shutdown cooling system (SCS), emergency heat removal is carried out by the RCCS. The RCCS includes two independent passive cooling channels of similar efficiency. Each RCCS channel consists of a water circuit with a surface cooler and a water tank, a heat tube circuit with evaporating sections arranged in the tank, an air circuit formed by special air ducts with condensation sections in heat tubes, and exhaust tubes. Heat from the reactor core is removed from the reactor vessel to the RCCS surface cooler, the heat tubes and then to atmospheric air due to natural processes of heat conduction, radiation and convection. Circulation of water and air in RCCS channels is driven by natural convection.

The RCCS functions continuously during normal operation and in accidents, i.e., it is continuously available, ruling out the need for operator or control system actions when switching over from normal operation mode to emergency heat removal. Passive RCCS removes residual heat released during a LOCA. In such a case, reactor core cooling does not require compensation of coolant loss.

The RCCS is a normal operation system, which also shoulders the functions of a safety system. It is a safety grade system.

Category C systems

Category C passive systems [VII-2], which incorporate direct action actuation devices requiring no energy sources, are represented by the primary circuit overpressure protection system.

The primary circuit overpressure protection system protects the reactor unit, including the PCU, and other primary circuit equipment items, from pressure increase above allowable limits. The primary circuit overpressure protection system includes:

— Two overpressure protection trains;
— Pipelines;
— Primary measuring transducers.

Each overpressure protection train is a passive device because they are actuated upon direct action of the working fluid on a sensitive element. The system working fluid is a primary circuit coolant; highly pure helium. Overpressure protection trains are arranged in the PCU cavity.

The primary circuit overpressure protection system is a safety grade system.

Category D systems

Category D passive systems [VII-2], which incorporate 'passive execution/active initiation' type features, include:

— Bypass valve system of the turbomachine control and protection system (TM CPS);
— Emergency reactor shutdown system;
— Control systems;
— Localizing valves.

The bypass valve system of the TM CPS fulfils the following functions:

— Prevention of turbomachine over speed during loss of external load;
— Turbomachine emergency shutdown during failure of the turbomachine or the PCU equipment, and in blackouts;
— Rapid decrease of electric power in reactor plant normal operation mode.

When the bypass valves open, a portion of primary coolant flow bypasses the reactor core and the turbine, thus decreasing electric power generated by the reactor plant, triggered by a decrease in the helium flow rate and expansion ratio in the turbine, or an increase of the flow rate and power in the compressors, or an increase in the power removed in the precooler and intercooler.

The TM CPS bypass valve system incorporates:

— Four bypass shut-off and control valves DN300;
— Electrically driven shut-off valves;
— Pipelines.

The adopted redundancy scheme of bypass shut-off and control valves is based on a single failure principle and allows the reactor plant power operation until shutdown and maintenance; all based on one failed valve.

The bypass valve system is a normal operation system, which shoulders the functions of a safety system. It is a safety grade system.

Two independent reactivity control systems based on different operation principles are used to execute reactor emergency shutdown and maintenance in a sub-critical state; these systems are:

(1) Electromechanical reactivity control system based on control rods moved into reactor core channels and the inner and outer reflectors;
(2) Reserve shutdown system (RSS) based on spherical absorbing elements that fill in channels in the fuel assembly stack over the whole height of a fuel assembly.

The electromechanical reactivity control system consists of 54 control rods with individual drives and provides for reactor emergency shutdown and maintenance in a subcritical state, taking into account cooling and unpoisoning, under a one (most effective) rod stuck condition. Control rods are inserted into the core driven by gravity, from any position and without the use of external power sources, in the case of de-energization actuated by control system signals. The electromechanical reactivity control system is a normal operation system, which shoulders the functions of a safety system. It is a safety grade system.

Reactor emergency shutdown signals are generated automatically according to parameters of different physical nature or via pressing corresponding buttons in the main and standby control rooms.

The RSS includes 18 RSS drives with individual hoppers containing absorbing elements, and 18 channels in the reactor core stack into which boric absorbing spheres are inserted. Each RSS channel may be filled individually. The RSS is intended to shut down the reactor and keep it in an unpoisoned cold subcritical state in case of a failure of the control rod based system, taking into account a postulated single failure in the system.

The RSS is started through a power supply to the RSS drive motors and through opening of the gates of hoppers containing absorbing elements. The RSS drives are powered by the emergency power supply system, which uses two emergency diesel generators. The absorbing boric spheres are inserted by gravity.

The design and materials of absorbing elements exclude primary coolant contamination by the absorber. RSS fulfils the functions of a protective safety system.

The RSS is a safety grade system.

GT-MHR NPP control and support safety systems (CSS) are intended to actuate equipment, mechanisms and valves, localizing and support safety systems in preaccidental conditions and in accidents; to monitor their operation; and generate control commands for the equipment of normal operation systems used in safety provision algorithms.

The CSS are based on the principles of redundancy, physical and functional separation, and safe failure.

The CSS include two independent three channel sets of equipment with emergency signal processing logic '2 out of 3', implemented in each set. Each set is capable of carrying out the safety functions in full. CSS sets are physically separated so that internal (fire, etc.) or external (aircraft crash, etc.) impacts do not lead to a control system failure, and inability to perform the required functions.

The CSS provide automated and remote control of equipment of safety systems from the independent main and standby control rooms. Principal technical features are selected using the concept of a safe failure – blackouts, short circuits, or phase breaks start emergency signals in the channels or initiate safety actions directly. The CSS are safety grade.

Redundant localizing valves are used to prevent loss of coolant at depressurization of auxiliary systems of the primary circuit and to localize inter-circuit leaks of coolant from the primary to the adjacent circuits.

Air-driven normally closed bellows shut-off valves are used for localization. During normal operation of the plant the shut-off valves are open. Air to the pneumatic drives of the shut-off valves is supplied by electromagnetic control air distributors. Shut-off valves are actuated by the energy of a compressed spring when there is a loss of power supply to air distributor electromagnets or air release from the pneumatic drives of the valves. The valves and air distributors can be controlled automatically (actuated upon control system signals), remotely, or manually (by a manual drive amending the pneumatic drive).

Localizing valves fulfil the function of a localizing safety system. The localizing valves are safety grade.

Active safety systems

The GT-MHR design has no dedicated active safety systems. Active systems of normal operation, such as the power control unit (PCU) and the shutdown cooling system (SCS), are used for safety purposes. These systems remove heat under abnormal operation conditions, during design basis accidents (DBA) and in beyond design basis accidents (BDBA).

VII–3. ROLE OF PASSIVE SAFETY DESIGN FEATURES IN DEFENCE IN DEPTH

Defence in depth concept

Safety of plant personnel and the population living near a NPP site is ensured by consecutive implementation of the defence in depth concept in plant design. This concept stipulates the application of several barriers to the release of ionizing and radioactive substances into the environment, as well as application of technical features and administrative measures to protect and maintain the effectiveness of barriers and to protect personnel, the population and the environment.

Effectiveness of the protective barriers under accident conditions is maintained mainly through inherent reactor (self-protection) features based on negative feedback and natural processes, and due to the use of passive safety systems.

Physical barriers for the GT-MHR are:

— Coated fuel particles;
— Fuel compacts;
— Fuel assemblies;
— Leaktight primary pressure boundary (vessel system);
— The containment.

The reliable retention of fission products within fuel assemblies is ensured by:

(1) The design of coated particle fuel and fuel assemblies based on available experience in fuel element design, testing and operation. The GT-MHR utilizes ceramic fuel in the form of 200 μm spherical particles with multilayer pyrocarbon and silicon carbide coatings (coated fuel particles), which are dispersed in the graphite matrix (fuel compact). Silicon carbide is the main barrier preventing a release of gaseous and

volatile fission products. Fuel compacts and fuel assemblies are made of graphite, which provides the effective retention of solid fission products;
(2) Design features to prevent fuel overheating under abnormal operation conditions;
(3) Design features to provide a large temperature margin between the operation limit and the safe operation limit; crisis free heat removal from the fuel elements during normal and abnormal operation, including design basis accidents;
(4) Design features ensuring that fuel temperature does not exceed 1600°C in any accident involving failure of heat removal from the reactor, including the failure of all 'active' means of reactor shutdown and cooling. In this way, the effectiveness of the main protective barrier (protective coating on fuel kernels limiting fission product release beyond the boundaries of coated fuel particles) is maintained.

Primary circuit integrity is secured by:

(1) Realization of prerequisites and conditions required to exclude brittle fracturing of the reactor vessel; these prerequisites include keeping the fast neutron fluence on the reactor vessel and the vessel temperature below allowable limits;
(2) High thermal inertia of the reactor, resulting in slow variation of reactor parameters;
(3) Accessibility of the base metal of welded joints for the purpose of diagnostics of the primary pressure boundary;
(4) Primary circuit in the premises designed to withstand external impacts, such as earthquakes, shock waves, aircraft crash, etc.;
(5) Provision of a sufficient design strength margin for all components of vessel equipment. For example, the vessel system retains its performance characteristics in all possible operation modes, including accidents;
(6) Seismic design of the primary circuit equipment;
(7) The overpressure protection system prevents overpressure in the primary circuit regardless of the condition of electric control circuits and of personnel actions.

Retention of radioactive fluids at primary circuit leaks is provided within the:

(1) Containment;
(2) Leaktight sections of the primary circuit are limited by redundant fast response isolation valves installed inside the containment;
(3) Isolation sections of the PCU and SCS cooling water systems are limited by redundant fast response isolation valves installed inside the containment.

Retention of radioactive products within the containment is achieved through:

(1) Arrangement of reactor plant equipment in a ferroconcrete leaktight containment;
(2) Keeping containment pressure lower than ambient pressure during normal operation;
(3) A system of leaktight hatches and gates in the containment;
(4) Containment resistance to impacts of external natural and human induced events, provided with a design strength margin;
(5) A system of containment radioactivity filtration during normal operation;
(6) Isolation of containment leaktight volume from groundwaters;
(7) Containment diagnostics systems (continuous monitoring for leaktightness).

Ingress of radioactive products to the cooling circuits connected with the environment is prevented through the use of intermediate circuits (+PCU and SCS cooling water circuits).

Some major highlights of passive safety design features in the GT-MHR, structured in accordance with the various levels of defence in depth [VII-3, VII-4], are related below.

Level 1: Prevention of abnormal operation and failure

The contributions to this defence in depth level generically come from:

— Proper evaluation and selection of a suitable NPP site;
— Design development based on a conservative approach with strong reliance on inherent safety features and preferential application of passive safety systems;
— Quality assurance of NPP systems and components; quality assurance of all steps in NPP design development and project realization;
— Compliance of NPP operations with the requirements of regulatory documents, technical regulations, and operation manuals;
— Maintenance of operability of safety related structures, systems and components with early detection of defects; application of preventive measures; and timely replacement of expired equipment; effective documentation of the output of all inspection and maintenance activities;
— Provision of required NPP staff qualifications, with a focus on operating personnel, who are to take action during normal and abnormal operation, including pre-accidental conditions and accidents; development of a safety culture.

The GT-MHR plant is being designed in compliance with a quality assurance programme. All design features and parameters incorporate required design margins.

In addition to the generic measures contributing to Level 1 of defence in depth, the GTMHR incorporates certain design features directly contributing to this level; they are:

— Direct closed gas turbine cycle, which provides considerable simplification, minimizes required NPP equipment and systems, and excludes the steam-turbine power circuit;
— TRISO coated particle fuel capable of reliable operation at high temperatures and burnup levels;
— Helium coolant, which offers good heat transfer properties, does not dissociate, is easily activated and chemically inert. Neutronic properties of helium exclude reactor power growth at coolant density variation;
— Large thermal inertia of the reactor core, large temperature margin between the operation limit and safe operation limit; slow temperature variation during power variation in a manoeuvring mode.

Level 2: Control of abnormal operation and detection of failure

The contributions to this level generically come from:

— Timely detection of defects; timely preventive measures; and on-time equipment replacement;
— Detection and correction of deviations from normal operation;
— Management of abnormal operation occurrences;
— Prevention of the progression of initiating events into design basis accidents using normal operation and safety systems.

The GT-MHR design provides for timely detection and correction of deviations from normal operation caused by malfunctions in external power grids, control systems, and by partial or complete inoperability of the equipment of redundant normal operation systems (pumps, heat exchangers, valves, etc.), as well as for other reasons.

Management of abnormal operation is secured by:

— Self-control properties of the reactor, including a large temperature margin between the operation limit and safe operation limit;
— Neutronic properties of the reactor, including negative feedback on reactor temperature and power increase;
— The use of reliable automated control systems with a self-diagnostic capability;
— The use of state of the art operator information support systems.

Stable operation of the reactor plant is provided in case of individual equipment failure such as failure of the PCU cooler module, of the generator gas cooler module, of the SCS heat exchanger section, or of the SCS gas circulator cooler section.

The allowable time for detection and correction of deviations, as well as the allowable power level at various deviations, is determined by safe operation conditions defined by the safety design features of the GT-MHR, such as the use of TRISO coated particle fuel, helium coolant, and graphite as a structural material, etc.

Level 3: Control of accidents within the design basis

The objectives of this defence in depth level are:

— Prevention of progression of design basis accidents into beyond design basis accidents, executed through the use of safety systems;
— Mitigation of those accident consequences that could not be prevented by localization of released radioactive substances.

In the GT-MHR, effective control of design basis accidents is ensured by:

— Strong reliance on the inherent safety features, such as negative reactivity feedback and natural processes;
— Preferential use of passive safety systems;
— Conservative approach used in the design of protective barriers and safety systems;
— Residual heat removal from the reactor in accidents, carried out without external power sources, control signals or human intervention;
— The limitation of radiation consequences of accidents via localization of released radioactive substances and radiation.

Provisions for effective control of design basis accidents are incorporated in the GT-MHR design. The key design components for this are safety systems and localization safety systems. Support and control systems are provided too; however, their role is not as critical as in existing NPPs, due to broader use of inherent safety features and passive safety systems in the GT-MHR.

According to redundancy and diversity principles, two independent systems are provided to shut down the reactor and keep it in a safe subcritical state.

Heat removal systems include a passive heat removal system, the RCCS, which comprises two independent cooling channels of equal efficiency.

During primary circuit depressurization, reactor core cooling does not require compensation of coolant loss. Radioactive products are localized by the containment system and by fast response shut-off valves.

Level 4: Control of severe plant conditions, including prevention of accident progression and mitigation of consequences of severe accidents

The objectives of this defence in depth level are:

— Prevention of beyond design basis accidents and mitigation of their consequences;
— Protection of the leaktight boundary against destruction during beyond design basis accidents and maintenance of its operability;
— Return of the NPP to a controllable condition when the chain reaction of fission is suppressed and continuous cooling of the nuclear fuel and retention of radioactive substances within the established boundaries are provided.

The GT-MHR plant design provides for the means of beyond design basis accident management such as:

— Prevention (decrease) of radioactive product release into the environment, which is achieved through incorporated physical barriers;

— Ensuring that final stable and safe conditions are reached when the chain reaction of fission is suppressed and when continuous cooling of nuclear fuel and retention of radioactive substances within established boundaries are provided.

In the case of failure of safety components and systems, management of beyond design basis accidents can be executed by personnel. This requirement is fulfilled by:

— Reactor design safety features, which limit the progression of accidents;
— The characteristics of passive safety systems;
— The capabilities of normal operation systems;
— Large time margins for implementation of accident management measures.

High heat storage capacity of the reactor core and high acceptable temperatures of the fuel and graphite allow for passive shutdown cooling of the reactor in accidents, including LOCA (heat removal from the reactor vessel by radiation, conduction and convection), while maintaining fuel and core temperatures within allowable limits.

Safety for the population in beyond design basis accidents is secured by specific features of the reactor design, without on-line intervention of personnel required.

The time margin available for personnel to take action in an accident management scenario varies from several dozens of hours to several days from the moment of accident initiation.

Level 5: Mitigation of radiological consequences of significant release of radioactive materials

The objective of this level is generically achieved by preparation and implementation (if needed) of plans for response measures within and beyond the NPP site.

Analysis of radiological consequences of beyond design basis accidents (including the most severe accident with primary circuit depressurization accompanied by the actuation failure of shutdown systems, NPP blackout, and long term loss of all PCU and SCS active heat removal systems) performed at the GT-MHR plant design development stage, showed that no accident prevention measures are required either within or beyond the NPP site.

VII–4. ACCEPTANCE CRITERIA FOR DESIGN BASIS AND BEYOND DESIGN BASIS ACCIDENTS

VII–4.1. List of abnormal operation occurrences, design basis and beyond design basis accidents

Selection of abnormal operation occurrences

Abnormal operation occurrences include: failures of reactor plant equipment and systems accompanied by the actuation of warning alarms, process interlocks and protection systems of individual equipment; personnel actions to recover normal operation conditions by electric load decrease to a house-load level; by actuation of the warning protection, by unscheduled shutdowns of the reactor plant, and by actuation of shutdown (emergency protection) systems with the emergency shutdown of the reactor (except for accidents with primary circuit depressurization). This category also includes operation modes with disruption of the normal operation schedule caused by personnel errors and failures of control and monitoring systems, including the unscheduled switch-on of individual reactor plant equipment and systems, and faulty actuation of emergency protection (shutdown) systems.

Depending on the type of failure which resulted in actuation of the reactor emergency protection system, the emergency cooling of a shutdown reactor is carried out in an operable condition by the heat removal systems — PCU, SCS, or RCCS.

Analysis of these modes of operation is performed using the same approach as for design basis accidents, taking into account the superposition of initiating events and single failures of safety system components and additional failures of components that affect operability of heat removal systems.

Single failures of GT-MHR safety systems are failures related to the sticking of a single most effective control rod during operation of the reactor emergency protection system or to failure of a single bypass shut-off control valve to open during operation of turbomachine overspeed protection or a turbomachine emergency shutdown. In addition to this, it is assumed that in the initial condition of the reactor plant one bypass valve has been disconnected on the inlet and outlet side by shut-off valves, for the purpose of further repair.

Additional failures are those of normal operation systems, including SCS failure to actuate upon request, e.g., due to an opening failure of the gas circulator shut-off valve or a start failure of the SCS unit gas circulator.

Emergency cooling of a shutdown reactor by the RCCS is a long lasting process; therefore, its progress is analyzed taking into consideration a potential restart of any of the active channels for heat removal from the reactor core through the PCU or the SCS after their operability is recovered.

Selection of design basis accidents

An analysis of design basis accidents considers the superposition of an initiating event and a failure (that does not depend on the initiating event) of any component of the active or passive safety system with mechanical moving parts, or an event independent personnel error.

The used definition of single failure is given in the previous subsection.

Analysis of design basis accidents in the GT-MHR also takes into account a superposition of initiating events and additional failures that affect the conditions of decay heat removal from a shutdown reactor.

Additional failures are those related to loss of the external power supply (blackout) or to a failure of the SCS to actuate upon request, which leads to reactor shutdown cooling by the RCCS.

Emergency cooling of a shutdown reactor by the RCCS is a long process accompanied by considerable temperature increases of the primary coolant, fuel, reactor core graphite structures, in-vessel metal structures, and the reactor vessel. At primary circuit depressurization and air ingress to the reactor core, such conditions of a shutdown reactor may result in considerable oxidation of the graphite blocks in the reactor core. Therefore, the progress of design basis accidents with a reactor shutdown cooling by the RCCS is analyzed considering the potential restart of any active channel for heat removal from the reactor core through the PCU and the SCS after their operability is recovered.

Selection of the beyond design basis accidents

Analysis of the beyond design basis accidents is performed taking into account a superposition of the initiating events (including those not considered in design basis accidents) and the failure of safety systems on top of a single failure, as well as the additional failure of normal operation systems, and their possible combinations that may affect the propagation of accidents.

Additional failures affecting emergency heat removal from the reactor core include a blackout that leads to a reactor shutdown cooling by the RCCS.

In addition to this, the list of beyond design basis accidents for the GT-MHR includes the postulated simultaneous failure of all heat removal systems – the PCU, the SCS, and the RCCS. This beyond design basis accident is considered in the design to derive the maximum time margin for personnel to take accident management actions aimed at preventing the violation of safe operation limits for fuel temperature in the reactor core, for temperatures of in-vessel metal structures, the reactor vessel, and the reactor cavity concrete.

Failure of pneumatic double isolation valves to close (which leads to bypassing of the containment) is considered an additional failure, which affects the localization (isolation) function at primary circuit depressurization.

Analysis of the above mentioned beyond design basis accidents is performed under an NPP blackout, which results in the emergency cooling of a shutdown reactor by the RCCS.

Failure of the reactor emergency protection system is considered an additional failure which affects the reactor emergency shutdown function. Emergency protection failure in the GT-MHR means failure of all control rods to be inserted into the reactor core upon a signal by the reactor control system.

Beyond design basis accidents with actuation failure of the reactor emergency protection system are analyzed taking into account a superposition of initiating events and additional failures that affect conditions of

emergency heat removal from the reactor, i.e., a NPP blackout and SCS failure to actuate upon request. An NPP blackout leads to a loss of PCU operability and requires SCS actuation. An SCS failure to actuate upon request leads to heat removal from the reactor by the RCCS.

In addition to this, the progression of beyond design basis accidents with primary circuit depressurization and emergency heat removal by the RCCS, including beyond design basis accidents with actuation failure of the reactor emergency protection system, is analyzed under an assumption that it is impossible to restart all active channels for heat removal from the reactor core – the PCU and the SCS – during the entire course of such an accident.

List of abnormal operational occurrences and pre-accidental conditions

The operation modes of the GT-MHR categorized as abnormal operation occurrences or pre-accidental conditions are listed below.

(1) Modes with reactivity and power distribution variations*:*
  1.1. Inadvertent removal of one or several of the most effective control rods from the reactor core;
  1.2. Inadvertent insertion of one or several of the most effective control rods into the reactor core;
  1.3. Inadvertent insertion of absorbing elements from the reactor shutdown system hoppers into the reactor core;
  1.4. Incorrect loading of a fuel assembly into the reactor core and the operation of such a fuel assembly.

(2) Modes with a decrease in heat removal from the primary circuit*:*
  2.1. Complete stop of water circulation through PCU heat exchangers;
  2.2. Ruptures of PCU cooling water system pipelines within and beyond the containment;
  2.3. SCS failures in standby mode (ceasing of water circulation and ruptures of SCS cooling water system pipelines within the containment).

(3) Modes with a decrease in coolant flow rate through the reactor core:
  3.1. Failure of a turbomachine or failure of individual turbomachine components which require the emergency shutdown of a turbomachine;
  3.2. Inadvertent opening of the bypass shut-off and control valves of the control and protection system of the turbomachine;
  3.3. Increase of bypass flows in the primary coolant circulation system due to inadvertent opening of valves or due to depressurization of in-vessel components.

(4) Modes with inter-circuit depressurization:
  4.1. Inter-circuit depressurization involving the primary circuit and circuits of the PCU and SCS cooling water systems.

(5) Modes with loss of power supply:
  5.1. NPP blackout — loss of normal (main and backup) power supply for the system's own needs with a loss of the external load of the generator.

(6) Modes with abnormal refuelling and nuclear fuel handling:
  6.1. Inadvertent withdrawal of a control rod during refuelling;
  6.2. Failure of heat removal from the reactor core during refuelling;
  6.3. Failure of the drum of spent fuel assemblies to cool;
  6.4. Drop of a fuel assembly during refuelling (into the reactor or into the drum of spent fuel assemblies);
  6.5. Drop of a fuel assembly transportation container during refuelling.

(7) Modes with external impacts:
  7.1. Design basis or maximum design basis earthquake;
  7.2. Impact of air shock wave;
  7.3. Aircraft crash.

List of design basis accidents

The initiating events of design basis accidents for the GT-MHR are categorized in brief below.

(1) Accidents with primary circuit depressurization:
  1.1. Primary circuit depressurization due to a loss of leaktightness or the guillotine break of a primary circuit pipeline with a coolant leak into the containment and further air ingress to the primary circuit:
    — Rupture of small lines (with equivalent outer diameter of less than or equal to 30 mm);
    — Rupture of a bypass pipeline in the control and protection system of the turbomachine (the equivalent outer diameter is 250 mm);
    — Depressurization of a standpipe of the reactor control and protection system.
  1.2. Rupture of the pipelines of the helium transportation and storage system beyond the containment.
(2) Accidents with abnormal fuel assembly cooling conditions:
  2.1. Partial clogging of the fuel assembly flow area by a fuel assembly fragment.
(3) Accidents with disruption of normal refuelling and nuclear fuel handling modes:
  3.1. Dropping of heavy objects and damage of fuel assemblies during refuelling;
  3.2. Depressurization of fuel assembly handling equipment;
  3.3. Fuel assembly damage during refuelling.

List of beyond design basis accidents

The initiating events/combinations of events for beyond design basis accidents regarding the GT-MHR are categorized in brief below.

(1) Beyond design basis accidents with loss of power supply sources:
  1.1. Blackout;
  1.2. Blackout with a complete RCCS failure;
  1.3. Blackout with a failure of the actuation of the reactor emergency protection (shutdown) system (anticipated transient without scram — ATWS).
(2) Beyond design basis accidents with reactivity variation (taking into account additional failures):
  2.1. Inadvertent withdrawal of several of the most effective control rods from the reactor core with an actuation failure of the reactor emergency protection system (ATWS).
(3) Beyond design basis accidents with a decrease of the coolant flow rate through the reactor core (taking into account additional failures):
  3.1. Failure of the turbomachine or failure of individual turbomachine components, requiring an emergency shutdown of the turbomachine, accompanied by an actuation failure of the reactor emergency protection system (ATWS).
(4) Beyond design basis accidents with primary circuit leakage (taking into account additional failures):
  4.1. Primary circuit depressurization with a blackout and an ingress of a considerable amount of air into the primary circuit (guillotine break of a standpipe of the control and protection system);
  4.2. Primary circuit depressurization with failure of the reactor protection system to actuate (ATWS), a blackout, and the ingress of a considerable amount of air into the primary circuit (guillotine break of a standpipe of the control and protection system);
  4.3. Rupture of the transportation and storage system helium pipelines beyond the containment, followed by a failure of the system of activity localization within the primary circuit and by a blackout;
  4.4. Inter-circuit depressurization between the primary circuit and the PCU or the SCS cooling water circuits, followed by a failure of the isolation systems and a blackout, and by ingress of a considerable amount of water into the primary circuit.

VII–4.2. Acceptance criteria

The acceptance criteria used for NPP designs with modular high temperature gas cooled reactors (HTGR) are as follows:

— Radiation safety criteria, which specify allowable radiation doses for personnel and population during normal plant operation and in the case of accidents;
— Probabilistic safety criteria, which establish the allowable overall probability of severe beyond design basis accidents and the probability of maximum reactivity releases during such accidents.

Radiation safety criteria

Radiation safety criteria are the radiation dose limits for NPP personnel and the population at the NPP site during normal operation and in the design basis and beyond design basis accidents.

The following dose limits are established for the population and for NPP personnel:

— The effective individual radiation dose for the population during normal operation should not exceed 20 μSv per year;
— The effective individual radiation dose for the population at the boundary of the buffer area during design basis and beyond design basis accidents should not exceed 5 mSv for the entire body during the first year after the accident. In this case, special protection measures for the population are not required;
— For NPP personnel working directly with radiation sources, the effective individual dose during normal operation should not exceed 20 mSv per year on average during any successive five years, with the absolute maximum being 50 mSv per year.

When designing the power unit – its structures and means of radiation protection and isolation (localization) – measures are taken to reduce radiation dose rates in NPP rooms, radionuclide releases to the environment, and radiation doses to personnel, and to keep these radiation parameters as low as possible in line with the ALARA concept.

Radiation safety criteria are met when the design limits for the following parameters are not exceeded:

— Level of primary coolant activity defined by fission products;
— Releases of radioactive substance into the atmosphere through the exhaust pipe;
— Radiation levels in NPP rooms.

Radiation safety criteria are fulfilled owing to consistent implementation of the defence in depth concept, which is based on application of several barriers to the release of ionizing and radioactive substances into the environment, and owing to application of technical and administrative measures to protect and maintain the effectiveness of these barriers.

Probabilistic safety criteria

Probabilistic safety criteria specify the basic safety indices of an NPP in probabilistic terms as the following:

(a) To avoid the need for population evacuation beyond plant boundaries established by the regulatory requirements regarding the location of NPPs, it is necessary to target a probable maximum release of no more than 10^{-7} per reactor per year; the value of this maximum release, established by the same regulatory documents, corresponds to radiation dose limits for the population in the case of beyond design basis accidents;
(b) The overall probability of severe beyond design basis accidents (evaluated on the basis of probabilistic safety analysis) should be targeted not to exceed 10^{-5} per reactor per year.

Design limits

The GT-MHR NPP project establishes operation limits and conditions, safe operation limits and conditions, and design limits for abnormal operation conditions, including design basis accidents. Maximum fuel temperature, which shall not exceed 1600ºC, is considered one of the most important design limits for pre-accidental situations and design basis accidents.

The operation limits for process parameters and characteristics of reactor plant equipment are specified based upon:

— Analytical results for reactor plant parameters and equipment operating conditions during normal operation, taking into account measurement errors;
— The evaluation of a control range of reactor plant process parameters during normal operation with evaluation of the accuracy of keeping these parameters within the control range, taking into account errors of the measurement and automation means.

Presently, the operation limits and the safe operation limits for fuel elements of the GT-MHR have not been established.

Safe operation limits for the basic process parameters are established to protect physical barriers against damages during abnormal operation. Barriers are protected by the safety systems, which have actuation set points assigned with some margin relative to safe operation limits or equal to them.

The range of safe operation limits corresponds to the list of plant process parameters according to which protection of the plant is provided. For the GT-MHR, this list includes:

— Reactor neutron (thermal) power;
— Helium pressure in the reactor;
— Containment pressure;
— PCU cooling water system pressure;
— Turbomachine rotor speed;
— Coolant temperature at the reactor outlet;
— Coolant temperature at the low pressure compressor inlet;
— Coolant temperature at the high pressure compressor inlet;
— Activity of the primary coolant.

The operation limits and safe operation limits for process parameters and reactor plant equipment characteristics, established as indicated above, are given in Tables VII-2 and VII-3. Design limits adopted for the analysis of design basis accidents are given in Table VII-4.

TABLE VII-2. OPERATION LIMITS AND SAFE OPERATION LIMITS FOR PROCESS PARAMETERS

Process parameter	Value	
	Operation limit	Safe operation limit
Reactor power, MW(th)	620	660
Primary coolant temperature, °C:		
– At the reactor inlet	500	Not established
– At the reactor outlet	870	890
Helium pressure in the reactor, MPa	7.5	$7.5^{+0.5}_{-1.4}$
Primary coolant activity, Bq/l	1.5×10^7	3.0×10^7
Turbomachine rotor speed, rpm	3180	3300
Containment fluid pressure, MPa	Vacuum not less than 50 kPa relative to the environment	0.15
PCU cooling water pressure, MPa	1.1	$1.0^{-0.5}_{+0.2}$

TABLE VII-3. OPERATION LIMITS FOR THE EQUIPMENT

Equipment	Operation limits	
	Temperature, °C	Pressure, MPa
Reactor vessel	440	7.5
Lower support plate	500	Not established
Reactor core barrel	500	Not established
Upper restricting device	550	Not established
Fuel assembly	1300	Not established
Units of:		
– Replaceable side reflector	800	Not established
– Permanent side reflector	500	Not established
– Central reflector	1200	Not established
– Upper reflector	500	Not established
Control and protection system (CPS) rods	700	Not established
CPS standpipe casing	Not established	7.5
Shutdown cooling system (SCS) unit casing	Not established	7.5
Tube system of the SCS heat exchanger	Not established	7.5
Power conversion unit (PCU) vessel	140	7.5
Connecting vessel:		
– Cold gas duct	500	7.5
– Hot gas duct	870	7.5

TABLE VII-4. DESIGN LIMITS ADOPTED FOR THE ANALYSIS OF DESIGN BASIS ACCIDENTS

Barrier	Safety criteria	Note
Fuel	Maximum temperature of coated fuel particles shall not exceed 1600ºC	
Primary circuit	Primary circuit pressure shall not exceed 8.6 MPa	Design limit
Containment	–Containment pressure shall not exceed 0.5 MPa	Design limit
	–Fluid leak from the containment shall not exceed 1% of the volume per day at a pressure of 0.5 MPa	Design limit

Acceptance criteria for operating modes

The operating modes (regimes) are rated as acceptable based on the following:

— Normal operation modes — non-excess of the operation limits;
— Modes with abnormal operation occurrences, including pre-accidental situations – non-excess of the safe operation limits;
— Design basis accidents – non-excess of the safe operation limits and the design limits for design basis accidents;
— Beyond design basis accidents – non-excess of the specified radiation criteria.

Summary of approaches to the provision of radiation safety

Radiation safety of personnel, the population and the environment is provided according to the following basic concepts:

- Radiation impact on personnel, the population and the environment during normal operation and accidents does not exceed limits established in the GT-MHR project, which are in full compliance with regulatory documents;
- The reactor plant structures and means of radiation protection and radioactive product localization (isolation) are designed taking into account technical and administrative measures aimed at a reduction of radiation levels and air radioactivity in the NPP rooms, at a reduction of emissions of radionuclides to the environment, and at a reduction of radiation doses to personnel and the population, as well as at maintaining these radiation parameters at a reasonably achievable low level.

(1) Physical barriers

Provision of radiation safety is based on the use of physical barriers intended to prevent releases of radioactive products into the environment.

(2) Biological shielding

Biological shielding is one of the barriers to the propagation of ionizing radiation from the reactor plant. According to regulatory requirements, biological shielding is designed with a margin factor of two for the radiation dose rate.

(3) Technical and administrative measures

Several administrative and technical measures are provided for in the project to maintain radiation doses to personnel and the population at a minimum possible level:

— Establishment of a buffer area and a restricted access area around the NPP;
— Execution of the radiation, dosimetric, and process control;
— Establishment of a restricted access area and a 'free' area at the NPP;
— Use of closed circuits with radioactive fluids;
— Filtering of radioactive substances emitted into the environment;
— Use of the containment to retain radioactive products.

Fuel handling operations are performed using protective containers to avoid fuel assembly damage and radioactive product release. Appropriately shielded containers are provided to protect personnel against radiation impacts during dismantling of reactor unit components.

The effective annual radiation dose for the population beyond the buffer area during normal operation of the GT-MHR is much lower than the quota of 20 μSv/year established in regulatory documents. Under abnormal operation conditions, the release of radioactive substances and/or ionizing irradiation does not exceed safe operation limits adopted in the design for normal operation.

VII–5. PROVISIONS FOR SAFETY UNDER EXTERNAL EVENTS

The equipment and systems of the GT-MHR are designed to withstand the impacts of natural and human induced external events, making it possible to accommodate the plant in a variety of siting conditions that meet regulatory requirements.

The external events considered include earthquakes, winds, low and high temperatures, aircraft crash, shock wave impacts, etc. Basic parameters of some of the external events considered in plant design are summarized in brief below.

Seismic impacts (on MSK-64 scale):

- Maximum design basis earthquake (MDBE) ..... 8 points
  (horizontal component of peak ground acceleration is 0.2g, vertical component equals 2/3 of the horizontal component)
- Design basis earthquake ..... 7 points
  (acceleration components are two times lower than in MDBE)

Aircraft crash:

- Mass of a falling aircraft ..... 20 000 kg
- Speed of a falling aircraft ..... 200 m/s
- Impact area of a falling aircraft ..... 7 m^2

Shock air wave:

- Front pressure ..... 30 kPa
- Duration of compression phase ..... up to 1 s
- Propagation direction ..... horizontal

The following design features are implemented in the GT-MHR to ensure plant safety under external impacts and combinations of internal and external impacts:

- Systems and equipment with radiation hazardous fluids and/or materials are arranged in structures (premises) designed to withstand external impacts (including the direct impact of a falling aircraft or its components) without being damaged;
- Safety related equipment, devices and components, and their fastening joints, are designed to withstand potential dynamic impacts of earthquakes, shock waves, etc.;
- Safety system channels have a redundancy and are arranged so that in the case of external impact the remaining operable channel is capable of fulfilling the required safety function to the full extent and in accordance with design requirements;
- The operation of safety systems is based on natural processes;
- A simultaneous failure of the main and the standby control panel is precluded by design (physical separation), as is a simultaneous loss of reactor power and cooling process control.

The reactor plant is arranged in a monolithic ferroconcrete underground containment that provides protection against external impacts. The reactor plant basic equipment and systems (cooling water systems of the PCU and the SCS, RCCS, primary circuit overpressure protection system and the pipelines) are located in cavities and on premises in the central part of the cylindrical containment. The internal leaktight enclosure of the containment (confinement) is made of stainless steel and serves as a hydraulic insulation barrier.

Apart from external impacts (earthquakes, aircraft crash, shock waves, etc.), the containment provides protection against internal impacts, such as those caused by jets and missiles, that might occur during abnormal operation or in accidents.

VII–6. PROBABILITY OF UNACCEPTABLE RADIOACTIVITY RELEASE BEYOND PLANT BOUNDARIES

The targeted probabilities are specified in the subsection called 'Probabilistic criteria' of Section VII-4.2 above.

VII–7. MEASURES PLANNED IN RESPONSE TO SEVERE ACCIDENTS

Physical properties of the reactor core and engineering features of the GT-MHR reactor plant ensure that the temperature of the coated particle fuel is kept below 1600ºC in any accidents with heat removal failure, including a complete failure of all active means of reactor emergency protection and shutdown. The effectiveness of fuel element claddings (coatings), which provide the main protective barrier for retention of fission products within fuel element boundaries, could, therefore, be maintained. With this measure, the radiation consequences of design basis and beyond design basis accidents do not exceed established limits. Altogether, this indicates that no protective measures would be required for the population beyond the buffer area.

VII–8. SUMMARY OF PASSIVE SAFETY DESIGN FEATURES FOR THE GT-MHR

Tables VII-5 to VII-9 below provide the designer's response to questionnaires developed at an IAEA technical meeting Review of Passive Safety Design Options for SMRs, held in Vienna on 13-17 June 2005. These questionnaires were developed to summarize passive safety design options for different SMRs according to a common format, based on provisions of IAEA Safety Standards [VII-3] and other IAEA publications [VII-4, VII-2]. The information presented in Tables VII-5 to VII-9 provided a basis for the conclusions and recommendations of the main part of this report.

TABLE VII-5. QUESTIONNAIRE 1 — LIST OF SAFETY DESIGN FEATURES CONSIDERED FOR/ INCORPORATED INTO THE GT-MHR DESIGN

#	Safety design features	What is targeted?
1.	Helium coolant	– Reliable cooling of the reactor core without phase changes of the coolant – Chemical inertness
2.	Graphite as structural material of the reactor core	Retaining of the reactor core configuration under various mechanical, thermal, radiation, and chemical impacts
3.	Large temperature margin between the operation limit and the safe operation limit	Prevention of the progression of abnormal operation occurrences to accidents
4.1	Negative reactivity coefficient on temperature	Passive shutdown of the reactor accomplished even in ATWS
4.2	Stop of reactor core cooling by helium as a safety action	
4.3	Limited reactivity margin in reactor operation	
4.4	Neutronic properties of helium prevents reactor power growth at coolant density variation	
5.1	Low power density of the core	Passive decay heat removal accomplished with a long grace period
5.2	Annular reactor core with a high surface to volume ratio to facilitate core cooling	
5.3	Central reflector	
5.4	High heat capacity of the reactor core and the reactor internals	
5.5	Heat resistant steel used for the reactor vessel and the reactor internals	

TABLE VII-5. QUESTIONNAIRE 1 — LIST OF SAFETY DESIGN FEATURES CONSIDERED FOR/ INCORPORATED INTO THE GT-MHR DESIGN (cont.)

#	Safety design features	What is targeted?
6.1	TRISO coated particle fuel capable of reliable operation at high temperatures and burnups	Reliable retention of fission products within a fuel particle by passive means
6.2	Safe operation limits for fuel are not exceeded in passive shutdown and aftercooling of the reactor	
7.	No large diameter pipelines and no steam generator in the primary circuit	Limitation of the scope and consequences of accidents with air and water ingress
8.	Containment designed to retain helium-air fluid and to withstand external loads	Limitation of a release of fission products by passive means

TABLE VII-6. QUESTIONNAIRE 2 — LIST OF INTERNAL HAZARDS

#	Specific hazards that are of concern for a reactor line (high temperature gas cooled reactors)	Explain how these hazards are addressed in a SMR
1.	Transient overpower	– Any possible changes of reactivity do not lead to an excess of the safe operation limits (high temperature margin to fuel failure; negative reactivity coefficient on temperature) – Ingress of water to the core is limited by design features (primary circuit pressure in operation modes is higher then pressure in the SCS and PCU water circuits)
2.	Loss of coolant	– Decay heat removal is accomplished by passive systems relying on radiation, conduction and convection in all reactor structures and media; loss of coolant does not lead to an excess of the design limits for design basis accidents – The activity is localized within the containment
3.	Loss of heat removal	Any possible disruptions of core cooling conditions does not lead to an excess of the safe operation limit (high temperature margin to fuel failure; negative reactivity coefficient on temperature; effective passive decay heat removal even in the event of a complete loss of coolant; primary system depressurization as a safety action)
4.	Loss of flow	
5.	Loss of external power sources	With the operation of passive safety systems (passive reactor shutdown on de-energization, passive decay heat removal), station blackout does not lead to an excess of safe operation limits
6.	Exothermic chemical reactions: Air ingress to the core	Oxidation of fuel compacts is precluded by design features limiting air and water ingress to the core (the containment and a limited size of possible breaks) and by an option to restart active normal operation heat removal systems during a long process of passive decay heat removal via the RCCS (which effectively limits the time of the mode with possible oxidation of fuel compacts)
7.	Violation of refuelling and fuel handling conditions	Corrective actions of normal operation systems or use of safety systems ensures that such a violation does not lead to an excess of safe operation limits
8.	Combinations of hazards 1-7 for BDBA	With the operation of passive safety systems, such combinations do not lead to an excess of established radiation criteria

TABLE VII-7. QUESTIONNAIRE 3 — LIST OF INITIATING EVENTS FOR ABNORMAL OPERATION OCCURRENCES (AOO)/DESIGN BASIS ACCIDENTS (DBA)/BEYOND DESIGN BASIS ACCIDENTS (BDBA)

#	List of initiating events for AOO/DBA/BDBA typical for a reactor line (high temperature gas cooled reactors)	Design features of the GT-MHR used to prevent progression of the initiating events to AOO/DBA/BDBA, to control DBA, to mitigate BDBA consequences, etc.	Initiating events specific to this particular SMR
	A. Events for abnormal operation and pre-accidental conditions		
1.	Events associated with changes of reactivity and power distribution	– Normal operation systems are effective to restore normal operation conditions and to wage control of abnormal operation – Control and protection system is effective with account of a single (absorber rod) failure – Inter-circuit leak localization systems are effective with account of a single failure of their active components – Active heat removal systems, PCU and SCS, remain effective if the initiating events are not related to their failure – Use of actuation systems that do not require operator actions – Passive heat removal by the permanently operating RCCS – Increase or reactor parameters at PCU and SCS failures limited by design – Design features limiting air ingress into the reactor core – A possibility to restart systems of normal operation, which ensure the integrity of physical barriers (a feature to control AOO)	Inadvertent insertion of absorbing elements from the RSS hoppers into the reactor core
1.1	Inadvertent removal of one or several of the most effective control rods from the reactor core		
1.2	Inadvertent insertion of one or several of the most effective control rods into the reactor core		
1.3	Inadvertent insertion of absorbing elements from the RSS hoppers into the reactor core		
1.4	Incorrect fuel assembly loading into the reactor core and then its operation		
2.	Events associated with failures of heat removal from the primary circuit		
2.1	Complete stop of water circulation through the PCU heat exchangers		
2.2	Ruptures of the PCU cooling water system pipelines within and beyond the containment		
2.3	SCS failures in standby modes (stop of water circulation and ruptures of the SCS cooling water system pipelines within the containment)		
3.	Events associated with a decrease of coolant flow rate through the reactor core		
3.1	Failures of the turbomachine or of individual turbomachine components, which require an emergency shutdown of the turbomachine		
3.2	Inadvertent opening of the bypass shut-off and control valves of the turbomachine control and protection system		
3.3	Increase of bypass flows in the primary coolant circulation path due to inadvertent opening of valves or due to depressurization of in-vessel components		

TABLE VII-7. QUESTIONNAIRE 3 — LIST OF INITIATING EVENTS FOR ABNORMAL OPERATION OCCURRENCES (AOO)/DESIGN BASIS ACCIDENTS (DBA)/BEYOND DESIGN BASIS ACCIDENTS (BDBA) (cont.)

#	List of initiating events for AOO/DBA/BDBA typical for a reactor line (high temperature gas cooled reactors)	Design features of the GT-MHR used to prevent progression of the initiating events to AOO/DBA/BDBA, to control DBA, to mitigate BDBA consequences, etc.	Initiating events specific to this particular SMR
	B. Events for design basis accidents		
1.	*Events associated with primary circuit depressurization*	– Control and protection system is effective with account of a single (absorber rod) failure – Activity localization systems are effective with account of a single failure of their active components – Active heat removal systems, PCU and SCS, remain effective if the initiating events are not related to their failure – Use of the actuation systems that do not require operator actions – Passive localization of radioactivity in the containment – Passive heat removal by the permanently operating RCCS – Increase or reactor parameters at PCU and SCS failures limited by design – Design features limiting air ingress into the reactor core – Possibility to restart systems of normal operation, which ensure the integrity of physical barriers, reduce fission product releases, and mitigate radiation consequences of accidents (*a feature to control accidents*)	Nothing in particular specified here
1.1	Primary circuit depressurization due to a loss of leaktightness or a guillotine break of a primary circuit pipeline with coolant leak into the containment and further air ingress to the primary circuit: – Rupture of small lines ($\leq DN_{equiv}30$) – Rupture of turbomachine CPS bypass pipeline ($DN_{equiv}250$) – CPS standpipe depressurization		
1.2	Rupture of helium transportation pipelines and storage system beyond the containment		
2.	*Events associated with abnormal cooling conditions of fuel assemblies*		
2.1	Partial clogging of the flow areas of fuel assemblies by fuel assembly fragments		
3.	*Events associated with abnormal refuelling and fuel handling*		
3.1	Drop of heavy objects during refuelling with damage to fuel assemblies		
3.2	Depressurization of the handling equipment of fuel assemblies		
3.5	Fuel assembly damage during refuelling		
	C. Events for beyond design basis accidents (taking into account additional failures)		
1.	*Events associated with loss of power supply sources*	– Effective reactor shutdown system (RSS) with spherical absorbing elements	
1.1	Blackout		
1.2	Blackout with a complete failure of the RCCS		
1.3	Blackout with a failure of actuation of the reactor emergency protection system (ATWS)		
2.	*Events associated with reactivity variation (taking into account additional failures)*	– Negative reactivity coefficient on temperature, passive reactor shutdown	
2.1	Inadvertent withdrawal of several most effective control rods from the reactor core with actuation failure of the reactor emergency protection system (ATWS)	– Passive localization of radioactivity in the containment	

TABLE VII-7. QUESTIONNAIRE 3 — LIST OF INITIATING EVENTS FOR ABNORMAL OPERATION OCCURRENCES (AOO)/DESIGN BASIS ACCIDENTS (DBA)/BEYOND DESIGN BASIS ACCIDENTS (BDBA) (cont.)

#	List of initiating events for AOO/DBA/BDBA typical for a reactor line (high temperature gas cooled reactors)	Design features of the GT-MHR used to prevent progression of the initiating events to AOO/DBA/BDBA, to control DBA, to mitigate BDBA consequences, etc.	Initiating events specific to this particular SMR
3.	*Events associated with a decrease of the coolant flow rate through the reactor core (taking into account additional failures)*	– Passive localization of radioactivity in the containment	
3.1	Turbomachine failure or failure of individual turbomachine components, which require an emergency shutdown of the turbomachine, with actuation failure of the reactor emergency protection system (ATWS)	– Increase or reactor parameters at PCU and SCS failures limited by design – Design features limiting air and water ingress into the reactor core	
4.	*Events associated with primary circuit leakage (taking into account additional failures)*	– Possibility to restart safety systems and normal operation systems, which ensures reactor transition to a controllable state; integrity of physical barriers (the containment), decrease of fission product release, and mitigation of radiation consequences of accidents (a feature to control accidents)	
4.1	Primary circuit depressurization with a blackout and ingress of a considerable amount of air into the primary circuit (CPS standpipe guillotine break)		
4.2	Primary circuit depressurization with actuation failure of the reactor emergency protection system (ATWS), a blackout and ingress of a considerable amount of air into the primary circuit (CPS standpipe guillotine break)		
4.3	Rupture of the helium transportation pipelines and storage system beyond the containment, followed by a failure of the system for activity localization within the primary circuit, and a blackout		
4.4	Inter-circuit depressurization of the primary circuit and of the PCU or SCS cooling water circuits, followed by a failure of the isolation systems, a blackout, and ingress of a considerable amount of water into the primary circuit		

TABLE VII-8. QUESTIONNAIRE 4 — SAFETY DESIGN FEATURES ATTRIBUTED TO DEFENSE IN DEPTH LEVELS

#	Safety design features	Category: A-D (for passive systems only), according to IAEA-TECDOC-626 [VII-2]	Relevant DID level, according to NS-R-1 [VII-3] and INSAG-10 [VII-4]
1.	Helium coolant properties	AOO (A)	Level 1, 2
2.	TRISO coated particle fuel capable of effective operation at high temperatures and fuel burnups	AOO, DBA, BDBA (A)	Level 1, 2, 3, 4
3.	Graphite as structural material of the reactor core	DBA, BDBA (A)	Level 3, 4
4.	Large margin between operation and safety limit temperature	AOO	Level 1, 2
5.	Negative temperature reactivity coefficient	AOO, DBA, BDBA	Level 1, 2, 3, 4
6.1	Limited excess reactivity during operation	AOO, DBA, BDBA	Level 1, 2, 3, 4
6.2	Helium neutronic properties preventing reactor power growth at coolant density variation		
7.	No large diameter pipelines in the primary circuit, and no steam generator	AOO, DBA, BDBA (A)	Level 1, 3, 4
8.	Stop of reactor core cooling for protective purposes	BDBA (active)	Level 4
9.	Passive decay heat removal from the reactor core accomplished in the absence of the primary helium, relying on conduction, convection, and radiation in all structures and media and assisted by passive operation of the RCCS	DBA, BDBA (B)	Level 3, 4
10.1	Low core power density	DBA, BDBA (A) Facilitate RCCS operation (A)	Level 3, 4
10.2	Annular reactor core with a high surface to volume ratio		
10.3	Central reflector		
10.4	High heat capacity of the reactor core and the reactor internals		
10.5	Heat resistant steel used for the reactor internals and vessel		
11.	Fuel safe operation limits met in the case of reactor passive shutdown and cooling	DBA	Level 3
12.	Containment designed to retain helium-air fluid and to withstand external loads	DBA, BDBA (A)	Level 3, 4

TABLE VII-9. QUESTIONNAIRE 5 — POSITIVE/ NEGATIVE EFFECTS OF PASSIVE SAFETY DESIGN FEATURES IN AREAS OTHER THAN SAFETY

#	Passive safety design features	Positive effects on economics, physical protection, etc.	Negative effects on economics, physical protection, etc.
1.	Helium coolant properties		Primary circuit and coolant costs are increased, taking into account helium volatility
2.	Graphite as a structural material for the reactor core		– Facilities should be constructed to produce graphite of specified properties – Increase of reactor core cost – Need to dispose of large volumes of graphite
3.	Low core power density		– Decrease of specific economic indices – Increase of reactor cost
4.	Annular reactor core with a high surface to volume ratio to facilitate core cooling		Increase in reactor vessel dimensions and cost
5.	Central reflector		
6.	Heat resistant steel used for the reactor internals and the reactor vessel		– Increase in reactor cost
7.	TRISO coated particle fuel capable of reliable operation at high temperatures and burnups		– Increase in fuel cost – Fuel production facilities need to be constructed
8.	No large diameter pipelines in the primary circuit and no steam generators	Decrease of reactor plant cost	
9.	Containment designed to retain the helium-air fluid and to withstand external loads		Increase of NPP cost

REFERENCES TO ANNEX VII

[VII–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Innovative Small and Medium Sized Reactor Designs 2005: Reactors with Conventional Refuelling Schemes, IAEA-TECDOC-1485, IAEA, Vienna (2006).

[VII–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Terms for Advanced Nuclear Plants, IAEA-TECDOC-626, IAEA, Vienna (1991).

[VII–3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[VII–4] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA,Vienna (1996).

Annex VIII

SAFETY DESIGN FEATURES OF THE 4S-LMR

Central Research Institute of Electric Power Industry and Toshiba Corporation, Japan

VIII–1. DESCRIPTION OF THE 4S-LMR CONCEPT

The Super-Safe Small and Simple Liquid Metal cooled Reactor (4S-LMR) is a small sodium cooled fast reactor concept under development in Japan by the Central Research Institute of Electric Power Industry (CRIEPI) and Toshiba Corporation features of which include long operation without on-site refuelling. This concept is described in detail in Annex XV of [VIII-1].

The 4S-LMR is being developed to meet the needs of certain segments of the diverse global energy market [VIII-1]. An economic disadvantage is pointed out as the principal obstacle to realizing small reactors. Higher safety levels are also needed, because the number of nuclear power plants would increase in case small reactors are deployed around the world. Improved economic performance tends to be incompatible with enhanced safety levels, as shown by the experience of nuclear power reactors of previous generations. Stronger reliance on passive safety design options is expected to establish a certain synergy between economic performance and safety. To facilitate such a synergy, the 4S-LMR is being designed to ensure simple operation, simplified maintenance, including refuelling, a high safety level, and improved economic performance. A specific design policy for the 4S-LMR could be summarized in the following nine design objectives:

(1) No refuelling over 10 – 30 years;
(2) Simple core burnup control without control rods and without control rod driving mechanisms;
(3) Reactor control and regulation executed by systems and components not belonging to the reactor system;
(4) Quality assurance and short construction period based on factory fabrication of the reactor unit;
(5) Minimum maintenance and inspection of reactor components;
(6) Negative reactivity coefficients on temperature; negative sodium void reactivity;
(7) No core damage in any conceivable initiating events without the reactor scram;
(8) Safety system independent of emergency power systems and not incorporating active decay heat removal systems;
(9) Complete confinement of radioactivity under any operational conditions and in decommissioning.

Items 1 through 5 are related to simplification of the systems and maintenance. Items 6 through 9 are related to safety design.

Based on the abovementioned design objectives, the 4S-LMR concept supplies multiple passive safety design features. Such an approach could help realize a high safety level and simultaneously reduce the number of auxiliary systems otherwise required to support safety functions of the safety system. The resulting reduction in the number of systems and system simplification may, in turn, reduce the required scope of maintenance work.

Small reactors are meant to be installed closer to end users. In order to allay public fears, a ‘sense of security’ is essential, which means that a transparent safety concept, a proven or easily demonstrable technology, and a small number of systems are cumulatively preferable. A fully passive heat removal system is employed in the 4S-LMR so that auxiliary support systems can be eliminated. 4S-LMR safety can easily be demonstrated in full scale tests, because of its small size. Design status and passive safety features of the 4S-LMR are described in reference [VIII-1]. This reference also presents safety performance of the reactor in anticipated transients without scram and combinations thereof, based on completed safety analyses.

The 4S-LMR incorporates a load following capability provided by a simple control of the feed water rate in the power circuit. Analyses have shown that the reactivity of core thermal expansion, which is one of the passive reactivity feedbacks, is important to realize this option. Core thermal expansion feedback also helps to secure reactor safety. Specifically, analytical results predict that the presently selected cladding material, HT-9, is

compatible with the mechanism of core expansion reactivity feedback. It is also shown that flow rate control of the secondary pump would enhance the power range of reliable reactor operation due to improved stability of the steam generator at the steam-water site. As the irregular load following operation affects schedule pre-programming, the plant control systems of the 4S-LMR would be reconsidered in case the reactor is assumed to operate at partial power.

The 4S-LMR is a pool type sodium cooled fast reactor with a steam-water power circuit. The power output is 50 MW(e), which corresponds to 135 MW(th). The refuelling interval for the variant considered in this description is 10 years. Major specifications of the 4S-LMR are listed in Tables VIII-1 and VIII-2.

Figure VIII-1 shows the vertical layout of the reactor, including the primary heat transport system (PHTS). The PHTS consists of the containment vessel (guard vessel), the reactor vessel, the intermediate heat exchanger (IHX), the electromagnetic (EM) pumps, the reflectors, the internal structures, the core, and the shielding.

The reactor vessel is 3 m in diameter and 18 m in height and is divided into the inner part of a coolant riser plenum and the outer part of a coolant down-comer by an inner cylinder of 1.8 m diameter. The inner cylinder accommodates the core and the reflector. It also accommodates the reflector drivelines and the ultimate shutdown driveline. In the outer part, there are the direct heat exchanger (DHX) of the primary reactor auxiliary cooling system (PRACS), the intermediate heat exchanger (IHX), the electromagnetic (EM) pumps, and the radial shield assemblies, from top to bottom. As a design option, PRACS can be replaced by intermediate reactor auxiliary cooling systems (IRACS), which removes shutdown heat via secondary sodium in active normal operation) or the passive (postulated initiating events) mode. The primary coolant travels from the riser into the down-comer and then returns into the coolant plenum underneath the core. There are no moving parts inside of the reactor vessel except for the reflector, which moves very slowly at 1~2 mm per week.

The guard vessel covers the reactor vessel to prevent a loss of the primary coolant. The guard vessel also forms the containment boundary, together with the top dome. A natural draught air cooling system between the guard vessel and the cavity wall, the so-called reactor vessel auxiliary cooling system (RVACS), is designed as a passive decay heat removal system. The PRACS (or IRACS) mentioned above is then the second passive decay heat removal system. These two systems are redundant and diverse.

TABLE VIII-1. MAJOR DESIGN PARAMETERS OF THE 4S-LMR

Items	Specifications
Reactor:	
Diameter [m]	3.0
Height [m]	18.0*
Reactor vessel thickness [mm]	25
Guard vessel thickness [mm]	15
Inner cylinder:	
Inner diameter [m]	1.84
Thickness [mm]	15
Reflector:	
Material	Graphite
Height [m]	2.1
Thickness [mm]	300
Core barrel:	
Inner diameter [m]	1.33
Thickness [mm]	10
Primary electromagnetic (EM) pump	
Rated flow [m^3/min.]	50
Head [MPa]	0.08 × 2

* from bottom to coolant free surface

TABLE VIII-2. MAJOR DESIGN SPECIFICATIONS OF THE 4S-LMR

Items	Specifications
Thermal output [MW]	135
Electrical output [MW]	50
Primary coolant condition [°C] (outlet/inlet)	510/355
Secondary coolant condition [°C] (outlet/inlet)	475/310
Steam condition [°C/MPa]	453/10.8
Core diameter [m]	1.2
Core height [m] (inner/outer)	1.0/1.5
Number of fuel sub-assemblies (inner/outer)	6/12
Number of reflector units	6
Reflector thickness [m]	0.3
Core lifetime [years]	10
Plant lifetime [years]	30
Number of fuel pins	469
Fuel pin diameter [mm]	10.0
Cladding thickness [mm]	0.59
Smear density [%TD]	75
Pitch/Diameter	1.15
Duct thickness [mm]	2
Duct gap [mm]	2
Bundle pitch [mm]	258
Assembly length [mm]	4800
Average burnup [GW day/t]	70
Pu enrichment [weight %] (inner/outer)	17.5/20.0
Maximum linear heat rate [kW/m]	25
Conversion ratio (middle of cycle)	0.71
Coolant void reactivity (end of cycle) [%]	~0
Burnup reactivity swing [%]	~9
Core pressure drop [MPa]	~0.1

The primary pump system consists of two EM pumps arranged in series. Each EM pump is a sodium immersed self-cooled type pump with an annular single stator coil. The total rated flow is 50 m^3/min, and each pump has a 0.08 MPa head. Such a system of pumps arranged in series provides a favourable inherent response in the case of single pump seizure, when it is necessary to mitigate a decrease of core flow through a pump that is still working, 'using' its Q-H (flow-head) curve. At the same time, reverse flow may occur at a failed pump in a parallel arranged pump system.

The annular reflector, divided into six segments, controls reactivity in the reactor core and compensates the burnup reactivity swing. Any stuck event or malfunction of the reflector driving systems will eventually result in a reactor subcritical state, when negative reactivity due to fuel burnup will not be compensated by a slow upward movement of the reflector. Dropping the reflector down will make the reactor subcritical from any operational state, due to the resulting increase in neutron leakage from the core.

The intermediate heat transport system (IHTS) consists of one EM pump, one steam generator (SG), the piping, and a dump tank. The EM pump is integrated in the SG.

The 4S-LMR core is designed for lifetime operation without on-site refuelling and provides for negative reactivity coefficients and a reduced pressure drop at a relatively large core height. The requirement of a 10-year core lifetime could reduce maintenance work and contribute to non-proliferation [VIII-1]. Negative reactivity coefficients and a reduced pressure drop could enhance safety by providing intrinsic protection against loss of

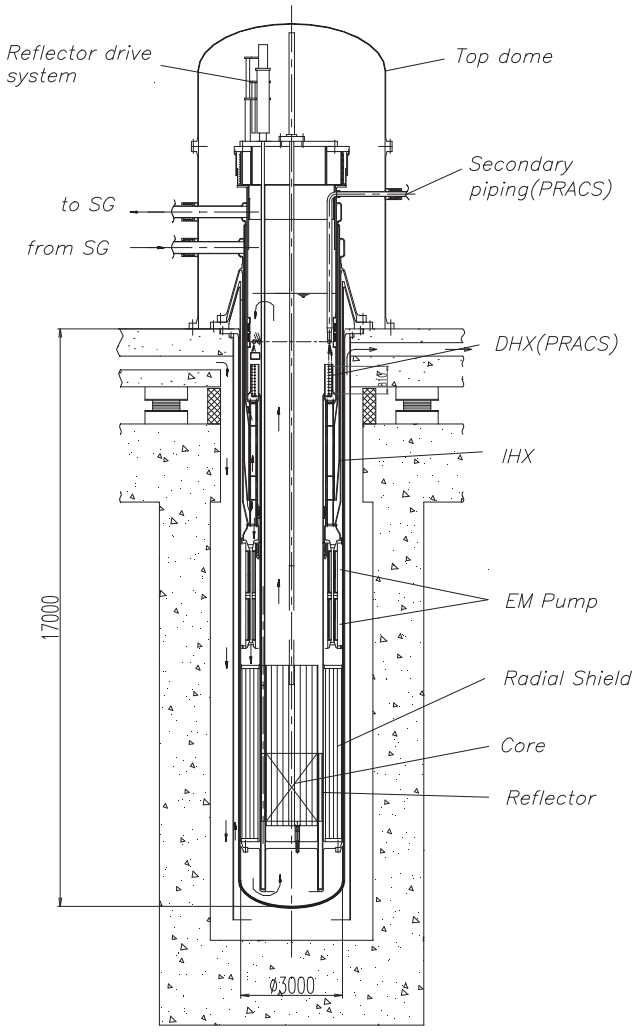


FIG. VIII-1. Vertical view of 4S-LMR layout.

flow (LOF) events. The selection of core height was also limited by the available choices for performing full-core irradiation tests, in view of the existing facilities.

Fig. VIII-2 shows the 4S-LMR core configuration. There are 6 inner sub-assemblies and 12 outer sub-assemblies. The ultimate shutdown rod is arranged at the centre of the core. It is a backup shutdown system; the primary shutdown system provides for dropping down the reflector. The active height of the inner core is shorter than that of the outer core. This 0.5 m sodium region above the inner core helps to decrease the coolant density reactivity coefficient over the entire core. Coolant void reactivity is kept below zero during the core lifetime and is nearly zero at the end of core life.

The average core outlet temperature was selected based on the condition of not exceeding the minimum liquefaction temperature of 650°C, at which a (metallic) fuel-steel eutectic starts to be formed. The hottest interface temperature between the outer fuel surface and the inner cladding surface was evaluated using the hot channel factor of ~1.9 (including the engineering safety factor), which is a conservative assumption. Safety design criteria for the cladding were also evaluated taking into consideration cladding thinning due to this metallurgical effect.

Reactivity feedback coefficients on temperature integrated over the core region are summarized in Table VIII-3. Reactivity feedback coefficients on fuel density, the coolant and the structures (cladding and duct) were derived from a diffusion calculation in R-Z geometry based on the perturbation theory. Density coefficients multiplied by thermal expansion rates of the fuel and structures make up the temperature coefficients. The thermal expansion rate of the cladding was used to describe fuel axial expansion. Because the

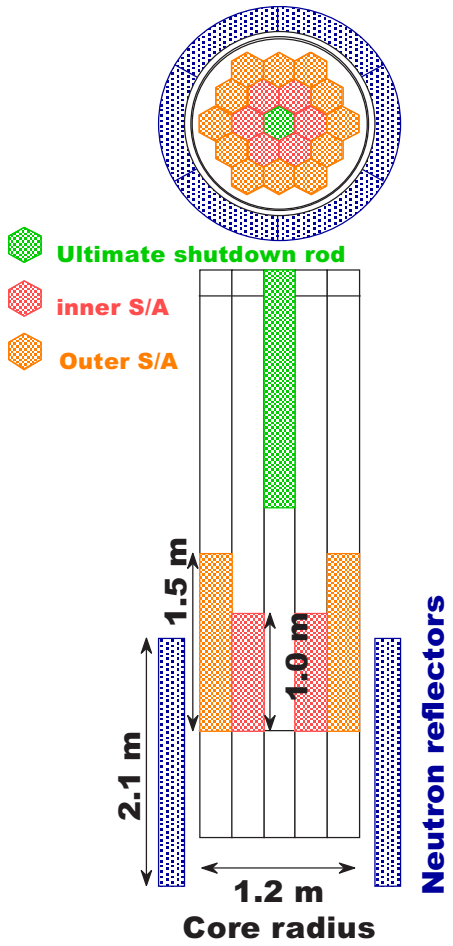


FIG. VIII-2. Core configuration of the 4S-LMR (Annex XV [VIII-1]).

TABLE VIII-3. REACTIVITY FEEDBACK COEFFICIENTS ON TEMPERATURE INTEGRATED OVER THE CORE VOLUME

Core design		Previous design	Current (modified) design
Doppler	$\left(T\frac{dk}{dT}\right)$	-2.80×10^{-3}	-7.07×10^{-3}
Fuel	$\left(\frac{\Delta k/kk'}{°C}\right)$	-7.29×10^{-6}	-2.68×10^{-6}
Coolant	$\left(\frac{\Delta k/kk'}{C}\right)$	-3.23×10^{-6}	~0
Structure	$\left(\frac{\Delta k/kk'}{C}\right)$	-0.50×10^{-6}	-8.94×10^{-8}

expansion rate of the cladding is smaller than that of the fuel, such an approach produced conservative results. The safety analyses performed considered spatial distributions of reactivity coefficients and expansion effects.

VIII–2. PASSIVE SAFETY DESIGN FEATURES OF THE 4S-LMR

The design philosophy of the 4S-LMR is to emphasize simple, passive and inherent safety features as a major part of the defence in depth strategy. The ultimate objective in the 4S-LMR safety design is to eliminate the requirement of population evacuation as an emergency response measure.

The *inherent safety features* of the 4S-LMR are:

- Low power density in the core;
- Good thermal characteristics of the metallic fuel bonded by sodium;
- Negative reactivity coefficients of temperature;
- Negative sodium void reactivity coefficients;
- Large coolant inventory;
- Elimination of active or feedback control systems operating inside the reactor vessel;
- Elimination of components consisting of rotating parts (application of static devices such as EM pumps);
- Limitation of the radioactivity confinement area (no on-site refuelling and no systems for fuel loading/unloading and shuffling, no fuel storage facilities in the reactor or on-site);
- Multiple barriers against fission product release, including:
  - —The fuel cladding;
  - —The reactor vessel, the upper plug and the IHX tubes;
  - —The top dome and the guard vessel as containment;
- Relatively small radioactive inventory of a small power reactor;
- Prevention of a sodium leakage and mitigation of its impact or influence if it occurs through double boundaries for sodium with a detection system for small leakage occurring in the event of one boundary failure:
  - —The reactor vessel and guard vessel for primary sodium;
  - —Double piping, tubes and vessels for secondary sodium, including heat transfer tubes of the SG.

The *passive safety systems* of the 4S-LMR are the following:

- An automatic sodium drain system from the SG to the dump tank — if a sodium-water reaction occurs, an increase in cover gas pressure in the SG causes secondary sodium to drain rapidly to the dump tank located beneath the SG (without rupture disks);
- Two diverse and redundant passive shutdown (residual) heat removal systems operating on natural convection of the coolant and natural air draft (PRACS or IRACS and RVACS).

For shutdown (residual) heat removal, two independent passive systems are provided; RVACS and IRACS (or PRACS, see Section VIII-1). The reactor vessel auxiliary cooling system (RVACS) is completely passive and removes shutdown heat from the surface of the guard vessel using natural draught of air. There are no valves, vanes or dampers in the flow path of the air; thus RVACS is always working, even in normal (rated) operation. Two stacks are provided to obtain sufficient draft.

The IRACS removes shutdown heat via the secondary sodium. In normal shutdown, heat is removed by forced circulation of air with a blower driven by normal electric power; IRACS can also remove the required amount of heat solely through natural circulation of both air and sodium in the case of postulated initiating events.

The 4S-LMR incorporates no *active safety systems*. However, there are several active systems providing normal operation of the reactor at rated (or derated) power. In normal operation heat is removed from the core by forced convection of sodium driven by EM pumps. The compensation of burnup reactivity swing is performed by very slow upward movement of the reflector. An advanced driving mechanism for such movement is being considered [VIII-1].

No information was provided on whether certain systems of the 4S-LMR are safety grade.

VIII–3. ROLE OF PASSIVE SAFETY DESIGN FEATURES IN DEFENCE IN DEPTH

Some major highlights of passive safety design features in the 4S-LMR, structured in accordance with the various levels of defence in depth [VIII-2, VIII-3], are described below.

Level 1: Prevention of abnormal operation and failure

(A) Prevention of transient over-power:

- Elimination of feedback control of the movable reflectors;
  - —A pre-programmed reflector-drive system, which drives the reflector without feedback signals;
  - —The moving speed of the reflector is approximately 1mm/week;
- The limitation of high speed reactivity insertion by adopting electromagnetic impulsive force (EMI) as a reflector driving system;
- The limitation of reactivity insertion at the startup of reactor operation;
- Negative whole core sodium void worth;
- Power control via pump flow rate in the power circuit (no control rods in the core).

(B) Prevention of loss of coolant:

- Double boundaries for primary and secondary sodium in SG tubes and continuously operating leak detection systems.

(C) Prevention of loss of flow:

- Primary EM pumps are arranged in two units connected in a series in which each single unit takes on one half of the pump head;
- A combined system of EM pumps and synchronous motor systems (SM) ensures sufficient flow coastdown characteristics.

(D) Prevention of loss of heat sink:

- Redundant and diverse passive auxiliary cooling systems (RVACS and IRACS or PRACS) with natural draught of environmental air acting as a heat sink.

(E) Prevention of sodium-water reaction:

- A leak detection system in the heat transfer tubes of the SG using wire meshes and helium gas, capable of detecting both:
  - —An inner tube failure (water/system side of the boundary);
  - —An outer tube failure (secondary sodium side of the boundary).

Level 2: Control of abnormal operation and detection of failure

The inherent and passive features contributing to such control are:

- All negative temperature reactivity feedback coefficient;
- Negative whole core sodium void worth;
- Effective radial expansion of core (negative feedback);
- Large thermal inertia of the coolant and the shielding structure;
- Two redundant power monitoring systems, the primary and the secondary; balance of plant temperature monitoring system; EM pump performance monitoring system, cover gas radioactivity monitoring system, etc.

Level 3: Control of accidents within the design basis

The inherent and passive features contributing to such control are:

- Metallic fuel (high thermal conductivity, low temperature);
- Low liner heat rate of fuel;
- Negative whole core sodium void worth;
- All negative temperature reactivity feedback coefficient;
- Low pressure loss in core region;
- Effective radial expansion of core (negative feedback);
- Redundant and diverse passive auxiliary cooling systems (RVACS and IRACS or PRACS) with natural draught of environmental air acting as a heat sink;
- Increased reliability of reactor shutdown systems achieved by the use of two independent systems, with each having enough reactivity for a shutdown, including:
  - —The drop of several sectors of the reflector;
  - —Gravity driven insertion of the ultimate shutdown rod.
- Increased reliability of the sodium leakage prevention systems achieved by the use of double wall SG tubes with detection systems for both inner and outer tubes.

Level 4: Control of severe plant conditions, including prevention of accident progression and mitigation of consequences of severe accidents

The inherent and passive features contributing to such control are:

- Redundant and diverse passive auxiliary cooling systems (RVACS and IRACS or PRACS) with natural draught of environmental air acting as a heat sink;
- Inherent safety features of a metal fuelled core, such as excellent thermal conductivity and low accumulated enthalpy;
- Low linear heat rate of fuel;
- Negative whole core sodium void worth;
- Large inventory of primary sodium to meet the requirements for increased grace periods;
- The rapid system of sodium drain from the SG to the dump tank as a mitigation system for sodium-water reaction.

Level 5: Mitigation of radiological consequences of significant release of radioactive materials

The inherent and passive safety features of the 4S are capable of eliminating an occurrence of fuel melting in any accident without scram (AWS) or anticipated transient without scram (ATWS), see Annex XIV and Annex XV in [VIII-1].

VIII–4. ACCEPTANCE CRITERIA FOR DESIGN BASIS AND BEYOND DESIGN BASIS ACCIDENTS

VIII–4.1. List of design basis and beyond design basis accidents

For the safety analysis of the 4S, design basis events (DBEs) were selected and identified systematically, considering the 4S operation cycle and events postulated for the MONJU and DFBR (Japan), and for LWRs. A broad variety of events were considered in the following categories [VIII-1]:

- Power transients;
- Loss of flow;
- Local fault;
- Sodium leakage;

- Balance of plant (BOP) failure and loss of off-site power;
- Multiple systems failure.

Beyond design basis events (BDBEs) have been selected and identified in a similar manner [VIII-1]. On a broad scale, beyond design basis accidents are divided into two big groups, which are anticipated transients without scram (ATWS) and accidents without scram (AWS). The ATWS comprise sequences in which one of the active reactor shutdown systems does not work for any reason. AWS sequences are listed as more severe than those of ATWS, which include failures of more than one redundant system, such as failures of both pumps, both shutdown systems, and failure of one or both decay heat removal systems.

The examples of ATWS are [VIII-1]:

- Loss of on-site power without scram;
- Failure of the reflector drive system in rated power operation without scram.

The examples of AWS are [VIII-1]:

- Sudden loss of head in all primary pumps without scram (AWS event);
- Failure of the reflector drive system in a startup without scram;
- Failure or IRACS and RVACS with the collapse of both of the two stacks (an event more severe than AWS).

VIII–4.2. Acceptance criteria

A general objective of the 4S-LMR safety design is to secure the capability of the plant to withstand a wide range of postulated initiating events and scenarios resulting thereof without exceeding pre-set limits for temperature of the fuel, the cladding, and the coolant, thereby maintaining fuel pin and coolant boundary integrity.
The criteria for DBE are based on experience with conventional light water reactors (LWRs) and previous design experience with sodium cooled fast reactors; specifically, they incorporate the requirements used in the Clinch River Breeder Reactor project [VIII-4]. Table VIII-4 shows the acceptance criteria for DBE. The frequency ranges are similar to those recommended by ANS standards for LWRs [VIII-5, 6].

The criteria for ATWS and AWS are as follows:

- ATWS events:
  - —Maximum cumulative damage fraction (CDF) is less than 0.5;
  - —Maximum fuel temperature is lower than the melting point;
  - —The coolant boundary limit does not exceed the service level D in ASME [VIII-5, 6].

TABLE VIII-4. ACCEPTANCE CRITERIA FOR DBE

Design basis event category	Frequency Range (F)/ (RY)	Evaluated point and criteria			
		CDF*	Primary coolant boundary	Radiation exposure to plant personnel	Offsite radiological dose
Normal operation	—	CDF < 0.05	ASME Service level “A” limits	10 CFR 20 limits	10 CFR 50 Appendix I limits
Anticipated event	$F > 10^{-2}$	Σ CDF all anticipated events + CDF max. unlikely event < 0.1	ASME service level “B” limits	10 CFR 20 limits	10 CFR 50.34
Unlikely event	$10^{-2} > F > 10^{-4}$		ASME service level “C” limits	10 CFR 20 limits	10 CFR 50.34
Extremely unlikely event	$10^{-4} > F > 10^{-6}$	CDF < 0.5	ASME service level “D” limits	10 CFR 20 limits	10 CFR 50.34

* CDF: Cumulative Damage Fraction

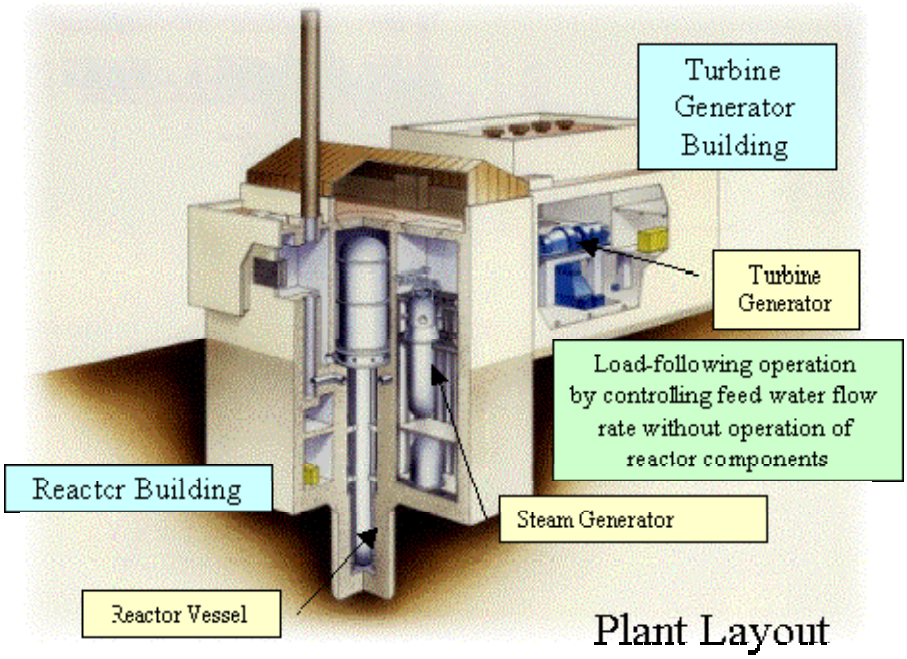


FIG. VIII-3. Reactor building of the 4S-LMR (1991 design) [VIII-1].

- AWS events:
  - —Maximum coolant temperature is lower than the boiling point;
  - —Maximum fuel temperature is lower than the melting point;
  - —The coolant boundary limit does not exceed the service level D in ASME [VIII-5, 6].

VIII–5. PROVISIONS FOR SAFETY UNDER EXTERNAL EVENTS

In the 4S-LMR design, the reactor building is isolated horizontally by seismic isolators. The design standard already exists for such isolators in Japanese NPPs. The 'tiny' reactor shape has a higher characteristic frequency, thus the 4S-LMR reactor can remain rigid against vertical shock. The reactor vessel is located in a shaft below ground level (see Fig. VIII-3), which together with the relatively small footprint of the plant contributes to increased protection against aircraft crash. The capability of the plant to survive all postulated accidents relying only on inherent and passive safety features without the need for operator intervention, emergency team actions, or external power and water supplies is rated as an important feature contributing to the plant protection against impacts of external events.

VIII–6. PROBABILITY OF UNACCEPTABLE RADIOACTIVITY RELEASE BEYOND THE PLANT BOUNDARY

For the 4S-LMR it has been shown that fuel never melts under any hypothetically postulated conditions such as ATWS or AWS (see Annex XIV and Annex XV of [VIII-1]). Some fuel pins with maximum cladding temperature might fail in more severe AWS events. Analyses have been performed for a hypothetical condition in which all fuel element claddings fail (Annex XIV of [VIII-1]). The analytical results show that the dose equivalent in this case is 0.01 Sv at a distance of 20 m from the reactor. It means that only 20 m are required as a site boundary for the 4S-LMR.

VIII–7. MEASURES PLANNED IN RESPONSE TO SEVERE ACCIDENTS

One of the most important design objectives of the 4S is to enhance the level of safety so as to eliminate the need for population evacuation beyond plant boundaries as a consequence of any postulated accident.

VIII–8. SUMMARY OF PASSIVE SAFETY DESIGN FEATURES FOR THE 4S-LMR

Tables VIII-5 to VIII-9 below provide the designer's response to the questionnaires developed at the IAEA technical meeting "Review of passive safety design options for SMRs" held in Vienna on 13-17 June 2005. These questionnaires were developed to summarize passive safety design options for different SMRs according to a common format, based on the provisions of IAEA Safety Standards [VIII-2] and other IAEA publications [VIII-3, VIII-7]. The information presented in Tables VIII-5 to VIII-9 provided a basis for the conclusions and recommendations in the main part of this report.

TABLE VIII-5. QUESTIONNAIRE 1 — LIST OF SAFETY DESIGN FEATURES CONSIDERED FOR/ INCORPORATED INTO THE 4S-LMR DESIGN

#	Safety design features	What is targeted?
1.	Low linear heat rate of fuel	A large margin to fuel melting
2.	Metallic fuel with high thermal conductivity	Decrease of fuel centreline temperature and temperature gradients in a fuel pin
3.	Double boundaries for primary and secondary sodium	Prevention of loss of coolant
4.	Secondary sodium coolant loop (intermediate heat transport system)	Prevent sodium-water reaction from affecting the core
5.	Increased reliability of sodium leakage prevention systems, achieved by the use of double wall SG tubes with detection systems for both inner and outer tubes	Prevention of sodium-water reaction
6.	All temperature reactivity feedback coefficients are negative	Accomplish passive shutdown and prevent accidents with core disruption
7.	Negative whole core sodium void reactivity	Accomplish passive shutdown and prevent DBE from progressing into severe accidents
8.	Effective radial expansion of the core (with negative feedback on reactivity)	Passive insertion of negative reactivity in transients with temperature rise; simple reactor control in load following mode
9.	Simple flow path of coolant in the primary loop	Enhance natural convection of the primary sodium coolant
10.	Low pressure loss in the core area	Enhance natural convection of the primary sodium coolant
11.	Electro-magnetic pump	Prevent immediate pump trips due to a stuck pump shaft
12.	Two electro-magnetic pumps in series	Prevent loss of flow or limit its consequences
13.	Two redundant and diverse passive auxiliary cooling systems (RVACS and IRACS or PRACS) with natural draught of environmental air acting as a heat sink	Assure reliable removal of decay heat
14.	Two diverse passive shutdown systems with each having enough reactivity for a reactor shutdown	Assure reliable reactor shutdown in normal operation and in accidents
15.	No control rods used in core; power control executed via feedwater flow rate control in the power circuit	Enhanced power range of reliable reactor operation; elimination of accidents with control rod ejection; simplified reactor design and operation
16.	Burnup reactivity compensation with a reflector moving upward at very low speed (1 mm per month) in a pre-programmed mode, with no feedback control	Prevention of transient over-power accidents

TABLE VIII-6. QUESTIONNAIRE 2 — LIST OF INTERNAL HAZARDS

#	Specific hazards that are of concern for a reactor line	Explain how these hazards are addressed in SMR
1.	Prevent unacceptable reactivity transients	– No control rods in the core, reactor power control via feedwater flow rate in the power circuit – All negative temperature reactivity feedbacks – Negative whole core sodium worth – Prevention system of reflector insertion accident
2.	Avoid loss of coolant	– Vessel pool configuration with a surrounding guard vessel – Double boundaries for primary and secondary sodium – Double wall SG tubes with detection systems for both inner and outer tubes – Because all temperature reactivity feedback coefficients are negative, coolant boiling will not occur
3.	Avoid loss of heat removal	– Decay heat transport by natural circulation with diverse IRACS and RVACS using environmental air as an ultimate heat sink – Relatively large volume of sodium in the interconnected primary and secondary coolant systems of a pool type reactor
4.	Avoid loss of flow	– The flow rate of natural convection sufficient to remove decay heat, boosted by simple flow path of the primary sodium and low pressure drop in the core – Local blockage of flow pass in the core is prevented by inlet geometry of a fuel assembly, providing an axial and a radial barrier to the debris – Two primary electromagnetic pumps arranged in series
5.	Avoid exothermic chemical reactions (sodium-water and sodium-air reactions)	– Secondary sodium coolant loop (intermediate heat transport system) – Double wall SG tubes with detection systems for both inner and outer tubes – Because all temperature reactivity feedback coefficients are negative, coolant boiling and consequent high pressure generation, which may lead to a disruption of the coolant pressure boundary, will not occur
6.	Prevent radiation exposure of public and plant personnel	– Low linear heat rate of fuel – Because all temperature reactivity feedback coefficients are negative, temperature of the cladding inner surface will not increase up to eutectic temperature – Progression to core melt is prevented by the inherent and passive safety features

TABLE VIII-7. QUESTIONNAIRE 3 — LIST OF INITIATING EVENTS FOR ABNORMAL OPERATION OCCURRENCES (AOO)/DESIGN BASIS ACCIDENTS (DBA)/BEYOND DESIGN BASIS ACCIDENTS (BDBA)

#	List of initiating events for AOO/DBA/BDBA typical for a reactor line (sodium cooled fast reactors)	Design features of the 4S-LMR used to prevent progression of the initiating events to AOO/DBA/BDBA, to control DBA, to mitigate BDBA consequences, etc.*	Initiating events specific to this particular SMR
1.	Loss of flow	– Two primary electromagnetic pumps arranged in series with each capable of handling 05 of the nominal coolant flow rate – Passive reduction of reactor power by all negative temperature reactivity coefficients – Heat transport by the flow rate of natural convection sufficient to remove decay heat, boosted by simple flow path of the primary sodium and low pressure drop in the core	
2.	Transient over-power	– All temperature reactivity feedback coefficients are negative – Whole-core sodium void reactivity is negative – No feedback control of a moveable reflector – No control rods in the core (power control via pump flow rate in the power circuit) – Limitation of high speed reactivity insertion by adopting electromagnetic impulsive force (EMI) as a reflector driving system – Limitation of reactivity insertion at the startup of reactor operation – High thermal conductivity of metallic fuel	– Failure in insertion of the ultimate shutdown rod – Failure in the operation of a pre-programmed moveable reflector
3.	Loss of heat sink	– Environmental air draught is used as an ultimate heat think, with two redundant and diverse passive decay heat removal systems (RVACS and IRACS) being provided – Relatively large volume of sodium in the interconnected primary and secondary coolant systems of a pool type reactor – Passive reduction of reactor power by all negative temperature reactivity coefficients – Whole-core sodium void reactivity is negative	
4.	Local fault	– High thermal conductivity and low centreline temperature of metallic fuel – Local blockage of flow pass in the core is prevented by inlet geometry of a fuel assembly, providing an axial and a radial barrier to debris	
5.	Loss of on-site power	– Gravity driven insertion of ultimate shutdown rod – Gravity driven drop of reflector parts to shut down the reactor – With a stuck moveable reflector, the reactor would operate for some time and then become subcritical because burnup reactivity loss will not be compensated by slow upward movement of the reflector – All temperature reactivity feedback coefficients are negative – Whole-core sodium void reactivity is negative – Natural convection in the primary circuit sufficient to remove decay heat – Environmental air draught is used as an ultimate heat think, with two redundant and diverse passive decay heat removal systems (RVACS and IRACS) being provided	
6.	Sodium leak	– Secondary sodium coolant loop (intermediate heat transport system) – Double-wall SG tubes with detection systems for both inner and outer tubes	

* The analyses performed have shown that all postulated designs basis and beyond design basis accidents can be terminated without core melting, relying only on the inherent and passive safety features of the plant [VIII-1].

TABLE VIII-8. QUESTIONNAIRE 4 — SAFETY DESIGN FEATURES ATTRIBUTED TO DEFENCE IN DEPTH LEVELS

#	Safety design features	Category: A-D (for passive systems only), according to IAEA-TECDOC-626 [VIII-5]	Relevant DID level, according to NS-R-1 [VIII-2] and INSAG-10 [VIII-3]
1.	Secondary sodium coolant loop (intermediate heat transport system)	A	1, 4
2.	Double wall SG tubes with (active) Na leak detection system for each wall	A	2
3.	Electromagnetic pump	B	1
4.	Two electromagnetic pumps in series	A	2
5.	Simple flow path in the primary loop	A	2, 3
6.	Low pressure loss in the core	A	2, 3
7.	Reactor vessel auxiliary cooling system (RVACS, IRACS or PRACS) with the environmental air as an ultimate heat sink	B	3, 4
8.	Two redundant and diverse passive decay heat removal systems (PRACS or IRACS and RVACS)	A	2, 3
9.	Metallic fuel (high thermal conductivity)	A	1, 3
10.	Low linear heat rate	A	1, 3
11.	Relatively large volume of sodium in the interconnected primary and secondary coolant systems of a pool type reactor	A	3, 4
12.	A whole core sodium void worth is negative	A	1, 3
13.	All temperature reactivity feedback coefficients are negative	A	1, 3
14.	Fuel assembly inlet geometry providing axial and radial barriers to the debris	A	1, 2
15.	Radial expansion of the core	B	2, 3
16.	Two redundant and diverse gravity driven reactor shutdown systems (drop of the reflector and ultimate control rod insertion)	C	1, 2, 3
17.	No feedback control of the reflector movement	A	1
18.	No control rods in the core	A	1

TABLE VIII-9. QUESTIONNAIRE 5 — POSITIVE/NEGATIVE EFFECTS OF PASSIVE SAFETY DESIGN FEATURES IN AREAS OTHER THAN SAFETY

Passive safety design features	Positive effects on economics, physical protection, etc.	Negative effects on economics, physical protection, etc.
Positive/negative effects of passive safety design features on economics, physical protection, etc. have not been investigated yet.		

REFERENCES TO ANNEX VIII

[VIII–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Small Reactor Designs Without On-site Refuelling, IAEA-TECDOC-1536, IAEA, Vienna (2007).

[VIII–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1, IAEA,Vienna (2000).

[VIII–3] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

[VIII–4] CLINCH RIVER BREEDER REACTOR PLANT PROJECT OFFICE, Clinch River Breeder Reactor Project Preliminary Safety Report, Clinch River Breeder Reactor Plant Project,Clinch River, USA (1978).

[VIII–5] AMERICAN NATIONAL STANDARDS INSTITUTE/AMERICAN NUCLEAR SOCIETY STANDARD, Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Power Plants, ANSI/ANS-51.1-1983 (1983).

[VIII–6] AMERICAN NATIONAL STANDARDS INSTITUTE/AMERICAN NUCLEAR SOCIETY STANDARD, Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Power Plants, ANSI/ANS-52.1-1983 (1983).

[VIII–7] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Terms for Advanced Nuclear Plants, IAEA-TECDOC-626, IAEA, Vienna (1991).

Annex IX

SAFETY DESIGN FEATURES OF THE STAR REACTORS

ANL, LLNL, LANL,
United States of America

The reactor concepts addressed in this section are the SSTAR and STAR-LM small lead cooled reactors without on-site refuelling, developed in the Argonne National Laboratory and other national laboratories of the USA. Detailed descriptions of these concepts are presented in [IX-1]; short summaries of the concepts are given in sections IX-1 (SSTAR) and IX-2 (STAR-LM) below. The inherent safety features and passive safety design options of the STAR-LM are similar to those of the SSTAR. Because it would be redundant to list them, they are not reproduced below; the reader is referred to section IX-3 and the following sections on SSTAR.

IX–1. DESCRIPTION OF THE SSTAR CONCEPT

The Small Secure Transportable Autonomous Reactor (SSTAR, [IX-1]) is a 20 MW(e) (45 MW(th)) exportable, small, proliferation resistant, fissile self-sufficient, autonomous load following, and passively safe lead cooled fast reactor (LFR) concept for international deployment and deployment at remote sites. Potential users for the SSTAR include customers looking for energy security with small capital outlay; cities in developing countries, and deregulated power producers in developed countries. SSTAR makes extensive use of inherent and passive safety features, most notably, natural circulation heat transport, lead (Pb) coolant, and transuranic nitride fuel. The SSTAR nuclear power plant incorporates a supercritical carbon dioxide (S-CO_2) Brayton cycle power converter for higher plant efficiency and lower balance of plant costs. The efficiency of the S-CO_2 Brayton cycle increases as the reactor core outlet temperature increases; an efficiency of about 45% can be attained for a turbine inlet temperature of about 550°C. To take advantage of the economic benefits of such high plant efficiency, there has been interest in operating at higher Pb coolant temperatures. In particular, a peak cladding inner surface temperature of 650°C has been an objective. SSTAR is scalable to a higher power level of 181 MW(e) (400 MW(th)); this is the STAR-LM concept discussed in section IX-2. SSTAR is currently at a pre-conceptual level of development. The engineering design for manufacturing the components and systems has not yet been carried out. A probabilistic risk assessment has not been performed. Accident analyses of a set of design basis and beyond design basis accidents have not yet been carried out.

Figure IX-1 illustrates SSTAR, which is a pool type reactor. Lead coolant is contained inside a reactor vessel surrounded by a guard vessel. Lead is chosen as the coolant rather than lead-bismuth eutectic (LBE) to reduce the amount of alpha-emitting ^{210}Po isotope formed in the coolant by two to three orders of magnitude relative to LBE, and to eliminate dependency upon bismuth, which might be a limited resource.

The Pb coolant flows through a perforated flow distributor head located beneath the core; this structure provides an essentially uniform pressure boundary condition at the inlet to the core. The Pb flows upward through the core and through a chimney above the core formed by a cylindrical shroud. SSTAR is a natural circulation reactor such that the vessel has a height to diameter ratio large enough to facilitate natural circulation heat removal at all power levels up to and exceeding 100% of the nominal. The coolant flows through flow openings near the top of the shroud and enters four modular Pb to CO_2 heat exchangers located in the annulus between the reactor vessel and the cylindrical shroud. Inside each heat exchanger, the Pb flows downwards over the exterior of tubes through which the CO_2 flows upwards. The CO_2 enters each heat exchanger through a top entry nozzle, which delivers the CO_2 to a lower plenum region in which the CO_2 enters each of the vertical tubes. The CO_2 is collected in an upper plenum and exits the heat exchanger through two smaller top diameter top entry nozzles. The Pb exits the heat exchangers and flows downward through the annular downcomer to enter the flow openings in the flow distributor head beneath the core.

A thermal baffle is provided near the Pb free surface. The baffle consists of a cylindrical shell welded to the reactor vessel and filled with argon cover gas providing thermal insulation to the reactor vessel. The insulating effect of the shroud is necessary to protect the vessel from thermal stresses that would result from exposure to

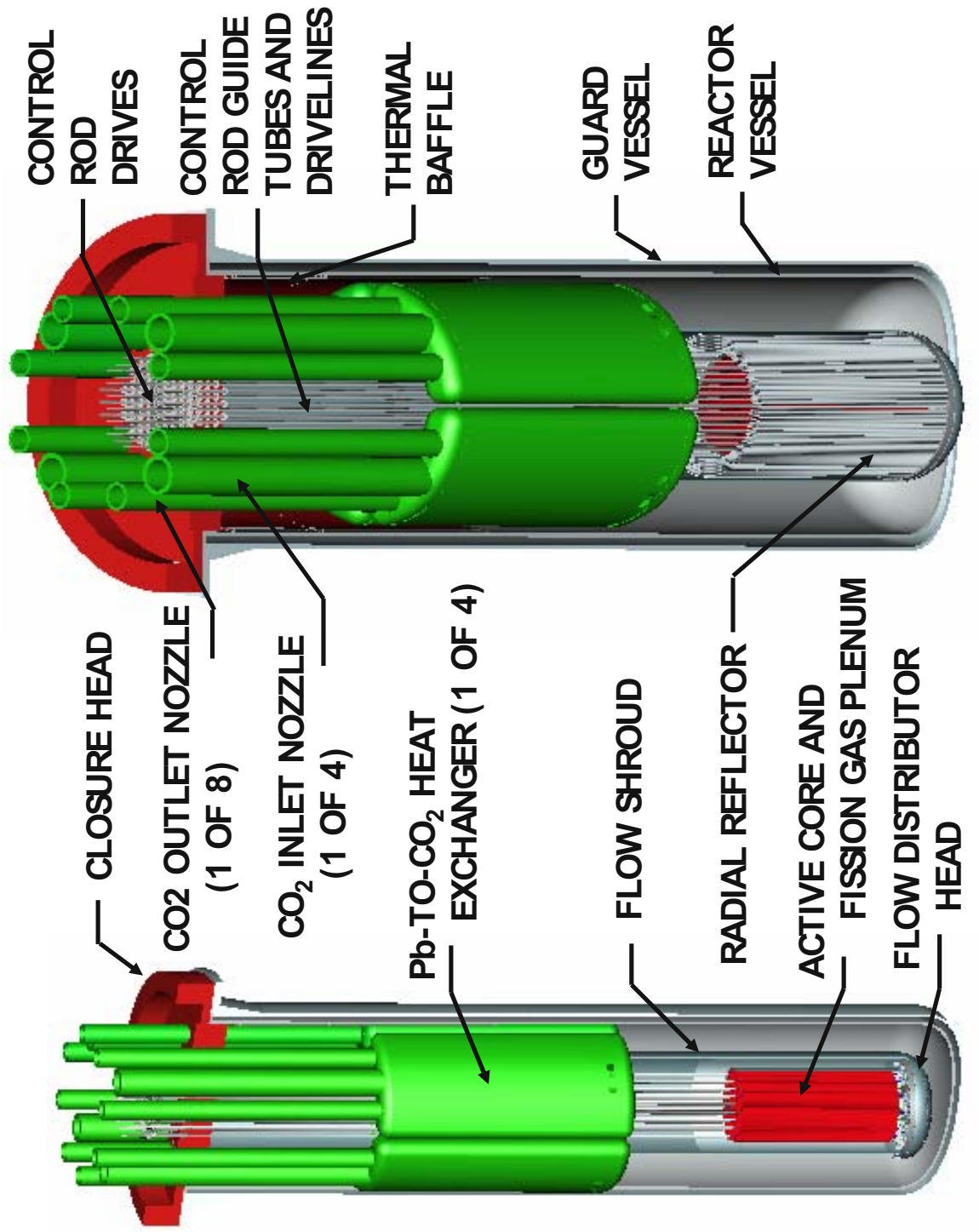


FIG. IX-1. General view of the SSTAR layout.

the heated Pb coolant during startup and shutdown transients. SSTAR does not incorporate an intermediate heat transport circuit. This is a simplification possible with Pb coolant which is calculated not to react chemically with working fluid below about 250°C (i.e., well below the 327°C Pb melting temperature). A passive pressure relief system is provided on the reactor system to vent CO_2 from the reactor, in the event of a heat exchanger tube rupture.

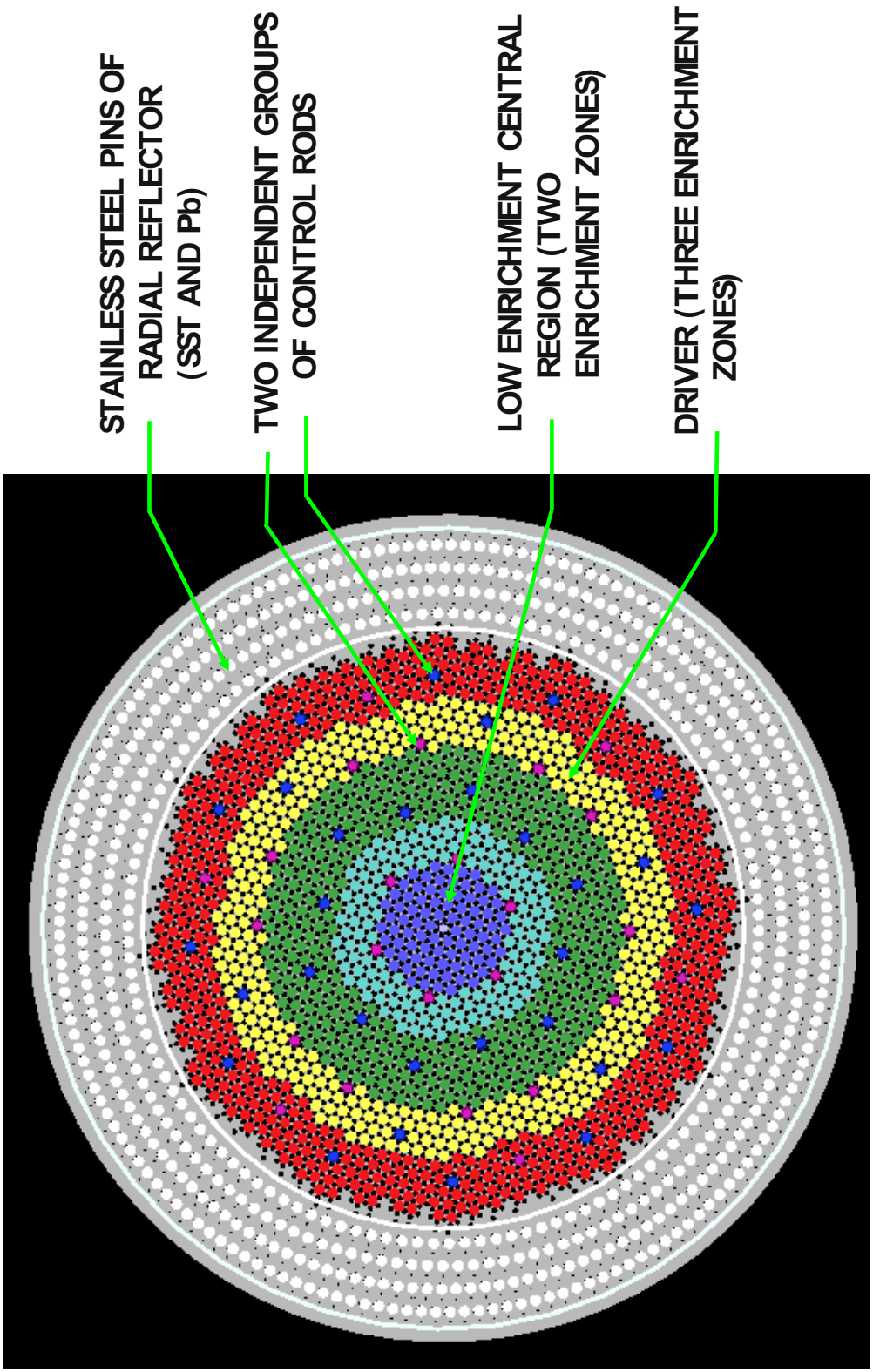


FIG. IX-2. Core configuration of SSTAR.

Figure IX-2 shows the 30-year lifetime core configuration. The core has an open lattice configuration of large diameter (2.5 cm) fuel pins arranged on a triangular pitch. This eliminates potential flow blockage accidents since crossflow paths are always available for cooling. The fuel consists of pellets of transuranic nitride fuel clad with a silicon enhanced ferritic/martensitic steel layer, providing protection against corrosion, co-extruded with a ferritic/martensitic base providing structural strength and irradiation stability. The fuel pellets are bonded to the cladding by molten Pb to reduce the temperature difference between the pellet outer surface and the cladding inner surface.

An active core diameter of 1.22 m is selected to minimize burnup reactivity swing over the 30-year core lifetime. The power level of 45 MW(th) is conservatively chosen to limit the peak fluence on the cladding to 4×10^{23} neutrons/cm^2; this is the maximum exposure for which HT9 ferritic/martensitic cladding has been irradiated. The core has three enrichment zones to reduce power peaking and two central low enrichment zones which further reduce burnup reactivity swing. The core has strong reactivity feedback coefficients, which enable autonomous load following, whereby the reactor power adjusts itself to heat removal from the reactor as a result of reactivity feedbacks. Because heat transport is accomplished by natural circulation, the primary coolant flow rate and system temperatures also adjust themselves to transport heat from the core.

The core does not consist of individual removable fuel assemblies but is a single cassette/assembly. The fuel pins are permanently attached by welding or other means to a core support plate at the bottom of the core. This limits access to either fuel or neutrons. Normally, refuelling equipment is not present at the site. Refuelling equipment, including a crawler crane, is brought onsite only following the 30-year lifetime. The upper closure head for the guard and reactor vessels is removed, the spent core is removed from the vessel and placed inside of a shipping cask; it is then transported to a fuel cycle support centre for reprocessing and refabrication under international oversight. A fresh core is installed in the reactor vessel and the refuelling equipment is removed from the site.

Two sets of control rods are provided for independence and redundancy of the scram. Small adjustments of the control rods are carried out to compensate for small changes in the burnup reactivity swing. The control rod locations have been uniformly distributed throughout the core. Each control rod moves inside of a control rod guide tube occupying a position in the triangular lattice. Spacing between fuel pins is maintained by two levels of grid spacers. Each grid spacer is welded to a control rod guide tube; the grid spacer holds the surrounding fuel pins by means of spring clips allowing for thermal expansion of the fuel pins relative to the control rod guide tube. The active core is surrounded by a radial reflector, which is an annular 'box' containing stainless steel rods and Pb having approximately equal volume proportions. Stainless steel is needed to shield the reactor vessel from neutron fluxes. There is a small Pb flow through the reflector removing the power deposition that takes place there.

SSTAR incorporates a reactor vessel auxiliary cooling system (RVACS) for decay heat removal, should the normal heat removal path involving Pb to CO_2 heat exchangers be unavailable. The RVACS involves heat removal from outside of the guard vessel due to natural circulation of air, which is always in effect. The RVACS is a safety grade system. To provide for greater reliability of emergency heat removal beyond that corresponding to the single RVACS system, it is planned to also incorporate safety grade direct reactor auxiliary cooling system (DRACS) heat exchangers into the reactor vessel.

Conditions, dimensions, and other parameters for SSTAR are included in Table IX-1. Notable achievements of the SSTAR development include:

Pb coolant;
30-year core lifetime;
Average (peak) discharge burnup of 81 (131) MW day/kg of heavy metal;
Burnup reactivity swing < 1 $;
Peak cladding temperature = 650°C;
Core outlet/inlet temperatures = 564/420°C;
Peak transuranic nitride fuel temperature = 882°C;
Small shippable reactor vessel (12 m height by 3.23 m diameter);
Autonomous load following;
Supercritical CO_2 Brayton cycle energy conversion efficiency = 44.1%;
Plant efficiency = 43.8%;
Cost of energy generation < 5.5 US$ cents/kWh (55 US$/MWh).

TABLE IX-1. CONDITIONS AND DIMENSIONS FOR SSTAR

Characteristic	Value
Reactor name	SSTAR (Small Secure Transportable Autonomous Reactor)
Power, MW(e) (MW(th))	19.7 (45)
Customer – Assume 4.0 tonnes of oil equivalent per capita per year = 167 GJ per capita per year = 5.3 KW(th)-year per capita per year, of which ~ 1/3 is used for electricity	Electricity for a town of ~ 25 400
Coolant	Pb
Fuel	Transuranic nitride (TRUN) enriched to N^{15}
Enrichment, %	1.7/3.5/17.2/19.0/20.7 TRU/HM, 5 radial zones
Core lifetime, years	30
Core inlet/outlet temperatures, °C	420/564
Coolant flow rate, kg/s	2150
Power density, W/cm^3	42
Average (peak) discharge burnup, MW day/Kg HM	81 (131)
Peak fuel temperature, °C	882
Cladding	Si-enhanced ferritic/martensitic steel layer for corrosion protection co-extruded with a ferritic/martensitic substrate for structural strength and irradiation stability
Peak cladding temperature, °C	650
Fuel/coolant volume fractions	0.45 / 0.35
Core lifetime, years	30
Fuel pin diameter, cm	2.50
Fuel pin triangular pitch to diameter ratio	1.185
Active core dimensions; Height/Diameter, m	0.976/1.22
Core hydraulic diameter, cm	1.371
Pb to CO_2 heat exchangers (HXs) type	Shell and tube
Number of Pb to CO_2 HXs	4
HX tube length, m	4.0
HX tube inner/outer diameters, cm	1.0 / 1.4
Number of tubes (all HXs)	10 688
HX tube pitch to diameter ratio	1.255
HX Pb hydraulic diameter, cm	1.030
HX-core thermal centres separation height, m	6.80
Reactor vessel dimensions; Height/Diameter, m	12.0 / 3.23
Reactor vessel thickness, cm	5.08
Gap between reactor vessel and guard vessel, cm	12.7
Gap filling material	Air
Guard vessel thickness, cm	5.08
Air channel thickness, cm	15
Air ambient temperature, °C	36
Working fluid	Supercritical CO_2
CO_2 turbine inlet temperature, °C	549
Minimum CO_2 temperature in cycle, °C	31.25
Max./Min. CO_2 pressure in cycle, MPa	20/7.4
CO_2 flow rate, kg/s	247
Net generator output, MW(e)	19.7
Supercritical CO_2 Brayton cycle efficiency, %	44.1
Net plant efficiency, %	43.8

TABLE IX-2. REACTIVITY FEEDBACK COEFFICIENTS OF A 45 MW(TH) SSTAR WITH 20-YEAR CORE LIFETIME

Characteristic/reactivity coefficient	BOC	Part of the cycle ~ 13 years	EOC
Delayed neutron fraction	0.0036	0.0035	0.0034
Prompt neutron lifetime, s	1.8×10^{-07}	1.8×10^{-07}	1.8×10^{-07}
Coolant density, cents/°C	–0.035	–0.001	–0.015
Core radial expansion, cents/°C	–0.16	–0.16	–0.16
Axial expansion, cents/°C	–0.08	–0.07	–0.07
Fuel Doppler, cents/°C	–0.07	–0.07	–0.06
Coolant void worth, $	–1.68	–1.63	–1.83

Table IX-2 presents reactivity feedback coefficients typical of SSTAR core configurations.

IX–2. DESCRIPTION OF THE STAR-LM CONCEPT

The Secure Transportable Autonomous Reactor-Liquid Metal (STAR-LM, [IX-1]) is a scaled up version of SSTAR at a power level of 181 MW(e) (400 MW(th)) for high efficiency electric power production with optional production of desalinated water using a portion of the reject heat. The STAR-LM reactor vessel size is assumed to be limited in height by a rail shipment limitation of 18.9 m. The power level of 400 MW(th) approaches the maximum value at which heat transport can be accomplished through single phase natural circulation given the reactor vessel height limitation. The scaled up version can alternately be used for hydrogen and oxygen generation using a Ca-Br thermo chemical ('water cracking') cycle, if cladding and structural materials for operation with the Pb up to about 800°C can be developed; this high temperature version is named STAR-H2, see the corresponding concept description in [IX-1]. Conditions and dimensions for STAR-LM are provided in Table IX-3. The reactivity feedback coefficients are given in Table IX-4.

IX–3. PASSIVE SAFETY DESIGN FEATURES OF SSTAR

The SSTAR safety design approach is based upon the defence in depth principle of providing multiple levels of protection against the release of radioactive materials by the following:

(i) Design to achieve a high level of reliability such that specific traditional accident initiators are eliminated or accident initiators are prevented from occurring;
(ii) Provision of protection in the event of equipment failure or operating error;
(iii) Provision of additional protection of public health and safety in an extremely unlikely event, which is not expected to occur during the lifetime of the plant or which was not foreseen at the time the plant was designed and constructed.

Inherent safety features

The inherent safety features of SSTAR take advantage of the key inherent properties of Pb coolant, transuranic nitride fuel, and a fast neutron spectrum core, together with specific design options including a pool reactor vessel containing all major primary coolant system components and natural circulation heat transport.

The Pb primary coolant has a high boiling temperature of about 1740°C, which is well above temperatures at which the stainless steel structures lose their strength and melt. Pb is, therefore, a low pressure coolant and does not flash should a leak develop in the primary coolant system boundary. All major primary system

TABLE IX-3. CONDITIONS AND DIMENSIONS FOR STAR-LM

Characteristics	Value
Reactor name	STAR-LM (Secure Transportable Autonomous Reactor-Liquid Metal)
Power, MW(e) (MW(th))	181 (400)
Customer – Assume 4.0 tonnes of oil equivalent per capita per year = 167 GJ per capita per year = 5.3 kW(th)-year per capita per year, of which ~ 1/3 is used for electricity	Electricity for a city of ~226 000
Coolant	Pb
Core inlet/outlet temperature, °C	438/578
Coolant flow rate, kg/s	19 708
Power density, W/cm^3	44
Average (peak) discharge burnup, MW·day/kg HM	83 (136)
Fuel	Transuranic nitride (TRUN) enriched to N^{15}
Enrichment (TRU), %	13.3/18.2/21.3; 3 enrichment zones
Peaking factor (BOC/EOC)	1.63/1.64
Burnup reactivity swing, %Δk/k ($)	0.61 (1.97)
Cladding	Si-enhanced ferritic/martensitic steel layer for corrosion protection co-extruded with a ferritic/martensitic substrate for structural strength and irradiation stability
Peak cladding temperature, °C	650
Fuel/coolant volume fractions	0.21/0.66
Core lifetime, years	15
Fuel pin diameter, cm	1.30
Fuel pin triangular pitch to diameter ratio	1.54
Active core dimensions; Height/Diameter, m	2.00/2.46
Core hydraulic diameter, cm	2.08
Pb to CO_2 HXs type	Shell and tube
Number of Pb to CO_2 HXs	4
HX tube length, m	6.0
HX tube inner/outer diameters, cm	0.5/0.9
Number of tubes (all HXs)	63 288
HX tube pitch to diameter ratio	1.632
HX Pb hydraulic diameter, cm	1.742
HX-core thermal centres separation height, m	8.25
Reactor vessel dimensions; Height/Diameter, m	16.9/5.5
Reactor vessel thickness, cm	5
Gap between reactor vessel and guard vessel, cm	12.7
Gap filling material	Pb-Bi eutectic
Guard vessel thickness, cm	5
Air channel thickness, cm	15
Air ambient temperature, °C	36
Working fluid	Supercritical CO_2
CO_2 turbine inlet temperature, °C	560
Minimum CO_2 temperature in cycle, °C	31.25
Max./Min. CO_2 pressure in cycle, MPa	20/7.4
CO_2 flow rate, kg/s	2,205
Net generator output, MW(e)	181
Supercritical CO_2 Brayton cycle efficiency, %	45.7
Net plant efficiency, %	45.2

TABLE IX-4. REACTIVITY FEEDBACK COEFFICIENTS OF A 400 MW(TH) STAR-LM WITH 15-YEAR CORE LIFETIME

Characteristic/reactivity coefficient	BOC	Part of the cycle ~13 years	EOC
Delayed neutron fraction	0.0035	0.0032	0.0031
Prompt neutron lifetime, s	5.34×10^{-07}	5.04×10^{-07}	4.98×10^{-07}
Coolant density, cents/°C	0.18	0.21	0.22
Core radial expansion, cents/°C	–0.14	–0.15	–0.15
Axial expansion, cents/°C	–0.19	–0.20	–0.21
Fuel Doppler, cents/°C	–0.12	–0.11	–0.10
Coolant void worth, $	11.64	12.20	12.20

components including the core and Pb to CO_2 heat exchangers are contained inside the reactor vessel, which is surrounded by a guard vessel. The coolant level inside the reactor vessel is such that, in the event of a reactor vessel leak, the faulted level of coolant contained by the guard vessel always exceeds the Pb entrances to the Pb to CO_2 heat exchangers. The lack of coolant flashing or boiling due to the high Pb boiling temperature, combined with the pool system configuration and a guard vessel, preclude the loss of primary coolant. It also assures that heat removal from the core and heat transfer to the in-vessel heat exchangers or the vessel wall for heat removal by the RVACS continues by means of natural circulation of a single phase primary Pb coolant.

The lead coolant is calculated not to react chemically with the working fluid above about 250°C, which is well below the Pb melting temperature of 327°C. In particular, there is no formation of combustible gas or exothermic energy release. Lead does not react vigorously with either water or air. Compatibility of Pb and the working fluid makes it possible to eliminate the need for an intermediate cooling circuit, enhancing plant reliability.

Lead has low neutron absorption. This permits the core to be opened up by increasing the coolant volume fraction without a significant reactivity penalty. Increasing the coolant volume fraction increases the hydraulic diameter for coolant flow through the core, reducing the core frictional pressure drop. As a result, natural circulation is more effective and can transport a greater core power. It is possible to design LFRs in which natural circulation is effective at power levels exceeding 100% of the nominal, eliminating the need for main coolant pumps. Eliminating main coolant pumps eliminates loss of flow accident initiators. The open lattice core configuration with wide openings for coolant crossflow eliminates flow blockage accident initiators in which coolant flow entering at the bottom of the core is postulated to be locally blocked.

The high heavy liquid metal coolant density (ρ_{Pb} = 10 400 kg/m^3) limits void growth and downward penetration following a postulated in-vessel heat exchanger tube rupture such that the void is not transported to the core, but instead rises benignly to the lead free surface through a deliberate escape channel between the in-vessel heat exchangers and the vessel wall.

The transuranic nitride fuel has a high thermal conductivity which, when combined with bonding of the fuel pellets to the cladding by means of liquid Pb between the pellets and cladding, reduces peak fuel temperatures during normal operation and accidents. This reduces the stored energy in the fuel and decreases the positive reactivity contribution resulting from cooldown of the fuel while fuel and coolant temperatures equilibrate during accidents as core power decreases.

Transuranic nitride fuel has a high decomposition temperature estimated to exceed 1350°C, such that the fuel maintains its integrity at temperatures above which stainless steel structural materials lose their strength or melt.

Nitride fuel is expected to be compatible with both the Pb bond and ferritic/martensitic steel cladding.

Nitride fuel has a high atom density, making it possible to reduce the volume which must be occupied by fuel and thus further enabling an increase of the coolant volume fraction without the loss of ability to achieve a core internal conversion ratio of unity and a low burnup reactivity swing, which in turn reduces the effects of rod withdrawal accident initiators.

Nitride fuel has a low volumetric swelling per unit burnup, which makes it possible to reduce the size of the gap between fuel pellets and cladding filled by the Pb bond, further facilitating an increase in the coolant volume fraction.

Nitride fuel has a low fission gas release per unit volume. This reduces the thermal creep of cladding resulting from hoop stress loading due to internal pressurization of the fuel pin by a released fission gas.

The fast neutron spectrum core with Pb coolant and transuranic nitride fuel has strong reactivity feedbacks, which provide significant negative reactivity upon a heat-up or equilibration of system temperatures. The strong reactivity feedback reduces core power to match heat removal from the reactor system inherently, shutting down the reactor in the event two shutdown systems fail to scram it.

The strong reactivity feedback of the fast neutron spectrum core with Pb coolant and transuranic nitride fuel enables autonomous load following, whereby core power adjusts itself through inherent mechanisms to match heat removal from the reactor system without operation of control rods, thereby simplifying operation and eliminating potential operator errors.

The low burnup reactivity swing of the 30-year lifetime fast neutron spectrum core decreases excess reactivity requirements, reducing the amount of reactivity insertion accompanying unintended withdrawal of one or more of the control rods.

Passive safety systems

The SSTAR currently incorporates a single safety grade emergency heat removal system, which is the reactor vessel auxiliary cooling system (RVACS). The RVACS cools the exterior of the guard vessel by natural draught of air, which is always in effect. Because the RVACS represents only a single safety grade system, it would be required to have a high reliability with respect to seismic events or sabotage. For example, a seismic event could result in blockage of airflow channels. At particular sites, flooding or dust storms might be factors. It is planned to add safety grade passive direct reactor auxiliary cooling system (DRACS) heat exchangers, located inside of the reactor vessel, to provide for independent and redundant means of emergency heat removal.

Passive pressure relief from the primary coolant system is provided to enable CO_2 to escape from the primary coolant system without over-pressurizing the primary coolant system boundary, in the event of a heat exchanger tube rupture.

Active safety systems

The SSTAR incorporates two independent and redundant safety grade active shutdown systems. The core layout in Fig. IX-2 shows primary and secondary control rod locations.

IX–4. ROLE OF PASSIVE SAFETY DESIGN FEATURES IN DEFENCE IN DEPTH

Some major highlights of passive safety design features in SSTAR, structured in accordance with various levels of defence in depth [IX-2, IX-3], are shown below.

Level 1: Prevention of abnormal operation and failure

The aim of the first level of defence in depth is to prevent deviations from normal operation and to prevent system failures. The inherent safety features of Pb coolant, nitride fuel, and a fast spectrum core, together with natural circulation heat transport and pool vessel configuration reduce the probability of failures through the elimination of reliance upon components, systems, or operator actions that would otherwise need to be considered possible sources of failure. Specific traditional postulated accidents such as loss of flow or local flow blockage are eliminated.

Cladding and structures are protected from significant corrosion by the Pb coolant through control of the dissolved oxygen potential in the coolant within a suitable regime that avoids the formation of lead oxide while allowing protective Fe_3O_4 solid oxide layers to be formed initially upon structures at lower temperatures. The systems for monitoring dissolved oxygen potential and maintaining oxygen levels in the desired regime shall be

designed to have high reliability. It is envisaged to keep sufficiently low the probability of failure of systems in modes that could threaten the long term integrity of the cladding or other structures, or result in the formation of solid debris that might locally block flow channels.

Level 2: Control of abnormal operation and detection of failure

The aim of the second level of defence is to detect and intercept deviations from normal operational states in order to prevent anticipated operational occurrences from escalating to accident conditions. Due to the inherent safety features and passive safety design options of SSTAR, the expectation is that anticipated operational occurrences will not escalate into accidents. Therefore, it is expected that detection is not a necessity in order to avoid escalation into accident conditions.

Level 3: Control of accidents within the design basis

For the third level of defence, it is assumed that, although very unlikely, the escalation of certain anticipated operational occurrences or postulated initiating events (PIEs) may not be arrested by a preceding level and a more serious event may develop. Traditionally, escalation into a more serious event requires the occurrence of additional failures following the onset of the accident initiator. Although specific traditional postulated accidents such as loss of flow or local flow blockage are eliminated, other traditional postulated accidents such as reactivity insertion due to withdrawal of one or more control rods, loss of normal heat sink, heat exchanger tube rupture, loss of load, or station blackout remain. Due to the inherent safety features of SSTAR, core and heat exchangers remain covered by molten Pb coolant and natural circulation heat transport removes the core power, which leaves the reactor system either by normal heat removal paths or by the RVACS. System fuel and coolant temperatures remain within acceptable values well below temperatures at which the structures begin to lose their strength or at which a failure of the cladding could occur. There is no need for reliance upon active systems or operator actions to provide for cooling of the core or heat removal from the reactor system.

For liquid metal cooled fast reactors, an example of a failure in addition to the accident initiator is the assumption of a failure to scram the reactor through the primary and secondary shutdown systems. For SSTAR, it is not necessary for either of the two independent and redundant shutdown systems to operate as well as for operators to take action to insert control rods. The inherent feedbacks of the fast spectrum core with Pb coolant and nitride fuel cause the power level to decrease such that the core power matches the heat removal from the reactor system. The reactor core self-regulates the power level to match heat removal through either the normal heat removal path involving in-vessel Pb to CO_2 heat exchangers or the emergency heat removal path through the RVACS.

If one or more in-vessel Pb to CO_2 heat exchanger tubes were to fail, the passive pressure relief system would release CO_2 from the reactor system, protecting the reactor vessel and upper closure head from over-pressurization.

If the reactor vessel were to fail in addition to the accident initiator, the guard vessel would retain the primary Pb coolant such that the core and in-vessel heat exchangers remain covered by a single phase Pb primary coolant.

If the normal heat removal path or a shutdown heat removal path were to fail, then the RVACS would remove the power generated in the core and transported to the reactor vessel through natural circulation of the Pb coolant. As discussed above, DRACS heat exchangers shall also be incorporated into the reactor vessel to enhance reliability of emergency heat removal beyond that provided by the RVACS. Therefore, it is not expected that a second failure would result in an escalation into a more serious event in terms of the release or transport of radioactivity from the fuel pins.

Level 4: Control of severe plant conditions, including prevention of accident progression and mitigation of consequences of severe accidents

The aim of the fourth level of defence is to address severe accidents in which the design basis could be exceeded and to ensure that radioactive releases are kept as low as practicable.

The SSTAR incorporates a guard vessel surrounding the reactor vessel and an upper closure head, which covers both the guard and the reactor vessels. A hermetic seal is established between the upper closure head and the guard vessel. Thus, the guard vessel and the upper closure head perform the function of a containment vessel surrounding the reactor vessel and retaining radioactivity as long as over-pressurization of the guard vessel and the upper closure head system does not occur. A containment structure is provided above the upper closure head. In the event of a rupture of one or more Pb to CO_2 heat exchanger tubes, the CO_2 would vent through the upper closure head into the volume of the containment structure.

Level 5: Mitigation of radiological consequences of significant release of radioactive materials

The fifth and final level of defence is aimed at mitigation of the radiological consequences of potential releases of radioactive materials that may result from accident conditions. It is envisioned that the exclusion zone surrounding a SSTAR reactor may at the least be reduced in size as a result of inherent safety features, as well as the expected low probability for radioactive material release relative to light water reactor designs with a similar power level.

IX–5. ACCEPTANCE CRITERIA FOR DESIGN BASIS AND BEYOND DESIGN BASIS ACCIDENTS

The U.S. NRC is considering developing a comprehensive set of risk informed, performance based, and technology neutral requirements for licensing power reactors [IX-4]. These requirements would be included in NRC regulations as a new 10 CFR Part 53 and could be used as an alternative to the existing requirements in 10 CFR Part 50. The new 10 CFR Part 53 would constitute a new set of risk informed requirements for both LWR and non-LWR designs. The NRC approved a recommendation from NRC staff to issue an advanced notice of proposed rulemaking (ANPR) in April 2006 on approaches for making the technical requirements for power reactors risk informed, performance based, and technology neutral. The staff was to complete the ANPR stage by December of 2006 and provide its recommendation on whether to have such requirements and, if so, how to proceed with rulemaking by May of 2007, having considered the views of the Advisory Committee on reactor safety. The December 2006 date was intended to provide stakeholders time to submit comments. On April 18, 2006, the NRC issued an update on the risk informed regulation implementation plan (RIRIP). The RIRIP covers many activities of which "Develop structure for new plant licensing" is only one.

The new 10 CFR Part 53 is to be technology neutral to accommodate different reactor technologies, risk informed to identify the more likely safety issues and gauge their significance, and performance based to provide flexibility, and will include defence in depth to address uncertainties. It is to be applicable to any reactor technology, thus avoiding the time consuming and less predictable process of reviewing non-LWR designs against LWR oriented 10 CFR 50 regulations, which requires case by case decisions (and possible litigations) on what 10 CFR Part 50 regulations are applicable and not applicable and where new requirements are needed. Examples include liquid metal cooled reactors, IRIS and HTGRs, as well as reactors being developed under the U.S. Department of Energy Generation IV nuclear energy systems initiative [IX-5]. The need for a technology neutral framework was identified through PBMR review experience. The technology neutral framework is not intended to be used for designs currently under review. The new 10 CFR Part 53 would require a broader use of design specific risk information in establishing the licensing basis; its safety analysis and regulatory oversight on those items most important to safety for that design. It would stress the use of performance as the metrics for acceptability, thus providing more flexibility to designers to decide on factors most appropriate for their design.

It is expected that the development of SSTAR would take place on a timescale consistent with application of the new 10 CFR Part 53. The new technology neutral framework would thus be applied to SSTAR. It remains to be seen what criteria would be applied to assess the performance of a design such as the SSTAR during specific accidents.

IX–5.1. List of design basis and beyond design basis accidents

In the meantime, while the 10 CFR Part 53 regulations are still being considered, a limited set of traditional design basis accidents have been identified for the SSTAR including loss of heat sink, in-vessel heat exchanger tube rupture, transient overcooling, transient overpower/reactivity insertion, and loss of load.

A corresponding set of beyond design basis accidents has also been identified which involves failure to scram due to the assumed failure of both safety grade active shutdown systems.

IX–5.2. Acceptance criteria

For all abovementioned accidents, acceptance criteria include the requirement that system temperatures remain sufficiently low to preclude cladding failures and release of radioactivity from the fuel pins into the coolant.

IX–6. SUMMARY OF PASSIVE SAFETY DESIGN FEATURES FOR SSTAR

Tables IX-5 to IX-9 below provide the designer's response to the questionnaires developed at the IAEA technical meeting "Review of passive safety design options for SMRs" held in Vienna on 13-17 June 2005. These questionnaires were developed to summarize passive safety design options for different SMRs according to a common format, based on the provisions of IAEA Safety Standards [IX-2] and other IAEA publications [IX-3, IX-6]. The information presented in Tables IX-5 to IX-9 provided a basis for the conclusions and recommendations made in the main part of this report.

TABLE IX-5. QUESTIONNAIRE 1 — LIST OF SAFETY DESIGN FEATURES CONSIDERED FOR/ INCORPORATED INTO THE SSTAR DESIGN

#	Safety design features	What is targeted?
1	Lead (Pb) coolant – ambient pressure coolant having a high boiling temperature (1740°C); does not react chemically with working fluid (CO_2); does not react vigorously with air or water/steam; Pb has a low neutron absorption enabling core with an opened up lattice, reducing core frictional pressure drop; Coolant high density retards bubble/void transient growth during blowdown of working fluid into the coolant; Pb is a liquid metal coolant with a low Prandtl number, providing high heat transfer coefficients	– Elimination of loss of coolant due to flashing – Assurance of single phase natural circulation heat transport in all operational transients and accidents at higher temperatures than in traditional liquid metal reactors – Avoidance of combustible gas formation and exothermic energy release due to interaction of coolant and working fluid – Avoidance of energetic reactions of coolant with air or water/steam
2	Nitride fuel – advanced fuel having a high decomposition temperature (> 1350°C) and high melting temperature; Nitride fuel has high thermal conductivity which, when combined with Pb bond, reduces the difference between fuel and coolant temperatures; Nitride fuel has low swelling and fission gas release, and high atom density	– Reduction of stored energy in fuel by reducing positive Doppler and axial expansion reactivity contributions upon fuel cooldown – Avoidance of melting or decomposition of fuel at higher temperatures than in traditional liquid metal cooled reactors – Reduction of a potential for fission gas pressure loading of cladding and pellet-cladding interactions – Reduction of fuel volume fraction enabling an increase in coolant volume fraction
3	Natural circulation heat transport	– Elimination of loss of flow accidents – Assurance of heat removal from the core
4	Vessel pool configuration with surrounding guard vessel	– Elimination of loss of coolant accidents –Elimination of core uncovery; assurance of a natural circulation heat transport path to ultimate heat sink
5	Open lattice core configuration	Avoidance of flow blockage accidents
6	Large reactivity feedbacks from fast spectrum core enabling passive load following and passive shutdown	– Improvement of reactor safety robustness with respect to human error during operation and/or maintenance – Elimination of a failure to decrease reactor power to decay heat levels, in the event of a failure to scram
7	Low burnup reactivity swing over long core lifetime/ refuelling interval, reducing reactivity investment in each control rod	Reduction of challenges from potential rod withdrawal accidents
8	Vessel air cooling by natural circulation of air – always in effect	Assurance of removal of afterheat from the reactor system
9	Escape path for gas/void to reach free surface, provided by design	Assures that gas/void is not transported to the core in the event of in-vessel heat exchanger tube rupture
10	Passive pressure relief from primary coolant system	Avoidance of over-pressurization of primary coolant system following a heat exchanger tube rupture
11	Supercritical carbon dioxide Brayton cycle energy conversion; CO_2 working fluid does not react chemically with Pb primary coolant	Elimination of combustible gas formation and exothermic reactions between primary coolant and working fluid
12	Containment (guard vessel + upper closure head); separate containment structure above upper closure head	Traditional defence in depth: prevents activity release in the event of vessel failure
13	Safety grade reactor trip system	Its functions are traditional, even though passive response is adequate

TABLE IX-6. QUESTIONNAIRE 2 — LIST OF INTERNAL HAZARDS

#	Specific hazards that are of concern for a reactor line	Explain how these hazards are addressed in a SMR
1	Prevent unacceptable reactivity transients	–Low burnup reactivity swing over long core lifetime/refuelling interval reduces the need for reactivity investment in control rods –Large inherent reactivity feedbacks of a fast spectrum core provide negative reactivity contribution upon rise in coolant and fuel temperatures, compensating positive reactivity insertion, reducing reactivity to zero, and stabilizing power and system temperatures
2	Avoid loss of coolant	–Vessel pool configuration with surrounding guard vessel –Ambient pressure Pb coolant with high boiling temperature (1740°C) eliminates flashing of primary coolant
3	Assure heat removal from core	–Natural circulation heat transport with ambient pressure single phase Pb coolant to remove core power –Provision of natural circulation driven air cooling of guard vessel enables removal of reactor power at decay heat levels in the event of loss of heat removal through the in-vessel heat exchangers
4	Avoid loss of flow	–Natural circulation heat transport at power level > 100% of the nominal. –Open lattice core configuration prevents flow blockage
5	Avoid overcooling of reactor system	To be defined
6	Avoid combustible gas generation or exothermic chemical reactions	–Pb primary coolant and CO_2 working fluid do not react chemically –Pb coolant does not react vigorously with air or water/steam
7	Prevent consequences of in-vessel heat exchanger tube rupture	–High inertia/density of Pb coolant retards transient bubble/void growth during blowdown of CO_2 working fluid into the coolant; formation of small bubbles that could be transported to core region does not occur –Escape path for gas/void to pool free surface, provided by design, avoids potential for transport of void to the core –Passive pressure relief from primary coolant system precludes over-pressurization of coolant pressure boundary
8	Maintain integrity of fuel pin cladding	Heat removal from the core by single phase natural circulation and large reactivity feedbacks of fast spectrum core limit system temperatures during operational transients and postulated accidents to values well below those at which cladding strength is significantly reduced or nitride fuel decomposition occurs
9	Maintain coolant pressure boundary	–Heat removal from core by single phase natural circulation –Large reactivity feedbacks of a fast spectrum core, and emergency decay heat removal by vessel air cooling of the guard vessel limit system temperatures during postulated accidents to values well below those at which vessel steel strength is significantly reduced –Passive pressure relief from primary coolant system precludes over-pressurization of coolant pressure boundary
10	Limit radiation exposure to public and plant personnel	–Progression to core melt is deterministically eliminated by passive safety features –Containment consisting of guard vessel and upper closure head is provided for defence in depth –Additional containment structure provides additional mitigation of radioactivity release

TABLE IX-7. QUESTIONNAIRE 3 — LIST OF INITIATING EVENTS FOR ABNORMAL OPERATION OCCURRENCES (AOO)/DESIGN BASIS ACCIDENTS (DBA)/BEYOND DESIGN BASIS ACCIDENTS (BDBA)

#	List of initiating events for AOO/DBA/BDBA typical for a reactor line (Liquid metal cooled fast reactors)	Design features of SSTAR used to prevent progression of the initiating events to AOO/DBA/BDBA, to control DBA, to mitigate BDBA consequences, etc.	Initiating events specific to this particular SMR
1	Loss of flow due to pump coastdown	Natural circulation heat transport at power levels >100% of the nominal; elimination of main coolant pumps	Not an accident initiator
2	Sub-assembly flow blockage	Open lattice core configuration and coolant chemistry control reduce the possibility of a flow blockage	Not an accident initiator
3	Loss of heat sink	–Core and heat exchangers remain covered by ambient pressure single phase Pb coolant, and single phase natural circulation removes core power under all operational transients and postulated accidents –Vessel air cooling removes decay heat power levels from the reactor system –In failure to scram accidents, passive shutdown reduces and maintains the reactor power to a low level representative of decay heat	Cessation of heat removal from in-vessel heat exchangers by CO_2 working fluid with or without scram
4	In-vessel heat exchanger tube rupture	–Transient bubble/void growth is retarded by high inertia/density of Pb primary coolant –Pb primary coolant and CO_2working fluid do not react chemically eliminating combustible gas formation and exothermic energy release –Absence of formation of small bubbles entrained into the coolant and provision of an escape path to pool free surface eliminates a potential for transport of bubbles/ void to the core –Passive pressure relief from primary coolant system precludes over-pressurization by CO_2	
5	Transient overcooling	To be defined	Transient overcooling due to initiating event on S-CO_2 Brayton cycle secondary side
6	Transient overpower/ reactivity insertion accident	– Inherent negative reactivity feedback due to increase in fuel and coolant temperatures returns net reactivity to zero, stabilizing the reactor power and system temperatures at higher than nominal values – Potential reactivity insertion due to rod withdrawal is reduced due to low burnup reactivity swing, reducing the need for reactivity investment in control rods to compensate for burnup effects	
7	Loss of coolant	Eliminated due to vessel pool configuration without external piping at low elevations and ambient pressure Pb coolant	Not an initiator

TABLE IX-8. QUESTIONNAIRE 4 — SAFETY DESIGN FEATURES ATTRIBUTED TO DEFENCE IN DEPTH LEVELS

#	Safety design features	Category: A-D (for passive systems only), according to IAEA-TECDOC-626 [IX-6]	Relevant DID level, according to NS-R-1 [IX-2] and INSAG-10 [IX-3]
1	Selection of Pb as a coolant	A,B	1,3
2	Selection of transuranic nitride as a fuel	A	1,3
3	Natural circulation heat transport	B	1,3
4	Vessel pool configuration with surrounding guard vessel	A	1,3,4
5	Open lattice core configuration	A	1
6	Large reactivity feedbacks from fast spectrum core enabling passive load following and passive shutdown	A	1,3
7	Low burnup reactivity swing over long core lifetime/ refuelling interval, reducing reactivity investment in each control rod	A	1
8	Vessel air cooling by natural circulation	B	3
9	Escape path for gas/void to reach free surface, provided by design	A	3
10	Passive pressure relief from primary coolant system	C	3
11	Supercritical carbon dioxide Brayton cycle energy conversion – CO_2 working fluid does not react chemically with Pb primary coolant	A	1
12	Containment	A	3, 4

TABLE IX-9. QUESTIONNAIRE 5 — POSITIVE/NEGATIVE EFFECTS OF PASSIVE SAFETY DESIGN FEATURES IN AREAS OTHER THAN SAFETY

Passive safety design features	Positive effects on economics, physical protection, etc.	Negative effects on economics, physical protection, etc.
Pb coolant	Lack of chemical interaction with working fluid enables elimination of intermediate heat transport circuit reducing capital and operating costs	– Weight resulting from high Pb density may require greater vessel thicknesses, increasing capital costs – Coolant chemistry control/filtering systems needed to prevent corrosion/corrosion effects contribute to increased cost
Transuranic nitride fuel	– Transuranics are self-protective in safeguards sense – Transuranic nitride fuel together with fast spectrum core and closed fuel cycle reduces fuel costs	
Natural circulation heat transport	Natural circulation cooling, enabled by Pb coolant properties, eliminates main coolant pumps, contributing to reduced plant cost	Need for height separation of thermal centres between heat exchangers and core may require taller reactor and guard vessels, increasing capital costs
Large reactivity feedbacks from fast spectrum core enabling passive load following and passive shutdown	Enhances reliability and reduces operator requirements potentially reducing operating costs	
Low burnup reactivity swing over long core lifetime/ refuelling interval, reducing reactivity investment in each control rod	Core is fissile self-sufficient with conversion ratio near unity such that the spent core can be reprocessed to further utilize its energy content, influencing positively upon fuel economics	
Escape path for gas/void to reach free surface in primary coolant system, provided by design		Requires slightly greater reactor and guard vessel diameters, increasing capital costs
Supercritical carbon dioxide Brayton cycle energy conversion; CO_2 working fluid does not react chemically with Pb primary coolant	– Lack of chemical reaction between primary Pb and CO_2 working fluids enables elimination of intermediate coolant circuit, reducing capital and operating costs – Use of supercritical carbon dioxide Brayton cycle with smaller turbo-machinery components than Rankine saturated steam cycle reduces plant capital and operating costs	– Research and development costs will be required for supercritical CO_2 Brayton cycle – Need to contain CO_2 with potential activity entrained from Pb coolant released from the reactor system following in-vessel heat exchanger tube rupture impacts upon containment requirements, potentially increasing the containment building costs – Need to preclude radiolytic decomposition of CO_2 may require additional shielding of in-vessel Pb to CO_2 heat exchangers, potentially increasing reactor system costs

REFERENCES TO ANNEX IX

[IX–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Small Reactor Designs Without On-site Refuelling, IAEA-TECDOC-1536, Vienna (2007).

[IX–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[IX–3] INTERNATIONAL ATOMIC ENERGY AGENCY, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

[IX–4] UNITED STATES NUCLEAR REGULATORY COMMISSION, New Reactor Licensing – Licensing Process (2008), http://www.nrc.gov/reactors/new-licensing/licensing-process.html#inspections

[IX–5] UNITED STATES DEPARTMENT OF ENVIRONMENT NUCLEAR RESEARCH ADVISORY COMMITTEE, GENERATION-IV INTERNATIONAL FORUM, A technology roadmap for Generation-IV nuclear energy systems, USA (2002).

[IX–6] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Terms for Advanced Nuclear Plants, IAEA-TECDOC-626, IAEA, Vienna (1991).

Annex X

SAFETY DESIGN FEATURES OF THE CHTR

Bhabha Atomic Research Centre (BARC),
India

X–1. DESCRIPTION OF THE CHTR CONCEPT

The Compact High Temperature Reactor (CHTR) is a lead-bismuth cooled beryllium oxide moderated reactor, designed to operate mainly with ^{233}U-Th fuel. The concept of this reactor, which is initially being developed to generate about 100 kW(th), has a core lifetime of 15 years and incorporates several advanced passive safety features to enable its operation as a compact power pack in remote areas not connected to the electrical grid. The reactor, being designed to operate at 1000°C, would also facilitate demonstration of technologies for high temperature process heat applications, such as hydrogen production by splitting of water. The CHTR concept is described in detail in [X-1].

The CHTR core consists of 19 prismatic beryllium oxide (BeO) moderator blocks. These moderator blocks have graphite fuel tubes located centrally. Each fuel tube carries fuel inside 12 equidistant longitudinal bores. The fuel tube also serves as a coolant channel. CHTR fuel is based on tri-isotropic (TRISO) coated particle fuel. Coated particles are mixed with graphite powder as a matrix material and shaped into cylindrical fuel compacts. Fuel bores of each of the 19 fuel tubes are packed with fuel compacts. Eighteen blocks of beryllium oxide reflector surround the moderator blocks. Centrally, these blocks accommodate the passive power regulation system. Graphite reflector blocks surround these beryllium oxide reflector blocks. Cross-sectional layout of the reactor core is shown in Fig. X-1 below.

The core and the reflector part of the reactor are contained in a metallic shell resistant to corrosion against Pb-Bi eutectic alloy coolant, and suitable for high temperature applications. Top and bottom closure plates made of similar material close this reactor shell. Above the top cover plate and below the bottom cover plate, coolant plenums are provided. These plenums have flow guiding blocks made of graphite and have passages for coolant flow to increase the velocity of coolant between fuel tubes and down-comer tubes. Two gas gaps surround the reactor shell and act as insulators during normal reactor operation, reducing heat loss in the radial direction. A finned outer steel shell is provided, which is surrounded by a heat sink. Nuclear heat from the reactor core is removed passively by Pb-Bi eutectic alloy coolant, which flows due to natural circulation between the bottom and the top plenums; upward through fuel tubes, and returning downward through down-comer tubes. Heat utilization vessels are located on top of the upper plenum, providing an interface to systems for high temperature heat applications. A set of sodium heat pipes is provided in the upper plenum of the reactor for passive transfer of heat from the upper plenum to the heat utilization vessels. Three passive systems are provided to remove heat in the case of postulated accident conditions. One of the systems has a set of heat pipes to transfer heat from the upper plenum to the atmosphere in the case of a postulated accident. Another passive system is intended to fill gas gaps with molten metal in the case of an abnormal rise in coolant outlet temperature, so as to facilitate conduction flow of reactor heat to the outside heat sink. To shut down the reactor, a set of seven shut off rods is included, which fall driven by gravity into the central seven coolant channels. Major design and operating parameters of the CHTR are shown in Table X-1.

CHTR component layout is shown in Fig. X-2.

CHTR fuel consists of $^{233}UC_2$, ThC_2, and small amounts of gadolinium as burnable poison (provided only in central fuel tube). Thorium and burnable poisons make the fuel temperature coefficient negative, thus making the reactor inherently safe. The fuel is in the form of fuel compacts made up of TRISO coated particle fuel embedded in graphite matrix. This type of fuel can withstand temperatures up to 1600°C [X-1, X-2]. A typical CHTR fuel bed consists of a prismatic BeO moderator block with a centrally located graphite fuel tube carrying the fuel compacts. Schematics of a fuel particle, a fuel compact, and a single fuel bed are shown in Fig. X-3.

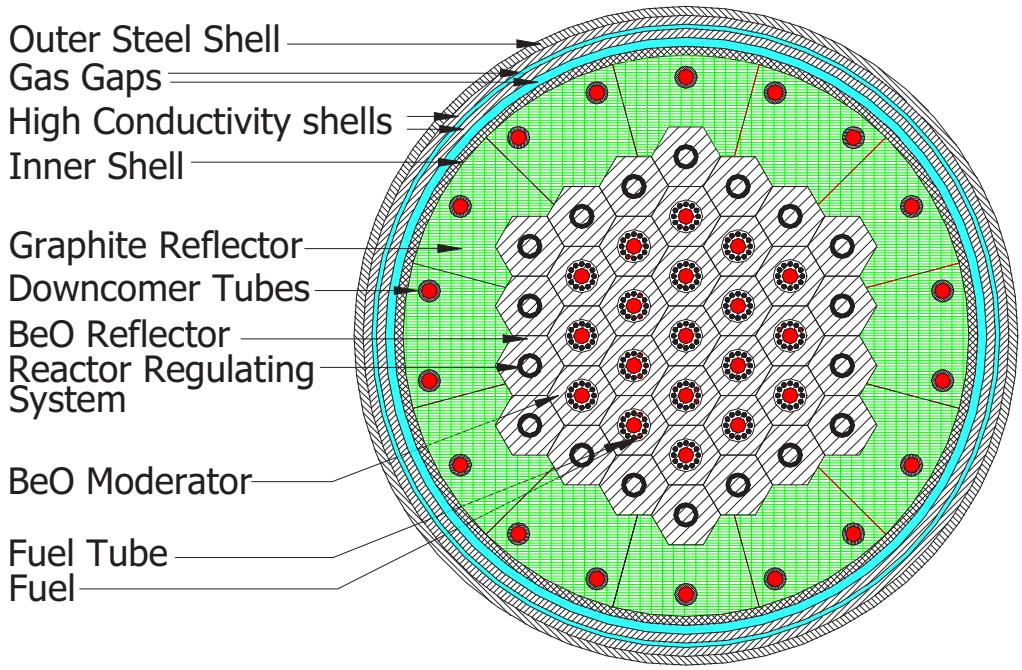


FIG. X-1. Cross-sectional layout of CHTR core.

TABLE X-1. MAJOR DESIGN AND OPERATING PARAMETERS OF CHTR [X-1]

Attributes	Design parameters
Reactor power	100 kW(th)
Core configuration	Vertical, prismatic block type
Fuel	$^{233}UC_2$+ ThC_2 based TRISO coated fuel particles shaped into fuel compacts
Fuel enrichment by ^{233}U	33.75 weight %
Refuelling interval	15 effective full power years
Fuel burnup	≈ 68 000 MW·day/t of heavy metal
Moderator	BeO
Reflector	Partly BeO, and partly graphite
Coolant	Molten Pb-Bi eutectic alloy (44.5% Pb and 55.5% Bi)
Mode of core heat removal	Natural circulation of coolant
Coolant flow rate through core	6.7 kg/s
Coolant inlet temperature	900°C
Coolant outlet temperature	1000°C
Loop height	1.4 m (actual length of the fuel tube)
Core diameter	1.27 m (including radial reflectors)
Core height	1.0 m (Height of the fuelled part and axial reflectors)
Primary shutdown system	18 floating annular B_4C elements in the passive power regulation system
Secondary shutdown system	7 mechanical shut off rods

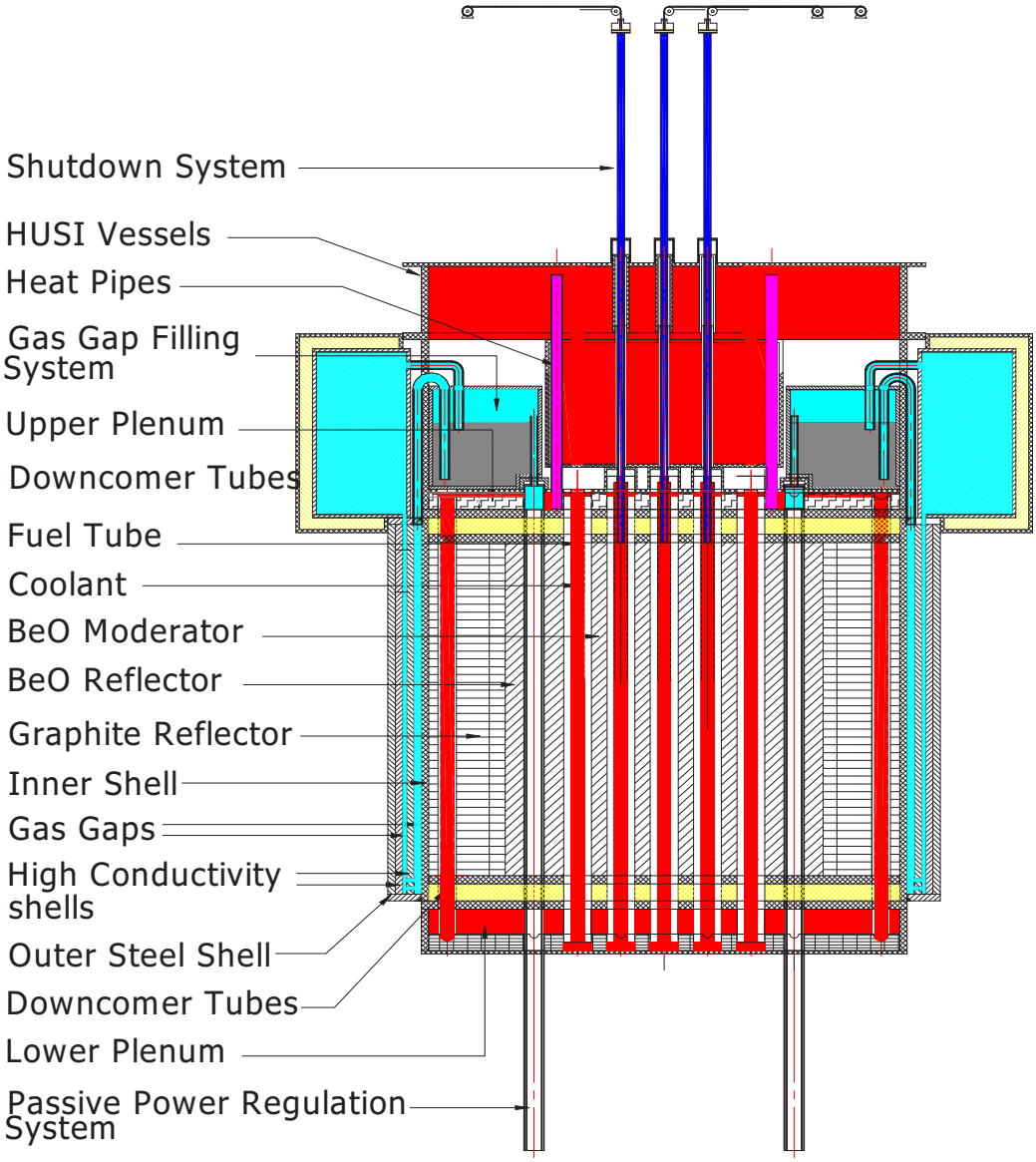


FIG. X-2. Layout of CHTR fuel.

X–2. PASSIVE SAFETY DESIGN FEATURES OF THE CHTR

The *inherent and passive safety features* falling under category A defined in IAEA-TECDOC-626 [X-3] are the following:

- A strong negative Doppler coefficient of the fuel for any operating condition, resulting in a reduction of reactor power in the case of fuel temperature rise during any postulated accident scenario;
- High thermal inertia of the all ceramic core and low core power density, resulting in very slow temperature rise of reactor core components as well as fuel during a condition when all heat sinks are lost;
- A large margin between normal operating temperature of the fuel (around 1100°C) and the allowable limit of TRISO coated particle fuels (1600°C), intended to retain fission products and gases and resulting in their negligible release during normal operating conditions. This also provides a 'healthy' margin of around 500°C to take care of any unwanted global or local power excursions;

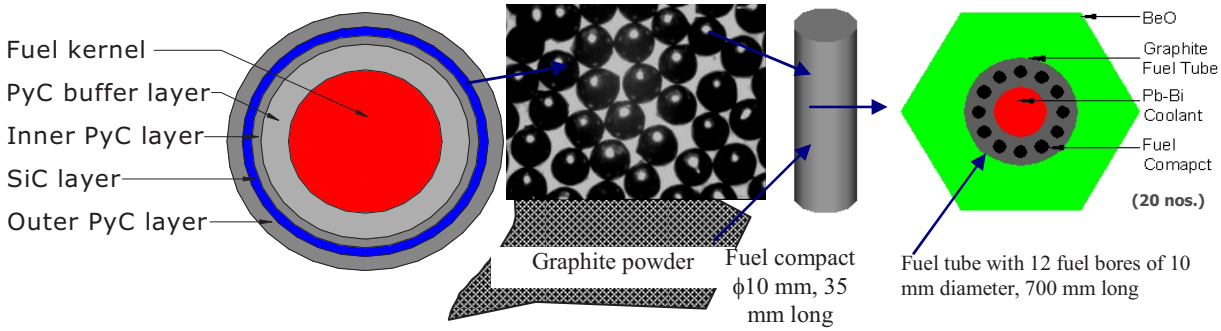


FIG. X-3. Schematic of TRISO coated particle fuel, fuel compact and a single fuel bed.

- A negative moderator temperature coefficient results in lowering of reactor power in the case of an increase in moderator temperature due to any postulated accident condition;
- Due to the use of a lead-bismuth alloy based coolant having a very high boiling point (1670°C), there is a very large thermal margin to Pb-Bi boiling, the normal operating temperature being 1000°C. This eliminates the possibility of heat exchange crisis and increases the reliability of heat removal from the core. The coolant operates at low pressure, there is no over pressurization and no chance of reactor thermal explosion due to coolant overheating;
- The high temperature Pb-Bi coolant, which is maintained in an inert gas atmosphere, is itself chemically inert. Even in the eventuality of accidental contact with air or water, it does not react violently and does not cause any explosions or fires;
- Due to the above atmospheric melting point of 123°C, even in the case of a primary system leakage, coolant solidifies and prevents further leakage;
- There is small thermal energy stored in the coolant, which is available for release in the event of a leak or accident;
- Very low coolant pressure allows for the use of a graphite/carbon based coolant channel having a low neutron absorption cross-section, thus improving the neutronics of the reactor;
- Low induced long lived gamma activity of the coolant, such that in the case of leakage the coolant retains iodine and other radio-nuclides;
- For Pb-Bi coolant, the reactivity effects (void, power, temperature, etc.) are negative; thus reducing reactor power in the case of any inadvertent power or temperature increase.

The *passive safety systems* falling under Categories B, C, D defined in IAEA-TECDOC-626 [X-3] are described below.

Passive power regulation system

CHTR incorporates a passive power regulation system (PPRS). This system operates on the principle of an increase in gas pressure with temperature, thereby pressurizing and forcing a column of molten metal with floating absorbing material into the core. This introduces negative reactivity in the core. Depending on the sensed temperature rise, the system would stabilize at a particular value of reactivity insertion. PPRS operation was analyzed using an in-house developed computer code. This passive system can be classified as a category-B passive system [X-3]. It is a safety grade system. A brief description of the system is provided below.

The passive power regulation system consists of 18 different passive power regulation units (PPRU), each of which is centrally housed in the 18 beryllia reflector blocks. Schematic view of a PPRU is shown in Fig. X-4.

The PPRU has a tube-in-tube design. The outer tube is a control tube and the inner tube is the driver tube. The driver tube also serves as a guide to the absorber. The boron carbide (B_4C) based absorber is an annular structure; it is housed in the annular space between the control and driver tubes. There is liquid lead-bismuth in these tubes, and the two tubes are in fluidic communication via orifices at the bottom of the driver tube. Free liquid surfaces are maintained in both of the tubes. The volume above the liquid is filled with helium. The

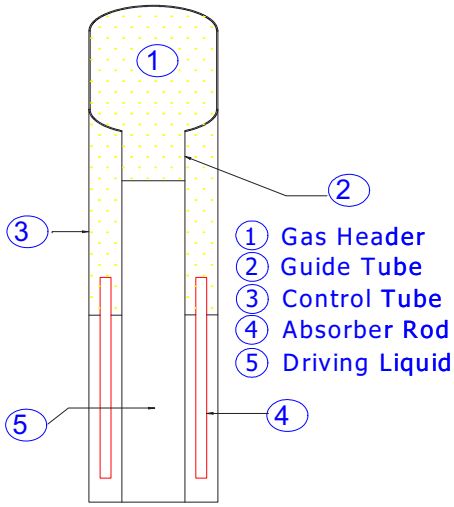


FIG. X-4. Schematic view of PPRS.

absorber floats on the lead-bismuth. A gas header is provided at the top of the driver tube; it is located in the upper plenum, submerged in the coolant. This system operates on the principle of a change in gas pressure with temperature and, therefore, is a category-B passive system [X-3].

When the reactor is critical, the PPRS absorber is located at particular insertion in the core. At this steady state, the gas in the header will be at equilibrium with the coolant temperature in the upper plenum. Any deviation from this equilibrium state will cause the gas to either pressurize or depressurize the driver tube, due to a respective increase or decrease in temperature. As the control and driver tubes are in fluidic communication, this pressure change will be communicated to the control tube. The net result will be a change in liquid lead-bismuth levels in both tubes. Since the absorber is riding on the free liquid surface in the annular space between the control and driver tubes, it will also be pushed in or pulled out with pressurization or depressurization, respectively, thereby changing the reactivity. This system is capable of shutting down the reactor.

Passive shutdown system

The CHTR incorporates a passive shutdown system. Under normal operation, this system has a set of seven shut off rods made of tungsten and held above the reactor core by individual electro-magnets, with their magnetic holding power energized by a set of low power batteries. These shut off rods are passively released under abnormal conditions when the temperature of the coolant or core goes up. These shut off rods fall into the central bore of the fuel tubes provided for coolant flow. This is a fail safe system; in case of a loss of battery power, the shut off rods would fall and shut down the reactor. This passive system can be classified as a Category-D passive system [X-3]. It is a safety grade system.

Passive core heat removal under normal operation

During normal operation of the reactor, core heat is removed by natural circulation of lead-bismuth eutectic alloy coolant. This passive system can be classified as a Category-B passive system. It is a safety grade system. A brief description of it is given below.

The reactor operates at 100 kW(th) and the lead-bismuth eutectic alloy coolant flowing in the main heat transport system by natural circulation removes heat generated in the fuel. Lead-bismuth eutectic alloy has a high boiling point (1670°C) at atmospheric pressure. This facilitates a low pressure primary system, which is a safety feature of liquid metal cooled reactors. The main coolant circulating loop comprises fuel tubes, down-comers and top and bottom plenums. A simplified view of the system discussed is shown in Fig. X-5. The fuel transfers energy to the coolant flowing upward inside the fuel tubes due to natural circulation. At 900°C, the

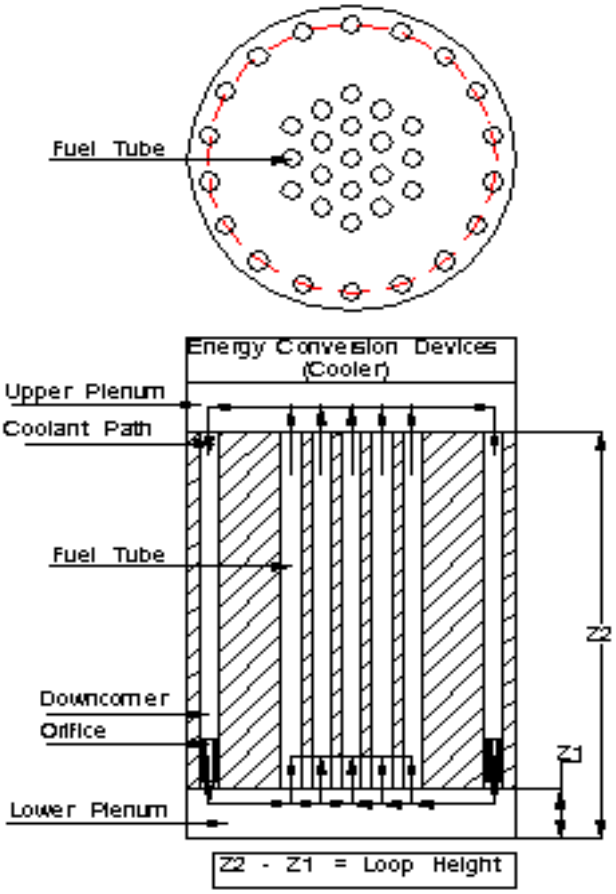


FIG. X-5. Schematic view of CHTR primary circuit loop.

coolant enters the fuel tube in the lower plenum and takes the reactor heat; at 1000°C it is delivered to the upper plenum. The active heat generation length in the reactor is 700 mm. The buoyancy head developed in the coolant loop is adequate to maintain the required flow rate for normal power levels. A computer code, based on the law of conservation of momentum, was developed for this analysis.

Passive transfer of heat to the secondary system

A set of 12 high temperature sodium heat pipes passively transfer heat from upper plenum of the reactor to a set of heat utilization vessels, which are kept directly above the upper plenum. This system can be classified as a Category-B passive system [X-3]. It is a safety grade system.

Passive heat removal under postulated accident conditions

The CHTR has three independent and redundant passive heat removal systems to cater to different postulated accident conditions. These heat removal systems, which are individually capable of removing a neutronically-limited power of 200 kW(th) (200% of normal reactor power), may operate together or independently to prevent the temperature of the core and coolant from increasing beyond a set point. For a loss of load condition, when coolant circuit is intact, a system of six variable conducting sodium heat pipes dissipates heat to the atmosphere. A system of 12 carbon-carbon composite variable conducting heat pipes provided in the reactor core fills the need when coolant is lost. Another passive heat removal system involves the filling of two gas gaps, provided outside the reactor vessel, by a siphon action with molten metal to provide a conduction heat path from the reactor core to a heat sink outside the outer steel shell. Each of these three systems can be

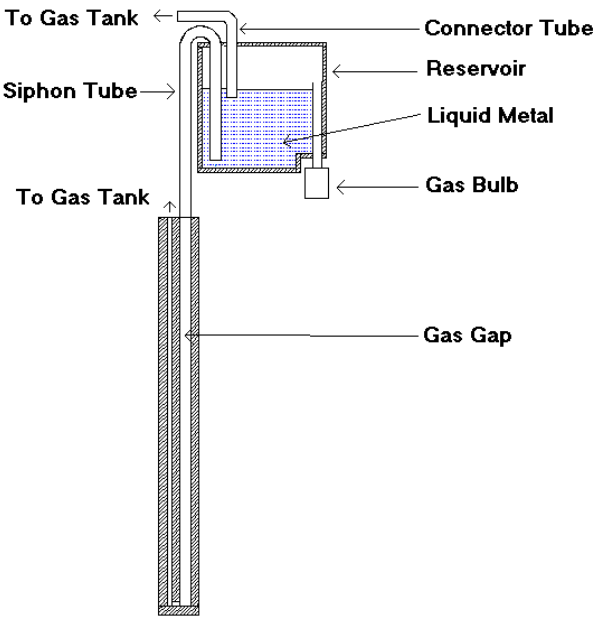


FIG. X-6. Gas gap molten metal filling based passive accident condition heat removal system.

classified as Category-B passive systems [X-3]. These are safety grade systems. A brief description of the gas gap filling system is provided below; its schematic view is shown in Fig. X-6.

The system consists of a reservoir located above the upper plenum and subdivided into compartments. Liquid metal is stored in the reservoir, which is fitted with siphon tubes and bulbs. One end of the siphon is dipped into the liquid metal and the other opens into the inner gas gap; multiple siphon tubes are employed. The bulb is located immediately downstream of the heat pipes and normally senses a temperature of 900°C. In a case of non-availability of the heat pipes, the coolant immediately senses a temperature of 1000°C. This would increase the pressure of the gas inside the bulb, cause the liquid metal to rise inside the siphon tube and ultimately, start the siphon. The liquid metal would then exit into the inner gas gap and also fill the outer air gap through holes in the inner gas gap wall. The gas inside the gas gap would be pushed into a gas tank. A connector between the liquid metal and the gas tank would handle the decrease in pressure caused by the fall in level of liquid metal in the reservoir, such that after some time, pressure in the reservoir and the gas gaps would be equalised.

The CHTR incorporates the following *active systems*, which are all non-safety-grade.

Passive shutdown – reset system:

In order to move the shut off rods to their position of suspension in electromagnets, CHTR employs a motorized and wire rope based active system. This is a backup system.

Passive gas gap heat removal – reset system:

In order to drain and move molten metal from the gas gaps to a reservoir, CHTR employs an electromagnetic pump based reset system. This is a backup system.

Defuelling and refuelling system:

After the operation of fuel up to a desired burnup, fuel tubes containing fuel compacts will be replaced by new fuel tubes carrying fresh fuel compacts. This replacement operation will be done using an active system. This is a backup system.

X–3. ROLE OF PASSIVE SAFETY DESIGN FEATURES IN DEFENCE IN DEPTH

Some major highlights of the CHTR's passive safety design features, structured in accordance with various levels of defence in depth [X-4, X-5], are described below.

Level 1: Prevention of abnormal operation and failure

CHTR design features contributing to this level are as follows:

(a) Heat removal from the core under normal operating conditions is accomplished through natural circulation of the coolant, which essentially eliminates the hazard of a loss of coolant flow;
(b) The extent of overpower transients and their consequences are limited by:
  (i) Low core power density;
  (ii) A highly negative Doppler (fuel temperature) coefficient, achieved through the selection of an appropriate fuel composition;
  (iii) Use of a burnable poison to compensate for reactivity change with burnup;
  (iv) Negative reactivity effects (void, power, temperature, etc.) achieved with the use of a lead-bismuth based coolant;
  (v) Use of an all ceramic core with high heat capacity and high temperatures margins;
  (vi) The resulting low excess reactivity.

Level 2: Control of abnormal operation and detection of failure

The CHTR design features contributing to this level are the following:

(i) Increased reliability of the control system achieved through the use of a passive power regulation system. This system inserts negative reactivity in the core when temperature increases beyond allowable limits;
(ii) The use of two independent, passively operating shutdown systems;
(iii) The use of a high heat capacity ceramic core to prevent fuel temperature from exceeding design limits for a long time.

The abovementioned design features are expected to result in reactor operation and safety functions being fully passive and requiring minimum operator intervention.

Level 3: Control of accidents within the design basis

Features of the CHTR that contribute to this level are:

(i) The use of two independent shutdown systems, one comprising mechanical shut off rods and the other employing a temperature feedback gas-expansion based passive shutdown system, altogether resulting in an increased shutdown reliability;
(ii) The use of two independent systems to transfer reactor core heat to the outside environment during abnormal conditions, one comprising a gas gap filling system and the other, a heat pipe based system;
(iii) The use of an independent system based on carbon-carbon composite heat pipes for the transfer of heat from the reactor core to the atmosphere in the case of a loss of coolant;
(iv) The use of a high heat capacity ceramic core to prevent fuel temperature from exceeding design limits for a long time.

Level 4: Control of severe plant conditions, including prevention of accident progression and mitigation of consequences of severe accidents

The features important for this level are:

(i) Excellent high temperature (up to 1600°C) performance of the TRISO coated particle fuel, ensuring that the probability of a release of fission products and gases is very low;
(ii) Large heat capacity ceramic core, resulting in a slow fuel temperature rise with more than 50 minutes available for corrective action even when all heat sinks are lost;
(iii) The use of a heat sink outside the outer steel shell;
(iv) Erection of the reactor in an underground pit with sealed barrier of reinforced concrete and steel covers is foreseen to provide an additional barrier for prevention of radioactive nuclide release.

Level 5: Mitigation of radiological consequences of significant release of radioactive materials

Passive design features mentioned in the previous levels remove the possibility of significant release of radioactive materials and the necessity for evacuation or relocation measures outside the plant site.

X–4. ACCEPTANCE CRITERIA FOR DESIGN BASIS AND BEYOND DESIGN BASIS ACCIDENTS

X–4.1. List of design basis and beyond design basis accidents

The following is a preliminary list of design basis accidents (DBA) and beyond design basis accidents (BDBA):

(a) Inadvertent withdrawal of one control rod from the passive power regulation system so positive reactivity is inserted;
(b) Loss of load accident;
(c) Loss of coolant accident;
(d) Air ingress.

A number of inherent and passive safety features in the design of the CHTR prevent the TRISO coated particle fuel from exceeding temperature limits in postulated accidents or abnormal events [X-1]. No further details were provided.

X–4.2. Acceptance criteria

To ensure safety (i.e. to meet allowable radiological consequences during all foreseeable plant conditions) the following fundamental safety functions should be ensured in operational states, in and following a DBA and in and after the occurrence of BDBA conditions for the events a), b), and c) specified in X-4.1:

- Control of reactor power so as to limit maximum fuel kernel centre temperature to less than 1600°C;
- Removal of heat from the core so as to maintain a fuel kernel centre temperature of less than 1600°C;
- Confinement of radioactive materials and control of operational discharges, as well as limitation of accidental releases. This is again ensured by keeping the fuel kernel centre temperature at less than 1600°C.

X–5. PROVISIONS FOR SAFETY UNDER EXTERNAL EVENTS

The safety design features of the CHTR intended to cope with external events and external/internal event combinations are described in detail in [X-6].

Combinations of events considered in the design are:

- Earthquakes;
- Aircraft crashes;
- Cyclones;
- Flooding.

Protection against earthquakes is provided by various structures, systems, and components of the CHTR, designed appropriately for high level and low probability seismic events such as an operating basis earthquake (OBE) or a safe shutdown earthquake (SSE) [X-6]. Seismic instrumentation, such as isolators and dampers, are also planned.

For protection against aircraft crashes and cyclones, the reactor will be installed in an underground pit, providing the reactor building a low exterior profile, to reduce the possibility of an aircraft impact and mitigate the adverse effects of cyclones. Additionally, the reactor will be provided with a low leakage thick steel vessel to absorb energy in the case of a postulated aircraft impact.

For protection against flooding, the reactor will be provided with a low leakage thick steel vessel with a reduced number and size of penetrations to prevent water ingress into the reactor systems. Additional watertight barriers and ducts will be provided for systems communicating to the control room.

X–6. PROBABILITY OF UNACCEPTABLE RADIOACTIVITY RELEASE BEYOND THE PLANT BOUNDARY

The probability of unacceptable radioactivity release beyond the plant boundary is targeted to be less than 1×10^{-7}/year.

X–7. MEASURES PLANNED IN RESPONSE TO SEVERE ACCIDENTS

Due to the above mentioned features provided in the reactor, no adverse effects in the public domain are anticipated.

X–8. SUMMARY OF PASSIVE SAFETY DESIGN FEATURES FOR CHTR

Tables X-2 to X-6 below provide the designer's response to questionnaires developed at an IAEA technical meeting, "Review of passive safety design options for SMRs", held in Vienna on 13-17 June 2005. These questionnaires were developed to summarize passive safety design options for different SMRs according to a common format, based on the provisions of IAEA Safety Standards [X-4] and other IAEA publications [X-5, X-3]. The information presented in Tables X-2 to X-6 provided a basis for the conclusions and recommendations of the main part of this report.

TABLE X-2. QUESTIONNAIRE 1 — LIST OF SAFETY DESIGN FEATURES CONSIDERED FOR/ INCORPORATED INTO THE CHTR DESIGN

#	Safety design features	What is targeted?
1.	High negative Doppler (fuel temperature) coefficient	Reduction of the extent of overpower transient so as to keep the maximum fuel (kernel of TRISO coated particle fuel) temperature less than 1600°C
2.	Burnable poison in fuel	
3.	Small excess reactivity	
4.	Pb-Bi coolant –reactivity effects (void, power, temperature, etc.) are negative	
5.	Negative moderator temperature coefficient	
6.	Low core power density	
7.	TRISO coated particle fuel	Low probability of release of fission products and gases even at very high temperatures of up to 1600°C
8.	High heat capacity ceramic core	Large thermal inertia ensures slow temperature rise of fuel even when all heat sinks are lost
9.	Use of Pb-Bi eutectic alloy as coolant	Chemically inert to water and air at high temperature
		High boiling point and good thermal properties increases reliability of heat removal from the core
		Operating temperature that is much below the boiling point – results in a low pressure system, reducing the possibility of high pressure related accidents as well as facilitating the use of carbon based coolant tubes so as to improve neutron economy
		In the case of a leakage, it solidifies, preventing further leakage as well as retaining the radioactive nuclides present in the coolant
10.	Heat removal from the core by natural circulation	Elimination of pump failure related initiating events, such as Loss of Coolant Flow
11.	Passive power regulation system	Passive power regulation
12.	Two independent shutdown systems	Redundancy in reactor protection during transient/postulated accident conditions
13.	A system of gas gap filling with high conductivity molten metal	Passive means of core heat removal under abnormal conditions and of transfer of heat to a heat sink outside the shell.
14.	Heat pipe based heat removal system during normal operation	Transfer of heat passively from coolant to heat utilizing system vessels
15.	Variable conductance heat pipes	Heat dissipation from coolant to the outside environment during postulated accident conditions
16.	Carbon-carbon composite heat pipes	Heat dissipation from the reactor core to the outside environment during postulated accident conditions
17.	Large capacity heat sink outside the outer steel shell	Absorb neutronically limited power fully in case of postulated accident condition

TABLE X-3. QUESTIONNAIRE 2 — LIST OF INTERNAL HAZARDS

#	Specific hazards that are of concern for a reactor line	Explain how these hazards are addressed in an SMR
1.	Prevent unacceptable reactivity transients	• Passive power regulation and shutdown systems • Highly negative Doppler (fuel temperature) coefficient • TRISO coated particle fuel – capable of withstanding very high temperature and retaining fission products • Large heat capacity all ceramic core, resulting in slow temperature rise • Negative moderator temperature coefficients • Three redundant and passive heat removal systems to dissipate neutronically limited power to the atmosphere/heat sink • Pb-Bi coolant, ensuring that reactivity effects (void, power, temperature etc.) are negative
2.	Avoid loss of coolant	• Low pressure, high density, and high melting point Pb-Bi coolant leaks out very slowly in case of a break in the circuit and eventually solidifies • Natural circulation of Pb-Bi coolant in normal operation mode with no piping or joints in the circuit, thus reducing chances of loss of coolant • High boiling point of Pb-Bi coolant (1670°C)
3.	Avoid loss of heat removal	• Natural circulation of Pb-Bi in normal operation mode • Three redundant and passive heat removal systems to dissipate neutronically limited power to atmosphere/heat sink under postulated accident conditions
4.	Avoid loss of flow	• Natural circulation of Pb-Bi coolant in normal operation mode; No piping or joints in the circuit, thus avoiding the possibility of loss of flow
5.	Avoid exothermic chemical reactions: Graphite fire (Reaction with oxygen/water)	Graphite with SiC as outer coating is unlikely to burn
		Blanket of inert gas on top of the coolant
		Low pressure, high density, and high melting point Pb-Bi coolant leaks out very slowly in the case of a break in the circuit and eventually solidifies – low probability of ingress of a large quantity of air
		Water ingress in the core and contact with the graphite is an unlikely event, as water is present only as an ultimate heat sink outside the thick steel vessel with no openings
6.	Polonium activity (specific for lead-bismuth eutectic cooled reactors)	– Inert gas blanket provided on top of the coolant prevents coolant from coming in contact with air thus preventing the release of radioactivity – In case of a leak; coolant will solidify, preventing further leakage

TABLE X-4. QUESTIONNAIRE 3 — LIST OF INITIATING EVENTS FOR ABNORMAL OPERATION OCCURRENCES (AOO)/DESIGN BASIS ACCIDENTS (DBA)/BEYOND DESIGN BASIS ACCIDENTS (BDBA)

#	List of initiating events for AOO/DBA/BDBA typical for a reactor line (heavy liquid metal cooled reactors)	Design features of CHTR used to prevent progression of initiating events to AOO/DBA/BDBA, to control DBA, to mitigate BDBA consequences, etc.	Initiating events specific to this particular SMR
1.	Inadvertent withdrawal of one control rod of the passive power regulation system creating positive reactivity	– High negative Doppler (fuel temperature) coefficient	Nothing in particular specified here
		– Passive power regulation and shutdown systems	
		– Negative moderator temperature coefficient	
		– Pb-Bi coolant, for which reactivity effects (void, power, temperature, etc.) are negative	
2.	Loss of load accident	– Highly negative Doppler (fuel temperature) coefficient	
		– Two redundant and passive heat removal systems to dissipate the neutronically limited power to a heat sink	
		– Passive power regulation and shutdown systems	
		– Large heat capacity of the all ceramic core results in a slow temperature rise	
		– Low core power density	
		– TRISO coated particle fuel with high temperature margin to failure	
3.	Loss of coolant accident	– High negative Doppler (fuel temperature) coefficient	
		– Passive shutdown system	
		– Carbon-carbon composite heat pipes provided in the core to dissipate heat	
		– Large heat capacity of the all ceramic core results in a slow temperature rise	
		– Low core power density	
		– TRISO coated particle fuel with high temperature margin to failure	
4.	Air ingress to the primary coolant system	– Graphite with SiC as outer coating is unlikely to burn	
		– Blanket of inert gas on top of the coolant	
		– Low pressure, high density, and high melting point Pb-Bi coolant leaks out very slowly in the case of a break in the circuit and eventually solidifies; creates low probability of a large quantity air ingress	

TABLE X-5. QUESTIONNAIRE 4 — SAFETY DESIGN FEATURES ATTRIBUTED TO DEFENCE IN DEPTH LEVELS

#	Safety design features	Category: A-D (for passive systems only), according to IAEA-TECDOC-626 [X-4]	Relevant DID level, according to NS-R-1 [X-4] and INSAG-10 [X-5]
1.	High negative Doppler (fuel temperature) coefficient	Reduction of the extent of overpower transient so as to limit the maximum fuel (kernel of TRISO coated particle fuel) temperature to less than 1600°C — A Mitigation of loss of load accident — A Mitigation of loss of coolant accident — A	1, 3
2.	Burnable poison in fuel, minimizing the reactivity margin for fuel burnup	Reduction of the extent of possible overpower transient so as to keep the maximum fuel (kernel of TRISO coated particle fuel) temperature less than 1600°C — A	1
3.	Small excess reactivity	Reduction of the extent of possible overpower transient so as to keep the maximum fuel (kernel of TRISO coated particle fuel) temperature less than 1600°C — A	1
4.	Pb-Bi coolant - the reactivity effects (void, power, temperature, etc.) are negative	Reduction of the extent of possible overpower transient so as to keep the maximum fuel (kernel of TRISO coated particle fuel) temperature less than 1600°C — A	1
5.	Negative moderator temperature coefficient	Reduction of the extent of possible overpower transient so as to keep the maximum fuel (kernel of TRISO coated particle fuel) temperature less than 1600°C — A	1
6.	Low core power density	Loss of coolant accident — A Loss of load accident	1, 3
7.	TRISO coated particle fuel with high margin to fuel failure	Loss of coolant accident — A Loss of load accident — A	4
8.	High heat capacity ceramic core	Loss of coolant accident — A Loss of load accident — A	1, 2, 3, 4
9.	Low pressure, high density, and high melting point Pb-Bi coolant leaks out very slowly in the case of a break in the circuit and eventually solidifies	Air ingress — A	1
10.	Heat removal from the core by natural circulation	Loss of flow accident — B	1
11.	Passive power regulation system	Reduction of the extent of possible overpower transient so as to keep the maximum fuel (kernel of TRISO coated particle fuel) temperature less than 1600°C — B Loss of load accident — B	2

TABLE X-5. QUESTIONNAIRE 4 — SAFETY DESIGN FEATURES ATTRIBUTED TO DEFENCE IN DEPTH LEVELS (cont.)

#	Safety design features	Category: A-D (for passive systems only), according to IAEA-TECDOC-626 [X-4]	Relevant DID level, according to NS-R-1 [X-4] and INSAG-10 [X-5]
12.	Two independent shutdown systems	Reduction of the extent of possible overpower transient so as to keep the maximum fuel (kernel of TRISO coated particle fuel) temperature less than 1600°C — One B, and the other D Loss of load accident — One B, and the other D Loss of coolant accident — One B, and the other D	2, 3
13.	A system of gas gap filling with high conductivity molten metal	Loss of load accident — A	3
14.	Heat pipe based heat removal system during normal operation	B	1, partially 3
15.	Variable conductance heat pipes, intended to dissipate core heat	Loss of load accident— B	3
16.	Carbon-carbon composite heat pipes, intended to dissipate core heat	Loss of coolant accident — B	3
17.	Large capacity heat sink outside the outer steel shell	Loss of load accident — A	4
18.	Construction of the reactor in an underground pit	External events — A	4

TABLE X-6. QUESTIONNAIRE 5 — POSITIVE/NEGATIVE EFFECTS OF PASSIVE SAFETY DESIGN FEATURES IN AREAS OTHER THAN SAFETY

Passive safety design features	Positive effects on economics, physical protection, etc.	Negative effects on economics, physical protection, etc.
Natural circulation of heavy metal coolant	Saving in pump costs and associated components; saving due to simplified design and maintenance	
Thorium fuel cycle with TRISO coating based fuel configuration	Increased proliferation resistance	
Heat pipe based heat transfer to secondary system	Simplified design and maintenance, saving in cost of heat exchanger and associated components	Higher specific cost of reactor due to lower core power density selected for demonstration, because TRISO particles occupy larger volume as compared to conventional fuel
Passive power regulation system	Simplified design and maintenance, saving in cost with respect to conventional complex mechanism based system	
Passive heat removal based on gas gap filling with molten metal in accident conditions	Simplified design and maintenance with an associated reduction in cost	

REFERENCES TO ANNEX X

[X–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Small Reactor Designs Without On-site Refuelling, IAEA-TECDOC-1536, IAEA, Vienna (2007).

[X–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Innovative Small and Medium Sized Reactor Designs 2005: Reactors with Conventional Refuelling Schemes, IAEA-TECDOC-1485, IAEA, Vienna (2006).

[X–3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Terms for Advanced Nuclear Plants, IAEA-TECDOC-626, IAEA, Vienna (1991).

[X–4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

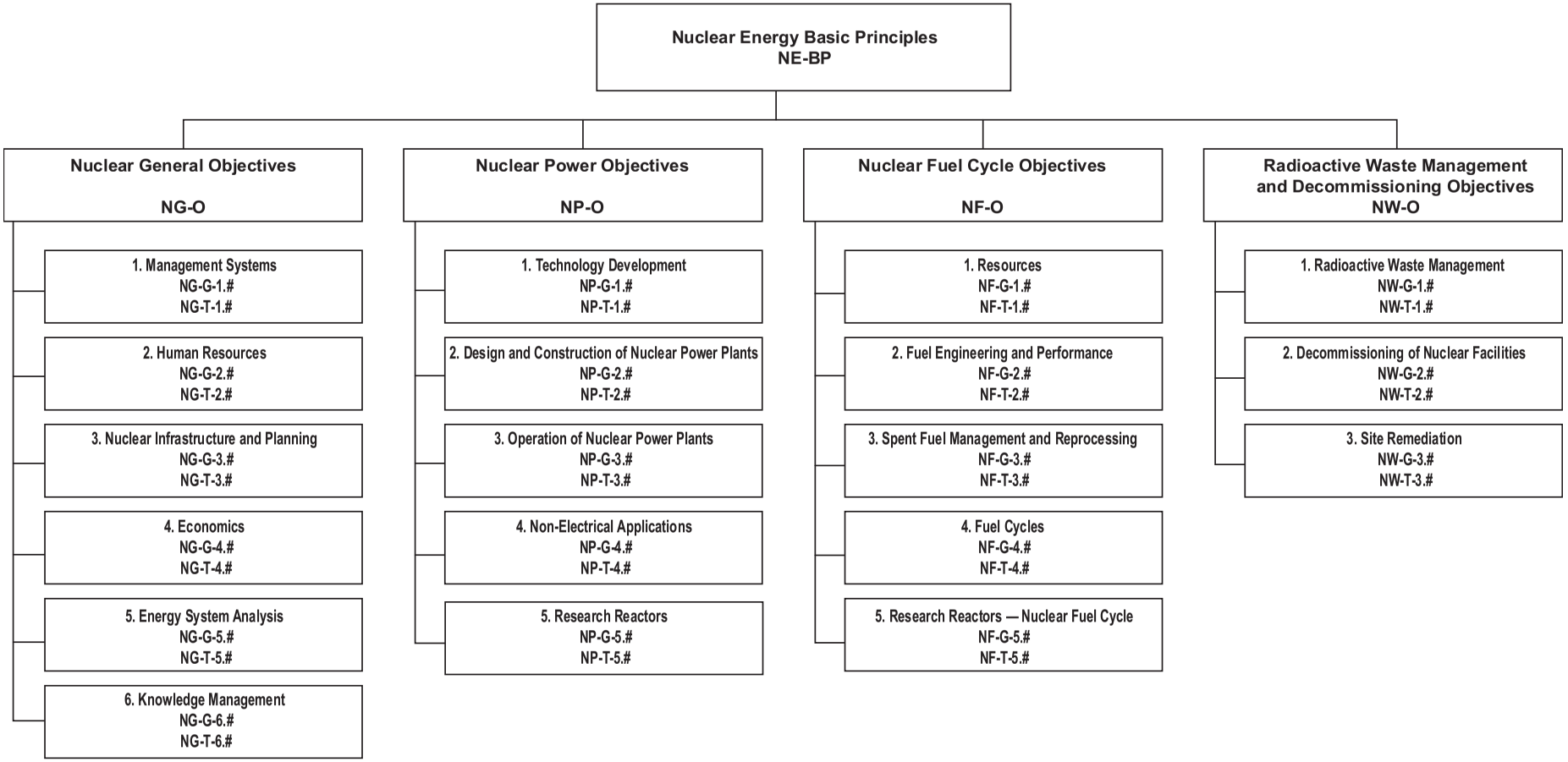
[X–5] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

[X–6] INTERNATIONAL ATOMIC ENERGY AGENCY, Advanced Nuclear Power Plant Design Options to Cope with External Events, IAEA-TECDOC-1487, IAEA, Vienna (2006).

CONTRIBUTORS TO DRAFTING AND REVIEW

Delmastro, D.	Comisión Nacional de Energía Atómica, Centro Atómico Bariloche,Argentina
Carelli, M.	Westinghouse Science and Technology, USA
Petrovic, B.	Westinghouse Science and Technology, USA
Mycoff, C.	Westinghouse Science and Technology, USA
Gautier, G.-M.	DER/SESI/LESA CEA Cadarache, France
Delpech, M.	CEA-Saclay-DEN-DDIN, France
Naviglio, A.	The University of Rome 'La Sapienza', Italy
Cumo, M.	The University of Rome 'La Sapienza', Italy
Nishimura, S.	Central Research Institute of Electric Power Industry (CRIEPI), Japan
Nayak, A.K.	Reactor Engineering Division, Thermal Hydraulics Section, Bhabha Atomic Research Centre, India
Devictor, N.	CEA/DEN/DER/SESI/LCFR, France
Saha, D.	Reactor Engineering Division, Bhabha Atomic Research Centre, India
Dulera, I.V.	Reactor Engineering Division, Bhabha Atomic Research Centre (BARC), Trombay, Mumbai, India
Shepelev, S.	Experimental Design Bureau of Machine Building (OKBM), Russian Federation
Lepekhin, A.N.	Experimental Design Bureau of Machine Building (OKBM), Russian Federation
Sienicki, J.J.	Innovative Systems Development, Nuclear Engineering Division, Argonne National Laboratory (ANL), USA
Wade, D.C.	Nuclear Engineering Division, Argonne National Laboratory (ANL), USA
Minato, A.	Nuclear Energy Strategy Office, Central Research Institute of Electric Power Industry (CRIEPI), Japan
Sinha, R.K.	Reactor Engineering Division, Bhabha Atomic Research Centre (BARC), Trombay, Mumbai, India
Kuznetsov, V.	International Atomic Energy Agency, Vienna, Austria

Structure of the IAEA Nuclear Energy Series



Key

BP: Basic Principles
O: Objectives
G: Guides
T: Technical Reports
Nos. 1-6: Topic designations
#: Guide or Report number (1, 2, 3, 4, etc.)

Examples

NG-G-3.1: Nuclear General (**NG**), **G**uide, Nuclear Infrastructure and Planning (topic **3**), **#1**
NP-T-5.4: Nuclear Power (**NP**), Report (**T**), Research Reactors (topic **5**), **#4**
NF-T-3.6: Nuclear Fuel (**NF**), Report (**T**), Spent Fuel Management and Reprocessing, **#6**
NW-G-1.1: Radioactive Waste Management and Decommissioning (**NW**), **G**uide, Radioactive Waste (topic **1**), **#1**

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–104209–5
ISSN 1995–7807