IAEA-TECDOC-1487

Advanced nuclear plant design options to cope with external events

IAEA
International Atomic Energy Agency

February 2006

IAEA-TECDOC-1487

Advanced nuclear plant design options to cope with external events

IAEA
International Atomic Energy Agency

February 2006

The originating Section of this publication in the IAEA was:

Nuclear Power Technology Development Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

ADVANCED NUCLEAR PLANT DESIGN OPTIONS TO
COPE WITH EXTERNAL EVENTS
IAEA, VIENNA, 2006
IAEA-TECDOC-1487
ISBN 92–0–100506–7
ISSN 1011–4289

Printed by the IAEA in Austria
February 2006

FOREWORD

With the stagnation period of nuclear power apparently coming to an end, there is a renewed interest in many Member States in the development and application of nuclear power plants (NPPs) with advanced reactors. Decisions on the construction of several NPPs with evolutionary light water reactors have been made (e.g. EPR Finland for Finland and France) and more are under consideration. There is a noticeable progress in the development and demonstration of innovative high temperature gas cooled reactors, for example, in China, South Africa and Japan. The Generation IV International Forum has defined the International Near Term Deployment programme and, for a more distant perspective, six innovative nuclear energy systems have been selected and certain R&D started by several participating countries. National efforts on design and technology development for NPPs with advanced reactors, both evolutionary and innovative, are ongoing in many Member States.

Advanced NPPs have an opportunity to be built at many sites around the world, with very broad siting conditions. There are special concerns that safety of these advanced reactors may be challenged by external events following new scenarios and failure modes, different from those well known for the currently operated reactors. Therefore, the engineering community identified the need to assess the proposed design configurations in relation to external scenarios at the earliest stages of the design development. It appears that an early design optimization in relation to external events is a necessary requirement to achieve safe and economical advanced nuclear power plants.

Reflecting on these developments, the IAEA has planned the preparation of a report to define design options for protection from external event impacts in NPPs with evolutionary and innovative reactors. The objective of this publication is to present the state-of-the-art in design approaches for the protection of NPPs with evolutionary and innovative reactors from external event impacts, as well as to assist the designers of advanced NPPs in the definition of a consistent strategy of design and siting evaluation in relation to extreme external events.

This publication was prepared through the collaboration of the designers of 14 advanced NPPs from Argentina, Canada, Germany, India, Japan, Lithuania, the Republic of Korea, the Russian Federation and the United States of America, and was supported by a dedicated IAEA technical meeting convened in Vienna 14–19 November 2004. This publication also incorporates the contributions from several international experts, who provided descriptions of the state of the art approaches and methodologies for site safety assessment, probabilistic safety assessment (PSA) in relation to external events, and component qualification.

The IAEA officers responsible for this publication were V. Kuznetsov of the Division of Nuclear Power and P. Contri of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

The papers in these proceedings are reproduced as submitted by the authors and have not undergone rigorous editorial review by the IAEA.

The views expressed do not necessarily reflect those of the IAEA, the governments of the nominating Member States or the nominating organizations.

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

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

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

CONTENTS

APPENDICES I-II

ANNEXES I-VII

1. INTRODUCTION

1.1. Background

The IAEA-TECDOC-936 Terms for Describing New, Advanced Nuclear Power Plants" [1.1] defines an *advanced design* as "a design of current interest for which improvement over its predecessors and/or existing designs is expected. Advanced designs consist of *evolutionary designs* and designs requiring substantial development efforts", i.e. *innovative designs*. An *evolutionary design* is defined as "an advanced design that achieves improvements over existing designs through small to moderate modifications, with a strong emphasis on maintaining design proveness to minimize technological risks", while "an *innovative design* is an advanced design which incorporates radical conceptual changes in design approaches or system configuration in comparison with existing practice. Substantial R&D, feasibility tests and a prototype or demonstration plant are probably required for an innovative design" [1.1].

Multiple concepts and projects of nuclear power plants (NPPs) with evolutionary or innovative nuclear reactors are being developed worldwide [1.2–1.6]. The IAEA activities to foster development of advanced water cooled, liquid metal cooled and gas cooled reactor technology are carried out on the advice and with the support of technical working groups (TWGs) that consist of representatives of national programmes and international organizations in these technologies. Upon the advice and with the support of these TWGs, the IAEA periodically prepares status reports and other publications on advanced reactor designs to provide all interested IAEA Member States with balanced and objective information on advances in nuclear plant technology, and coordinates international efforts on selected issued of technology development for such reactors [1.2–1.5]. Reflecting on the needs of many developing countries, the IAEA also carries out dedicated activities for small and medium sized reactors (SMRs), i.e. reactors with the equivalent electric power less than 700 MW(e) [1.6].

Under the terms of Article III of its Statute, the IAEA is authorized to establish standards of safety for protection against ionizing radiation and to provide for the application of these standards to peaceful nuclear activities. The regulatory related publications by means of which the IAEA establishes safety standards and measures are issued in the IAEA Safety Standards Series. This series covers nuclear safety, radiation safety, transport safety and waste safety, and also general safety (that is, of relevance in two or more of the four areas), and the categories within it are Safety Fundamentals, Safety Requirements and Safety Guides. Full information on the IAEA's safety standards programme is available at the IAEA Internet site: <http://www.iaea.org/OurWork/SS/index.html>. The IAEA has recently produced the updated safety guides and other publications on NPP design and siting regarding external events [1.7, 1.8, 1.9–1.14]. The purpose of these safety guides is to provide recommendations and guidance on design and siting for the protection of nuclear power plants from the effects of human induced and natural external events. Other IAEA publications describe good practices and give practical examples and detailed methods that can be used to meet safety requirements in relevant area [1.8, 1.14]. The IAEA is also running a dedicated programme to develop a consensus safety approach for innovative reactors [1.15].

High level of safety and improved economic competitiveness are common goals for advanced NPPs [1.2–1.6]. In particular, provision of a high level of safety remains and will be the crucial issue for all evolutionary and innovative NPPs. An overall NPP safety is defined by many factors, among which an important one is plant protection from external events[1].

This aspect may become even more important in the future in view of possible global deployment of nuclear power accompanied by general globalization of the world economy, which would facilitate

[1] Reference [1.9] defines an external event as the "event that originates outside the site and whose effects on the nuclear power plant should be considered. Such events could be of natural or human induced origin and are identified and selected for design purposes during the site evaluation process. In some cases events originating on the site but outside the safety related buildings can be treated as external events if the characteristics of the generated loads are similar to those caused by off-site events".

increased export of NPPs and their deployment in a variety of siting conditions, particularly in today's developing countries [1.16].

The IAEA periodically reviews the status of protection from external events for many operating NPPs worldwide [1.8, 1.14]. However, only a few advanced NPP designs have so far been addressed by the IAEA for this issue.

The IAEA maintains communications with the designers of many evolutionary and innovative NPPs worldwide, and through these communications it was found that a systematic consideration of the issues of plant protection from impacts of external events at an early design stage is not a common practice in Member States, especially for NPPs with innovative reactors. At the same time, designers of many such reactors target an improved plant economy and reduced design complexity as achieved by strong reliance on inherent and passive safety features and, based on the analysis of internal events only, provide very low figures for a probability of radioactivity release beyond the plant boundary. If a consistent strategy regarding protection from external events is not defined at an early stage in plant design, this may result in incremental costs and narrowed siting options for the NPP, when these issues are brought out at final design stages.

1.2. Objectives

In line with the abovementioned developments, the objectives of this report are the following:

(1) Through direct cooperation with the designers of advanced NPPs, to define, collate and present the state-of-the art in design features and approaches used to protect plants from external event impacts, making a focus on NPPs with evolutionary and, when possible, innovative designs;

(2) Reflecting best practices achieved in Member States, to provide a technical and information background to assist designers of advanced NPPs in defining a consistent strategy regarding selected design and site evaluation issues in relation to extreme external events;

(3) To bring to the attention of designers of advanced NPPs the recently updated IAEA safety guides and other publications on issues of plant protection from external event impacts; to collect comments on their applicability to NPPs with evolutionary and innovative reactors; to identify safety and technological issues and proposals for their resolution; and to outline future challenges and potential contribution of the IAEA.

1.3. Scope

No limitations were set on the scope of external events, which, according to the recommendations of [1.9], may include:

(a) *Human induced events:*

- Aircraft crashes;
- Explosions (deflagrations and detonations) with or without fire, originated from off-site sources and on-site (but external to safety related buildings), like storage of hazardous materials, transformers, high energy rotating equipment;
- Release of hazardous gas (asphyxiant, toxic) from off-site and on-site storage;
- Release of corrosive gas and liquids from off-site and on-site storage;
- Fire generated from off-site sources (mainly for its potential for smoke and toxic gas production);
- Collision of ships and floating debris (ice, logs, etc.) with essential water intakes;
- Electromagnetic interference from off-site (e.g. from communication centres, portable phone antennas) and on-site (e.g. from the activation of high voltage electric switch gears);
- Any combination of the above as a result of a common initiating event (e.g. explosion with release of hazardous gases, smoke and fire);

(b) *Natural events:*

- Earthquakes;
- Extreme meteorological conditions (temperature, snow, hail, frost, subsurface freezing, drought);
- Floods (from tides, tsunamis, seiches, storm surges, precipitation (rain, snow and ice), waterspouts, dam forming and dam failures, snow melt, landslides into water bodies, channel changes, work in the channel);
- Landslides and avalanches;
- Cyclones (hurricanes, tornadoes and tropical typhoons);
- Abrasive dust and sand storms;
- Lightning;
- Volcanism.

Likewise, there were no limitations on specific types of evolutionary or innovative reactors within the NPP projects to be addressed, and many designers around the world were invited to participate. As a result, 14 designs of advanced NPPs ranging from the evolutionary EPR Finland (AREVA) and ABWR-II (Hitachi, Japan) to the innovative Advanced Heavy Water Reactor (AHWR) and Compact High Temperature Reactor (CHTR) of Bhabha Atomic Research Centre (BARC), India were addressed. A summary list of the advanced NPPs addressed in this report is given in Table 1. Although many designers of innovative reactors were invited to participate, most of the NPPs addressed were with reactors of evolutionary type.

TABLE 1. NPP DESIGNS CONSIDERED IN THIS REPORT

#	REACTOR	DESIGNER/ COUNTRY	TYPE*	SOURCES
1.	APR 1400	KEPCO/ Republic of Korea	Loop type PWR (E)	APPENDICES I & II and [1.2]
2.	EPR Finland	AREVA/ Europe	Loop type PWR (E)	APPENDICES I & II and [1.2]
3.	VBER-300 (Floating NPP)	OKBM/ Russian Federation	Loop type PWR (E/I)	APPENDICES I & II, ANNEX VII and [1.2]
4.	VVER-91/99	SPb AEP/ Russian Federation	Loop type PWR (E)	APPENDICES I & II and [1.2]
5.	CAREM	CNEA/ Argentina	Integral design PWR (I)	APPENDICES I & II, ANNEX V and [1.2, 1.6]
6.	IRIS	International consortium led by Westinghouse/ USA	Integral design PWR (I)	APPENDICES I & II, ANNEX VI and [1.2, 1.6]
7.	PHWR-540	Operating reactor/ India	PHWR /CANDU (O)	APPENDICES I & II and ANNEX III
8.	ACR-700	AECL/ Canada	PHWR /CANDU (E)	APPENDICES I & II, ANNEX IV and [1.3]
9.	AHWR	BARC/ India	Heavy water moderated boiling light water cooled pressure tube type reactor (I)	APPENDICES I & II and [1.6]

#	REACTOR	DESIGNER/ COUNTRY	TYPE*	SOURCES
10.	SWR 1000	AREVA/ Europe	BWR (E)	APPENDICES I & II and [1.2]
11.	VK-300	NIKIET/ Russian Federation	BWR (E/I)	APPENDICES I & II and [1.2]
12.	ABWR-II	Toshiba/ Japan	BWR (E)	APPENDICES I & II, ANNEX VIII and [1.2]
13.	BN-800	SPb AEP/ Russian Federation	Sodium cooled fast reactor (E/I)	APPENDICES I & II and [1.5]
14.	CHTR	BARC/ India	Lead-bismuth cooled high temperature reactor with HTGR type prismatic fuel (I)	APPENDICES I & II and [1.6]

* E is for evolutionary; I is for innovative; E/I is for evolutionary design with innovative features; O is for operating NPP.

1.4. Content

The report includes introduction, 5 dedicated sections on selected topics, conclusion, 2 appendices and 8 annexes.

Section 1 is the introduction and presents the background, the objectives, the scope and the structure of this report.

Section 2 presents a summary of responses from Member States to the IAEA questionnaire, which requested designers of advanced NPPs to identify, for their respective designs, the scope of accidental mean or median external events considered in the design, the definition of hazard, the event combination criteria, the definition of loads, and load combination rules applied in the design (also with internal events). The designers were also requested to comment on where the criteria of site evaluation and design for advanced NPPs are different from those used in assessment of the existing plants, and to identify certain design features and approaches used in their respective NPPs, that are different from those used in currently operated plants. The responses to questionnaires were received from 11 advanced NPP projects and one operating NPP (PHWR-540 of India, Tarapur units 3,4), specifically, for all NPPs presented in Table 1 except the AHWR and CHTR of India. A summary table of responses to the IAEA questionnaire is included as APPENDIX I.

Section 3 addresses safety requirements for siting of NPPs with advanced reactors. The topics addressed include hazard types and combinations and relevant return periods. Referring to the best practices achieved in Member States, this section presents the criteria and methodology for hazard assessment, compatible with the design features and overall design goals of evolutionary and innovative reactors. In particular, the following issues are addressed: external event scenarios in relation to the expected challenges posed to plant safety, combination criteria for external events, interfaces with the implementation of emergency planning (triggered by external events) and the need to accommodate “unanticipated” scenarios of different nature (including malevolent human actions).

Section 4 collates, presents and analyzes the design features and approaches used in 14 advanced NPPs, with respect to protection from both external and internal events. The topics include: passive features, defence in depth, combinations of internal and external sequences, and emergency planning issues. For this section, a format for the presentation of design features related to plant protection from both, external and internal events was developed, and the requested information was provided and reviewed first-hand by the designers of all 14 NPPs. The original inputs received from the designers are included as APPENDIX II. Section 4 outlines the interactions between engineering and passive features developed to cope with external events, as well as other features typical of advanced reactors. Specifically, it produces an insight on how the consideration of external events can be accomplished at the early stages of plant design. This section also discusses on the role of passive safety design options[2] and outlines an approach to assess their reliability.

Section 5 addresses the issues of component qualification, including special testing, mock-ups, fragility evaluations, and special requirements. This section outlines the use of mock-ups for the qualification of structures, systems and components in advanced reactors (in relation to external events). In particular, the need to use experimental techniques, their outcome, their integration with the design and their impact on the total costs is discussed. A state-of-the-art methodology for seismic fragility evaluation is described in section 4 of ANNEX I.

Section 6 is dedicated to probabilistic safety assessment (PSA) in application to external events. A summary of the experience in Member States is provided, and the applicability of IAEA safety guides is analysed. A state-of-the-art PSA methodology for external events is described in ANNEX I, which also provides a comprehensive list of basic references.

Section 7 presents the conclusions and suggestions for further work.

APPENDICES I and II, and ANNEX I supplement Sections 2, 4, 5 and 6 of this report, respectively.

Certain inputs to this report were provided by an IAEA technical meeting on “Definition of plant safety design options to cope with external events”, held on 14–19 November 2004 in Vienna.

ANNEXES II-VIII present the original papers submitted by the participants of that meeting for publication in this report.

ANNEX II presents a paper on elaboration and application of the methodology to assess external hazards and uncertainties in the design of an NPP.

ANNEXES III to VIII address issues of protection from external events for certain NPPs, as indicated in Table 1.

REFERENCES TO SECTION 1

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

[1.2] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Advanced Light Water Reactor Designs — 2004, IAEA-TECDOC-1439, IAEA, Vienna (2002).

[1.3] INTERNATIONAL ATOMIC ENERGY AGENCY, HWRs — Status and Projected Development, Technical Reports Series, IAEA-TRS-407, IAEA, Vienna (2002).

[1.4] INTERNATIONAL ATOMIC ENERGY AGENCY, Current Status and Future Development of Modular High-Temperature Gas-Cooled Reactor Technology, IAEA-TECDOC-1198, IAEA, Vienna (2001).

[1.5] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Liquid Metal Cooled Fast Reactor Technology, IAEA-TECDOC-1083, IAEA, Vienna (1999).

[1.6] INTERNATIONAL ATOMIC ENERGY AGENCY, Innovative Small and Medium Sized Reactors: Design Approaches, Safety Features and R&D Trends, Final Report of IAEA Technical Meeting Convened in Vienna on 7–11 June 2004, IAEA-TECDOC-1451, IAEA, Vienna (2005).

[1.7] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, Safety Guide, IAEA Safety Standards Series, No. NS-G-1.5, IAEA, Vienna (2003).

[1.8] INTERNATIONAL ATOMIC ENERGY AGENCY, Extreme External Events in the Design and Assessment of Nuclear Power Plants, IAEA-TECDOC-1341, IAEA, Vienna (2003).

[1.9] INTERNATIONAL ATOMIC ENERGY AGENCY, External Human Induced Events in Site Evaluation for Nuclear Power Plants, Safety Standards Series, No. NS-G-3.1, IAEA, Vienna (2002).

[2] The wording ‘passive safety design options’ is optionally used to denote combinations of inherent safety features, passive safety features and passive systems, in line with the definitions suggested in IAEA-TECDOC-626 [1.17].

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

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

[1.12] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, Safety Standards Series, No. NS-G-1.2, IAEA, Vienna (2001).

[1.13] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, Safety Standards Series, No. NS-G-1.6, IAEA, Vienna (2003).

[1.14] INTERNATIONAL ATOMIC ENERGY AGENCY, Earthquake Experience and Seismic Qualification by Indirect Methods in Nuclear Installations, IAEA-TECDOC-1333, IAEA, Vienna (2003).

[1.15] INTERNATIONAL ATOMIC ENERGY AGENCY, Considerations in the Development of Safety Requirements for Innovative Reactors: Application to Modular High Temperature Gas Cooled Reactors, IAEA-TECDOC-1366, IAEA, Vienna (2003).

[1.16] INTERNATIONAL PANEL ON CLIMATE CHANGE, Special Report on Emission Scenarios, A Special Report of Working Group III, Cambridge University Press, Cambridge (2000).

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

2. EXPERIENCES IN MEMBER STATES: ANALYSIS OF QUESTIONNAIRES

2.1. Introduction

In conjunction with a technical meeting on definition of plant safety design options to cope with external events, held on 14-19 November 2004 in Vienna, the IAEA secretariat has developed a questionnaire targeted at the advanced, both evolutionary and innovative NPP designs. The objective was to collect experiences of Member States in relation to the hazard evaluation, selection of classified structures, systems and components (SSCs) and plant protection measures. The analysis of responses to this questionnaire, performed by the scientific secretaries, clarified the approaches adopted in certain Member States for the protection of advanced reactors in relation to external events and, specifically, outlined the differences in safety requirements, siting and engineering approach.

The questionnaire was sent to Member States prior to the meeting with clear indications on the required information. The reference external event scenarios were selected according to [2.1]; their list is provided in Section 1.

Understanding that some advanced NPPs may be at a design stage that it is too early to address the issues of plant protection from external events, the organizers did not expect all topics to be uniformly addressed by all respondents. Moreover, some projects appear to be unified projects, with the siting addressed within an “envelope” approach to make the design suitable for a large selection of sites.

Twelve responses to the questionnaire were received from Member States, related to all NPPs specified in Table 1, except the AHWR and CHTR[3] of India. Among them, two are site specific projects (EPR Finland for the Olkiluoto site and PHWR, which is an NPP operating at the Tarapur site in India) and 10 are unified standard projects. Summary of the responses is presented as Table 1 in Appendix I.

2.2. Data analysis

Preliminary evaluation of the questionnaires indicated that a quantitative comparison was not always possible. Therefore, the following template was selected for the analysis:

(1) Plant configuration and layout: are they influenced by external events?

(2) External event hazard and design basis for the advanced reactors: are they related to other design assumptions?

(3) Selection of the SSCs to be qualified/ protected in relation to external events: which classification process is used in relation to external events?

(4) Strategy of plant protection and design features: are they specific to advanced reactors?The data processing resulted in a synthesis table presented in APPENDIX I. The main engineering conclusions are summarized in this section, always compared with the IAEA recommendations collected in the requirements for design and siting [2.2, 2.3] and relevant safety guides [2.1, 2.4, 2.5, 2.6].

2.2.1. Plant configurations

The following could be summarized in relation to reactor type and structural configurations of the presented NPPs:

- The reactor types are as follows: pressurized water reactors (PWRs) – 6; pressure tube reactors (PHWR, CANDU) – 2; boiling water reactors (BWRs) – 3; sodium cooled fast reactors (SCFR) – 1;
- The power range is very broad; it varies from 27 to 1700 MW(e);
- In terms of construction technology, five projects show a double concrete containment, not always with steel liner. One project (the VBER-300) is very peculiar as it refers to a “floating”,

[3] CHTR is at a conceptual design stage currently [2.7].

e.g. barge-mounted NPP technology. Only one project shows a containment of pressure suppression type;

- The structural technology for the auxiliary buildings is very different from one project to another. However, the technology is of a “traditional type” and apparently influenced by considerations of a reduced construction time; specifically, concrete frames, shear walls and steel frames are used.
- The foundation embedment of the reactor building ranges from 5 to 20 m;

It could be concluded that four layouts, i.e. EPR Finland, IRIS, VVER-1000 and VBER-300 are strongly influenced by considerations of the external events, both natural and human induced. Conversely, in some projects some external events have not been addressed yet.

It is also clear that the construction technology for both reactor building and auxiliary buildings is influenced by both external events and the need to keep the construction schedule as short as possible.

The IAEA recommendations on layout selection, as defined in reference [2.2], could be summarized as follows. The layout configuration and structural technology should be chosen in order to provide a high degree of robustness of the whole facility in relation to external events, and also to accommodate unanticipated events. Moreover, beyond design basis events (BDBE) should be explicitly addressed, maybe with special assessment techniques such as the ‘safety margin approach’ or PSA.

2.2.2. Site hazard and design basis

The responses related to site hazard development and selection of the design basis could be summarized as the following:

- The external event scenarios that are most commonly addressed and that have a recognized significant impact on the designs of engineering features are: an earthquake, an aircraft crash (ACC) and a cyclonic wind. There is a trend to give more emphasis to other scenarios, which proved severe in some cases, according to recent operating experiences, such as a flood, mechanical and indirect interactions, etc.
- Administrative measures to exclude ACC, explosions, human induced events and, in some cases, even natural hazards appear to be applied in a very diffuse way;
- In general, no connection between the design assumptions and the probability targets associated with the design basis is observed; the targets are often selected on the basis of national standards for conventional buildings;
- The goal of a reduced off-site emergency planning in some cases becomes a matter of project optimization (e.g. IRIS);
- Combinations of extreme scenarios of different nature are never addressed;
- Combinations of internal and external scenarios are addressed in a conventional way (usually with LOCA); there is no connection to the respective probabilities of occurrence. In some cases, the acceptance criteria for such load combinations are different from those used in standard design combinations;
- There is a generic increase of requirements to advanced reactors as compared with the existing plants: higher earthquake design basis (0.5 g PGA), improved flood protection, increased requirements to BDBE (0.5 g HCLPF), increased material capacity values, etc.

More specifically, concerning certain scenarios, the following was recorded (see also Table 1 of Appendix I):

- ACC is addressed mainly in relation to the impact loads; therefore, fires, smoke and access impairment are usually not considered. Sometimes the scenario is represented with an impacting mass, sometimes with a load-time curve;
- Explosion is considered negligible in some plants, while in others (e.g. EPR Finland) it is very demanding;

- Earthquake consideration is almost uniform among the presented NPPs, with an exceedance probability of 10^{-4}/year. The design basis is in general quite high (0.5 g PGA). There is a disagreement on the vertical component of an earthquake to be used in the design: sometimes it is 0.75 of the horizontal, sometimes it is not mentioned;
- Flood is considered negligible in some plants and chosen at 10^{-1}/year of probability of exceedance; in other projects it is very demanding (such as 3.5 m of water at the site);
- For wind, sometimes the design basis is chosen as maximum historical value over a period of 50–100 years; sometimes it is evaluated on a probabilistic basis at 10^{-7}/year probability of exceedance;
- Hazards associated with malevolent human actions are probably covered by hazards within other categories, with some minimum deterministic values. In some cases they impact the layout, as is the case with the IRIS, which is embedded at half of the reactor building height.

Even if some advanced NPP designs incorporate a thorough protection from external events, the responses provide no data on how external events affect the core damage frequency (CDF) or similar parameters measuring the plant vulnerability. This stems from very uneven consideration of the external event scenarios, which, in turn, could be explained by their complexity (interactions, secondary effects, effects on the evacuation/ access, etc.). In this way, most of the projects considered do not take an advantage of performing plant safety analysis when the external event design basis is addressed; they rather apply the same design approaches as already established for the conventional plants.

Beyond design basis events receive more and more emphasis in siting procedures for advanced NPPs; however, there is no common stance on the probability of exceedance to be associated with such scenarios: sometimes it is 10^{-7}/year; sometimes it is 10^{-4}/year; and sometimes it is deterministic.

The IAEA recommendations on design basis development, as defined in reference [2.2], could be summarized as the following. Selection of scenarios for consideration in the design should neither be related to a specific plant design, nor to the cost of plant protection. The emphasis should be on scenario evaluation, and not on single effects for a specific plant. Moreover, since administrative measures proved to be ineffective in hazard mitigation, they should not be considered at this stage (they could be considered as additional measures only).

For most operating NPPs, it is accepted that external events should have a lower probability of occurrence than internal initiators (postulated initiating events) and therefore, their load combinations can be explicitly addressed in a probabilistic framework. However, it is worthwhile to mention that the coefficients in load combinations are often used to compensate for the defects in construction and mounting, for anomalies, etc. Therefore, their review should either include the associated potential effects or use a more reliability-oriented system, such as quality assurance (QA) in design, construction, etc.

2.2.3. Items to be qualified in relation to external events

The responses provided neither the criteria nor the detailed lists of SSCs (to be) qualified in relation to external events, although safety classification of the SSCs was mentioned.

The IAEA recommendation on item qualification, as defined in [2.8], is that it is convenient to develop an ‘external event classification’ associating different design limits and inspection and maintenance procedures with the items according to their importance or vulnerability in case of a design basis external event (DBEE). The following criteria could be used for item classification:

- Items whose failure induced by an external event could directly or indirectly cause plant accident conditions;
- Items required for shutting down the reactor, monitoring critical parameters, maintaining the reactor in a shutdown condition and removing residual heat over a long period;
- Items that are required to prevent or limit radioactive releases in case of accident conditions (e.g. all levels and barriers of the defence in depth, evacuation routes, etc);

- Items which in case of a design basis external event can affect the functionality of a safety classified item;
- Items required to prevent or mitigate accident conditions for such a long period that there is a reasonable likelihood that a DBEE may occur during that period.

2.2.4. Design of the protection

Regarding the engineering features adopted in the addressed NPP designs, at a first glance it could be concluded that some of them offer an excessive protection through 'bunkerized' solutions, while the others look quite vulnerable. Such a conclusion is misleading, because the design bases chosen for the two 'extremes' are actually different. Within the same design basis, the engineering solutions would probably be the same.

The design approaches used for the protection of NPPs with advanced reactors against external events are discussed in detail in Section 4. The IAEA recommendations, as defined in reference [2.8], could be summarized in the following:

- Preference should be given to design measures over administrative and operational, as the latter proved to be difficult to maintain in time and their reliability is questionable.

2.3. Conclusions from the questionnaire analysis

An analysis of the responses shows that most of the considered advanced NPP projects apply the same approach for design and siting in relation to external events as already established for the conventional plants. Some projects tend to envelope all deterministic requirements from all countries of potential commercial interest (e.g. all equipment is qualified at 0.25 g PGA, ACC load of 250 MN, etc.) In this way, the design becomes extremely conservative, although it may be a valuable trade-off when compared to the adoption of the improved but complicated design and assessment methods and the costs and uncertainties of their licensing. When addressing external event design basis, most of the advanced designs considered do not take an advantage of the innovative technological solutions adopted for the rest of the plant.

This consideration suggests that there is a generic need for improved and more flexible safety requirements, which would allow for more realistic siting, design and assessment procedures, without the excessive deterministic conservatism coming from traditional concerns, accumulated in years of engineering. In particular, the analysis of the responses suggests the following:

- Safety goals could be made quantitative and probabilistic (as they are already in very few countries);
- The application of the defence in depth (DID) approach could be made more flexible and integrated with some probabilistic considerations and risk-informed concepts. Also, the external events could be formally included as initiators, and the requirements for protection of the DID levels (emergency systems, safety systems, etc.) in relation to external events could be developed. As a redundancy requirement, high confidence may be shown that the reliability of the DID levels can be achieved by other means, for example by design;
- For better use of the existing rules and knowledge, the rationale behind them could be reassessed to avoid excessive conservatisms or to reiterate plant-dependent sequences, which may be not safe enough for the innovative plants.

In relation to the reactor layout and configuration, some projects of advanced NPPs showed that an early consideration of realistic external event scenarios at the design stage could provide a substantial improvement in the overall plant safety, specifically in relation to the security challenges that are often addressed a-posteriori to existing design configurations. In advanced reactors, the layout may be optimized according to a more systematic application of the external event PSA at the early design stages. This could result in a broader use of passive systems and also could help substantiate the reduced emergency planning, etc.

Concerning the design basis for NPPs with advanced reactors, a generic trend toward higher external event input was noted, particularly in relation to seismic events, which is due to the demanding hazard evaluation procedures; therefore, the calculated percentage contribution of external events to the core damage frequency (CDF) is going to rise. Another reason for this rise could come from the reduced contribution of internal events achieved through a broader implementation of the enhanced safety features and measures.

The operating life is stretched for advanced reactors (reaching 60 years), which may require further research to understand its effect on siting and design procedures. Also, the hazard modification in time becomes relevant, and it should be addressed at the design stage.

The design could give more emphasis to facilities other than the reactor building; specifically to those that proved to be particularly vulnerable and contributing significantly to the CDF in case of external events, e.g. the balance of plant (BOP), the spent fuel pool (especially, in case of aircraft crash (ACC)), the emergency control room (ECR), etc.The responses also showed a large emphasis on beyond design basis events (BDBEs), which is apparently a lesson learnt from existing plants applied to the advanced ones. The reasons behind this may vary: increased public acceptance requirements; high uncertainties in the hazard; requirements for robustness of the design; prevention of “cliff–edge” effects in the structural response to external events. Different reasons facilitate different engineering solutions that might be further developed for advanced reactors.

The relevant assessment procedures are well settled only for seismic events (seismic margin assessment (SMA)); there is a need to extend and validate them for other external events. The walkdown approach, widely used in SMA, could well be extended to design basis scenarios, specifically for the assessment of the potential interactions, construction quality, anchoring devices, water access from flooding, etc.

In general, all questionnaires showed a broader application of PSA to substantiate some innovative engineering assumptions. According to the responses, the reasons for broader application of external event PSA are the following:

- In design: to identify weaknesses;
- In operation: to optimize operational safety.

However, both PSA and risk-informed decision making imply a requirement for an adequate quality of both tools and analyses. The following trends of PSA technique improvement appear to be urgent from the questionnaire analysis:

- Better integration with the probabilistic hazard development is needed to manage large uncertainties in site hazards; these uncertainties, difficult to be reduced, may in some cases vanish the efforts to improve PSA reliability on the plant side;
- Management of large uncertainties in the development of the floor response spectra from seismic and/ or ACC events is needed to improve equipment qualification;
- More realistic human reliability models could be developed for the periods during and after an external event, including the implementation of emergency plans. In general, the reliability of operational measures could be explored, including monitoring and alerting actions;
- Ageing models could be developed for PSA applications;
- External event PSA modelling has been extended to shutdown modes (with open containment, open vessel, etc.).
- Fragility evaluation of safety-classified components could be improved; specifically, the instrumentation and control (I&C) systems need more research on assessment methods in relation to all external events, including fire, smoke, vibrations, etc. Civil structures require more detailed modelling of the acceptance criteria in relation to some limit states, such as leak-tightness, liner durability (for 60 years), etc.

In conclusion, the questionnaires highlighted an effort of the nuclear community to develop innovative engineering solutions for NPPs with evolutionary and innovative reactors. However, certain additional developments at an early design stage may be needed to exploit the potentiality of new design approaches to the utmost. Some suggestions for such developments have been provided in the responses to the questionnaire; others were produced through the discussion at a technical meeting held on 14–19 November 2004 in Vienna and through communications with the designers of advanced NPPs and international experts. All of them are presented in the following sections.

REFERENCES TO SECTION 2

[2.1] INTERNATIONAL ATOMIC ENERGY AGENCY, External Human Induced Events in Site Evaluation for Nuclear Power Plants, Safety Standards Series, No. NS-G-3.1, IAEA, Vienna (2002).

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

[2.3] INTERNATIONAL ATOMIC ENERGY AGENCY, Code on the Safety of Nuclear Power Plants: Siting, Safety Series No. 50-C-S (Rev. 1), IAEA, Vienna (1988).

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

[2.5] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, Safety Standards Series, No. NS-G-1.6, IAEA, Vienna (2003).

[2.6] INTERNATIONAL ATOMIC ENERGY AGENCY, Meteorological Events in Site Evaluation for Nuclear Power Plants Safety Guide, IAEA Safety Standards Series No. NS-G-3.4, IAEA, Vienna (2003).

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

[2.8] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, Safety Guide, IAEA Safety Standards Series, No. NS-G-1.5, IAEA, Vienna (2003).

3. SAFETY REQUIREMENTS FOR SITING OF NPPS WITH ADVANCED REACTORS: RETURN PERIODS, RELEVANT HAZARD TYPES AND THEIR COMBINATIONS

This section, prepared by international experts as indicated in the end of this report, was based on the following:

- Responses to the questionnaire, relevant to safety requirements for siting (full summary of the responses is provided in Section 2);
- Outputs of a technical meeting on Definition of plant safety design options to cope with external events, convened on 14–19 November 2004 in Vienna;
- Contributions from international experts, as indicated in the end of this report.

3.1. Summary of the experience

3.1.1. General

The questionnaire analysis has shown that the advanced NPP designs considered do not address the specific external hazards in proportion to the frequency with which incidents with specific external hazards as root causes were reported through the IAEA/ NEA Incident Reporting System (IRS). The view that the distribution of risk of a severe accident due to specific external events would not correlate directly with low level events, primarily having economic effects such as outages due to scrams, is balanced by the argument that these low level events still represent a loss of the defence in depth. It is not the frequency of the external hazards *per se* that is important, but the frequency and level of release above a defined limit of release, i.e. the consequence which is the product or convolving of the initiating event, the conditional probability of failure given the event and the conditional probability of release given a failure of the containment or confinement barrier.

It should also be understood that the majority of the advanced reactor systems surveyed (12 out of 14, see APPENDIX I) were water moderated and cooled with a relatively high core energy densities capable of core melt or at least significant core damage and hydrogen generation. As a result, it is not expected that basic accident scenarios and design requirements, or engineering safety features and planning from the standpoint of regulations will change significantly from current requirements. Other reactor systems with relatively low core energy densities, not subject to core melt or damage, source term or combustion might rationally have significantly different engineered safety systems or emergency planning (e.g. confinement versus containment requirements).

3.1.2. Siting

Siting is a matter based on the following:

- Economic consideration (where power is needed, the availability of existing grid);
- Social and political factors;
- Relative intensity and consequences of hazards (external and internal; natural and human induced);
- Topography affecting the dispersion of air borne radionuclides through the atmosphere, and water borne dispersion through surface water system (rivers, bays and seas) and ground water;
- Public safety considerations;
- Demographic characteristics in some Member States.

In some cases, such as the presence of a capable seismic fault; hence, long term large ground displacements or a nearby airport, consideration of external hazards may eliminate a site from further consideration for an NPP, but most external hazards are either screened out from the necessity of being considered further as a design basis, based on risk considerations, or are taken into account in plant designs.

Some Member States only address the risk to an individual member of the public, others have requirements to consider the potential aggregated effects to the population as a whole – societal risk. Current government siting policy in most Member States is for NPP to be built at a site remote from large population. However, there is no general agreement as to what constitutes a remote site. Sites for new advanced NPPs, because many of the existing sites suitable for reactor remote location are already taken, would be more sensitive to this requirement.

Off-site emergency measures are still seen as part of the defence in depth approach, and are mainly understood in a deterministic sense, but to take full advantage of advanced NPP designs should be moved towards a more probabilistic approach. It should be understood that emergency measures are a function of plant operation and accident analysis, which may or may not be a consequence of an external event.

3.1.3. Screening

Several of the responses were silent on the consideration of specific external events. It is not clear whether this is a result of a screening process, which eliminated them, or they have not yet been considered in the preliminary design process or in the particular national practice they haven't been considered as a design basis in the past.

Conversely, some designs made a consideration of the events that were not typical of the majority of responses. For example, the IRIS response addressed landslides and volcanism. The VBER-300 floating plant would be towed to a safe place in the event of volcanism. Two responses (BN-800 and IRIS) addressed terrorism explicitly.

In many cases probabilistic screening was the only approach formerly used for accidental aircraft crash, but Member States are increasingly examining the consequences, partly in response to the possibility of malevolent human actions. Double containment and certain layouts of some advanced NPP designs to reduce above ground vertical profiles offer advantages in the resistance of malevolent human-induced external events, which cannot be probabilistically defined.

3.1.4. Return period, probability of exceedence and relationship to probabilistically defined safety goals

Regarding the design basis return period or its reciprocal yearly probability of exceedence for earthquakes, there was an agreement that 10^{-4} of mean per annum probability of exceedence (or return period of 10^4 years) is reasonable for water cooled and moderated reactors capable of core melt. The resultant most recent Seismic Level 2 (SL-2)[4] peak ground accelerations are typically higher than the SL-2 levels for existing NPPs, which were by and large based on deterministic evaluations of the historical earthquakes, which may have affected the site. Wind loads in some cases (CAREM, IRIS, VK-300) were based on tornadoes of 10^{-4} - 10^{-7}/year probability of exceedence as an extreme load, i.e. the allowable stress in structural steel equal to yield, or a historical maximum treated as a straight wind severe load (BN-800, Indian designs, SWR 1000, VK-300) with a return period of 1000 years or less.

The return period for flood ranged from 10^3 (PHWR, Tarapur 3,4) to 10^6 (APR 1400) years but was sometimes unspecified (SWR 1000), or said to be site dependent (ACR, CAREM). In some cases it was expressed as a margin (greater than 1 m for VK-300; or not defined, BN-800). The IRIS is being designed to resist a Probable Maximum Flood (PMF) site, used to define greater than 1.0 m finished plant grade elevation. For the floating NPP (VBER-300), flooding is impossible.

Precipitation when defined in the form of snow, rain or ice, when identified, was usually considered under the severe rather than extreme category. For existing NPPs it is often based on conventional

[4] In the plant design Seismic Level 2 (SL-2) is associated with the most stringent safety requirements, while Seismic Level 1 (SL-1) corresponds to a less severe, more probable earthquake level that normally has different safety implications [3.5]

industrial plant design practice with return periods of 2 ×10^2 to 10^{-2}/year probability of exceedence multiplied by a load factor that typically varies between 1.5 and 2.0.

None of the responses mentioned allowance for the effects of climate change despite the IAEA guidance on this subject. However, it should be understood that true climate changes typically occur over a period of several hundred or thousands of years, and it is often impossible to distinguish between true changes and natural variation or randomness in the existing cycle.

In the United Kingdom, some failures and hazards may be excluded, including failure internal to the plant, which have an expected frequency less than about 10^{-5} per year. For external natural hazards, such as seismic, it is recognized that the uncertainty of data may prevent reasonable prediction of design basis events (DBEs) for frequencies less than once in 10 000 years or 10^{-4}/year probability of exceedence. Where this is the case, which is generally considered to apply to earthquakes in the UK, the expectation is the establishment of a design basis event (e.g. Safe Shutdown Earthquake (SSE)), which conservatively has a mean predicted frequency of being exceeded no more than once in 10 000 years.

Earthquakes in the present state of technology are not amenable to forewarning with a useful degree of certainty. This is in contrast to a number of other external hazards, such as extreme wind, flooding and lightning, considered in the design and operation of NPPs. Plants can be shut down in advance when the likelihood of extreme wind, flooding or lightning is high. However, this implies dependence on administrative control.

It could be observed that the safety goal associated with excessive radiation to the general public for water moderated and cooled NPPs, when defined, is typically set at 10^{-6}/year probability of exceedence. This goal is established in recognition of the source term, which could result from the release of the reactor coolant inventory to the environment. It also considers the extremely robust design of secondary containments, which in most countries are not assumed to fail in design basis accident scenarios. A similar safety goal has not been established for release of undefined radioactive material from a plant accident for a NPP where core melt or combustion is not a credible scenario. However, it has been observed in at least one county (the USA) that the safety goal is reduced to 10^{-5}/year probability of exceedence for radiological releases from non-reactor nuclear facilities with source terms comparable to facilities without potential for core melt or combustion [3.1].

3.1.5. Standard plant design for natural external events

Most designers of advanced reactors desire to standardize their designs with respect to external events so that their NPPs can be placed at the largest number of potential sites without significant non-standard design changes, which cause increases in cost. This suggests that they will attempt to provide a reactor design that can be placed on at least 80 to 90 percent of potential sites. The mean seismic peak ground acceleration for existing reactor sites worldwide is about 0.20 g where this value was selected based on deterministic historical earthquakes in the region. Some Member States today (Canada, USA, Russian Federation) would define SL-2 earthquake peak ground accelerations, PGA based on a 10^{-4}/year mean probability of exceedence. Such a definition would typically increase the mean site PGA to about 0.3 g.

A similar situation exists for wind design. For mean yearly probabilities of exceedence at a site larger than about 10^{-3}/year (1000 year return period), straight winds (caused by weather fronts and squall lines) would govern maximum wind speed at a site. Below 10^{-3}/year probability of exceedence, typical cyclonic windstorms (hurricanes, tornadoes and typhoons) would begin to control wind speed and then only in regions where such tropical cyclones occur with any regularity. As a result of varying national experience with wind loads, there does not appear to be any consensus with respect to wind load design with probabilities of exceedence, which range from 10^{-2}/year for straight wind to 10^{-7}/year for tropical cyclones (tornadoes). A reasonable compromise may be a 10^{-4}/year probability of exceedence from all wind sources in the range of 50 m/sec for a 3 second gust. It should further be noted that total plant costs are relatively insensitive to design basis wind load. The increase in cost in going from 50 m/sec wind speed design to a 100 m/sec wind speed design is less than 1.0 percent.

Flood design is usually accomplished by placing the plant grade above flood elevation. Flood elevation is typically based on a probability of exceedence, which ranges between 10^{-3}/year to 10^{-6}/year. A reasonable probability of exceedence consistent with other design basis external events might be 10^{-4}/year probability of exceedence, recognizing the need to avoid cliff edge effects.

Precipitation (rain, snow or ice) loads appear to be based on national norms. Where such norms exist, they are usually given as numerical values taken from national maps. These maps are typically based on a probability of exceedence level of 2×10^{-2}/year. Once these precipitation loads are determined for design purposes, they are typically multiplied by load factors, which range between 1.5 and 2.0. As a result, the actual probability of exceedence of such precipitation loads, when explicitly considered in design, is between 2×10^{-3}/year and 10^{-3}/year probability of exceedence. Precipitation typically effects only roof design and, to some extent, plant grading and storm sewer design. Costs associated with precipitation are typically much less than 1.0 percent of total plant costs down to a probability of exceedence less than 10^{-7}/year. or alternatively the site is considered inappropriate for NPP siting.

3.2. Applicability of the IAEA safety requirements and safety guides

The current IAEA guidance concerning siting and design of NPPs in respect to external hazards has been substantially revised and re-organized [3.2–3.7] since 'Safety of NPP – Requirements' was published in 2000 [3.8].

Paragraphs 5.16 and 5.17 of the Requirements [3.8] set the high-level design basis for external events. There is no perceived need for change. On maintenance of levels of defence, paragraph 4.4 may need re-examination for operational modes other than power operation — the rate of occurrence of incidents during maintenance and refuelling, plus the general trend towards more definitive technical specifications, suggest that the requirements are too vague.

Paragraph 1.9 of reference [3.2] defines its scope as the design and safety assessment of land based stationary nuclear power plants with water cooled reactors. It is not clear if these restrictions are a necessary limitation of scope or are due to the limits of the performed consideration. Paragraph 1.16 states that the safety guide might be applied to reactor types other than water cooled reactors at stationary nuclear power plants, but that engineering judgement should be used to assess such applicability in compliance with the specific safety objectives or goals defined for any plant type. As discussed in Section 3.1.4 of this section; in general, the consequences of accidents or failures resulting from external events are different as a function of cooling media characteristics and core energy densities and combustibility which could effect basic design concepts as well as engineered safety system design in advanced reactors.

The reactor systems presented at the technical meeting or in the questionnaires were mainly evolutionary PWRs, rather than innovative reactor systems that use other than water moderated and cooled systems, but included two liquid metal cooled reactors, one of which was with a graphite moderated core, presumably capable of combustion, see Table 1. One design considered with respect to siting was a floating, i.e. not land-based NPP. Had more innovative reactor systems been represented, the challenge to the recently published IAEA requirements and guides might have been greater. Even so, the advanced NPPs considered at the meeting variously showed innovative layout, increased reliability to resist internal faults, or even elimination of some internal fault sequences, and greater use of passive systems. It is well to judge the suitability of the IAEA requirements and guides against even the limited set of these NPPs before the true Generation IV designs become available.

The design oriented safety requirement document [3.8] does not appear to define internal events or external events. In the USA [3.1], the following definitions have been found useful from a regulatory point of view because they are on the basis as to whether or not the licensee has control of the hazard:

- Internal hazards are those hazards to plant and structures such as fire, explosions, release of hazardous material or gas, flooding due to process failures, etc, which originate within the site boundary, but external to the process in the case of nuclear chemical plant or primary circuit in the case of power reactors, i.e. the licensee has control over the initiating event in some form;

- External hazards are those hazards to safety related SSC such as earthquake, aircraft impact, extreme wind and associated missiles, electromagnetic interference (off-site case) and flooding which originate outside the site boundary, external to both the site and the process in the cases of both nuclear chemical plant and power reactors, i.e. the licensee has very little or no control over the initiating event, namely occurrences of nature, external organizations or humans with or without mal-intent.

The scope of reference [3.2] given in paragraph 1.9 of reference [3.2] includes human induced events from both on-site and off-site sources, and is therefore a mix of both internal and external events according to the above definitions. The issue of who has control of a hazard is evident in paragraphs 9.1 and 9.2 of reference [3.3], where administrative control of development around a nuclear site subsequent to site evaluation is discussed. The competent authority may need arrangements in respect of development applications meeting specified criteria within specified distances of NPP sites. The competent authority should ensure that man-made external hazards from outside the nuclear site are either controlled via the planning system or included within the safety evaluation. The need for clarity as to whether an event is internal or external may also be important in those Member States where different screening levels are applied to the two classes.

In paragraph 1.13 of reference [3.2], some natural external events are treated as exclusion criteria for the site itself and therefore treated in the IAEA guides for siting. The IAEA draws attention to its Provisional Safety Standards Series document [3.9] on volcanoes and related topics.

Paragraph 2.36 of reference [3.2] provides recommendations concerning redundancy, diversity, robustness, segregation and the single failure approach. In part these are cascaded from the higher tier requirements document [3.8]. There appears to be a need to re-examine these requirements and guidance for application to evolutionary or innovative reactors.

Paragraph 2.39 of reference [3.2] notes that provisions in the design to protect the plant against design basis external events (DBEEs) should not impair its response in the other design basis events. Although the objective is clear, every design is a compromise, and what is the most efficient design against one DBEE may well not be so against some other DBEE or interval event. For example, mounting equipment high in a structure provides good protection against flooding, while increasing the seismic demand upon it by restraining high temperature piping to resist earthquake inertia loads increase thermally induced stress levels. Thus, this guidance appears insufficiently pragmatic even for existing NPPs. The IRIS design, with a deep basement to reduce vulnerability to seismic or aircraft impact DBEEs, would tend to increase flooding or buoyancy loads further, which points to the need to reconsider the published guidance.

Reference [3.2] provides guidance for the passive barriers to resist external events. However, if Safe Operating Limits (SOLs) are dependant on monitoring systems, forecasting systems, or calculations of the margin between time to shut down and the time before an external event exceeds the barriers capacity, the safety system, as distinct from the barrier itself, is not passive.

Paragraph 1.15 of reference [3.2] excludes wilful human events by third parties; whether or not this exclusion remains appropriate was extensively discussed at a technical meeting held on 14-19 November in Vienna with no clear-cut opinion on its applicability as a design basis. It should be noted at least one Member State (the USA) requires a design to resist a malevolent load vehicle intrusion to the site.

Reference [3.2] only considers deterministic approaches to design. Whereas paragraphs 3.1 to 3.3 recognize that Member States variously use deterministic and probabilistic design input values for DBEEs, the design remains deterministic. Paragraph 3.4 of reference [3.2] notes that even when the hazard is defined probabilistically, a single point on the hazard curve should be selected, to be used as the design basis. When return period or mean probability of exceedence is not specified, there is an implicit probabilistic assumption concerning the risk of a radiological accident. The final target, reference [3.2] explains, is to keep the risk acceptably small, or presumably within national limits where these are set. Both imply an assumption of the probability that the DBEE will affect safety related items and then the probability of unacceptable consequences of their failure. The selection of return period — the single point on a hazard curve — cannot be entirely left to the designer; it may be verified by the external event PSA. Whether or not there is a requirement for an external event PSA varies from Member State to Member State. Moreover, there is a general consensus in favour of a risk-informed, rather than risk based, approach and that deterministic design is appropriate once design basis loads and acceptance criteria are defined in accordance with specified design basis codes and standards. Further guidance on return periods and the use of load factors is required.

On the detailed methods of treating individual external hazards, sections 4 to 16 of reference [3.2] appear to remain valid for evolutionary or innovative reactors.

In assessing the applicability of existing regulatory requirements, particularly to evolutionary and innovative reactors, it is relevant to ask why a requirement has been found to be useful.

The total design basis for external events is usually a combination of probabilistic and deterministic procedures with loading parameters defined probabilistically and failure or capacity methods and acceptance criteria defined deterministically.

3.3. Identified safety and technological issues and proposal for resolution

3.3.1. Safety goals

The IAEA safety goals are currently defined in qualitative terms, but there is increasing interest in seeking quantitative goals, based initially on inventory and source terms and finally on radiological consequences to the environment or dose to a member of the public versus a frequency of occurrence. This would help communicate the risk to the public and aid public acceptance of NPPs. Currently, Argentina has such an objective as a continuous curve between 10^{-2} and 10^{-7} per annum, recently updated to take account of changes to recommendations of International Commission on Radiological Protection (ICRP). A similar approach, based on 4 categories of frequency, is under discussion in India, and there is discussion of targets for core damage in Japan and Lithuania. The United Kingdom has a stepladder covering four magnitudes of frequency, with separate goals for safety objectives and for minimum acceptable safety, and additional frequency goals and limits for plant damage and for large radiological releases. The USA has safety goals for core damage and for large release.

Should safety requirements become more onerous, this could jeopardize public acceptance of existing nuclear plants in some Member States.

Some external events are a challenge to the primary line of defence; others challenge lesser safety functions. There is a question as to whether different return periods of occurrence should apply to different systems. Alternatively expressed, should the return frequencies be related to the consequences? The safety goals for the same level and type of radiological release (consequences) should be similar. However, this does not mean that the individual external event design basis probability of exceedence needs to be the same. The design basis resistance criteria, since they also play a significant role in SSC failure probability, need also to be considered. There is general consensus that the basis for NPP design against external hazards should remain that of sound engineering design using proven design methods, risk informed, but not necessarily determined by the PSA.

A design outcome could be spending proportionately more on protecting those systems, the consequence of failure of which to an external event would be more serious. However, to an extent this is already done by the application of more rigorous design codes to such items.

The hierarchy of Westinghouse PWR Safety Critical Functions could be adopted as a practical implementation of the aspiration for safety significance given in paragraph 3.13 of reference [3.8]:

- Safe shutdown;
- Safe hold-down;
- Safe decay heat removal;
- Safe containment;
- Safe cooling of spent fuel.

Some protection measures against external events are passive. Others may involve active systems. Innovative NPP, such as the IRIS, which mitigate the effects of some external events (for example, aircraft crash and earthquake) by a plant layout, which places critical components in a deep basement, may require more stringent consideration of both fire and flooding than that of a plant constructed entirely at ground level above any rational flood plain. From such considerations, rigid rules applicable to all types of NPP may prove illusive or result in an excessive conservatism.

3.3.2. Better design for high seismic areas

Japan identified as an issue for future work the need for better design for high seismic areas. Since a common finding from several of the questionnaires was that the design basis earthquake for new NPPs was higher than for existing plants, this view may be widely shared.

3.3.3. Rational for return periods

There is general agreement that some external events may be eliminated from further consideration by a two stage screening process, e.g. as defined in paragraph (14.1) of reference [3.3].

A preliminary, simple deterministic study, based on the information on the magnitude or distance and characteristics of the source, may be sufficient to show that no significant interaction with the plant may occur. A second screening criterion is based on the probability of occurrence.

There is an issue as to the corresponding treatments of internal and external initiating events at this second level of screening. There is general agreement that the uncertainty of data for natural hazards may prevent reasonable prediction of events for frequencies less than once in 10 000 years. Internal initiating events with different less frequent return periods are frequently included in the design basis.

3.4. Future challenges and IAEA potential contribution

3.4.1. Margin assessments

There is an agreement that whilst design code approaches are suitable for design basis external hazards, beyond code, e.g. high confidence, low probability of failure (HCLPF), methods when required such as to demonstrate margin should be used for beyond design basis, or margin, assessments. More work is needed on such methods.

3.4.2. Homogeneity of internal and external events

Load combinations and harmonization of load factors are required to address the question as to whether higher reliability in innovative reactor systems can be offset against a lesser hazard. There are increasingly findings from PSA studies that with better systems design and better trained operators the risk of core damage from internal postulated initiating event (PIE) has decreased, such that the proportion of the risk from seismic PIE has apparently increased.

In at least two Member States there is a regulatory expectation that no single class of accidents should contribute more than 10% of the total risk. This helps ensure a balanced plant design and reduces the sensitivity of the results of PSA to uncertainties in one particular class of accidents. However, as external events come to contribute a larger proportion of the total risk, this becomes a requirement to further reduce the total risk.

3.4.3. Eliminating the need for a detailed emergency planning zone

The full benefit of innovative and evolutionary NPPs would require the ability to licence without the need of a detailed emergency planning zone (DPZ). However, as long as radiological source terms in terms of radiological intensity and unmitigated consequences are there, it is not likely there would be significant changes in DPZ requirements.

3.4.4. Terrorism

Agreement on whether or not terrorism is an external hazard to be considered in design is desirable because some plant layouts, which offer improved conceptual protection against such threats, suffer a detriment in designing against other external hazards.

3.4.5. Meeting multiple regulator requirements

Vendors generally are interested in meeting the regulatory requirements of more than one Member State, if this can be achieved without a significant increase in unit cost due to divergent regulatory requirements. The IRIS, for example, is aimed at the US certification; the EPR is under construction or soon to be under construction in more than one Member State.

3.4.6. Future changes related to external hazards

A consequence of the longer design life envisaged for advanced NPPs is that the total life, that is the period for which a particular design is to be valid plus the design life and plus the decommissioning time, is in many cases well over 60 years. Changes in regulation and hazards (as a function of frequency in some external hazards) can be expected in that time. Changes in regulation should not, and need not be anticipated.

Considerable change in the both the aircraft speed and, more especially, the mass of aircraft have occurred in the last sixty years. Some of the questionnaire responses indicate design impact against smaller aircraft than the largest flying today. At the technical meeting, there was no support for a suggestion that new NPPs should anticipate some growth in the size of civil airliners, although one national expert believed that this was previously the IAEA position. As described above, Member States are increasingly examining the characteristics and consequences of aircraft crashes, partly in response to the possibility of malevolent human actions, but even if new NPPs (including control rooms, intake structures and spent fuel storage facilities) were hardened against a large aircraft (at a considerable cost), other vulnerable societal features cannot be. The principle of the hierarchy of hazard mitigation commences with hazard elimination, and in this context aircraft designers are expected to innovate, so as to eliminate the hazard as a design basis event.

3.4.7. Site environmental change

The flood hazard may change over time as a result of various causes, including changes to the environment, see paragraph 14.1 of reference [3.4]. The major effects of human induced environment change with regard to the hazards to nuclear power plants are related to the following causes (paragraph 14.8 of reference [3.4]):

- Apparent changes in the external hazard as a function of the data gathering duration;
- Changes in the rises and anomalies in sea levels;
- Changes in the flow rates of rivers and water shed vegetation.

Some safety margin should be taken into account in the design of a nuclear power plant (paragraph 14.10 of reference [3.4]). Paragraph (14.10) of [3.4] suggests generally agreed estimated variations if the whole plant lifetime is considered, even though design basis event probabilities are defined on a per annum basis, if used. Changes in natural hazards (e.g. because of environmental change or additional event data) may need to be considered at the time of Periodic Safety Reviews (see paragraph 1.11 of [3.2]).

The regulatory body in one Member State wrote a generic letter to all nuclear site licensees in November 1997, stating that it expected safety submissions for new construction projects plants and periodic safety reviews of existing facilities to take account of the potential effects of climate change.

Experience in the Republic of Korea has shown that allowance could be made in seawater temperature for the possible subsequent construction of other NPPs nearby.

There is no change in per year probabilities of exceedence as a design basis if the facility is designed to operate 10 or 60 years.

3.4.8. Load combinations

The IAEA (paragraphs 2.27–2.29 of reference [3.5]) provides a guidance for the combination of earthquake loads with operating condition loads, i.e. loads during low probability transients and normal operation, additional loads during anticipated operational conditions and loads during accident conditions. The safety margins or load factors are not specified, but reference is made to design codes. Such design standards differ between Member States and between different engineering disciplines (paragraph 3.14 of reference [3.5]). Safety margins and uncertainty levels vary between nuclear and non-nuclear design codes, and between standards whose scope includes a specified external hazard, e.g. seismic, or not.

A vast number of load combinations could in theory be required, but a common objective is to determine the minimum cut-set necessary employing envelope loading conditions, which govern design. Some advances in automated computational methods are allowing a degree of consideration of the stochastic variation in loads, thereby, lessening the need for enveloping loads.

The design basis flood, as is the case with all design basis events, should be appropriately combined with all the design basis events generating the flooding itself (paragraph 10.14 of reference [3.2]).

REFERENCES TO SECTION 3

[3.1] DOE Std. 1020, “Natural Phenomena Hazard Design and Evaluation Criteria for DOE Facilities,” U.S. Department of Energy, 2002.

[3.2] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, Safety Guide, IAEA Safety Standards Series, No. NS-G-1.5, IAEA, Vienna (2003).

[3.3] INTERNATIONAL ATOMIC ENERGY AGENCY, External Human Induced Events in Site Evaluation for Nuclear Power Plants, IAEA Safety Standards Series, No. NS-G-3.1, IAEA, Vienna (2002).

[3.4] INTERNATIONAL ATOMIC ENERGY AGENCY IAEA, Flood Hazard for Nuclear Power Plants on Coastal and River Sites, IAEA Safety Standards Series, No. NS-G-3.5, IAEA, Vienna (2003).

[3.5] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, IAEA Safety Standards Series, No. NS-G-1.6, IAEA, Vienna (2003).

[3.6] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, IAEA Safety Standards Series, No. NS-G-1.2, IAEA, Vienna (2001).

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

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

[3.8] INTERNATIONAL ATOMIC ENERGY AGENCY, Volcanoes and Associated Topics in Relation to Nuclear Power Plant Siting, Provisional Safety Standards Series No. 1:, IAEA, Vienna (July 1997).

4. APPROACH IN DESIGN: LAYOUT, PASSIVE FEATURES, DEFENCE IN DEPTH, COMBINATION OF INTERNAL AND EXTERNAL SEQUENCES AND EMERGENCY PLANNING ISSUES

Except where indicated, this section was prepared through collaboration of the designers of 14 advanced NPPs, which included responses to the questionnaires analyzed in Section 2, participation in a technical meeting on Definition of plant safety design options to cope with external events held on 14–19 November 2004 in Vienna, and direct communications to the designers to produce the structured descriptions of safety design features of advanced NPPs as well as to review this section.

4.1 .Summary of the experience

4.1.1. Reactor concepts addressed

Thirteen projects of NPPs with advanced reactors and one operating NPP addressed in this section are listed in Table 1 of Section 1. These fourteen designs represent a wide variety of concepts, and different levels and directions of innovation.

4.1.2. Datasheet for presentation of design approaches

On the basis of an analysis of information made available by the designers of advanced reactors, a common structure of a datasheet was formulated for the presentation of design approaches, including those used for dealing with external events. This structure is given in Table 2.

TABLE 2. STRUCTURE OF A DATASHEET FOR PRESENTATION OF DESIGN APPROACHES USED IN ADVANCED REACTORS TO ENHANCE DEFENCE-IN-DEPTH IN GENERAL AND ADDRESS EXTERNAL EVENTS IN PARTICULAR

#	TITLE OF THE ITEM IN THE DATASHEET
1	List of postulated external events
2	Protection by structural design of buildings, containing structures, systems and components important to safety, against postulated extreme external events
3	Spatial separation of redundant safety related systems to secure protection against localized adverse effects, including those resulting from external events
4	Design features, implemented within protected buildings, to maintain fuel temperature within acceptance limits under postulated extreme external events when all sources of power, cooling water supply, and compressed air external to the protected building are assumed to be lost, and no credit is given to operator actions within a stipulated grace period.
4.1	Active safety systems requiring emergency power supply
4.2	Passive systems for reactor shutdown and heat removal within protected buildings that remain available to provide safety functions
4.2.1	Passive systems requiring emergency power supply based instrumentation and electrical signals to get actuated
4.2.2	Passive systems not requiring any electrical signals to get actuated
4.3	Heat sinks that remain available with loss of external coolant supply
4.4	Inherent safety features
5.	Features for prevention and mitigation of consequences of hypothetical severe accidents

#	TITLE OF THE ITEM IN THE DATASHEET
6.	Features for preventing unacceptable release of radioactivity following postulated beyond design basis accidents
7.	Other important safety features, including other special features provided to deal with external events
7.1	Features to enhance defence in depth in general
7.2	Features addressing external events in particular
8.	Emergency planning issues

The information available from the presentations and papers submitted by the participants was gathered to prepare first draft of a datasheet for each of the fourteen reactor types. This datasheet was subsequently sent to the concerned designers for a review. The datasheets, thus reviewed are provided in APPENDIX II.

4.1.3. Postulated external events

The IAEA-TECDOC-1341 [4.1] provides a non-exhaustive list of reference external events usually considered in the design of NPPs. Taking this list as a starting point, and using the inputs from datasheets mentioned in section 4.1.2, a broad trend for the postulated external events considered in the design of advanced NPPs has been derived. This information is brought out in Table 3.

TABLE 3. POSTULATION OF EXTERNAL EVENTS IN THE DESIGN OF SOME ADVANCED NPPS

CATEGORY	EXTERNAL EVENT (EE) GROUP	NAMES OF NPP DESIGNS IN WHICH CONSIDERATION OF SOME PART OF THE EE GROUP IS EXPLICITLY MENTIONED IN THE DATASHEET CONSIDERED	NUMBER OF RELEVANT NPPS
I. Natural Events considered in several plants	Earthquakes	APR1400, EPR Finland, VBER-300 FNPP[5], VVER 91/99, IRIS, PHWR-540, ACR-700, SWR 1000, VK-300, ABWR-II, BN-800, AHWR, CHTR	13
	Extreme meteorological conditions (temperature, snow, hail, frost, subsurface freezing, drought).	APR1400, EPR Finland, VVER 91/99, IRIS, PHWR-540, SWR 1000, VK-300, ABWR-II, BN-800, AHWR, CHTR	11
	Floods (from tides, tsunamis, seiches, storm surges, precipitation, waterspouts, dam forming and dam failures, snow melt, landslides into water bodies, channel changes, work in the channel).	APR1400, EPR Finland, VVER 91/99, CAREM-25, IRIS, PHWR-540, SWR 1000, VK-300, AHWR, ABWR-II, CHTR	11

[5] FNPP is the acronym used to denote a floating, i.e. barge-mounted NPP

CATEGORY	EXTERNAL EVENT (EE) GROUP	NAMES OF NPP DESIGNS IN WHICH CONSIDERATION OF SOME PART OF THE EE GROUP IS EXPLICITLY MENTIONED IN THE DATASHEET CONSIDERED	NUMBER OF RELEVANT NPPS
I. Natural Events considered in several plants	Cyclones (hurricanes, tornadoes and tropical typhoons)	APR1400, VVER 91/99, CAREM-25, IRIS, ACR-700, PHWR-540, VK-300, ABWR-II, BN-800, AHWR, CHTR	11
	Lightning	EPR Finland, CAREM-25, IRIS, ACR-700, PHWR-540, SWR 1000, ABWR-II, AHWR, CHTR	9
	Landslides and avalanches.	SWR 1000, CHTR	2
II. Human induced events considered in several plants	Aircraft crashes	EPR Finland, VBER-300 FNPP, VVER 91/99, IRIS, PHWR-540, ACR-700, SWR 1000, VK-300, BN-800, AHWR	13
	Explosions (deflagrations and detonations) with or without fire, originated from offsite sources and on-site (but external to safety related buildings), like storage of hazardous materials, transformers, high energy rotating equipment.	EPR Finland, VVER 91/99, CAREM-25, PHWR-540, SWR 1000, VK-300, BN-800 VBER-300 FNPP, AHWR	9
	Electromagnetic interference from off-site (e.g. from communication centres, portable phone antennas) and on-site (e.g. from the activation of high voltage electric switch gears).	EPR Finland, VVER 91/99, IRIS, ACR-700, SWR 1000, BN-800, AHWR, CHTR	8
	Collision of ships and floating debris (ice, logs, etc.) with the water intakes and other hazards with potential influence on cooling water intakes	VBER-300 FNPP, VVER 91/99, VK-300, EPR-Finland, SWR 1000, AHWR	6
	Fire generated from off-site sources (mainly for its potential for smoke and toxic gas production).	EPR Finland, APR1400, VBER-300 FNPP, SWR 1000, PHWR-540	5
III. Additional external events	Internal flooding	APR1400, VBER-300 FNPP, AHWR	3
	Internal hazard loads	BN-800	1

CATEGORY	EXTERNAL EVENT (EE) GROUP	NAMES OF NPP DESIGNS IN WHICH CONSIDERATION OF SOME PART OF THE EE GROUP IS EXPLICITLY MENTIONED IN THE DATASHEET CONSIDERED	NUMBER OF RELEVANT NPPS
IV. External events specific to floating NPPs	Breakdown of attachment or rigid mooring bars due to ice lock with further grounding under strong wind and heavy sea; Minor shock against mooring ship (service ships); Ship-to-shore communication pipeline rupture; Floating power unit grounding, including rocky ground natural phenomena during haul (heavy sea, wind, ice)	VBER-300 FNPP	1
V. External events not considered in any of the 14 NPPs.	Release of corrosive gas and liquids from off-site and on-site storage; Abrasive dust and sand storms; Volcanism.		0

As it is seen from Table 3, the natural external events, viz. earthquakes, wind, floods are considered, as applicable to a site, for a majority of the NPP designs surveyed. Among the human-induced external events, accidental aircraft crash evaluation and external stationary explosions lead with their consideration in at least nine of the fourteen designs, even though the extent of the event definition (impact of small aircraft vs. large commercial airliner at various crash speeds) vary. In at least one design, internal flooding has been treated as an external event.

In this context, the recommendations of [4.2] may be considered to be generally valid for current generation plants. However, for several advanced reactors with huge water inventories, e.g. located at top of the reactor building, it seems appropriate to classify internal flood as an external event. To rationalize this, a broader definition of external events may be borrowed from a recent EPRI draft report [4.3] as under:

“Internal events” are typically failures or transient events that occur within a particular system of a nuclear power plant (such as a loss of coolant accident, or a failure of a support system}. “External events” are typically events that occur outside the boundary of a particular plant system (often, from outside the plant itself) and which typically affect multiple systems within a given spatial area.”

Some of the external events are specific to a floating NPP alone, while a group of reference external events (as per IAEA-TECDOC-1341) has not been taken into consideration for any of the fourteen designs, obviously on account of their inapplicability based on site features considered for these reactor designs.

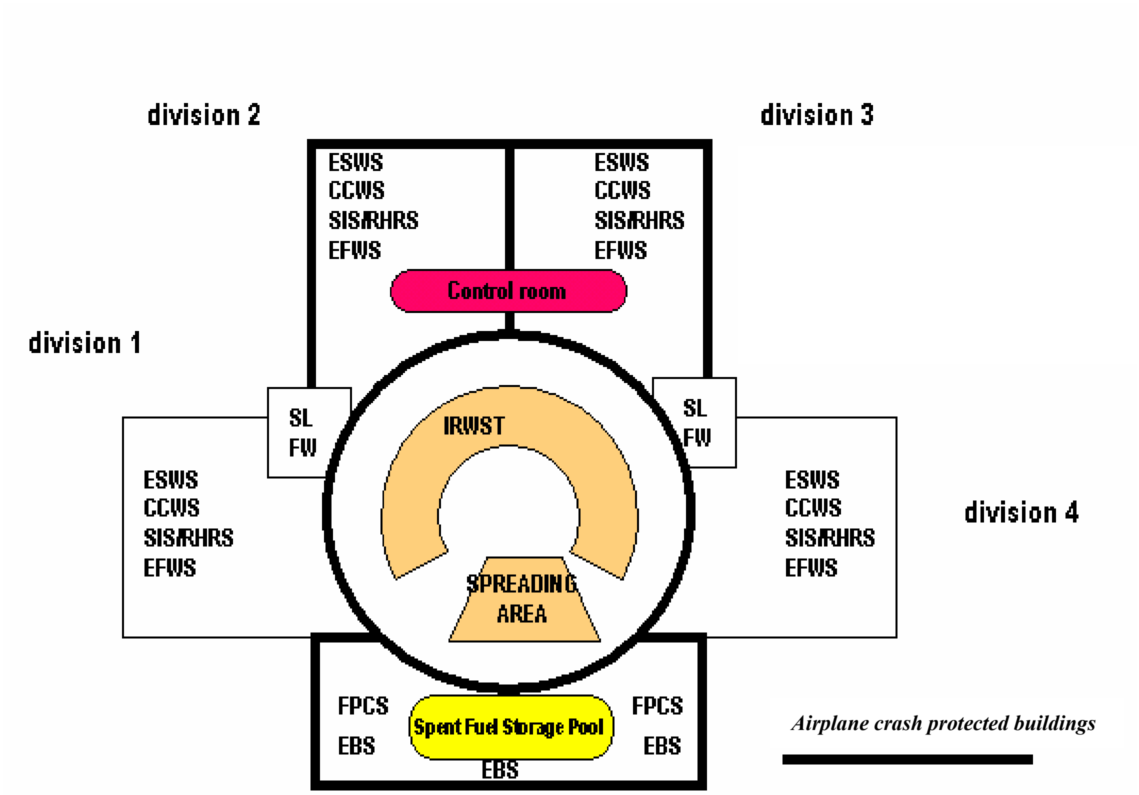
4.2. Approaches in design

On an analysis of the different reactor designs it is noted that the approaches to deal with external events might be classified into two categories:

(a) Structural design and layout based approaches which provide protection to safety related buildings and structures, systems and components against external events;

(b) Design measures that strengthen the plant robustness or redundancy in general, to resist effects of both internal and external events.

4.2.1. Structural design and layout based approaches



Emergency feedwater system (EFWS)
Component cooling water system (CCWS)
Emergency boration system (EBS)
Valve compartments (SL/FW)

Essential service water system (ESWS)
Safety injection system (SIS)
Fuel pool cooling system (FPCS)

FIG. 1. Layout of EPR Finland showing features for protection against aircraft impact.

In all the presented designs, the safety related structures are designed for design basis earthquakes, winds, extreme and severe meteorological conditions and design basis flood in line with national codes.

In addition, in several designs, a major emphasis is noted in the treatment of aircraft impact, and in the attention to achieve robustness of design that could enhance safety under extreme external events beyond the design basis. One approach used in the design is to ensure that buildings and structures have a capability to withstand the specific design basis external events. For example, in EPR Finland design (Fig. 1), the reactor building as well as the surrounding auxiliary buildings housing safety related equipment are structurally strengthened to the extent needed for surviving the impact of a large commercial aircraft. Some design measures, provided to deal with specific external events, call for additional protective features in plant layout and design. In EPR and SWR 1000, for example, aircraft crash protection measures have been implemented through attention being paid to plant layout, low vertical profile of containment, and additional robustness of protective external structures.

In a large number of the designs presented at the technical meeting, provision of redundancy of safety related systems and their physical separation in plant and building layout is an important element of defence in depth to ensure that in the event of limited damage to a portion of the safety related system, caused by EE, the remaining undamaged portion can still perform the required safety function.

Another common approach used in several designs relates to provision of redundancy and physical (layout) separation of systems fulfilling safety functions. In several designs, with either outer containment (VVER 91/99, PHWR-540, EPR Finland, AHWR) or a reactor/auxiliary building (or compartment) surrounding the inner containment (IRIS, CAREM, SWR 1000, VBER-300), the outer structure provides the protection to inner containment against direct damage caused by impact or blast loads. The ACR-700, AHWR and PHWR-540 designs provide for two physically separate, mutually independent trains of safety and plant protection systems, with an auxiliary control room being available in case the main control room becomes unavailable.

On an analysis of the description provided for the fourteen NPP designs considered, some generic design approaches to deal with external events, other than those conventionally adopted for most current generation reactors, are identified. These approaches for protection against external missile effects are summarized in Table 4.

TABLE 4. STRUCTURAL DESIGN AND LAYOUT BASED APPROACHES THAT FACILITATE PROTECTION AGAINST IMPACT OF EXTERNAL MISSILES

#	GENERIC DESIGN APPROACHES	NPPS (BASED ON DATASHEETS)	NUMBER OF RELEVANT NPPS
1.	Primary containment located within either a secondary containment or an external structure or building capable of withstanding postulated external impacts	APR1400, EPR Finland, VVER 91/99, CAREM-25, IRIS, PHWR-540, AHWR, SWR 1000, VK-300, CHTR	10
2.	Redundant physically separated safety trains with single containment capable of withstanding postulated external impacts	EPR Finland, APR1400, VBER-300 FNPP, VVER 91/99, ACR-700, AHWR, SWR 1000, ABWR-II, BN-800, CHTR, VK-300	11
3.	Physical and electrical separation of safety related equipment and cables.	APR1400, EPR Finland, VVER 91/99, PHWR-540, ACR-700, AHWR, ABWR-II, SWR 1000, BN-800, VK-300	10
4.	Structural design of structures against extended missile loading, e.g. aircraft impact	APR1400, EPR Finland, VBER-300 FNPP, SWR 1000, BN-800, VK-300	6
5.	Structural decoupling of inner structures with external containment to reduce the loads on these structures and safety related equipment arising out of external impact	EPR Finland, SWR 1000, PHWR-540, AHWR, VK-300	5
6.	Special measures to prevent poisonous gases intake into habitable areas and/or providing for a passive habitability system.	EPR Finland, IRIS, AHWR, SWR 1000	4

#	GENERIC DESIGN APPROACHES	NPPS (BASED ON DATASHEETS)	NUMBER OF RELEVANT NPPS
7.	Low vertical profile of reactor building to reduce possibility of aircraft impact.	IRIS, CHTR	2
8.	Safety significant equipment and systems such as diesel generator and spent fuel storage building located within protected structures	APR-1400, EPR Finland, SWR 1000	3
9.	Common base slab of auxiliary and containment buildings for enhanced seismic resistance	APR1400, EPR Finland	2

Most of the current designs of advanced NPPs need explicitly to address only a subset of the possible natural and human induced external events, and are in general, able to cope with external events on account of features provided for enveloping loads and to enhance defence in depth.

There are some other generic features, not discussed at the meeting, which are now generally considered in NPP layout and design. These include:

- Location of safety related structures, systems, and components (SSCs) plant grade, above 10^{-4}/year probability of exceedence flood levels;
- Assuring other safety related SSCs will not be in the plane of rotation of rotating equipment capable of generating missiles;
- Elimination of the use of parapets and roof layouts, which permit the build-up of snow, rain and ice;
- Assuring that metal towers and stacks will not be susceptible to vortex shedding wind loads.

Several types of future advanced NPPs are expected to have a wider spectrum of applications and designs (floating NPPs, desalination plants, combined electricity and district heating plants, hydrogen generating NPPs, power packs for remote areas, reactors with ceramic cores and structures, very high temperature reactors, molten salt reactors, reactors with very long plant life — up to 100 years, etc.). Many of these designs may adopt new design approaches to address specific external events. For example, for a reactor coupled with a hydrogen generating plant in close proximity, a major consideration could be events originating in the hydrogen generating plant. One may also visualize that in a situation of large scale of deployment, some NPPs may need to be deployed in regions currently considered inappropriate from siting considerations. Special design measures for the design of such plants from external event considerations may then need to be developed.

4.2.2. Design measures that strengthen the plant robustness in general, to resist both internal and external events

A desirable goal for the safety characteristics of an innovative reactor is that its primary defence against serious accidents is achieved through its design features preventing the occurrence of such accidents. Active safety systems or prompt operator actions are then not required to prevent significant fuel failure and fission product release. The plant can be designed such that its passive features provide adequate protection despite operational errors or equipment failure. Such robustness in design contributes to a significant reduction in the conditional probability of severe accident scenarios arising out of initiating events of internal and external origin. The function of confinement of any radioactivity released in the containment is also made more reliable by adopting robust, redundant, and sometimes, passive design features.

The current generation nuclear power reactors have several safety features to enable the plant to meet all the safety objectives under a variety of postulated initiating events and several combinations thereof. An important criterion for setting up a goal for safety, either implicitly or explicitly, has been the probability of large release of radioactivity outside the plant or site boundary as a consequence of any credible accident scenario. Even in designs, where probabilistic safety targets are not explicitly expressed, the selection of combination of postulated initiating events indirectly relates to probability of occurrence of large release. Many of the innovative reactor designs aim to minimize this probability by introducing additional robustness (often as a consequence of larger design margins) and by introduction of passive safety features, which do not require dependence on external sources of power or operator actions to perform their stipulated functions. An analysis of passive features is separately provided in this section.

4.3. Role of passive safety features in the prevention and mitigation of severe accident scenarios

4.3.1. Passive systems — some definitions

Some of the most commonly accepted definitions relating to passive safety features were arrived at, on the basis of a consensus among several international experts, in a series of meetings organized by the IAEA. Some of these definitions, considered relevant for further discussion, are reproduced from IAEA-TECDOC-626 [4.4].

Inherent safety characteristic:

Safety achieved by the 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.

4.3.2. Classification of passive systems, relevant for mitigation of consequences of external events

One of the important considerations in the treatment of external events is the possibility of disruption of external sources of electricity, cooling water, other essential supplies and possibly prompt operator action following an extreme external event. In such a situation, some innovative reactor designs take advantage of passive safety features provided within the protected reactor building or inner containment, disregarding the availability of external sources of supply of electricity, cooling water, etc. Several designs provide for physical presence of large thermal capacity heat sinks (e.g. AHWR, ACR-700, IRIS, ABWR-II, SWR 1000) available to cool the reactor core without depending on availability of externally powered pumps within the containment or elsewhere.

In this context, several passive systems enable prolonged grace period to the operator during which the reactor is maintained in a safe state without any operator intervention. This, in essence, implies availability of a large heat sink within the reactor building, and its highly reliable uninterruptible thermal communication with the reactor core to facilitate continued removal of core heat for prolonged durations without any involvement of active systems or operator interventions (e.g. natural convection, radiation, and conduction cooling). This feature too, is highly relevant for some extreme external events when, on account of possible devastation outside the protected reactor building, it is quite likely that all the external sources of cooling water, electricity, and instrumentation air and ventilation system become non-available. In such scenarios, it is also conceivable that the operators may not be in a position to act in an efficient or effective manner.

Going a step further, even among the passive features, certain innovative designs contemplate a situation (for example, a specific combination of initiating events, or a malevolent act by an insider) when a wired system incorporating sensors or actuators or a control system relevant to safety, is assumed to be disabled in a manner that the desired safety function cannot be performed in the absence of required signals or power supplies becoming available. It may be noted that provision of progressively increasing levels of defence in depth not only enhances the reliability of safety systems under postulated internal events, but also under a range of postulated external events.

In IAEA-TECDOC-626 [4.4], 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; and
- 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 in tubes covering the inner walls of silos of underground reactors; and
- 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; and
- 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); and
- Emergency reactor shutdown systems based on gravity driven, or static pressure driven control rods, activated by fail-safe trip logic.

Keeping the aforementioned in mind, it is logical to consider enhancement in the robustness of the defence-in-depth with possibility of using passive safety features as mentioned above for the purpose of augmentation of capability of the nuclear power plant to safely survive an extreme external event. The design of the data sheets (Table 2) seeks to obtain reactor specific information in the following design areas generally dealing with enhancement of defence-in-depth:

(a) Active safety systems requiring emergency power supply to ensure the coolability of the fuel in the event of loss of external sources of power, cooling water supply and compressed air; and without any credit to operator access within a stipulated grace period;

(b) Heat sinks that remain available with the loss of external coolant supply;

(c) Passive systems for reactor shutdown and heat removal within protected buildings that remain available to provide safety functions during the scenario postulated in (a) above with the help of instrumentation and electrical signals to get actuated;

(d) Passive systems, which do not require any electrical signals for actuation and provide the required safety functions under the scenario given in a) above.

(e) Inherent characteristics and category A (IAEA-TECDOC-626) safety features that arise out of basic selection of materials, physical geometry and layout of the reactor core and associated systems.

4.3.3. Passive and inherent safety features used in some designs of advanced reactors

Several specific passive safety features are being adopted in the designs of evolutionary and innovative NPPs. Many of these features are common to the different advanced NPP designs addressed in this section. On the basis of information gathered from the data sheets, a non-exhaustive list of design approaches and enabling technologies, specifically used in these NPP designs has been prepared and provided in Tables 5, 6, 7 and 8.

TABLE 5. HEAT SINKS THAT REMAIN AVAILABLE WITH THE LOSS OF EXTERNAL COOLANT SUPPLY

SAFETY FUNCTION	SPECIFIC DESIGN APPROACHES OR ENABLING TECHNOLOGIES	NAMES OF NPP DESIGNS IN WHICH A USE OF GIVEN DESIGN APPROACH OR ENABLING TECHNOLOGY IS EXPLICITLY MENTIONED IN THE ASSOCIATED DATASHEET.
Post shut-down decay heat removal	Availability of large heat sink either within containment or in thermal communication with the containment (e.g. large pool of water, ambient atmosphere) for decay heat removal.	APR1400, CAREM-25, SWR 1000, ABWR-II, AHWR, IRIS, VK-300, ACR-700
Emergency condition core (ECC) heat removal	Availability of large pool of water within containment acting as a source for passive ECC injection.	EPR Finland, PHWR-540, AHWR, CAREM-25, IRIS, ABWR-II, SWR 1000, VK-300, APR1400, ACR-700

TABLE 6. PASSIVE SAFETY SYSTEMS REQUIRING INSTRUMENTATION AND ELECTRICAL SIGNALS TO GET ACTUATED, TO PERFORM SAFETY FUNCTIONS EVEN WITH NON-AVAILABILITY OF ALL SOURCES OF POWER, COOLANT AND OTHER NECESSARY SUPPLIES EXTERNAL TO PROTECTED BUILDINGS

SAFETY FUNCTION	SPECIFIC DESIGN APPROACHES OR ENABLING TECHNOLOGIES	NAMES OF NPP DESIGNS IN WHICH A USE OF GIVEN DESIGN APPROACH OR ENABLING TECHNOLOGY IS EXPLICITLY MENTIONED IN THE ASSOCIATED DATASHEET.
Shutdown / power regulation	Control rods/ shut-off rods insertion by gravity force, stored hydraulic or pneumatic energy, etc. when the drives are de-energized by emergency protection signals or loss of power sources	ACR-700, AHWR, CAREM-25, IRIS, PHWR-540, VK-300, BN-800, VBER 300 FNPP
	Fast acting second shutdown system providing injection of neutron poison at high pressure (back up to first shutdown system)	CAREM-25, ACR-700, AHWR, VK-300, SWR 1000, IRIS, PHWR-540
Post shutdown decay heat removal	Passive post shut-down decay heat removal	VVER 91/99, CAREM-25, ABWR-II, ACR-700, VK-300
	Passive emergency heat removal from inside the reactor vessel	IRIS, VBER-300 FNPP, VK-300
Emergency condition heat removal	Post LOCA high pressure emergency coolant injection system, automatic depressurization system	ACR-700, VVER 91/99, CAREM-25, IRIS, VBER-300 FNPP, PHWR-540, VK-300
	Gravity driven core flooding, and/or long term core heat removal after opening of active valves	APR1400, ACR-700, IRIS, VK-300
Other heat removal paths	Steam generator atmosphere discharge valves, which open on instrument air failure	PHWR-540

TABLE 7. PASSIVE SAFETY SYSTEMS, WHICH DO NOT REQUIRE ANY ELECTRICAL SIGNALS TO GET ACTUATED OR TO PERFORM SAFETY FUNCTIONS EVEN WITH NON-AVAILABILITY OF ALL SOURCES OF POWER, COOLANT AND OTHER SUPPLIES EXTERNAL TO PROTECTED BUILDINGS

SAFETY FUNCTION	SPECIFIC DESIGN APPROACHES OR ENABLING TECHNOLOGIES	NPP DESIGNS ADOPTING SPECIFIC DESIGN APPROACH (INFORMATION BASED ON DATASHEETS).
Shut down/ power regulation	Passive Pressure Pulse Transmitters (PPPT) used to activate control rod drives (CRD) with scram system	SWR 1000
	Use of steam over-pressure to drive a valve that passively effects reactor shut down.	AHWR
	Use of high (liquid heavy metal) coolant temperature to passively effect shut-off rod drop	CHTR
	Passive power regulation with feedback from coolant outlet temperature	CHTR
Full power core heat removal	Natural circulation for heat removal under normal power condition	CAREM-25, AHWR, VK-300, CHTR, VBER-300 FNPP
Post shutdown decay heat removal	Use of passive valves actuated by steam over-pressure to valve-in natural circulation based decay heat removal system.	AHWR
	Natural circulation capability in the reactor coolant system to cope with transients due to loss of forced flow	ACR – 700 SWR 1000
	Natural circulation driven decay heat removal	IRIS, CHTR, VK-300
Emergency condition heat removal	Use of high coolant temperature to passively effect heat removal through vessel wall	CHTR
	Passive emergency core cooling system (ECCS) coolant injection	APR1400, AHWR, VBER-300 FNPP
	Passive core flooding in the event of LOCA	SWR 1000, VK-300
	Emergency condensers for heat removal from the reactor pressure vessel (RPV)	SWR 1000, VK-300
	Passive containment cooling system	ABWR-II
	Passive core water make-up from containment	IRIS

An illustration of some of the passive features of AHWR, indicated in Table 7, is provided in Fig. 2.

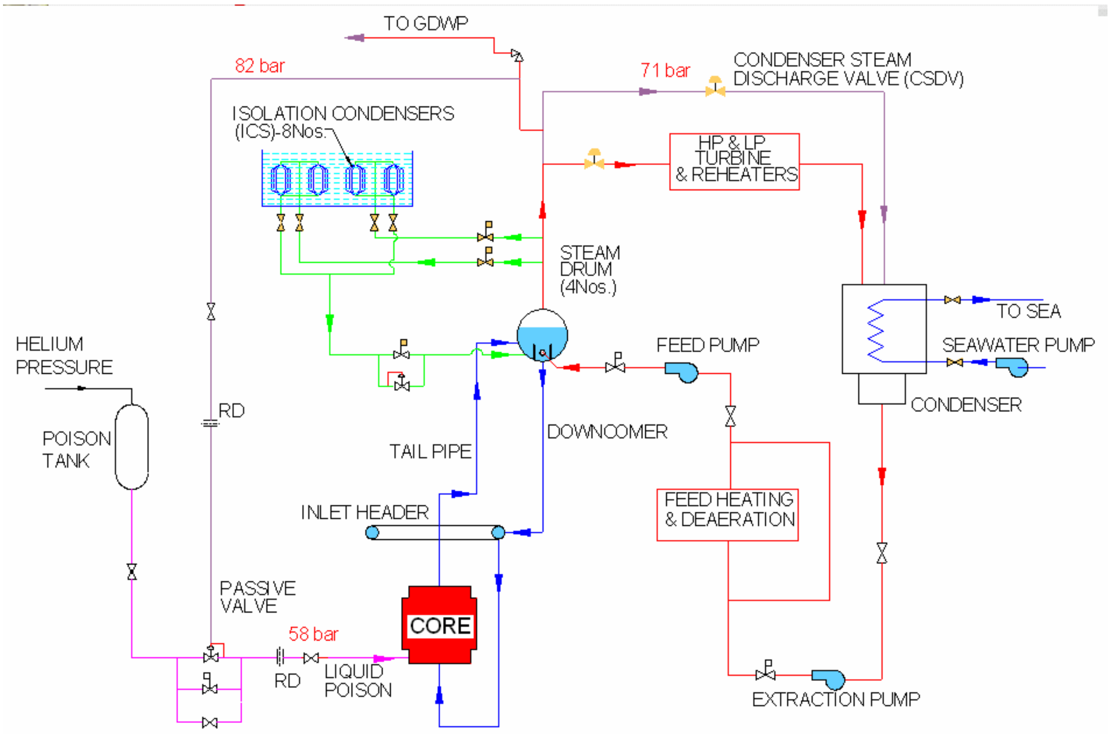


FIG. 2. Schematic of AHWR main heat transport system flow sheet indicating natural circulation driven core heat removal and steam overpressure (at 82 bar) driven shutdown feature for protection when failure of wired shutdown systems is postulated.

TABLE 8. INHERENT CHARACTERISTICS AND CATEGORY A (IAEA-TECDOC-626) PASSIVE SAFETY FEATURES THAT ARISE OUT OF BASIC SELECTION OF MATERIALS, PHYSICAL GEOMETRY AND LAYOUT OF THE REACTOR CORE AND ASSOCIATED SYSTEMS, WHICH ENSURE SAFETY ON ACCOUNT OF INHERENT PHYSICAL CHARACTERISTICS

CHARACTERISTICS	**SPECIFIC DESIGN APPROACHES OR ENABLING TECHNOLOGIES**	**NPPS ADOPTING SPECIFIC DESIGN APPROACH (INFORMATION BASED ON DATASHEETS).**
Neutronic characteristics to control reactivity excursion	Eliminating the possibility of a control rod ejection accident by either CRDMs located within the RV or by locating reactivity devices in low pressure moderator	IRIS, ACR-700, AHWR, PHWR-540
	Negative power reactivity coefficient[5] sufficient to accommodate any foreseeable reactivity insertions during start-up and power operation without damage to the fuel.	APR1400, ACR-700, SWR 1000, VBER-300 FNPP, VK-300, AHWR, CHTR, ABWR-II, EPR Finland
	Low excess reactivity in the core	AHWR, CHTR, PHWR-540, ACR-700

[5] The power reactivity coefficient is the one that governs the inherent safety behaviour of a reactor. The power coefficient is made up by the contribution of several coefficients: moderator temperature, fuel temperature, moderator density, etc.

CHARACTERISTICS	SPECIFIC DESIGN APPROACHES OR ENABLING TECHNOLOGIES	NPPS ADOPTING SPECIFIC DESIGN APPROACH (INFORMATION BASED ON DATASHEETS).
Enhanced fission product retention characteristics of fuel	Fuel with adequate ability to contain radioactive fission products over the full range of operating and accident conditions (e.g. coated particle type fuel).	CHTR
Thermal characteristics to control fuel temperature rise following power rise transients	Coolant with either no or very large heat transfer limits (e.g. helium, supercritical water, heavy liquid metals)	CHTR
	Large thermal inertia of fuel, core and core cooling system contributing to slower increase of fuel clad temperature following transients	CHTR, IRIS, AHWR
	Low core power density	CHTR, PHWR-540, IRIS, AHWR, VK-300
	Natural circulation driven core cooling under all operating conditions.	AHWR, CHTR, VK-300
	Capability for primary coolant natural circulation	PHWR-540, SWR 1000, EPR Finland
Structural features to prevent some major accident sequences	Integral vessel configuration, integral pressurizer, eliminated loop piping and external components - no large primary piping	IRIS, VBER-300 FNPP, VK-300

4.3.4. Reliability of passive safety features

Passive systems should, by definition, be able to carry out their mission with minimum or no reliance on external sources of energy and should operate only on the basis of fundamental natural physical laws, such as gravity. Passive systems generally have the advantages of simplicity, reduction of the need for human interaction, and reduction or avoidance of the need for external electrical power, instrumentation or control signals for their actuation. In view of their potential advantages in terms of reliability and independence from other systems and operator actions, passive systems have been proposed in several designs of advanced reactors.

Passive systems may play a significant role to reduce the conditional probabilities of occurrence of severe accident scenarios following extreme external events, which could jeopardise operator initiated and plant protection system initiated interventions. To evaluate these conditional probabilities, and to establish the contribution of passive systems in the development of accident scenarios, it is important to have an assessment of reliability of passive systems. An approach to carry out such an assessment, mainly based on the work of F. Bianchi, et al [4.5], is outlined in the following paragraphs.

It may be stipulated that a passive system may fail to fulfil its mission because of a consequence of the following two failures:

Component failure: Classical failure of a component or components (passive or active) of the passive system;

Phenomenological failure: Deviation from expected behaviour due to physical phenomena mainly related to thermal hydraulics or due to different boundary or initial conditions.

The reliability of components of a passive system can be evaluated by means of well-proven classical methods. However, aspects like lack of data on some phenomena, missing operating experience over the wide range of conditions, and the smaller driving forces make the reliability evaluation of passive system phenomena a challenging one. For evaluating the failure probability of passive systems, the methodology may move from the classical methods used for Probabilistic Risk Analysis (PRA) and consider, in addition to real components (valves, pumps, instrumentation, etc), virtual components, that represent the natural mechanism upon which the system operation is based (natural circulation, gravity, internal stored energy, etc.). Therefore, the reliability of passive systems may be determined by evaluating the failure probability of all the components (real and virtual). The contribution of real components can be easily assessed by resorting to the reliability databases available, whereas for evaluating the virtual component (process condition related) contribution it is necessary to develop a procedure that allows such assessment despite the lack of failure data.

A generic methodology for evaluation of passive system reliability, based on this approach, is shown in the Fig. 3.

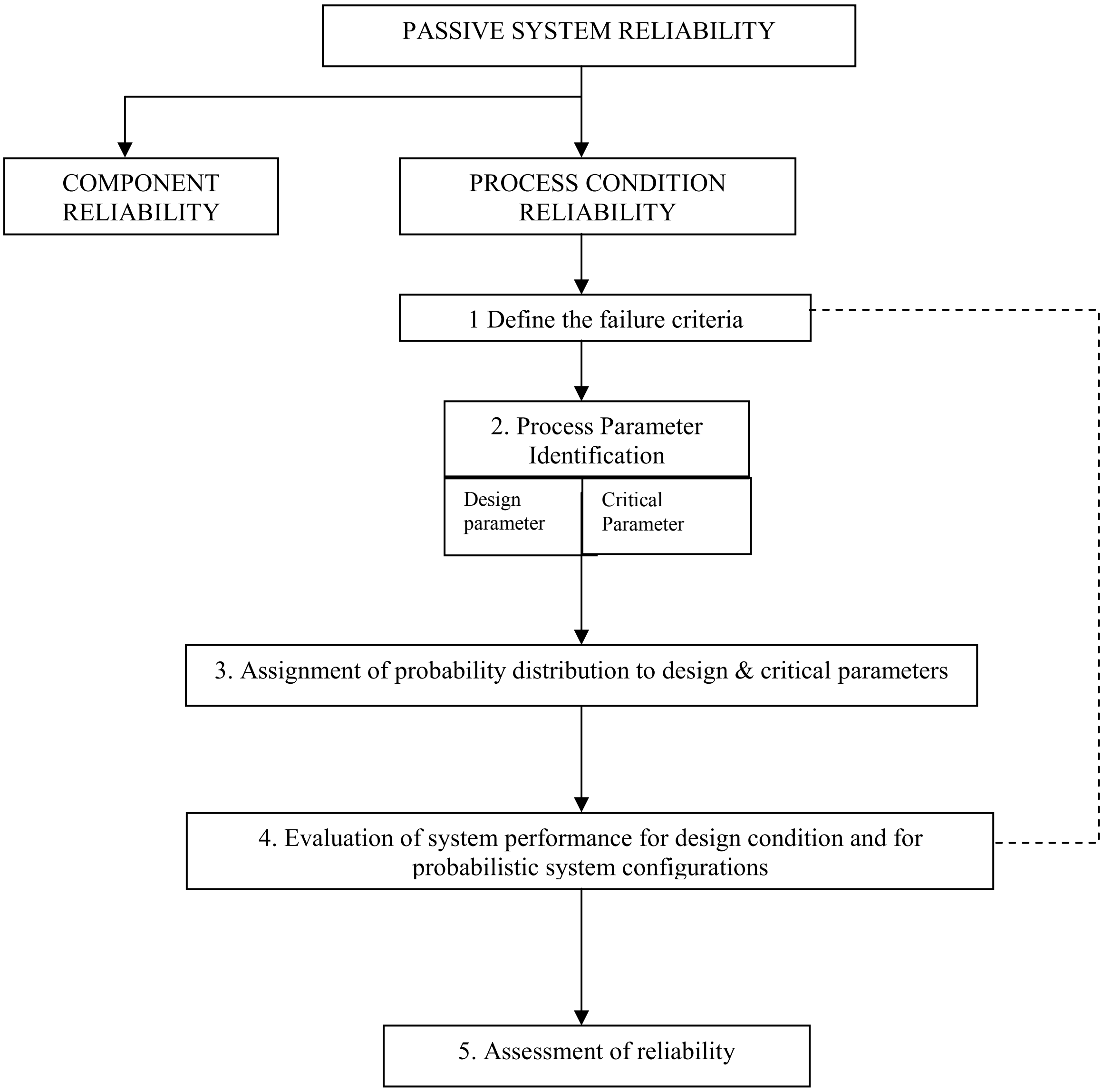

PASSIVE SYSTEM RELIABILITY
COMPONENT RELIABILITY
PROCESS CONDITION RELIABILITY
1 Define the failure criteria
2. Process Parameter Identification
Design parameter
Critical Parameter
3. Assignment of probability distribution to design & critical parameters
4. Evaluation of system performance for design condition and for probabilistic system configurations
5. Assessment of reliability

FIG. 3. Passive system reliability evaluation methodology.

4.3.5. Design approaches to address beyond design basis accidents

Beyond design basis accidents (BDBAs) are defined as accident conditions which are more severe than a design basis accident. Within this category of accidents, the following two classifications exist:

- Beyond design basis accidents without significant core degradation;
- Severe accidents – which are accident conditions more severe than a design basis accident and involve significant core degradation.

The approaches to address BDBAs, followed in the fourteen designs presented at the meeting, have been summarized in Table 9.

TABLE 9. DESIGN APPROACHES TO ADDRESS BEYOND DESIGN BASIS ACCIDENTS

SAFETY FUNCTION	**SPECIFIC DESIGN APPROACHES OR ENABLING TECHNOLOGIES**	**NPPS ADOPTING SPECIFIC DESIGN APPROACH (INFORMATION BASED ON DATASHEETS).**
Prevention of fuel failure	Fast acting diverse shutdown systems	APR1400, AHWR, IRIS, PHWR-540, ACR-700, SWR 1000
	Multiple redundant passive ECCS trains	AHWR, VK-300
	Coated particle type fuel	CHTR
Prevention of pressure boundary failure	Cold moderator surrounding the fuel channels, which can serve as heat sink; water filled reactor vault	PHWR-540, AHWR, ACR -700
	Passive make-up from the reserve water tank to moderator and shield water increases the time duration of the passive heat removal capabilities of these two separate water volumes, thus enhancing prevention and mitigation of severe core damage accidents	ACR-700
	Flooding of reactor cavity following LOCA and external reactor vessel cooling system	SWR 1000, APR1400, IRIS, AHWR
	Increased ratio of primary coolant inventory to reactor power increases the passive heat removal capability, thus enhancing mitigation of severe core damage sequences	IRIS
Avoidance of high pressure core melt ejection	RPV depressurization by highly redundant and diverse safety relief valves (SRV) / automatic depressurization system (ADS) to avoid high pressure core melt sequences	EPR Finland, ABWR-II, SWR 1000, IRIS
	Low pressure calandria or reactor vessel	AHWR, PHWR-540, ACR-700, CHTR

SAFETY FUNCTION	SPECIFIC DESIGN APPROACHES OR ENABLING TECHNOLOGIES	NPPS ADOPTING SPECIFIC DESIGN APPROACH (INFORMATION BASED ON DATASHEETS).
Containing and confining postulated core melt	Core melt stabilization through use of fully passive measures in all stages (retention, spreading, flooding, cooling)	EPR Finland
	Core catcher	VVER 91/99
	Use of reactor vessel bottom cooling system to confine the melt inside the vessel (In-Vessel Retention - IRV)	VBER-300 FNPP, IRIS
	Cooling by shield water in reactor vault surrounding the calandria vessel arrests core melt progression at calandria vessel boundary	ACR-700
Hydrogen mitigation (for water cooled reactors)	Hydrogen mitigation after core melt by passive autocatalytic recombiners	ABWR-II, IRIS, APR1400, ACR-700, EPR Finland, VK-300
	Containment inerted by nitrogen to avoid hydrogen-oxygen reactions	IRIS, ABWR-II, SWR 1000
	Containment hydrogen removal system	VVER 91/99
Maintaining containment integrity	Emergency containment spray back-up system	APR1400, VVER 91/99
	Containment heat removal systems	EPR Finland, IRIS, ACR-700, AHWR, SWR 1000, ABWR-II, VK-300
	Low-leakage thick-steel containment vessel with reduced number and size of penetrations	IRIS
	Containment is designed for hydrogen generation of 100% zirconium oxidation	SWR 1000, VK-300
Control of releases outside containment	Limiting radioactive releases by containment isolation and filtering of potential leakages	EPR Finland, PHWR-540, ACR-700, SWR 1000, AHWR, VBER-300 FNPP, ABWR-II
	Secondary containment, with purging arrangement to maintain negative pressure in annular space between primary & secondary containments	PHWR-540, AHWR, VK-300, SWR 1000, EPR Finland
	Passive containment isolation system	AHWR, SWR 1000

4.4. Applicability of IAEA safety requirements

4.4.1. Design basis external events

The IAEA safety standards document NS-R-1 [4.6] makes the following stipulation with regard to External Events:

"The design basis natural and human induced external events shall be determined for the proposed combination of site and plant. All those events with which significant radiological risk may be associated shall be considered. A combination of deterministic and probabilistic methods shall be used to select a subset of external events which the plant is designed to withstand, and from which the design bases are determined."

In the context of advanced reactors, the exclusion criteria for selection of external events may need to have a lower cut-off threshold for the frequency of occurrence, to be consistent with lower targets for Core Damage Frequency (CDF) and Large Release Frequency (LRF). This would lead to inclusion of low probability events on one hand and a larger uncertainty in their definition on the other, since the database for such low probability events could be too small. This uncertainty also creates difficulties in applying criteria for deciding the credible combination of events. There is also a need for a balanced definition of all design basis accident scenarios, of the internal as well as external origin, so that their contributions to the CDF and LRF are comparable.

It is also pertinent to consider the necessity for including malevolent scenarios, including sabotage, among Postulated Initiating Events (PIEs). These scenarios could manifest themselves either as an internal event, or as an external event, or as a combination of both. Their probability of occurrence is practically impossible to estimate [4.7].

4.4.2. Combination of internal and external sequences

NS-R-1 [4.6] makes the following stipulations in the context of combination of PIEs:

"Where combinations of randomly occurring individual events could credibly lead to anticipated operational occurrences or accident conditions, they shall be considered in the design. Certain events may be the consequences of other events, such as a flood following an earthquake. Such consequential effects shall be considered to be part of the original PIE.

Care needs to be taken in combining individual events in analyzing accidents to ensure that there is some rationale for the particular combination. A random combination of events may represent an extremely unlikely scenario that should be shown in the probabilistic safety analysis to be sufficiently rare as to be discounted rather than being taken as a postulated accident. In probabilistic safety analysis, an approach using best estimate analysis is adopted for severe accidents while conservatism should be applied in the analytical approach for postulated accidents that have a relatively higher likelihood of occurrence."

NS-G-1.5 [4.2] provides some further guidelines for combination of internal and external events.

During the initial design stage it is convenient to separately define design basis external events to conceptualize the appropriate design features and determine associated preliminary layouts and sizes for further optimization. To achieve a balanced 'risk-informed design', given the target CDF and LRF for a Nuclear Power Plant (NPP), the NPP may then be designed to achieve these targets for any credible combination of internal events and external events. Such an integrated assessment methodology could be the logical basis for final evaluation of the plant design. The current IAEA safety requirements and guides do recognize the merit of adopting this approach in design; however, the Probabilistic Safety Assessment (PSA) methodology to carry out such a combination of events is not yet fully developed.

4.4.3. Defence in depth for advanced reactors

The defence in depth approach will continue to be the basis of sound design for future plants. Moreover, it will be strengthened by additional margins in the design and, in general, by the explicit consideration of realistically conceivable severe accidents.

For the future plants, a detailed treatment of defence in depth is provided in INSAG-10 [4.8]. For the future reactors, this document envisages the following trends of the 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 melt-through.
- 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."

A pictorial representation of the difference in the treatment of defence in depth in existing and future innovative NPPs is given in Fig. 4 taken from IAEA-TECDOC-752 [4.9]. The figure illustrates that in the innovative NPPs the treatment of BDBAs is to be done on a realistic evaluation basis with the objective to eliminate the need for rapid response and evacuation.

As already indicated, most of the advanced NPP designs considered in this section address both internal as well as external event related scenarios by enhancing the quality of the first three levels of defence in depth dealing with accident prevention. In IAEA-TECDOC-1434 [4.10], addressing in particular the case of innovative reactors, a rationale for emphasizing accident prevention and control related levels of defence in depth is provided.

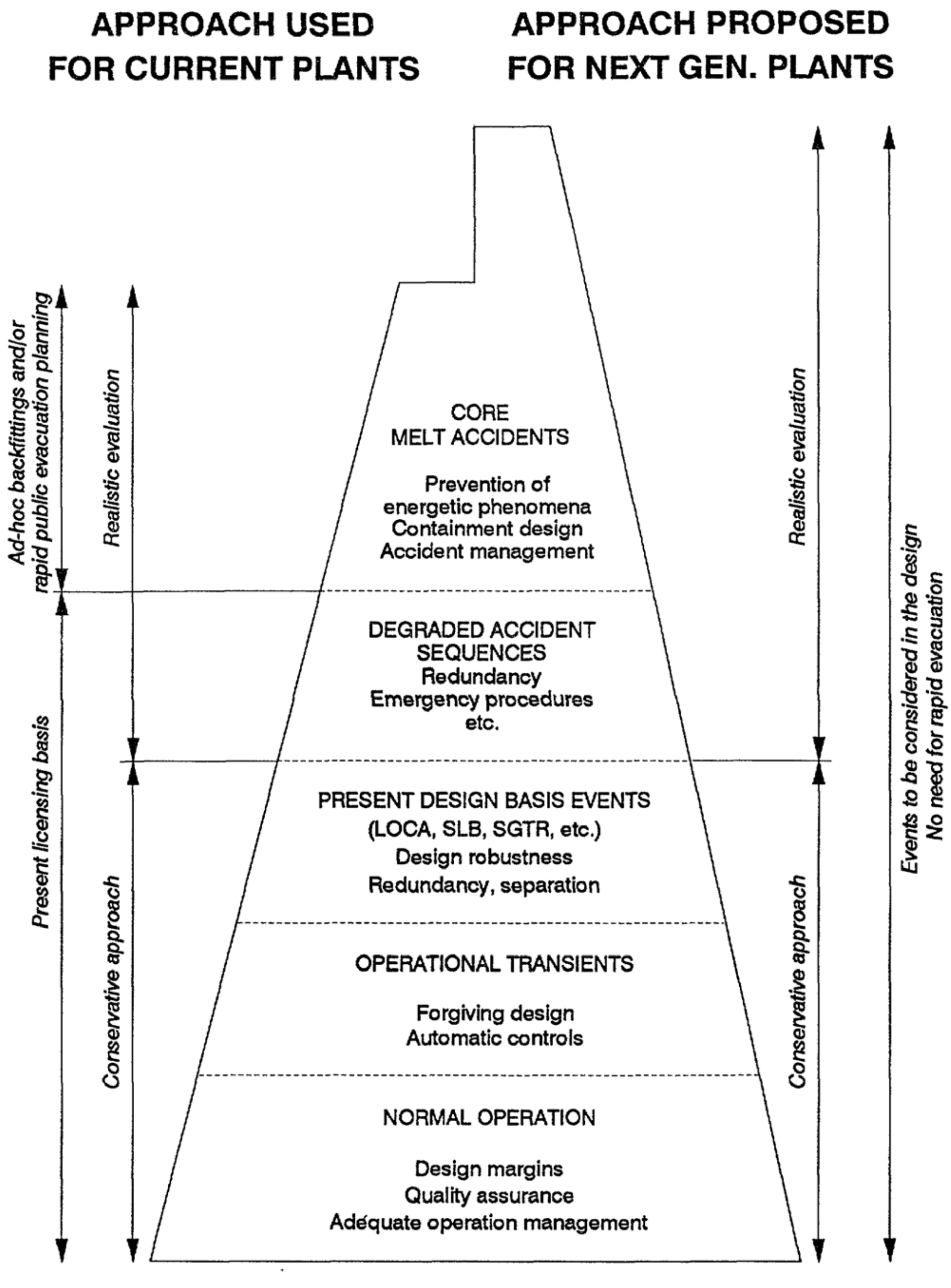


FIG. 4. The treatment of defence in depth in current and next generation plants [4.9].

Defence in depth provides an overall strategy for safety measures and features of nuclear installations. The strategy is twofold: first, to prevent accidents and, second, if prevention fails, to limit or mitigate their potential consequences and prevent any evolution to more serious conditions. Accident prevention is the first priority. The rationale for the priority is that provisions to prevent deviations of the plant state from well-known operating conditions are generally more effective and more predictable than measures aimed at mitigation of such departure, because the plant performance generally deteriorates when the status of the plant or a component departs from normal or anticipated transient conditions. Thus, preventing the degradation of plant status and performance generally will provide the most effective protection of the public and the environment. For innovative nuclear energy systems (INSs), the effectiveness of preventive measures should be enhanced compared with existing installations [4.10]. The general directions for innovation to enhance defence in depth, taken from IAEA-TECDOC-1434 are presented in Table 10.

TABLE 10. INNOVATION DIRECTIONS TO ENHANCE THE LEVELS OF DEFENCE IN DEPTH (FROM IAEA-TECDOC-1434) [4.10]

LEVEL OF DEFENCE IN DEPTH	OBJECTIVES	INNOVATION DIRECTION (INPRO)
1	Prevention of abnormal operation and failures	Enhance prevention by increased emphasis on inherently safe design characteristics and passive safety features.
2	Control of abnormal operation and detection of failures.	Give priority to advanced control and monitoring systems with enhanced reliability, intelligence and limiting features.
3	Control of accidents within the design basis.	Achieve fundamental safety functions by optimized combination of active and passive design features; limit fuel failures; increase grace period to several hours.
4	Control of severe plant conditions, including prevention and mitigation of the consequences of severe accidents.	Increase reliability of systems to control complex accident sequences; decrease severe core damage frequency by at least one order of magnitude, and even more for urban-sited facilities.
5	Mitigation of radiological consequences of significant releases of radioactive materials	No need for evacuation or relocation measures outside the plant site.

The design philosophy adopted for several advanced reactor designs, including those addressed in this section, appear to be close to the directions indicated in this Table (refer to Tables 5, 6, 7, 8, 9 and 11).

4.4.4. Emergency planning issues for advanced reactors

Most of the NPPs with innovative reactors aim to eliminate the need for intervention in public domain (outside the plant boundary) through the use of enhanced passive safety features in their design. Many of these designs also aim to take advantage of the advanced safety characteristics to seek exemption from maintaining a large exclusion distance around the nuclear power plants.

Indeed, particularly in the case of some of the extreme external natural events, when the region surrounding the NPP may be generally devastated, it is highly desirable for a nuclear power plant, which does not need frequent supply of fuel from outside, to be available to contribute to the rescue and rehabilitation effort, rather than become a burden on the state emergency response infrastructure.

In this context, INSAG-10 [4.8] brings out some of the desirable features in the defence-in-depth approach, for advanced reactors as indicated below:

“The confinement function for advanced reactors will be strengthened by approaches and initiatives consistent with the following concepts:

- For advanced designs, it would be demonstrated, by deterministic and probabilistic means, that hypothetical severe accident sequences that could lead to large radioactive releases due to early containment failure are essentially eliminated with a high degree of confidence.
- Severe accidents that could lead to late containment failure would be considered explicitly in the design process for advanced reactors. This applies to both the prevention of such accidents and

mitigation of their consequences, and includes a careful, realistic (best estimate) review of the confinement function and opportunities for improvement in such scenarios.

- For accident situations without core melt, it will need to be demonstrated for advanced designs that there is no necessity for protective measures (evacuation or sheltering for people living in the vicinity of a plant). For those severe accidents that are considered explicitly in the design, it would be demonstrated by best estimate analysis that only protective measures that are very limited in scope in terms of both area and time would be needed (including restrictions in food consumption)."

IAEA-TECDOC-1434 [4.10] is more categorical in stipulating the following requirement for innovative nuclear energy systems in the area of safety:

"The innovative nuclear reactors and fuel cycle installations shall not need relocation or evacuation measures outside the plant site, apart from those generic emergency measures developed for any industrial facility."

Notwithstanding the enhanced safety objectives for the advanced reactors, some of the current IAEA safety documents clearly stipulate a need for emergency planning. INSAG-12 [4.11] stipulates several principles concerning emergency planning. Some of these are reproduced below:

"140. Principle: The site selected for a nuclear power plant is compatible with the off-site countermeasures that may be necessary to limit the effects of accidental releases of radioactive substances, and is expected to remain compatible with such measures.

333. Principle: Emergency plans are prepared before the start-up of the plant, and are exercised periodically to ensure that protection measures can be implemented in the event of an accident which results in, or has the potential for, significant releases of radioactive materials within and beyond the site boundary. Emergency planning zones defined around the plant allow for the use of a graded response.

336. Principle: A permanently equipped emergency centre is available off the site for emergency response. On the site, a similar centre is provided for directing emergency activities within the plant and communicating with the off-site emergency organization.

339. Principle: Means are available to the responsible site staff to be used in early prediction of the extent and significance of any release of radioactive materials if an accident were to occur, for rapid and continuous assessment of the radiological situation, and for determining the need for protective measures."

Clearly these stipulations assume a very low but cognizable frequency of occurrence of severe accidents in the plant leading to a large off-site release of radioactivity. The document does, however, make a mention that "for future nuclear power plants, the protective emergency measures could be reduced in terms of both area of coverage and time of application."

There is therefore, a need to define the scope of off-site emergency planning activities for advanced reactors, consistent with the ability of these reactor designs to meet enhanced safety objectives. This need also emerges from the study carried out in the context of modular high temperature gas cooled reactors (MHTGRs). In IAEA-TECDOC-1366 [4.12], the following comments are made in this context:

"For existing plants, the term 'severe accidents" is widely associated with significant melting of the core and large releases of radionuclides from the reactor vessel. Because of the characteristics and features of MHTGRs ... ...and in particular the low core power density and high temperature capability of the coated fuel particles, no scenarios involving extensive melting of the core are apparent, even for very low probabilities/highly hypothetical events. Thus in the case of MHTGRs, the term 'severe accident' is taken to mean events which could challenge the structural integrity of the core and thus the ability to predict the course of the event, e.g. sustained (days) air ingress through large openings in the primary system and the confinement building. However, some action to manage these situations would be advisable to maintain the plant in a state that can be analysed. While such conditions could serve as a basis for considerations associated with Level 4 of defence in depth, it is important to point out that these extreme conditions will not necessarily involve large releases from the fuel, since existing data show effective radionuclide retention at elevated temperatures when the fuel has burned back to the silicon carbide layer of the coated particles and remains in a high temperature air environment for days."

Several designers that reviewed the present section, in connection with advanced NPP designs that are considered immune to severe accidents on account of very low core damage frequencies, expressed similar views. Seven out of the fourteen designs presented specifically consider the strengthening of safety features in these designs a sufficient basis for contemplating either 'nil' or significantly reduced need for intervention in public domain under BDBA conditions. The related specific statements made in the datasheets in respect of these designs are reproduced in Table 11.

TABLE 11. ADVANCED NPP DESIGNS WITH, IN DESIGNER'S VIEW, NO OR SIGNIFICANTLY REDUCED NEED FOR EMERGENCY INTERVENTION MEASURES IN PUBLIC DOMAIN

NAMES OF NPP DESIGNS	SPECIFIC STATEMENT IN THE DATASHEET CONCERNING EMERGENCY PLANNING ASPECTS
AHWR, CHTR, VK-300	No need for emergency planning in public domain.
ABWR-II	Practical exclusion of the probability of emergency evacuation/ resettlement.
IRIS	Reduced or eliminated requirement for emergency response planning
CAREM-25	CAREM-25 design allows an important reduction in the emergency planning.
SWR 1000	Off-site emergency response actions as evacuation, relocation are not required. Food control is restricted to the immediate vicinity of the plant.
EPR Finland	Off-site emergency response actions as evacuation, relocation and food control to be restricted to the immediate vicinity of the plant.
ACR-700	Large, separate water volumes in and around the reactor core (moderator and shield water) practically allow excluding large early release for BDBA and reduce the probability of containment failure and consequential late large release due to severe core damage. These characteristics help reducing generic requirements for emergency planning[6]. Site-dependent requirements and provisions for emergency planning will be identified for each specific project.

[6] These ACR-700 characteristics are relevant to the scope of the emergency planning review as provided in Section 4.4.4 of this report; see also section on ACR-700 in APPENDIX II.

4.5. Identified safety and technological issues

Based on the presentations and discussions at an IAEA technical meeting of 14-19 November 2004, several safety and technological issues, pertaining to approach in design for NPPs with advanced reactors were identified. The main issues are listed below:

(a) Considering the expected large diversities in the designs, applications and regions of deployment (some of which may not meet the current siting criteria) of advanced reactors, the design approach for dealing with external events for advanced reactors may need some modifications, with respect to the conventional approach for older reactors.

(b) Carrying out PSA in tandem with plant design helps identify the vulnerabilities as well as overly conservative design features at an early stage, leading to a well-balanced and cost-effective improvement in safety.

(c) The PSA methodologies to deal with external events have not reached the same level of maturity as has been reached for internal events. In particular, in order to deal with several external event scenarios it is desirable to couple the engineering design with PSA. In general, it should be understood that there is a significantly greater uncertainty associated with external event loads than that associated with internal event loads.

(d) Accident prevention is the main driving force for advanced reactor designs. Several design innovations are aimed towards bringing down conditional core damage frequencies (CCDF) to an extent that make the plant less vulnerable to extreme external event based and malevolent event based accident scenarios. Elements of a typical design approach that could contribute to achieve such robustness are:

   (i) Capability to limit reactor power through inherent neutronic characteristics in the event of any failure of normal shutdown systems, and/ or provision of a passive shutdown system not requiring any trip signal, power source, or operator action to effect a shut-down of the reactor if the safety critical plant parameters tend to exceed the design limits;

   (ii) Availability of a sufficiently large heat sink within the containment to indefinitely (or for a long grace period) remove core heat corresponding to abovementioned event;

   (iii) Availability of very reliable passive heat transfer mechanisms for transfer of core heat to this heat sink;

   (iv) Measures to ensure deterministically the immunity of abovementioned functions from external events and malevolent events;

(e) Implementation of innovative design measures needs to be supported and encouraged by a rational technical and non-prescriptive basis to define a severe accident (core melt need not be presupposed to occur). The rational technical basis could be derived from realistic scenarios applicable to the plant design. This implies that to take full advantage of new reactor designs it could be necessary to carry out best estimate calculation of source term.

(f) Most of the innovative reactor designs aim to eliminate the need for relocation or evacuation measures outside the plant site, through the use of enhanced safety features in design. Many of these designs also aim to take advantage of these advanced safety characteristics to seek exemption from maintaining a large exclusion distance around the nuclear power plants.

(g) In the context of some severe external events, the assumption of continued availability of infrastructure required to administer emergency measures (for example roads and bridges) may not be valid. Under such situation, it is more effective to enhance the quality of the other levels of defence in depth. There is therefore a need to define the scope of off-site emergency planning activities for advanced reactors, consistent with the ability of these reactor designs to meet enhanced safety objectives.

(h) In view of their potential advantages in terms of reliability and independence from other systems and operator actions, passive systems have been proposed in several designs of advanced reactors. Passive systems may play very significant role to reduce the conditional probabilities of occurrence of severe accident scenarios following extreme external events, which could jeopardise operator initiated and plant protection system initiated interventions. However, in specific instances the most conservative design basis increase in reliability of active systems and components may to a considerable degree offset the advantages of the use of passives components and systems.

(i) To arrive at the conditional probabilities mentioned above, and to establish the event trees considering the contribution of passive systems, it is important to have an assessment of reliability of systems being used.

(j) The performance of passive systems under extreme external events needs to be fully addressed in the design of advanced reactors. For example, performance of natural circulation based systems (low driving head), fluidic devices, passive valves etc. needs to be assessed under strong ground motion conditions, fire, etc.

(k) Several features that make plant safe for internal events also make the plant safer under external events. However, any new features should be checked for additional or peculiar vulnerabilities under external event scenarios.

4.6. Enhanced safety objectives for advanced NPPs

There was a consensus at an IAEA technical meeting of 14-19 November 2004 that the design of future advanced reactors should progressively be based upon an integrated approach taking into account both internal and external events together, using technology independent quantitative probabilistic safety criteria as a basis. Evolution of quantitative probabilistic safety criteria is a prerequisite for such approach.

Consistent with the requirement of sustainable growth of nuclear energy in the projected scenario of large-scale deployment, particularly in currently developing countries, the future advanced (evolutionary and innovative) nuclear power plants are generally expected to meet more stringent goals in the areas of economics, safety, environment, proliferation resistance and waste management. These goals, elaborated in the form of basic principles, user requirements and criteria, have been developed under the ongoing INPRO activity of IAEA [4.10]**.**

The current nuclear energy systems are designed to meet stringent safety criteria, as laid down in various international and national regulatory codes, guides and other documents. The risk to the general public, and the environment, from the operation of these NPPs has been demonstrated to be far less than that from any other comparable industrial activity. Nevertheless, an anticipated several fold increase in the global population of nuclear energy systems as required to meet large energy needs in densely inhabited regions, should potentially call for, as a minimum, one of the following enhanced safety related goals:

- The core damage frequency (CDF) should be reduced, at least in inverse proportion to the number of reactors in operation (this is related to the risk of latent fatalities);
- The large release frequency (LRF) should be reduced to such an insignificant level that implementation of emergency measures in public domain is not needed, and it is possible, in principle, to site the NPPs in close vicinity of population centres (this is related to the risk of prompt fatalities).

With the logic given above, the target for CDF and LRF should depend upon the number of reactor units (and other nuclear facilities) that could have an adverse radiological impact in a given geographical region following a severe accident. This would imply that the number of reactor units at a given site should be adequately factored in deciding the target value of the CDF and LRF per reactor unit per year.

The abovementioned enhanced safety goals are also considered to be of special importance to public acceptability. Lessons learnt from the past clearly indicate that public acceptability of nuclear power may be severely affected if any accident with severe consequences occurs anywhere in the world. The target value of CDF and LRF could therefore also take into account the global population of NPP reactor units.

Reflecting the aforementioned considerations, INSAG-12 [4.11] spells out the objective of the achievement of an improved goal of not more than 10–5 severe core damage events per plant operating year for future plants. The document stipulates that severe accident management and mitigation measures could reduce by a factor of at least ten the probability of large off-site releases requiring short-term off-site response. It also spells out another objective for these future plants as the practical elimination of accident sequences that could lead to large early radioactive releases, whereas severe accidents that could imply late containment failure would be considered in the design process with realistic assumptions and best estimate analyses so that their consequences would necessitate only protective measures limited in space and in time. In this context, it is important to consider the definition of severe core damage. One proposal is that core damage could be considered severe if the resulting source term (radioactivity within the containment) and the resulting pressure and temperature within the containment (driving forces for containment failure and early releases) could lead to large early release. However, this definition needs further discussion and elaboration.

4.7. Future challenges and IAEA potential contribution

The discussions in an IAEA technical meeting of 14–19 November 2004 brought into focus some gaps in the existing system of IAEA requirements and guides with respect to due treatment and consideration of the enhanced safety objectives for advanced reactors. It was amply brought out that the quality and depth of individual levels of defence in depth are very important attributes, and these should be given due consideration when prescribing a requirement for safety of such reactors. In particular, in the context of extreme external events, it was observed that the very assumption of continued availability of external infrastructure to manage emergencies in the public domain is questionable. Considering these factors, the following major conclusions and recommendations were made at the meeting:

(a) As a first step, the approach used for the existing reactors could be applied also to the characteristics of advanced, innovative or evolutionary reactors with regard to confirmation of site acceptability. Later on, considering the expected large diversities in the designs, applications and regions of deployment (some of which may not meet the current siting criteria) of advanced reactors, the design approach for dealing with external events for advanced reactors may need some modifications, with respect to the existing conventional approach.

(b) External events should be considered together with internal events in an integrated risk-informed approach in design, yielding cost effective solutions that meet quantitative probabilistic safety criteria for the plant, as well as deterministic success criteria for the systems, structures and components important to safety. Combination of events and combination of loads could arise out of this approach, which is yet to be developed. However, for preliminary design of the plant, provisions of existing safety standards and national practices, including those relating to the treatment of external events, could be a starting point.

(c) Agreement on whether or not malevolent actions including sabotage are to be addressed as an external hazard to be considered in design is desirable.

(d) Off-site emergency measures are still seen as part of the defence in depth approach, and are mainly understood in deterministic sense. However, most of the innovative reactor designs aim to eliminate the need for relocation or evacuation measures outside the plant site, through the use of enhanced safety features in design. Many of these designs also aim to take advantage of these advanced safety characteristics to seek exemption from maintaining a large exclusion distance around the nuclear power plants.

(e) The IAEA could review and as appropriate revise its safety requirements and guides for their applicability to evolutionary and innovative reactors.

(f) The IAEA safety goals are currently defined in qualitative terms, but there is increasing interest in seeking quantitative goals, such as a radiological dose to a member of the public versus a frequency of occurrence. This would help communicate the risk to the public and aid public acceptance of nuclear power;

(g) The IAEA could facilitate information exchange in the area of reliability of passive systems under external event scenarios;

(h) The IAEA could convene discussion on the topic of emergency planning issues for advanced reactors, particularly taking into account the fact of non-availability of external infrastructure for administration of emergency planning measures under severe external events, and other observations made by the participants of this technical meeting.

REFERENCES TO SECTION 4

[4.1] INTERNATIONAL ATOMIC ENERGY AGENCY, Extreme External Events in the Design and Assessment of Nuclear Power Plants, IAEA-TECDOC-1341, IAEA, Vienna (2003).

[4.2] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants: Safety Guide, IAEA Safety Standard Series No. NS-G-1.5, IAEA, Vienna (2003).

[4.3] EPRI, P. A., CA, "A Frame work for the Treatment of External Events in Configuration Risk Management", (http://www.epri.com/attachments/294895_CRMF2004Task.pdf), Draft Report (December 2004).

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

[4.5] BIANCHI, F., BURGAZZI, L., AURIA , F.D. RICOTTI, M.E., 'The REPAS approach to the evaluation of passive safety systems reliability', Proceedings of an International Workshop hosted by the Commissariat à l'Enérgie Atomique (CEA) on Passive System Reliability — A Challenge to Reliability Engineering and Licensing of Advanced NPPs, March 4–6, 2002.

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

[4.7] CONTRI, P., GÜRPINAR, A., 'Protection of nuclear power plants against external events of malevolent origin', Transactions of the 17th International Conference on Structural Mechanics in Reactor Technology (SMiRT 17) Prague, Czech Republic, August 17 –22, 2003.

[4.8] INTERNATIONAL ATOMIC ENERGY AGENCY, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

[4.9] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Advanced Containment Systems for Next Generation Water Reactors, IAEA-TECDOC-752, IAEA, Vienna (1994).

[4.10] INTERNATIONAL ATOMIC ENERGY AGENCY, Methodology for the Assessment of Innovative Nuclear Reactors and Fuel Cycles, IAEA-TECDOC-1434, IAEA, Vienna (2004).

[4.11] INTERNATIONAL ATOMIC ENERGY AGENCY, Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1 / INSAG-12, IAEA, Vienna (1999).

[4.12] INTERNATIONAL ATOMIC ENERGY AGENCY, Considerations in the Development of Safety Requirements for Innovative Reactors: Application to Modular High Temperature Gas-Cooled Reactors, IAEA-TECDOC-1366, IAEA, Vienna (2003).

[4.13]] INTERNATIONAL ATOMIC ENERGY AGENCY, Extreme External Events in the Design and Assessment of Nuclear Power Plants, IAEA-TECDOC-1341, IAEA, Vienna (2003).

5. EQUIPMENT QUALIFICATION AND TESTING

This section was prepared by international experts (as indicated in the end of this report) and is based on the outputs of an IAEA technical meeting held on 14-19 November 2005 in Vienna, as well as on the responses to the questionnaire, relevant for the topic (see also Section 2).

5.1. Introduction

Qualification to carry design basis loads and effects for safety related structures, systems and components (SSCs) in nuclear power plants typically considers one of 3 procedures, (1) design by analysis; (2) design by test; and (3) design by experience. Design by analysis is typically used for all external event load design qualifications except earthquake where test and experience are also used. Design by analysis tends to be used for passive type SSCs subject to earthquake loads, while qualification of active SSCs may use any one or a combination of the three procedures.

Design by analysis typically uses computed stress levels and displacement or deformation limits for active SSC and stress limitations for passive SSC qualification. Active SSCs typically use design by test or experience or a combination of analysis test and experience.

5.2. Design by analysis

In design by analysis, loads in the form of external forces and moments and deformations or displacements are applied to SSCs to determine resultant stresses or internal forces and moments and displacements and deformations. These are compared with design basis code or operational limits to determine design adequacy. It should be understood that the design code limits used for passive SSCs are generally less conservatively defined than those limits prescribed for active SSCs (i.e. Service Level B versus Service Level D limits for pressure retaining SSCs designed to the ASME B&PVC Section III Nuclear Components Code) [5.1]. For load combinations, which include the design basis event (DBE), active component limits are typically taken as 0.8 times yield stress and passive component limits are taken as 2 times yield stress.

5.3. Design by test

Design by test of SSCs usually employs a shake table (seismic) or autoclave (pressure) device, which simulate limiting external loads, and is usually applied to active SSCs to determine this ability to perform their required safety function during or following such loading. Testing may be in the form of fragility testing where the external loading is increased until failure occurs, which can provide a basis and a measure of the margin between design and failure loads. A second form of testing involves proof testing loads where external loads are applied up to some pre-selected level to demonstrate there is no failure up to that level. Proof testing is often done to an envelope type external load so that the SSC in question can be qualified in one test for a number of potential applications. However, such testing does not provide any estimate of the margin to failure.

A special form of qualification testing is by mock-up testing where the SSC to be qualified is mocked-up, usually in reduced scale or a single cell of a many cell device, and tested to demonstrate its operation behaviour characteristics. Examples of mock-up testing have been the development of pressure suppression systems for pressure suppression containment for BWR and PWR nuclear power plants (NPPs). In using mock-up testing for design verification, it is important to accurately simulate (including modelling) effects of the loads and behaviour of the SSC in service and to correlate the observed response with applicable design codes or standards. In both the PWR and BWR mock-up experience, the mock-up testing had to be supplemented by analysis and design changes under limiting loading conditions to demonstrate design adequacy.

5.4. Design by experience

Design by experience typically relies on the ability to find dynamically and statically similar systems and components subjected to equal or greater loads, which have withstood such loads without malfunction or failure. In general, structures and their external loads are so dissimilar that this design procedure is not applicable. The key issue in the use of experience data for design is the ability to demonstrate dynamic and static similarity of a system or a component, and equal or envelope input loading and similarity of operation of the system or component in question.

5.5. Fragility evaluations

Fragility evaluations are of use in performing a probabilistic safety assessment (PSA) or in developing margins to failure or malfunction. Such evaluations are based primarily on test and experience procedures used to evaluate failure or malfunction of systems and components where failure or malfunction is defined at beyond design code behaviour limits. Fragility limits are typically defined at a conditional 0.01 probability of failure with 50 percent confidence or 0.05 probability of failure at 95 percent confidence, as discussed in detail in ANNEX I.

5.6. Application to advanced reactors

There is an obvious desire on the part of advanced reactor designers to use “design by experience” methods of qualification in load combinations, which include earthquake load. The cost of the use of such a method of qualification, once an experienced database has been established, is typically one-tenth or less than qualification by analysis or test. It should be understood that design by experience sees its greatest application to active components and systems. Design by analysis, in accordance with applicable codes and standards, is still required to be applied to the leak tight or structural integrity of SSCs of all pressure retaining components and systems whether active or passive. Design by experience is usually applied as a supplement to active pressure retaining components where safety related active operation is required.

5.7. Review of papers and presentations

At a technical meeting held on 14-19 November 2004 in Vienna, several presentations were delivered on external event design of current as well as future NPPs with evolutionary and innovative reactors (see Table 1 in Section 1 of this report). For some of them, e.g. ACR, IRIS, APR 1400, a PSA based seismic margin assessment has been or is being performed to show that the design has inherent large seismic margin beyond the design basis[9]. For APR-1400, a partial external event PSA has been conducted to identify all potential external events and screen out some of them. External event PSA is planned for several others, including CAREM, IRIS, and EPR Finland (seismic). However, no seismic fragility analysis has been conducted so far for any of the designs considered at the meeting.

5.8. Seismic fragility analysis methodology

The seismic fragility of a structure or equipment is defined at the conditional probability of its failure at a given value of acceleration (i.e. peak ground acceleration or peak spectral acceleration at different frequencies). The methodology for evaluating seismic fragilities of structures and equipment is documented in the PRA Procedures Guide [5.2] and is more specifically described for application to NPPs in [5.3] and [5.4]. This general methodology has been applied in over 40 seismic probabilistic risk assessments of nuclear power plants. The ANS standard [5.5] provides requirements for performing the seismic fragility evaluation.

A detailed summary of seismic fragility analysis methodology complete with the list of references is provided in Section 4 of ANNEX I. Table 12 shows typical fragility values for NPP structures and equipment obtained from a seismic PSA.

[9] See Section 6 for more details.

TABLE 12. TYPICAL FRAGILITY VALUES FOR STRUCTURES AND EQUIPMENT FROM A SEISMIC PSA[10]

COMPONENT/STRUCTURE	MEDIAN CAPACITY (g)	Variabilities β_R	β_U	HCLPF CAPACITY (g)
Containment Building	1.76	0.26	0.30	0.70
Auxiliary Building	1.07	0.21	0.26	0.50
Reactor Pressure Vessel	2.34	0.25	0.33	0.90
RHR Pumps	1.86	0.33	0.22	0.75
Boron Injection Tank	0.95	0.27	0.36	0.34
Diesel Generators	1.02	0.26	0.20	0.48
Diesel Generator Control Panel	0.59	0.30	0.25	0.24
4,160V/480V Transformers	0.82	0.28	0.20	0.37
AFW Heat Exchanger	1.02	0.30	0.25	0.41

It could be noted that in general the ratio between the median and the HCLPF value exceeds a factor 2, which indicates that there is no cliff edge of system or component failure if the seismic event exceeds the HCLPF value.

5.9. Fragility analysis for other external events

Fragility analysis for other external events is not commonly performed in PSA of current nuclear power plants. However, the methodology used for seismic events (see section 4 of ANNEX I) could be extended to these other events, such as wind, flood, aircraft impact, and gas explosion. For passive failure modes of structure and equipment, the fragility could be estimated using analytical methods. The technique is to define the failure mode, calculate the median capacity and variabilities in the capacity analogous to the seismic fragility evaluation procedures. In addition, a fragility parameter appropriate for the external event should be defined (e.g. wind speed, flood depth, blast peak overpressure etc.). For functional failures, test data would be needed. For example, tests have been conducted on missile impacts on concrete barriers, and empirical relationships have been derived. These could be used to derive the fragility of the component [5.6]. For external events other than seismic, fragility evaluation is typically limited to that of the structural barriers (walls and roof). The equipment items housed inside the buildings are rarely affected by the external event. If the structural barrier is breached, the analyst may make the conservative assumption that the equipment items inside the building are all damaged. However, the fragility analyst has to use judgement in extending the analysis to the component level.

5.10. Fragility estimates for new reactor components

While fragility analysis methodology is universally applicable to any component in the reactor, some of the underlying data on new types of equipment or new materials may not be readily available. This is especially true for components whose failure modes are functional by nature. Also, the databases for fragility analysis such as earthquake experience data; generic equipment qualification data and fragility test data are adequate for current NPP with design basis earthquakes in the range of 0.10 g to 0.30 g peak ground acceleration. For higher design basis, more plant specific testing is needed.

[10] The definitions of parameters used in Table 12 are given in Section 4 of ANNEX I.

5.11. Conclusions and recommendations

Based on the presentations and discussions that ensued at a technical meeting held on 14-19 November 2004 in Vienna, certain conclusions have been derived. They have also led to recommendations for the IAEA and Member States in regards to NPPs with future evolutionary and innovative reactors in their safety evaluation against external events. The conclusions and recommendations are the following:

(1) Many of the components modelled in the external event PSA of innovative reactors are similar to those in existing NPPs. Therefore the current mature methodology for fragility calculation can be easily adapted for use in innovative reactors. If there should be new component types (e.g. passive components and ceramic core), some additional research will be necessary;

(2) For failure modes governing structural integrity of equipment (e.g. loss of pressure boundary, buckling, etc.), seismic fragility can be calculated using analytical formulations. For most functional failure modes, fragility calculation depends on the seismic qualification test information. For new equipment types not used in the current NPPs, specific qualification/ fragility tests are needed to obtain fragility data. This would help reduce the seismic CDF otherwise obtained from extrapolation from current NPPs. The reactor vendors and Member States could conduct such fragility tests;

(3) There may be a need for component fragility data for external hazards additional to that of earthquakes;

(4) There may be a need for data on operator response (human reliability models) in the case of an external event, possibly available from training and evaluation of personnel on simulators;

(5) Walkdown approach could address not just seismic issues, but also other external events, particularly where interactions are foreseen, operational measures are part of the protection and the effect of propagation from one area to another may be difficult to be evaluated by design;

(6) Future NPPs have design basis earthquake PGA higher than existing NPPs, and better design methodologies and therefore, the extension of fragility data/experience data to higher demands is required;

(7) There is a generic tendency to address beyond design basis events since the design stage. In this case, more realistic design and analysis approaches are in use, often borrowed from the assessment methods developed for existing plants (e.g. CDFM, SMA, etc.);

(8) In the framework of long operating life, equipment qualification should be maintained throughout the operating life, through maintenance and plant modifications. New methods may be needed to minimize inspection and maintenance cost, with predefined performance goals for the equipment;

(9) It is anticipated that new component designs (digital I&C) and materials (e.g. ceramic) will be used in the innovative reactors. There will be a need for large qualification programmes for calculating their seismic fragilities as the available experience data will not be applicable to them.

REFERENCES TO SECTION 5

[5.1] ABRAMS, P., et al, "Out-of-plane strength of unreinforced masonry infill panels", Earthquake Spectra, Vol. 12, No. 4, 1996.

[5.2] Nuclear Regulatory Commission, PRA Procedures Guide, Vol. 2, NUREG/CR-2300, USA (1983).

[5.3] KENNEDY, R.P. RAVINDRA, M.K., Seismic fragilities for nuclear power plant risk studies, Nuclear Engineering and Design, Vol. 79, No. 1 pp 47-68 (May 1984).

[5.4] REED, J.W., KENNED, R.P., "Methodology for developing seismic fragilities," EPRI TR-103959, Research Project RP2722-23, prepared for Electric Power Research Institute, Palo Alto, California (August 1993).

[5.5] ANS (2003) "External Events PRA Methodology — an American National Standard" ANSI/ANS-58.21-2003, published by the American Nuclear Society.

[5.6] TWISDALE, L.A., VICKERY, P.J., "Wind risk assessment", in Probabilistic Structural Mechanics Handbook — Theory and Industrial Applications*,* Editor C. (Raj) Sundararajan, Chapman and Hall, Chapter 19, (1995).

6. APPROACH TO SAFETY: PROBABILISTIC SAFETY ASSESSMENT (PSA)

This section was prepared by international experts (as indicated in the end of this report) and is based on the outputs of an IAEA technical meeting held on 14–19 November 2005 in Vienna, as well as on the responses to the questionnaire, relevant for the topic (see also Section 2).

6.1. Introduction

A full probabilistic safety assessment (PSA) should consider internal events as well as all external events that may affect the nuclear power plant. Further, all modes of operation, i.e. full power, low power and shutdown conditions should be evaluated. External events have been shown to be important since they can affect all structures, systems and components (SSCs) in the plant and could compromise system redundancies. The contribution of external events to plant risks is not insignificant thereby necessitating their systematic evaluation in a PSA.

In the following, a summary of the external event PSA methodology including seismic PSA (with more details given in ANNEX I) and industry experience with current NPPs is provided, as well as a summary of external event PSA performed for innovative reactors. External event PSAs have been performed for nuclear power plants in the USA since 1980. Many research programmes to develop the methodology and databases were sponsored by the US Nuclear Regulatory Commission (NRC) and the Electric Power Research Institute (EPRI). Guidance documents on performing external event PSA have also been developed in the US and have been followed by nuclear plant operators in different parts of the world. More recently, a US national standard providing requirements on external event PSA has been published. These represent the current state-of-the-art in the field of external event PSA. The IAEA has also published several safety standards reflecting on this topic. These are generally similar to the guidance documents developed in the USA.

6.2. External event PSA methodology

Generally, the evaluation covered in this section is the first task undertaken in a full-scope external event PSA. Through the work here, the analysis team ascertains which of the external events can be screened out so that no further PSA analysis is needed. This allows the team to focus on those events that remain (unscreened) within the analysis. Experience reveals that earthquakes can never be screened out using the methods herein; that sometimes high winds and external flooding can be screened out but sometimes they require further analysis, either a bounding analysis, a semi-quantitative analysis, or perhaps even a full PSA; and that occasionally one or more other external events also require a full PSA.

An external event analysis in a PSA has three important goals. The first one is that no significant event should be overlooked. The second goal is an optimal allocation of limited resources to the study of significant events, and the last is that the differences between external events and internal events (i.e. common-cause and fragility-related failures) should be recognized and explicitly treated. Based on these goals, three tasks could be identified:

(1) Identification of potential external events;

(2) Initial screening of external events;

(3) Approximate bounding analysis to calculate risks from external events.

A general description of each task is given in the following sections.

6.2.1. Identification of external events

The PRA Procedures Guide [6.1] provides guidance on identification of potential external events at a NPP site. Table 10-1 of the PRA Procedures Guide lists most of the possible external events that may affect a plant site. This information should be augmented with a review of information on the site region and plant design to identify all external events to be considered. The data in the Safety Analysis Report (SAR) regarding the geologic, seismologic, hydrologic, and meteorological characteristics of the site region as well as present and projected industrial activities (i.e. increases in the number of flights, construction of new industrial facilities) in the vicinity of the plant is also reviewed for this purpose.

6.2.2. Screening criteria

The external events identified are screened in order to select the events for either approximate or detailed risk quantification. A set of screening criteria is formulated to minimize the possibility of omitting significant risk contributors while reducing the amount of detailed analyses to manageable proportions. The set of screening criteria given by the PRA Procedures Guide are as follows:

(1) The event is of equal or lesser damage potential than the events for which the plant has been designed. This screening criterion is not applicable to events such as earthquakes, floods, and extreme winds since their hazard intensities could conceivably exceed the plant design basis. This requires an evaluation of plant design basis in order to estimate the resistance of plant structures and systems to a particular external event. For example, it is established that safety-related structures designed for earthquake and tornado loadings in tornado intensity Zone I in USA can safely withstand a 20 kPa static pressure from explosions. Hence, if the PRA analyst demonstrates that the overpressure resulting from explosions at a source (e.g. railroad, highway, or industrial facility) has an acceptable low frequency of exceeding 20 kPa, these postulated explosions need not be considered;

(2) The event has a significantly lower mean frequency of occurrence than other events with similar uncertainties and could not result in worse consequences than those events. For example, the PSA analyst may exclude an event whose mean frequency of occurrence is less than some small fraction of those for other events. In this case, the uncertainty in the frequency estimate for the excluded event is judged by the PSA analyst as not significantly influencing the total risk;

(3) The event cannot occur close enough to the plant to affect it. This is also a function of the magnitude of the event. Examples of such events are landslides, volcanic eruptions, and earthquake fault ruptures;

(4) The event is included in the definition of another event. For example, storm surges and seiches are included in external flooding; the release of toxic gases from sources external to the plant is included in the effects of either pipeline accidents, industrial or military facility accidents, or transportation accidents;

(5) The event is slow in developing and there is sufficient time to eliminate the source of the threat or to provide an adequate response.

This process of initial screening identifies a smaller set of external events identified for risk assessment. A bounding analysis is then performed for these external events as described below. A list of external hazards typically considered in PSA can also be found in the ANS Standard [6.2].

6.2.3. Bounding analysis

The preliminary screening could lead to identifying certain events as requiring further examination. The PSA analyst could perform either a bounding analysis to estimate the risk contribution of the event or conduct a detailed probabilistic safety assessment for the event. Generally, seismic event is not screened out at this stage and requires a detailed PSA. For other events such as extreme winds, external flooding, transportation and nearby facility accidents, aircraft impact and pipeline accident, bounding analysis may typically be sufficient. Examples of such analysis are found in NUREG-1150 studies and in reference [6.3].

6.3. Seismic PSA methodology

Seismic Probabilistic Safety Assessments (PSAs) have been conducted for over 50 nuclear power plants worldwide in the last 25 years. The methodology has been well established and the necessary data on the parameters of the PSA models have been generally collected. Detailed summary of the procedures used in seismic PSA complete with the list of references is given in ANNEX I. In response to the need for risk-informed decisions, a US national standard [6.2] on external event PSA has been developed, which prescribes the standard requirements for different elements of a seismic PSA.

6.4. Industry experience in current NPPs

The nuclear industry in different Member States has gained valuable insights by performing external event PSAs of current nuclear power plants. External event PSA is also increasingly used to aid in design decisions for new plants. In the context of innovative reactors, following are some of the areas that need to be examined further.

6.4.1. Seismic hazard studies

Probabilistic seismic hazard analyses have been conducted for a number of nuclear power plant sites around the world. These analyses have relied on regional and local seismological and geological information, historical seismicity and ground motion attenuation. Since the historical data is limited and there are different opinions and interpretations of seismic sources and ground motion among the experts, a comprehensive approach for expert elicitation has been developed recently by the Senior Seismic Hazard Analysis Committee [6.4]. This is known as the SSHAC methodology. The application of this methodology has indicated that the epistemic uncertainty in seismic hazard could be high. Further, the mean hazard at most sites has been shown to be higher than the previous estimates as a result of detailed seismic source modelling and increased knowledge of ground motion characteristics.

Although the operating nuclear power plants in the USA have been designed for a Safe Shutdown Earthquake (SSE) selected using deterministic procedure established in early 1970s, the probability of exceeding the SSE was till recently considered to be in the range of 1.10-4 to 1.10-3 per year. For the advanced reactors, the vendors have chosen an SSE of 0.3 g peak ground acceleration (PGA) anchored to a broadband ground response spectrum on the basis that the probability of exceeding this earthquake level at any site is less than 1.10-4 per year. However, the recent probabilistic safety hazard assessments seem to indicate that the seismic hazard at 0.3 g could be much higher. In other words, the SSE selected on the basis of an exceedance probability of 1.10-4 per year could be higher than 0.3 g PGA at some potential nuclear power plant sites.

For advanced reactors, the internal event core damage frequency (CDF) and large early release frequency (LERF) are expected to be much lower than those for existing plants, as a result of innovations in design and insights gained through four decades of nuclear plant operation. Paradoxically, seismic contribution to CDF is expected to increase substantially because of better understanding of the hazard potential. Therefore, the impact of new probabilistic safety hazard assessments is expected to linger.

Comparable hazard studies for other external events (e.g. hurricane, tornado, external flooding, aircraft impact and gas explosions) are rarely conducted. Since the impact of most of these events is limited to the external barriers (i.e. walls and roofs) of nuclear power plant structures, any increase in the hazard may have only a minor effect on the design of innovative reactors and could be handled in siting of the reactors.

6.4.2. Lessons learned from current external event PSAs

Several important lessons have been obtained from the external event PSA of current NPPs:

- The risk contribution from external events could be significant for some plants; but it is very site specific, and generalizations should not be made. Only a systematic analysis would show the significance or not of any external event;
- The uncertainties in external event induced CDF and LERF could be much larger compared to those for internal events;
- Dominant contributors to CDF and LERF at any plant are functions of the plant design basis; any analyst contemplating a new external event PSA would benefit from studying the past PSAs

to ensure that some important contributors are not missed. Further, these could provide valuable insights for future designs so as to avoid such contributors;

- Walkdown for external events (especially for seismic events) has been very helpful in identifying the potential interactions and vulnerabilities.

6.4.3. Stringent safety goals and uncertainty analysis

Current seismic PSAs have shown the seismic contribution to CDF is in the range of $1\cdot10^{-5}$ per year to $1\cdot10^{-6}$ per year. This is about 10% to 1% of the CDF from internal events but for the innovative reactors, the internal event CDF goal is being lowered to as much as $1\cdot10^{-8}$ per year. Experience shows that similar low CDF goal for seismic events is not reasonably achievable, especially in view of the increased estimates of seismic hazard obtained in recent probabilistic safety hazard assessments.

While the focus is on mean CDF estimates, one should not forget the uncertainties in the external event analysis. It is true that the uncertainty in seismic CDF is dominated by the uncertainty in seismic hazard. However, the uncertainty in hazard from other external events (e.g. extreme wind, flooding, and tsunami) may also be large because of limited empirical data and lack of phenomenological models.

6.5. Review of external event PSA for innovative reactors

The review in this section is limited to NPP designs considered at a technical meeting held on 14-19 November 2004 in Vienna and/ or addressed in the questionnaires as discussed in more detail in Sections 1 and 2. Throughout this section, reference is made to Table 1 in Section 1.

The APR 1400 is an evolutionary PWR (see Table 1). Its safety goals are CDF less than $1\cdot10^{-5}$/year and LERF less than $1\cdot10^{-6}$/year. The external event PSA included identification of all potential external events that may affect the plant, and screened out a number of the events based on established screening criteria [6.1]. Detailed PSA was performed for internal fire and internal flooding events. For seismic events, a PSA based seismic margin assessment was conducted. The lowest HCLPF capacity was estimated as 0.5g, which is higher than the design basis earthquake of 0.3 g.

The EPR Finland is an evolutionary PWR (see Table 1). The first plant will be built on the Olkiluoto site in Finland. External events are being considered in the plant layout and design. For example, the layout has been finalized to withstand a large commercial aircraft crash in that the reactor could be brought to a safe shutdown because of system redundancies, separation and barrier design. Following the Finnish regulations, a design phase seismic PSA is being conducted to identify any system level seismic vulnerabilities.

The VBER-300 is an advanced small PWR (see Table 1 and ANNEX VII). It is being proposed for a floating nuclear power plant. Currently, there is no external event PSA for this reactor.

The VVER 91/99 is an evolutionary VVER (see Table 1). The reactor is designed to meet several external events (seismic, aircraft crash, extreme winds etc.). Currently, there is no external event PSA for this reactor.

The CAREM reactor (see Table 1 and ANNEX V) is an integral PWR incorporating many passive features. All external events with frequency of exceedence of $1\cdot10^{-7}$ per year are considered in the design. By proper siting and barrier design, some of the external events are screened out. The design basis earthquake is chosen as 0.4 g PGA anchored to a broadband ground response spectrum. The design basis tornado is F3 on the Fujita scale. Because of the passive design, external event induced station blackout and loss of heat sink are not considered dominant risk contributors (ANNEX V). Since the Argentinean regulation is risk-based, external event PSA is expected after the design is completed to demonstrate conformance. No such PSA has been completed.

The IRIS is an integral type PWR incorporating many passive features (see Table 1 and ANNEX VI). Its design precludes some accidents and reduces the probability and/ or consequences of other accident scenarios. As a result, the emergency planning requirements are considerably reduced. IRIS combines passive systems and active non-safety systems, which reduce the core damage frequency. The IRIS design team and the PSA team are working together and simultaneously to finalize the design that meets the rather stringent safety goals on CDF ($1^{.}10^{-8}$/year) and LERF ($1^{.}10^{-9}$/year). All external events that may affect the plant are identified and systematically screened out following an established set of screening criteria. The external events analyzed in detail include tornadoes, aircraft crash, seismic events, internal flooding and internal fires. For seismic events, a PSA based seismic margin assessment has been performed. It is concluded that the IRIS design has a seismic margin of at least 0.5 g PGA, which is well beyond the design basis earthquake of 0.3 g PGA. The IRIS designers have recognized that " the CDF due to external events such as seismic, could be a preponderant factor in the total CDF for IRIS. Consequently, plans have already been made to apply both the safety-by-design philosophy and the PRA guided design approach to design the plant such as to minimize the external event contribution to CDF".

For the PHWR-540 of India, the only operating NPP considered (see Table 1), there is a description of a probabilistic seismic hazard analysis conducted for the Tarapur Atomic Power Station site, see ANNEX III. Uniform hazard spectra for different return periods are developed. Screening distance values for different types of aircraft activity around the site are provided. Recently, impact analyses for beyond the design basis aircraft crashes onto the containment structures have been performed. Another paper of relevance, provided as ANNEX II, describes how external events are treated in the siting and design of Indian nuclear power plants. The approaches used are similar to those recommended by the IAEA and the USNRC. The paper describes the flooding incident at Kakrapar Atomic Power Station in June 1994 and the lessons learned for future NPP designs. These papers are focused on the design of NPPs rather than on external event PSA. It is not clear whether full-scope external event PSAs have been conducted for any Indian NPP.

The Advanced CANDU Reactor (ACR, see Table 1 and ANNEX IV) is being designed to withstand design basis earthquake (DBE) and design basis tornado (DBT). All other external events (e.g. aircraft crash, flooding, explosions and snow) will be handled during the siting of the plant through a combination of measures: maintaining safe distance; protective design and administrative actions such as installation of advance warning system. The design basis earthquake for the ACR is chosen as 0.3 g peak ground acceleration (PGA) anchored to a broadband ground response spectrum. In order to demonstrate the robustness of the ACR design to handle beyond design basis earthquakes, a PSA based seismic margin assessment (SMA) is being performed. This should provide insights to improve the system design of the ACR as needed.

The SWR 1000 is an advanced BWR (see Table 1). It has several passive safety systems. Plant layout and system design have explicitly considered external events such as airplane crash. Currently, there is no external event PSA available for the reactor.

The VK-300 is an advanced BWR with many passive features (see Table 1). An internal event PSA has shown that the CDF is less than $2^{.}10^{-8}$/year. The reactor will be designed to meet several external events (seismic, aircraft crash, explosions, etc.). Currently, there is no external event PSA for this reactor.

The ABWR-II is an advanced BWR incorporating several innovative safety features (see Table 1 and ANNEX VIII). A preliminary PSA evaluation was performed for the internal events. A simplified PSA evaluation was performed at the design selection stage to optimize the features of the ABWR-II safety system configuration that secure its robustness even in seismic induced (station blackout) or shutdown events. Currently, there is no external event PSA for this reactor.

The BN-800 is a fast reactor with liquid sodium coolant (see Table 1). The reactor is being designed to meet several external events (seismic, aircraft crash, extreme winds, etc.). Currently, there is no external event PSA for this reactor.

No information on external event PSA was provided for the Indian AHWR and CHTR reactors (see Table 1), tentatively because of their too early design stage.

6.6. Applicability of IAEA safety requirements

The IAEA has published several safety guides and TECDOCs providing guidance on treatment of external events in design and safety assessments [6.5-6.16]. These documents provide guidance on performing hazard analysis for different external events and on external event PSA. This guidance could be judged adequate and useful for innovative reactors. In the course of performing the external event PSA of innovative reactors, needs for further guidance documents may be identified.

6.7. Identified safety and technological issues and proposal for resolution

The major findings for this topic were as follows:

(1) Whereas there are substantial progress and innovations in the reactor designs as reflected in the internal event PSAs, there are no similar progresses in the treatment of external event design and relevant external event PSA. This lack of consistency in the overall principle of treatment of internal and external event is seen as a major drawback;

(2) The approaches presented for treatment of external events (for design as well as PSA) are similar to the approaches followed in the nuclear industry over the last 20 years. There is no innovation in the external event PSA, that an innovative reactor would demand;

(3) The contribution of external events to plant risk estimates is seen to be higher (in percentage) for evolutionary and innovative reactors, since the internal event risks have been substantially reduced through better system design, avoidance of identified accident sequences, etc. It is not clear whether a plant driven by external event risks (compared to internal events) would be acceptable;

(4) For some innovative reactor designs, refuelling outage may be longer (e.g. some design modifications of IRIS) during which time the containment and the reactor head are open. The impact of any external event during this shutdown and low power mode may be more significant than for the existing reactors. This should be explicitly addressed in the analysis;

(5) Probabilistic treatment of external events has not been uniformly done for all evolutionary and innovative reactors. There are examples of enveloping the extreme deterministic parameters for different designs and sites derived from current LWRs;

(6) Large uncertainties in seismic hazard at any potential NPP site are a fact. The situation may not improve in a foreseeable feature. Therefore, siting procedures for innovative reactors could be further developed in order to reduce this large uncertainties and to provide a more realistic design basis;

(7) The management of the uncertainties in the PSA process should be improved, as current practice is very conservative and recent studies highlighted the need for new methods to keep under control the uncertainties from expert judgement, the random and the epistemic uncertainties;

(8) The new reactor designs are planned for an operating life of 60 years or more. Our knowledge on ageing effects of concrete is limited. Further research would be needed to confidently forecast a longer operating life, particularly for embedded structures, avoiding expensive inspection and upgrading programmes;

(9) In order to reduce the external event risks (particularly from seismic events), better modelling assumptions and computational methods are needed. For example, the assumption that all redundant components fail under the same earthquake (i.e. “one fails, all fail” model) would lead to excessively conservative results. This may have worked well in the past seismic PSAs but will not suffice for new designs.

6.8. Future challenges and IAEA potential contribution

Meeting the stringent safety goals for innovative reactors (e.g. core damage frequency of $2^{\cdot}10^{-8}$ per year) would be a major challenge. A reasonable balance should be maintained between safety targets for internal and external events considering the very low safety targets set for internal events. Innovative approaches for treating external events rather than by purely depending on hardening or on additional barriers are needed in order to reduce the plant costs and make the advanced reactors deployable. The IAEA could coordinate research programmes to enhance external event PSA methodology. Some of the issues that are not important for current NPPs may become significant for innovative reactors because of the stringent safety goals. The examples are treatment of correlation between component failures, large uncertainties in seismic hazard and better computational methods for seismic risk quantification.

REFERENCES TO SECTION 6

[6.1] Nuclear Regulatory Commission, PRA Procedures Guide, Vol. 2, NUREG/CR-2300, USA (1983).

[6.2] ANS (2003) "External Events PRA Methodology – an American National Standard" ANSI/ANS-58.21-2003, published by the American Nuclear Society.

[6.3] TWINSDALE, L.A. VICKERY, P.J., "Wind risk assessment", in Probabilistic Structural Mechanics Handbook — Theory and Industrial Applications*,* Editor C. (Raj) Sundararajan, Chapman and Hall, Chapter 19 (1995).

[6.4] BUDNITZ, R.J., "State-of-the-art report on the current status of methodologies for seismic PSA", Report to Nuclear Energy Agency of the Organization for Economic Cooperation and Development, Paris, (July 1997).

[6.5] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, Safety Guide, IAEA Safety Standards Series, No. NS-G-1.5, IAEA, Vienna (2003).

[6.6] INTERNATIONAL ATOMIC ENERGY AGENCY, External Human Induced Events in Site Evaluation for Nuclear Power Plants, IAEA Safety Standards Series, No. NS-G-3.1, IAEA, Vienna (2002).

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

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

[6.9] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, IAEA Safety Standards Series, No. NS-G-1.2, IAEA, Vienna (2001).

[6.10] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, IAEA Safety Standards Series, No. NS-G-1.6, IAEA, Vienna (2003).

[6.11] INTERNATIONAL ATOMIC ENERGY AGENCY, Code on the Safety of Nuclear Power Plants: Siting, IAEA Safety Series No. 50-C-S (Rev. 1), IAEA, Vienna (1988).

[6.12] INTERNATIONAL ATOMIC ENERGY AGENCY, Design Basis Flood for Nuclear Power Plants on River Sites, IAEA Safety Series No. 50-SG-S10A, IAEA, Vienna (1983).

[6.13] INTERNATIONAL ATOMIC ENERGY AGENCY, Meteorological Events in Site Evaluation for Nuclear Power Plants, Safety Guide, IAEA Safety Standards Series No. NS-G-3.4, IAEA, Vienna (2003)

[6.14] INTERNATIONAL ATOMIC ENERGY AGENCY, Extreme External Events in the Design and Assessment of Nuclear Power Plants, IAEA-TECDOC-1341, IAEA, Vienna (2003).

[6.15] INTERNATIONAL ATOMIC ENERGY AGENCY, Considerations in the Development of Safety Requirements for Innovative Reactors: Application to Modular High Temperature Gas Cooled Reactors, IAEA-TECDOC-1366, IAEA, Vienna (2003).

[6.16] INTERNATIONAL ATOMIC ENERGY AGENCY, Earthquake experience and seismic qualification by indirect methods in nuclear installations, IAEA-TECDOC-1333, IAEA, Vienna (2003).

7. CONCLUSIONS

This section collects the most relevant conclusions from this report, according to the areas of interest identified in the document scope.

7.1. Technical issues

Regarding *safety requirements for siting, return periods, and load* combinations, the conclusions and recommendations are the following:

(7.1.1) Safety requirements for design in relation to external events are considered quite onerous; their review and application to the nuclear power plants (NPPs) with advanced reactors should be carried out with care because of their very significant effect on both plant safety and plant cost;

(7.1.2) In assessing the applicability of existing regulatory requirements to NPPs with innovative and evolutionary reactors, it is important to analyze the operational experience collected in recent years, to recalibrate the requirements and to avoid unnecessary burdens on the design;

(7.1.3) The selection of the return period for a design basis event might be correlated with the plant safety performance and therefore, to the potential consequences. Very reliable design might accept lower return periods for the design basis, provided the performance goal of the overall plant is met. However, this implies a fully probabilistic goal for the plant as a whole, which is not accepted yet by many designers and regulators;

(7.1.4) There is general agreement that some external events may be excluded from consideration in the design by a two stage screening process:

- Performing a preliminary, simple deterministic study, based on the information on the distance and characteristics of the source, could be sufficient to show that no significant interaction with the plant may occur;
- Applying a second screening criterion, based on the probability of occurrence, would increase this confidence;

(7.1.5) There is general agreement that the uncertainty in the data for natural hazards may prevent reasonable prediction of events for frequencies lower than one in 10000 years. Internal initiating events with lower return periods are often included in the design basis, also as “minimum deterministic loads”. The target frequency for the design basis external events could also be chosen with consideration to the frequency of internal events;

(7.1.6) Load factors for external events in design load combinations are sometimes not consistently chosen. Although some design standards have attempted to be reliability based, and even to facilitate the adjustment of parameters to achieve a user requirement of particular target reliability, they have mostly been back calibrated to existing design standards. The factors (e.g. 1.4 to 1.6) applied to dead load for structural design are typically derived from non-nuclear practice, and may appear too high for nuclear application where the dead load is likely to be known with a greater degree of certainty;

(7.1.7) The load factor, together with material factors, used in conservative methods for calculation of load demand and calculations of load capacity, provide reasonable confidence that the design can accommodate other unanticipated scenarios. Therefore, load factors should not be reduced only with reference to the conservatism/ robustness in the design process. The current values of load factors are indirect means of ensuring that serviceability limit states, as well as ultimate limit states, will probably be met;

(7.1.8) The IAEA provides guidance for the combination of earthquake loads with operating condition loads, i.e. loads during normal operation, additional loads during anticipated operational conditions and loads during accident conditions. The safety margins or load factors are not specified, but reference is made to design codes. Such design standards differ between Member States and between different engineering disciplines. Safety margins and uncertainty levels vary between nuclear and non-nuclear design codes, and between standards whose scope includes a specified external hazard and standards where it is not provided;

(7.1.9) In many cases in the past, aircraft crash was screened out on a probabilistic basis, but Member States are increasingly examining the consequences of this scenario, partially in response to the possibility of malevolent human actions. Double containment and certain layouts of new NPPs could offer certain advantages;

(7.1.10) None of the considered designs of NPPs with advanced reactors mentioned an allowance for the effects of climate change, despite of the IAEA guidance on this.

Regarding *approach in design, layout, passive features, defence in depth, combination of internal and external sequences, and emergency planning issues,* the conclusions and recommendations are as follows:

(7.1.11) Considering the expected large diversities in design, applications and regions of deployment (some of which may not meet the current siting criteria) of NPPs with advanced reactors, the design approach for dealing with external events for such NPPs may need some modifications, with respect to the conventional approach for NPPs with older reactors;

(7.1.12) The need for more robust design for high seismic areas was identified as an issue for future work. A common finding from several of the questionnaires was that the design basis earthquake for advanced unified NPPs was higher than for existing plants;

(7.1.13) The development of an external event PSA in parallel with the early plant design may help identifying the vulnerabilities as well as overly conservative design features at an early stage, leading to a well balanced and cost-effective improvement in safety;

(7.1.14) It was observed that the PSA methodologies to deal with external events have not reached the same level of maturity that has been reached for internal event PSA. In particular, in order to deal with several external event scenarios, it is desirable to couple the civil engineering design with PSA, as a design and safety assessment tool, as also suggested in the IAEA requirements for design;

(7.1.15) Accident prevention is the main driving force for advanced NPP designs. Several design innovations are aimed towards bringing down conditional core damage frequencies (CCDF) to an extent that make the plant less vulnerable to extreme external event based and malevolent event based accident scenarios. Typical design approaches that, among others, could contribute to achieve such robustness in design are:

- Capability to limit reactor power through inherent neutronic characteristics in the event of any failure of normal shutdown systems, and/ or provision of a passive shutdown system not requiring any trip signal, power source, or operator action to effect a shutdown of the reactor if the safety critical plant parameters tend to exceed the design limits;
- Availability of a sufficiently large heat sink within the containment to indefinitely (or for a long grace period) remove core heat corresponding to abovementioned event;
- Availability of very reliable passive heat transfer mechanisms for the transfer of core heat to this heat sink;
- Measures to ensure deterministically the immunity of abovementioned functions from external events and malevolent human actions.

(7.1.16) It was observed that innovative design measures need to be supported and encouraged by a rational technical and non-prescriptive basis to define a severe accident (core melt need not be postulated to occur). The rational technical basis could be derived from realistic scenarios applicable to the specific plant design. This implies that it could be necessary to carry out best estimate calculation of source term in order to take full advantage of new reactor designs;

(7.1.17) Most of the innovative reactor designs aim at eliminating the need for relocation or evacuation measures outside the plant site, through the use of enhanced safety features. Many of these designs also aim to take advantage of these advanced safety characteristics to seek exemption from maintaining a large exclusion distance around the nuclear power plants;

(7.1.18) It was observed that, in the context of some severe external events, the assumption of continued availability of the infrastructure required to implement emergency measures (for example, roads and bridges for site access/ evacuation) may not be valid. Under such situation, it is more effective to enhance quality of the other levels of the defence in depth. There is, therefore, a need to define the scope of the off-site emergency planning activities for NPPs with advanced reactors, consistent with the capability of these reactor designs to meet enhanced safety objectives;

(7.1.19) In view of their potential advantages in terms of reliability and independence from other systems and operator actions, passive systems have been proposed in many designs of advanced reactors. Passive systems may play a very significant role to reduce the conditional probabilities of occurrence of severe accident scenarios following the extreme external events, which could jeopardise operator initiated and plant protection system initiated interventions;

(7.1.20) A reliable safety assessment of NPPs with innovative reactors requires well-developed assessment procedures for the reliability of passive systems. The performance of passive systems under extreme external events needs to be fully addressed in the design of advanced reactors. For example, performance of natural circulation based systems (low driving head), fluid devices, passive valves etc. needs to be assessed under strong ground motion conditions, fire, etc.;

(7.1.21) It is noted that design measures for protection of an NPP from the consequences of aircraft crash have been implemented in some designs with very significant modifications to the plant layout, low profile of containment, and additional robustness of protective external structures;

(7.1.22) It is often observed that engineering features that make plants safe for internal events also make the plant safer under external events. However, any new features should be checked for additional or peculiar vulnerabilities under external event scenarios.

In relation to *component qualification, special testing, mock-ups, fragility evaluations, and special requirements,* the conclusions and recommendations are the following:

(7.1.23) Many of the components modelled in the external event PSA of NPPs with innovative reactors are similar to those in existing NPPs. Therefore; the current mature methodology for fragility calculation can be easily adapted for use in innovative reactors. If there should be new component types (e.g. passive components or ceramic core), some additional research will be necessary;

(7.1.24) For failure modes governing structural integrity of the equipment (e.g. loss of pressure boundary, buckling, etc.), seismic fragility can be calculated using analytical formulations. For most functional failure modes, fragility calculation depends on the seismic qualification test information. For new equipment types not used in the current NPPs, specific qualification/ fragility tests are needed;

(7.1.25) There may be a need for component fragility data for external hazards additional to that of an earthquake;

(7.1.26) There may be a need for data on operator response (human reliability models) in the case of an external event, possibly available from training and evaluation of personnel on simulators;

(7.1.27) Walkdown approach could address not just seismic issues, but also other external events, particularly where interactions are foreseen, operational measures are part of the protection, and the effect of propagation from one area to another may be difficult to be evaluated by design;

(7.1.28) Future NPPs have design basis earthquake levels higher than some existing NPPs. Therefore, improved design methodologies and the extension of fragility data/ experience data to higher demands are required;

(7.1.29) There is a generic tendency to address beyond design basis events at the design stage of NPPs with the advanced reactors. In this case, more realistic design and analysis approaches are in use, often borrowed from the assessment methods developed for existing plants (e.g. seismic margin assessment (SMA), etc.);

(7.1.30) In the framework of long operating life, equipment qualification should be maintained throughout the operating life, through maintenance and plant modifications. New methods may be needed to minimize inspection and maintenance cost, with predefined performance goals for the equipment;

(7.1.31) It is anticipated that new component designs, e.g. digital instrumentation and control (I&C) systems and materials (e.g. ceramic), will be used in NPPs with the innovative reactors. There may be a need for large qualification programmes for calculating their seismic fragilities, as the available experience data could be not applicable to them.

Regarding *an approach in safety assessment, the external event PSA,* the conclusions and recommendations are as follows:

(7.1.32) Whereas there are substantial progress and innovations in the reactor designs as reflected in the internal event probabilistic safety assessments (PSAs), there are no similar progresses in the treatment of external event design and relevant external event PSA. This lack of consistency in the overall principle of treatment of internal and external events is seen as a major drawback;

(7.1.33) The approaches available for treatment of external events (for design as well as PSA) are similar to the approaches followed in the nuclear industry over the last 20 years. There is no innovation in the external event PSA that an innovative reactor to be designed to last for 60 years would demand;

(7.1.34) The contribution of external events to plant risk estimates is seen to be higher (in percentage) for evolutionary and innovative reactors since the internal event risks have been substantially reduced through better system design, avoidance of identified accident sequences, etc. It is not clear whether a plant driven by external event risks (compared to internal events) would be acceptable;

(7.1.35) For some reactor designs, refuelling outage may be longer, during which time the containment and the reactor head are open. The impact of any external event during this shutdown and low power mode may be more significant than for the existing reactors. This should be explicitly addressed in the analysis;

(7.1.36) Probabilistic treatment of external events has not been uniformly done for all NPPs with evolutionary and innovative reactors. There are examples of enveloping all the extreme deterministic parameters for different designs and sites derived from current LWRs;

(7.1.37) Large uncertainties in seismic hazard at any potential NPP site are a fact. The situation may not improve in a foreseeable feature. Therefore, siting procedures for innovative reactors should be further developed in order to reduce this large uncertainties and to provide a more realistic design basis;

(7.1.38) The management of the uncertainties in the PSA process could be improved, as current practice is very conservative and recent studies highlighted the need for new methods to keep under control the uncertainties from expert judgement, the random and the epistemic uncertainties;

(7.1.39) The new reactor designs are planned for an operating life of 60 years or more. Our knowledge on ageing effects of concrete is limited. Further research would be needed to confidently forecast a longer operating life, particularly for embedded structures, avoiding expensive inspection and upgrading programmes;

(7.1.40) In order to reduce the external event risks (particularly from seismic events), better modelling assumptions and computational methods are needed. For example, the assumption that all redundant components fail under the same earthquake (i.e. "one fails, all fail" model) would lead to excessively conservative results. This may have worked well in the past seismic PSAs but will not suffice for new designs.

7.2. General conclusions

General conclusions and recommendations are the following:

(7.2.1) External events should be considered at the early stages of the reactor design (e.g. plant layout, containment design, etc.). If external event considerations are added at later stages, they may lead to major modifications or even unacceptable safety levels;

(7.2.2) External events should be considered together with internal events in an integrated approach in design, yielding cost effective solutions that meet quantitative probabilistic safety criteria for the plant, as well as deterministic success criteria for the systems, structures and components important to safety. Rules for combination of events and combination of loads could come out of this approach, which is yet to be developed. However, for preliminary design of the plant, provisions of existing safety standards and national practices, including those relating to the treatment of external events, could be a starting point (IAEA-TECDOCs-1264, 1341);

(7.2.3) Agreement could be developed in the engineering community on whether malevolent scenarios are to be addressed in design;

(7.2.4) There is general consensus that the design basis for advanced NPP design against external hazards could apply risk informed approach combining sound engineering design, and using proven design methods based on defence-in-depth with PSA;

(7.2.5) The consideration of external hazard in design could take into account not only the frequency of initiating events, but also the conditional probability of radiological consequences;

(7.2.6) There is agreement that whilst design code approaches are suitable for design basis external hazards, less conservative methods could be used for beyond design basis assessments. More work is needed on such methods;

(7.2.7) Off-site emergency measures are still seen as part of the defence in depth approach, and are mainly understood in deterministic sense. However, some of the designs of NPPs with innovative reactors aim to eliminate the need for relocation or evacuation measures outside the plant site, through the use of enhanced safety features in design. Many of these designs also aim to take advantage of these advanced safety characteristics to seek exemption from maintaining a large exclusion distance around the nuclear power plants. Under the same subject, also the source term for design basis accidents and severe accidents could be discussed with the intent of moving away from postulated source terms and towards calculated source terms.

7.3. Suggestions for further work

The recommendations for further activities are as follows:

(7.3.1) It is reasonably expected that Member States could review and as appropriate revise safety requirements and guides for their applicability to NPPs with evolutionary and innovative reactors;

(7.3.2) The safety goals are currently often defined in qualitative terms, but there is an increasing interest in seeking the quantitative goals, as a radiological dose to a member of the public versus a frequency of occurrence. This would help communicate the risk to the public and aid the public acceptance of nuclear power;

(7.3.3) Information exchange and coordinated research programmes to facilitate development of PSA methodologies to deal with external events should be encouraged. The scope of these activities could also include treatment of civil engineering structures in the PSA study;

(7.3.4) A guide on external event PSA for operating plants and NPPs with advanced reactors could be developed, and this should, inter alia, address the following:

- Proper treatment of common-cause failures in seismic PSA;
- Uncertainties related to new, relatively unproven materials, structures, components and systems, and lack of previous operating experience;
- Need for better design methodologies and the extension of fragility/ experience data to cover external hazards of higher intensity;
- PSA application to give credit to balance-of-plant systems in dealing with external events where such systems are used to perform safety related functions (note that the definition of balance-of-plant varies among Member States);
- Balanced consideration of uncertainties associated with internal and external events.

(7.3.5) There is a need to develop an integrated probabilistic — deterministic approach taking into account all initiating events of any origin, internal and external;

(7.3.6) An approach to incorporate safety in the original design concept used by the designers of several advanced reactors to eliminate certain severe accidents could be applied to external events also. In doing this, the focus may be on the balance of plant — an NPP component that has not been analyzed as deeply as the nuclear islands;

(7.3.7) An alternative definition of safety classification for structures and components in relation to external events could well support the designers in the analysis of consequences of failures triggered by external events. The relevant guides on system classification could be developed in this direction;

(7.3.8) Experience of Member States in the selection of the return periods of external events in relation to the design reliability could be collected, and the correlation criteria between them could be developed, to be applied to NPPs with innovative reactors;

(7.3.9) More refined recommendations on the principles of combining loads and relevant effects in plant design in relation to the protection from external events could be elaborated;

(7.3.10) Information exchange in the area of reliability of passive systems under external event scenarios should be facilitated;

(7.3.11) New methodologies to determine seismic and fire fragility of passive safety systems and components (e.g. passively activated relief valves, naturally circulated systems, etc.) are needed. The criteria for such data collection, processing and use in the design should be developed;

(7.3.12) Discussion forums on the topic of emergency planning for advanced reactors, particularly taking into account the fact of non-availability of external infrastructure needed for emergency planning measures under severe external events should be convened. Under the same subject, also the calculation of the source terms for design basis accidents and severe accidents could be discussed with the intent of moving away from postulated source terms and towards calculated, more realistic source terms.

APPENDICES

I—III

APPENDIX I

SUMMARY OF RESPONSES TO IAEA QUESTIONNAIRE

TABLE 1. SUMMARY OF RESPONSES FROM MEMBER STATES TO THE IAEA QUESTIONNAIRE ON PLANT PROTECTION FROM THE IMPACTS OF EXTERNAL EVENTS

Reactor name	ABWR-II	ACR-700	APR 1400	BN-800	CAREM	EPR FINLAND	PHWR-540	IRIS	SWR 1000	VBER-300	VK-300	VVER 91/99
1 General plant configuration												
Country of origin	Japan	Canada	The Republic of Korea	Russian Federation	Argentina	AREVA, Europe	India	International consortium led by Westing-house, USA	AREVA, Europe	Russian Federation	Russian Federation	Russian Federation
Reactor type	BWR	PHWR	PWR	FBR	PWR	PWR	PHWR	PWR	BWR	PWR	BWR	PWR
Electric power	1700 MW	700 MW	1450 MW	880 MW	27 MW	1600 MW	540 MW	335 MW	1250 MW	295 MW	250 MW	1060 MW
Containment structure	Pressure suppression containment. Reinforced concrete	Pre-stressed concrete structure steel liner	Pre-stressed concrete structure	Reinforced concrete	Reinforced concrete structure with an embedded steel liner	Inner containment: pre-stressed concrete (liner); outer containment: reinforced concrete	Inner containment of pre-stressed concrete (without metallic liner), outer containment of reinforced concrete	Steel	Reinforced concrete with an interior steel liner	Steel cylindrical shell with multi-layer ceilings and walls forming external protective circuit capable to withstand external impacts	Double containment	Outer shell with reinforced concrete structure; inner containment with pre-stressed reinforced concrete shell with hermetic steel liner
Embedment		10 m	16 m	8 m	5.8 m	9.60 m	20 m	13 m	12.0 m			8 m

(table continued – 2)

REACTOR NAME	ABWR-II	ACR-700	APR 1400	BN-800	CAREM	EPR FINLAND	PHWR-540	IRIS	SWR 1000	VBER-300	VK-300	VVER 91/99
1. General plant configuration												
Structural technology of auxiliary building	Combination of steel frame and reinforced concrete	Multi-storey, reinforced concrete/structural steel structure	Concrete frames and shear walls	Single shear-walls structure with shell dome	Reinforced concrete	The reactor building with a strong outer shell surrounds the containment. Walls and floors of the inner structures are decoupled from the outer shell in order to reduce the loads induced by an aircraft crash. The building is made with watertight reinforced concrete and provided with a ventilation system to maintain the building at a slight negative pressure relative to the atmosphere	Framed RCC structure with shear walls	Reinforced concrete basemat and reactor auxiliary building	The containment is surrounded by the reactor building with a strong outer shell. Walls and floors of the inner structures are decoupled from the outer shell in order to reduce the loads induced by an aircraft crash	Floating vessel. The enclosure consists of multi-layer ceilings; partitioning of stern and blow machine rooms and board side rooms of the floating power unit superstructure is provided		Shear walls
2. Hazard definition												
Unified design, if not indicated otherwise		Envelope of potential sites				Olkiluoto site	Tarapur site					

(table continued – 3)

REACTOR NAME	ABWR-II	ACR-700	APR 1400	BN-800	CAREM	EPR FINLAND	PHWR-540	IRIS	SWR 1000	VBER-300	VK-300	VVER 91/99
3. Events considered												
Aircraft crash (ACC)		Load function	Excluded by administrative measures	10^{-4}/year		Load function, fire, smoke, access impairment, interactions	Excluded by administrative measures	Excluded by administrative measures	Load function, fire, smoke, access impairment, interactions	20 tons, 200 m/s, 10^{-7}/year (helicopter $1.5\cdot10^{-7}$/ year)	20 t	10^{-6}/year, with fire and explosion
Explosion			Excluded by administrative measures	Addressed	10^{-7}/year	Load function	Excluded by administrative measures	Excluded by administrative measures	Load function	50 kPa, moored tank, underwater explosion	30 kPa	On-site
Hazardous gases			Excluded by administrative measures			Addressed	Excluded by administrative measures	Excluded by administrative measures	Addressed	Addressed		
Corrosive gas and liquids			10^{-7}/year			Addressed		Excluded by administrative measures	Addressed	Addressed		
Off-site fire						Addressed	Exclusion zone	Excluded by administrative measures	Addressed	Addressed		
Collision of ships						Addressed		Excluded by adminis trative measures	Addressed	Addressed	20 t	10^{-4}/year
Electromagnetic interference		Source shielding				Addressed		Addressed	Addressed			Addressed
Combination of human induced events						Addressed		Addressed	Addressed			
Earthquake	10^{-5}/year + $5\cdot10^{-4}$/year	0.3 g, 10^{-4}/year. Vertical component is 0.75	0.3 g, 10^{-4}/year	10^{-4}/year	0.4 g	Addressed: interactions, access impairment, fire, flood, smoke	Deterministic; vertical component is 0.4	0.5 g	Addressed: interactions, access impairment, fire, flood, smoke	0.2 g, 10^{-4}/year	8 MSK 64	10^{-4}/year

(table continued – 4)

REACTOR NAME	ABWR-II	ACR-700	APR 1400	BN-800	CAREM	EPR FINLAND	PHWR-540	IRIS	SWR 1000	VBER-300	VK-300	VVER 91/99
3. Events considered												
Extreme meteorological conditions				10^{-4}/year		Addressed		Addressed	Addressed	Addressed	Addressed	10^{-4}/year
Precipitation		120 mm, 10^{-1}/year	10^{-4}/year			Addressed		500 mm/h	Addressed		Addressed	
Snow		3 kPa; 10^{-1}/year	10^{-2}/year			Addressed		75 psf static load	Addressed		Addressed	
Floods			10^{-6}/year			Addressed	10^{-3}/year	Water height 0 m	3.5 m above grade	Addressed	1 m above grade	10^{-4}/year
Landslides												
Straight wind		3.6 kPa, 10^{-2}/year	10^{-2}/year		42 m/s at 20 m	Addressed		145 mph × 1.15	Addressed	Addressed	50 m/s	
Cyclones		530 km/h, air pressure drop of 14 kPa, 10^{-6}/year	10^{-7}/year	10^{-4}/year	F3		10^{-3}/year	300 mph		80 m/s		10^{-4}/year
Tornado missile		1820 kg automobile at 110 km/h	1820 kg automobile at 110 km/h		Addressed			1820 kg automobile at 110 km/h				
Sandstorms								Addressed				
Lightning		Addressed			Addressed	Addressed	Addressed	Addressed	Addressed			
Volcanism												
Terrorism				Addressed				Addressed				
4. Design basis												
AOO		10^{-2}/year										
DBA		10^{-3}/year – 10^{-4}/year			10^{-3}/year - 10^{-4}/year			$6{\cdot}10^{-2}$/year				$4.9{\cdot}10^{-5}$
BDBA		10^{-5}/year – 10^{-6}/year, with limits on large releases only (no dose)										$6.9{\cdot}10^{-7}$

(table continued – 5)

REACTOR NAME	ABWR-II	ACR-700	APR 1400	BN-800	CAREM	EPR FINLAND	PHWR-540	IRIS	SWR 1000	VBER-300	VK-300	VVER 91/99
5. Combination criteria												
External with external	No											
Internal with normal external	Yes	Yes		Yes						Yes		
Internal with extreme external	Yes, with different acceptance criteria according to the component classification	Only if causal		E + DBA	E + DBA	Only if causal	E + DBA, fire barriers are qualified to SL-2	Only if causal	Only if causal	DBA + E		E + DBA
6. Differences with the siting criteria of existing plants												
	No difference	Earthquake is 0.3 g	Earthquake is 0.3 g. HCLPF 0.5 g	Median + sigma spectra. ACC is probabilistic (10^{-4}/year)				Eliminated off-site emergency planning				Median + sigma spectra. ACC is probabilistic (10^{-4}/year).
7. Design features in relation to external events												
	Passive heat removal systems (reactor cooling system / containment cooling system); separation; RCIC with generator; diversified EPS	Qualifica-tion; separation	Qualification; separation		The contain-ment is included in the reactor building, which acts as a second contain-ment also protecting the plant from external events	Passive systems, separation; qualification; bunkerized emergency control room (ECR). Special construction to prevent vibration transfer to I&C.	Qualification; separation; flooding protection; dry site for EPS	Compact design; passive systems	Passive systems; separation; qualification; bunkerized ECR. Special construction to prevent vibration transfer to I&C.	Separation; passive features; fire compart-ments; flood compart-ments; impact energy absorbers		Damping devices are installed on primary loop for reduction of seismic vibrations; layout separation and redundancy of safety channels and systems; the goal is to achieve safe shutdown of the plant in ACC case

(table continued – 6)

REACTOR NAME	ABWR-II	ACR-700	APR 1400	BN-800	CAREM	EPR FINLAND	PHWR-540	IRIS	SWR 1000	VBER-300	VK-300	VVER 91/99
						8. Design features different from existing plants						
	Broad use of SMA techniques for BDBA scenarios	High elevated reserve tank. Separation of emergency trains of power supplies.	Physical and electrical quadrant separation of safety related equipment and cables	PGA level for the design is higher compared with current operating plants; layout separation and redundancy of safety channels and systems; passive safety systems designed to reduce the accident consequences	CAREM relies on the use of passive safety systems and, once they are operated, they have autonomy of 48 hours to control and mitigate accidents. During this period no operator action or external element are needed.	ACC design	Protecting walls on the seaside; common foundation raft for all safety related structures – simplifies structural design, specifically, for seismic loads	Safety-by-design^{TM} approach to prevent accidents from occurring rather than deal with their consequences. All safety systems are passive.	Passive safety systems located inside the containment; accommodation of the safety related I&C and switch gears within special compartments in the fully protected reactor building	Floating capability (towing, mooring); resistance to helicopter impact; resistance to seismic impact transferred through water wave	All safety systems are passive; two containments, primary and secondary, are used	Passive systems; separation; double wall containment

(table continued – 7)

REACTOR NAME	ABWR-II	ACR-700	APR 1400	BN-800	CAREM	EPR FINLAND	PHWR-540	IRIS	SWR 1000	VBER-300	VK-300	VVER 91/99
9. Approaches and measures to manage severe situations related to the external events												
Monitoring systems	Range of monitoring systems expanded to cover extreme external events	Two separate control centres are provided to monitor plant conditions during and following design basis events.	Monitoring systems for coolant flow, heat removal, reactivity control, containment integrity, vibration, water level	Critical parameters obtained from reactor monitoring, control and diagnostic system and anti seismic protection system, as well as loss of electric supply of safety channels cause the operation of the emergency reactor shutdown and activating systems of safety facilities	A tornado warning will be emitted by the corresponding meteorological station		Micro-earthquake stations around site. Monitoring and warning system of Indian Meteorological Department. Meteorological data (including wind speed) recording in Environmental Survey Laboratory. Sump level high alarms (flood warning)		A seismic monitoring system and a monitoring system for burnable and explosive gases are installed			Critical parameters obtained from reactor monitoring, control and diagnostic system and anti seismic protection system, as well as loss of electric supply of safety channels cause the operation of the emergency reactor shutdown and activating systems of safety facilities

(table continued – 8)

REACTOR NAME	ABWR-II	ACR-700	APR 1400	BN-800	CAREM	EPR FINLAND	PHWR-540	IRIS	SWR 1000	VBER-300	VK-300	VVER 91/99
9. Approaches and measures to manage severe situations related to the external events												
Operator actions	Longer grace period	Operator actions are performed from the main control room and, in the unlikely event that the main control room becomes unavailable, from the secondary control area. The reference ACR is designed so that all the safety actions to be taken in the short term after an initiating event are automatic.	The operator actions include: fire suppression, draining pump operation, manual depressurization, manual reactor trip, manual ECCS injection, abnormal operation procedure, emergency operation procedure	Shutdown system and safety facilities activating systems work automatically, no operator actions are required	In case of hazardous gases or tornado warning, the containment injection and extraction system is closed and ventilation is switched to recirculation mode		Shutdown for SL-1		No operator actions are required immediately after onset of an external event, because the passive safety systems manage all required safety functions.			Shutdown system and safety facilities activating systems work automatically, no operator actions arerequired

(table continued – 9)

REACTOR NAME	ABWR-II	ACR-700	APR 1400	BN-800	CAREM	EPR FINLAND	PHWR-540	IRIS	SWR 1000	VBER-300	VK-300	VVER 91/99
9. Approaches and measures to manage severe situations related to the external events												
Operator actions	Longer grace period	Operator actions are performed from the main control room and, in the unlikely event that the main control room becomes unavailable, from the secondary control area. The reference ACR is designed so that all the safety actions to be taken in the short term after an initiating event are automatic.	The operator actions include: fire suppression, draining pump operation, manual depressurization, manual reactor trip, manual ECCS injection, abnormal operation procedure, emergency operation procedure	Shutdown system and safety facilities activating systems work automatically, no operator actions are required	In case of hazardous gases or tornado warning, the containment injection and extraction system is closed and ventilation is switched to recirculation mode		Shutdown for SL-1		No operator actions are required immediately after onset of an external event, because the passive safety systems manage all required safety functions.			Shutdown system and safety facilities activating systems work automatically, no operator actions are required

(table continued – 10)

REACTOR NAME	ABWR-II	ACR-700	APR 1400	BN-800	CAREM	EPR FINLAND	PHWR-540	IRIS	SWR 1000	VBER-300	VK-300	VVER 91/99
9. Approaches and measures to manage severe situations related to the external events												
Access of emergency teams	Combination of conventional resource (emergency power and its fuel) and passive system backup provides longer ample time for the access from off-site.	Site-specific measures for access to site by emergency teams are not part of the reference ACR design. They will be factored in the overall design of the plant for a site-specific project.	Technical Support Center is located next to MCR in same building; separation of non radiation area from radiation area; avoidance of crossing between workers' path and general path	Special automatic system unlocks gates for access of emergency teams in case of fire, other accident or loss of electric supply			Access roads are provided from different directions to access the site in case of emergency. For coastal sites, sea route is also available.					Special automatic system unlocks gates for access of emergency teams in case of fire, other accident or loss of electric supply

APPENDIX II

DESIGN FEATURES TO ADDRESS EXTERNAL EVENTS DATASHEETS FOR 14 ADVANCED REACTOR CONCEPTS

1. APR1400 (KEPRI, the Republic of Korea)

1. LIST OF POSTULATED EXTERNAL EVENTS:

- Release of hazardous gas (asphyxiant, toxic) from off-site and on-site storage,
- Earthquake,
- Extreme meteorological conditions (snow),
- Floods (from tsunamis, storm surges, precipitations),
- Cyclones (typhoon, tornado),
- Internal fire,
- Internal flooding.

2. PROTECTION BY STRUCTURAL DESIGN OF BUILDINGS, CONTAINING STRUCTURES, SYSTEMS AND COMPONENTS IMPORTANT TO SAFETY, AGAINST POSTULATED EXTREME EXTERNAL EVENTS:

- Wrap-around type auxiliary building (protects containment from direct impact loads).
- Common basement of auxiliary building with containment building (provides enhanced seismic safety).
- Fuel building and diesel generator building embedded in auxiliary building.
- Concrete and steel plate barrier designed to protect the structure containing safety-related components and systems against the missiles resulting from typhoon or tornado.
- Safety-related structures, components, and systems designed for the Safe Shutdown Earthquake (SSE).
- Top elevation of the grade floor of the safety-related structure determined above the ground elevation by the submergence depth corresponding to design basis flood.
- Fire protection measures comprising physical separation, barriers, and use of fire resistant materials.

3. PATIAL SEPARATION OF REDUNDANT SAFETY RELATED SYSTEMS TO SECURE PROTECTION AGAINST LOCALIZED ADVERSE EFFECTS, INCLUDING THOSE RESULTING FROM EXTERNAL EVENTS.

- Physical and electrical quadrant separation of safety related equipment and cables,
- Four separated safety trains located in auxiliary building,
- Independent emergency sump in each quadrant.

4. DESIGN FEATURES, IMPLEMENTED WITHIN PROTECTED BUILDINGS, TO MAINTAIN FUEL TEMPERATURE WITHIN ACCEPTANCE LIMITS UNDER POSTULATED EXTREME EXTERNAL EVENTS WHEN ALL SOURCES OF POWER, COOLING WATER SUPPLY, AND COMPRESSED AIR EXTERNAL TO THE PROTECTED BUILDING ARE ASSUMED TO BE LOST, AND NO CREDIT IS GIVEN TO OPERATOR ACTIONS WITHIN A STIPULATED GRACE PERIOD.

4.1. Active safety systems requiring emergency power supply:

- Four train safety injection system;
- Direct vessel injection.

4.2. Passive systems for reactor shutdown and heat removal within protected buildings that remain available to provide safety functions.

4.2.1. Passive systems requiring emergency power supply based instrumentation and electrical signals to get actuated:

- Reactor coolant flooding system - it requires electrical power to open the valves to flood the reactor cavity from in-containment refuelling water storage tank (IRWST), and then water fills the cavity by gravitational force.

4.2.2. Passive systems not requiring any electrical signals to get actuated:

- Safety injection tank - it injects emergency core cooing water to the reactor vessel by pressure difference.
- Fluidic device in safety injection tank - it regulates the flow rate of injection water by vortex.

4.2.3. Heat sinks that remain available with loss of external coolant supply:

- In-containment Refuelling Water Storage Tank (IRWST).

4.2.4. Inherent safety features:

- Negative reactivity coefficient for all power levels within the whole operating period.

5. FEATURES FOR PREVENTION AND MITIGATION OF CONSEQUENCES OF HYPOTHETICAL SEVERE ACCIDENTS:

- External reactor vessel cooling system for filling reactor cavity,
- Cavity flooding system,
- Safety depressurization system,
- Diverse protection system.

6. FEATURES FOR PREVENTING UNACCEPTABLE RELEASE OF RADIOACTIVITY FOLLOWING POSTULATED BEYOND DESIGN BASIS ACCIDENTS.

- Emergency containment spray back-up system.
- Passive autocatalytic recombiner and igniters.

7. OTHER IMPORTANT SAFETY FEATURES, INCLUDING OTHER SPECIAL FEATURES PROVIDED TO DEAL WITH EXTERNAL EVENTS.

7.1. Features to enhance defence in depth in general:

- Redundancy in plant shutdown systems.
- Redundancy in emergency power supply — there are two emergency diesel generators and one auxiliary AC power supply**.**

7.2. Features addressing external events in particular:

- Elevated doors and installation pads for flooding protection.
- Minimization of fire sources.

8. EMERGENCY PLANNING ISSUES

Nothing specifically indicated here.

2. EPR FINLAND (AREVA, Europe)

1. LIST OF POSTULATED EXTERNAL EVENTS:

- Safe shutdown earthquake (SSE);
- Airplane crash (small sporting aircraft, large commercial aircraft, military aircraft);
- Explosion pressure wave;
- External air temperatures and humidity conditions;
- Wind and wind-generated missiles;
- Cooling water temperatures;
- Precipitation and external flooding;
- Lightning;
- Electromagnetic interference from off-site and on-site;
- Hazards with potential influence on cooling water intakes, air intakes, e.g. ice, frazil ice, debris, seaweed, marine life, algae, oil slicks.

2. PROTECTION BY STRUCTURAL DESIGN OF BUILDINGS, CONTAINING STRUCTURES, SYSTEMS AND COMPONENTS IMPORTANT TO SAFETY, AGAINST POSTULATED EXTREME EXTERNAL EVENTS:

- The containment surrounded by a reactor building with a strong outer shell.
- Walls and floors of the inner structures decoupled from the outer shell of the containment in order to reduce the loads induced by an aircraft crash.
- The reactor building including the containment, the fuel building, the safeguard buildings 2 and 3 are protected by design against large commercial aircraft crash; they are located on a common base slab for enhanced seismic safety and airplane crash stability (large passenger aircraft).
- The fuel building belongs to the fully protected structures and the diesel generator buildings are designed against safe shutdown earthquake loads and wreckage loads.
- Detection of poisonous gases and prevention of their penetration into compartments in which the personnel stays is possible.

3. SPATIAL SEPARATION OF REDUNDANT SAFETY RELATED SYSTEMS TO SECURE PROTECTION AGAINST LOCALIZED ADVERSE EFFECTS, INCLUDING THOSE RESULTING FROM EXTERNAL EVENTS:

- The safeguard buildings 1 and 4, the main steam and feedwater valve compartments, the diesel generator buildings and the service water pump buildings are protected against large commercial aircraft crash by geographical separation. Protection against wreckage is provided.

4. DESIGN FEATURES, IMPLEMENTED WITHIN PROTECTED BUILDINGS, TO MAINTAIN FUEL TEMPERATURE WITHIN ACCEPTANCE LIMITS UNDER POSTULATED EXTREME EXTERNAL EVENTS WHEN ALL SOURCES OF POWER, COOLING WATER SUPPLY, AND COMPRESSED AIR EXTERNAL TO THE PROTECTED BUILDING ARE ASSUMED TO BE LOST, AND NO CREDIT IS GIVEN TO OPERATOR ACTIONS WITHIN A STIPULATED GRACE PERIOD.

4.1. Active safety systems requiring emergency power supply:

- Extra borating system (2 trains).
- Emergency feedwater system (4 trains).

- Medium head safety injection system (4 trains).
- Low head safety injection and residual heat removal system (4 trains).
- Containment heat removal and spray system (2 trains).

These systems are connected to the emergency power supply (4 diesel generator sets). In addition, two of the four emergency feedwater systems and two containment heat removal systems are provided with power supply from the Station Blackout (SBO) diesels.

4.2. Passive systems for reactor shutdown and heat removal within protected buildings that remain available to provide safety functions.

4.2.1. Passive systems requiring emergency power supply based instrumentation and electrical signals to get actuated:

- Reactor trip system (fail-safe);
- Safety relief valves (primary side), 2 of 3 main valves are equipped with solenoid pilot and motor operated pilot valves.

4.2.2. Passive systems not requiring any electrical signals to get actuated:

- Safety relief valves (primary side) with spring loaded pilot valves;
- Accumulators for safety injection (4 trains);
- Two safety valves (spring loaded) for each steam generator.

4.3. Heat sinks that remain available with loss of external coolant supply:

- Increased grace periods achieved by enlarged water inventories of primary components;
- Large In-Containment Refuelling Water Storage Tank (IRWST).

4.4. Inherent safety features:

- Negative Doppler coefficient;
- Negative temperature reactivity coefficient during power operation.

5. FEATURES FOR PREVENTION AND MITIGATION OF CONSEQUENCES OF HYPOTHETICAL SEVERE ACCIDENTS:

- Avoidance of high pressure core melt sequences by dedicated depressurization devices;
- Hydrogen mitigation after core melt by recombiner;
- Core melt stabilization through use of fully passive measures in all stages (retention, spreading, flooding, cooling).

6. FEATURES FOR PREVENTING UNACCEPTABLE RELEASE OF RADIOACTIVITY FOLLOWING POSTULATED BEYOND DESIGN BASIS ACCIDENTS:

- Containment heat removal;
- Containment integrity, limitation of radioactive releases by containment isolation and filtering of potential leakages.

7. OTHER IMPORTANT SAFETY FEATURES, INCLUDING OTHER SPECIAL FEATURES PROVIDED TO DEAL WITH EXTERNAL EVENTS.

7.1. Features to enhance defence in depth in general:

- Combination of multiple redundancy (in general n + 2 design of safety systems) and diversity of safety systems (systems to cope with anticipated operational occurrences are diversified)
- Avoidance of sump clogging

7.2. Features addressing external events in particular:

Nothing specifically indicated here (already covered under items 2 and 3)

8. EMERGENCY PLANNING ISSUES:

- Offsite emergency response actions, such as evacuation, relocation and food control, to be restricted to the immediate vicinity of the plant.

3. FLOATING NPP WITH VBER-300 (OKBM, the Russian Federation)

1. LIST OF POSTULATED EXTERNAL EVENTS:

List of external events considered by design[1]:

- Breakdown of attachment or rigid mooring bars due to ice lock with further grounding under strong wind and heavy sea;
- Earthquake;
- Explosion of external source on the shore;
- Explosion at a moored tanker;
- Minor shock against mooring ship (service ship);
- Ship-to-shore communication pipeline rupture;
- Helicopter falling during landing onto a floating power unit;
- High-pressure cylinder explosion;
- Fire in floating power unit compartments;
- Floating power unit collision with another ship;
- Grounding.

Beyond design-basis accidents:

- Floating power unit collision with other ships moving at a high speed;
- Water flooding of a floating power unit;
- Floating power unit grounding, including rocky ground;
- Falling of a flying vehicle onto floating power unit from a big height.

[1] Natural phenomena that could occur during a haul (heavy sea, wind, ice) are taken into account at the design stage of a floating power unit to ensure the compliance with relevant codes and standards of the Russian Maritime Register of Shipping, and are not considered as initiating events for design basis accidents.

2. Protection by structural design of buildings, containing structures, systems and components important to safety, against postulated extreme external events.

Protection from postulated external events is provided by the design of a floating power unit and its compartments containing safety-related structures, systems and components:

- Steel leak-tight safeguard shell is designed to withstand 1.0 MPa pressure;
- Protective enclosure consisting of multi-layer floors and walls of a floating NPP makes up the external protective circuit of reactor compartment, which is capable of taking up external physical loads;
- Structural shielding is provided in the area of the reactor compartment of a floating NPP to absorb energy that is released after collision with another ship or, in case of a grounding, to prevent damage of the protective enclosure.

3. Spatial separation of redundant safety related systems to secure protection against localized adverse effects, including those resulting from external events:

- Compact arrangement of all nuclear radiation components within a floating NPP; location of other NPP components at large distances from the floating NPP;
- Division of a floating NPP into fire-resistant areas, separate fire-resistant circuits and water tight rooms;
- Redundancy of safety system channels with their spatial separation, so that a surviving system channel could perform the required safety function under design basis external impacts.

4. Design features, implemented within protected buildings, to maintain fuel temperature within acceptance limits under postulated extreme external events when all sources of power, cooling water supply, and compressed air external to the protected building are assumed to be lost, and no credit is given to operator actions within a stipulated grace period.

4.1. Active safety systems requiring emergency power supply

The VBER-300 has active safety systems that require permanent power supply to fulfil their functions. These active safety systems are:

- Emergency protection system (control rod insertion according to emergency protection signals);
- Liquid absorber supply system (boric acid solution supply to the reactor by pumps; remote actuation of the system by operator);
- Systems of emergency cooling through heat exchangers (HXs) of the coolant purification system (the fluid circulation in circuits is provided by pumps; the systems are actuated by the reactor protection system according to emergency protection signals);
- Emergency cooling systems using secondary circuit equipment (the fluid circulation in circuits is provided by pumps; the systems are actuated by the reactor protection system according to emergency protection signals);
- System of water supply to the reactor by pumps, including recirculation subsystem;
- System of isolation valves at primary and secondary circuit pipelines and at the equipment cooling circuit.

Implementing the following solutions ensures the reliability of safety systems under external impacts:

- Redundancy and diversity of the reactor shutdown, core cooling and residual heat removal;
- Separation of safety system channels to prevent common cause failures; use of elements meeting a safe failure principle;

- Redundancy and diversity of control systems;
- Use of a two-channel structure of safety systems with redundancy of elements inside the channels.

The protection systems ensure automatic control as well as remote control of safety system equipment from two independent control panels: main control room and standby control panel.

4.2. Passive systems for reactor shutdown and heat removal within protected buildings that remain available to provide safety functions.

4.2.1. Passive Systems requiring emergency power supply based instrumentation and electrical signals to get actuated.

The VBER-300 has passive safety systems, which do not require power supply for operation (i.e. do not require signals from electric protection systems to get actuated):

- Emergency protection system (control rod insertion by gravity force when the drives are de-energized by emergency protection signals or loss of power sources);
- Passive emergency cooling system (natural circulation of fluids in all heat transfer circuits, evaporation of water stock in tanks);
- System of emergency water supply to reactor from hydraulic accumulators and hydraulic tanks (use of the energy of compressed gas and hydrostatic head);
- System of passive heat removal from safeguard shell that allows restricting pressure inside the safeguard shell in loss-of-coolant accidents;
- Normally closed air-operated isolation valves;
- Leak-tight steel safeguard shell.

The reliability of passive safety systems under external impacts is ensured by implementing the following design solutions:

- Use of safety systems based on natural processes (coolant natural circulation; expansion of compressed air; movement caused by gravity force);
- Separation of safety system channels to prevent common cause failures; use of elements meeting a safe failure principle (the actuation under a loss of fluids is provided by compressed air, power supply);
- Redundancy and diversity of control systems.

4.2.2. Passive systems not requiring any electrical signals to get actuated:

- The VBER-300 design provides for actuation of the emergency protection system (de-energization of control drive mechanism (CRDM) motors) by using a special self-actuated device (pressure-actuated power breaker), which allows bringing the reactor to a subcritical state without the electric control systems and instrumentation.
- It is also provided to actuate passive emergency heat removal system using the hydro-controlled pneumatic valves, which allow discharging air from the air-operated drives of the normally open valves, connecting the emergency heat removal system.

4.3. Heat sinks that remain available with loss of external coolant supply.

Nothing specifically indicated here (already covered under 4.2.1).

4.4. Inherent safety features:

- Negative reactivity coefficients on fuel and coolant temperature, on specific volume of coolant, as well as negative steam and integral power reactivity coefficients;

- Decreased power density of the reactor core (below 72 kW/l) as compared to ship-based reactors and WWER-1000 type reactors;
- Stable natural circulation in all heat transfer circuits, ensuring reliable heat removal from the shutdown reactor;
- Connection of most primary pipelines to “hot” sections of the circuit with arranging the nozzles on reactor vessel above the core, which allows switching over to steam discharge and increases time margin for accident control actions of the personnel;
- Use of a reactor unit with short load-carrying nozzles between main pieces of the equipment; avoiding long large-diameter primary pipelines;
- Use of the low-diameter orifices in nozzles of the primary circuit auxiliary systems.

The stability of ship-based nuclear installations under external impacts is confirmed by the experience of actual accidents.

5. FEATURES FOR PREVENTION AND MITIGATION OF CONSEQUENCES OF HYPOTHETICAL SEVERE ACCIDENTS.

Nothing specifically indicated here (already covered under 4 and 6).

6. FEATURES FOR PREVENTING UNACCEPTABLE RELEASE OF RADIOACTIVITY FOLLOWING POSTULATED BEYOND DESIGN BASIS ACCIDENTS.

The design solutions to prevent reactivity release after postulated beyond design basis accidents followed by reactor core damage are:

- Use of reactor vessel bottom cooling system to confine the melt inside the vessel;
- The system of iodine and aerosol purification of inter-shell space air (space between the safeguard shell and the protective enclosure) from radioactive leakages from the safeguard shell under accidents related to inner pressure increase.

7. OTHER IMPORTANT SAFETY FEATURES, INCLUDING OTHER SPECIAL FEATURES PROVIDED TO DEAL WITH EXTERNAL EVENTS.

7.1. Features to enhance defence in depth in general

The floating NPP safety, including accidents caused by external events, is ensured by consistent implementation of the defence in-depth principle. This principle includes the strategy of accident prevention and consequence limitation and assumes using physical barriers on the way of ionizing radiation and radioactive substance propagation into the environment. It also provides for a system of engineering and organizational measures to protect the barriers and maintain their efficiency, as well as to protect the personnel, population and environment. The top-priority trend in floating NPP construction is accident prevention taking into account the experience in construction and operation of ship-based as well as land-based NPPs. In parallel with this, certain measures to enhance safety system reliability and to introduce technologies to control beyond design basis accidents, including the severe ones, are being implemented.

The system of physical barriers within the reactor compartment boundaries includes:

- Fuel matrix;
- Fuel element cladding;
- Leak-tight primary circuit;
- Biological shielding.

Within the floating power unit, the system of physical barriers is complemented by a safeguard shell and protective enclosure.

The reliability of radioactive product confinement within the leak-tight enclosure is ensured by:

- The separation of functions of taking up the external both natural and human-induced loads and the internal emergency loads between outer and inner safeguard shells respectively;
- Passive systems that reduce accident parameters of the fluid inside the safeguard shell during primary or secondary circuit depressurization.

7.2. Features addressing external events in particular.

- A floating NPP can be towed to a safe location in the cases of volcanism, landslides and avalanches, etc.
- A number of geological processes and phenomena hazardous for land-based NPPs, like caves, slope washout and retrogression of rivers, groundwater washouts, dips, water flooding, are not hazardous for a floating NPP.

8. EMERGENCY PLANNING ISSUES:

- The dose rate for residents in a beyond design basis accident with a severe core damage does not exceed 5 mSv;
- The emergency response area is 1 km

4. VVER-91/92 (Sankt-Peterburg Atomenergoproekt, the Russian Federation)

1. LIST OF POSTULATED EXTERNAL EVENTS:

- Aircraft crashes;
- Collision of ships and floating debris;
- Earthquakes,
- Extreme meteorological conditions,
- Floods,
- Cyclones,l
- Explosions,
- Electromagnetic interference from off-site.

2. PROTECTION BY STRUCTURAL DESIGN OF BUILDINGS, CONTAINING STRUCTURES, SYSTEMS AND COMPONENTS IMPORTANT TO SAFETY, AGAINST POSTULATED EXTREME EXTERNAL EVENTS.

- Double wall containment with the outer shell made of reinforced concrete structure capable of withstanding external hazards, and inner containment that is a pre-stressed reinforced concrete shell with the hermetic steel liner designed for loss of coolant accidents (LOCAs).
- Structural and component design taking into account all postulated external events. Buildings and structures which refer to Category I are designed taking into consideration the impacts of external events of human-induced and natural origin, having a recurrence period of once in 10 000 years. All extreme external loads are taken into account.

3. SPATIAL SEPARATION OF REDUNDANT SAFETY RELATED SYSTEMS TO SECURE PROTECTION AGAINST LOCALIZED ADVERSE EFFECTS, INCLUDING THOSE RESULTING FROM EXTERNAL EVENTS.

- Layout separation and redundancy of safety channels and systems are implemented with the goal of achieving a safe shutdown of the plant in case of an aircraft crash.

4. DESIGN FEATURES, IMPLEMENTED WITHIN PROTECTED BUILDINGS, TO MAINTAIN FUEL TEMPERATURE WITHIN ACCEPTANCE LIMITS UNDER POSTULATED EXTREME EXTERNAL EVENTS WHEN ALL SOURCES OF POWER, COOLING WATER SUPPLY, AND COMPRESSED AIR EXTERNAL TO THE PROTECTED BUILDING ARE ASSUMED TO BE LOST, AND NO CREDIT IS GIVEN TO OPERATOR ACTIONS WITHIN A STIPULATED GRACE PERIOD.

4.1. Active safety systems requiring emergency power supply:

- Shutdown system;
- Containment spray system,
- Emergency boron injection system,
- High and low pressure safety injection systems.

4.2. Passive systems for reactor shutdown and heat removal within protected buildings that remain available to provide safety functions.

4.2.1. Passive systems requiring emergency power supply based instrumentation and electrical signals to get actuated:

- Emergency core cooling system;
- Full pressure containment system;
- Residual heat removal system.

4.2.2. Passive systems not requiring any electrical signals to get actuated.

Nothing specifically indicated here.

4.3. Heat sinks that remain available with loss of external coolant supply.

Nothing specifically indicated here.

4.4. Inherent safety features.

Nothing specifically indicated here.

5. FEATURES FOR PREVENTION AND MITIGATION OF CONSEQUENCES OF HYPOTHETICAL SEVERE ACCIDENTS:

- Core catcher.

6. FEATURES FOR PREVENTING UNACCEPTABLE RELEASE OF RADIOACTIVITY FOLLOWING POSTULATED BEYOND DESIGN BASIS ACCIDENTS:

- Containment hydrogen removal system.

7. OTHER IMPORTANT SAFETY FEATURES, INCLUDING OTHER SPECIAL FEATURES PROVIDED TO DEAL WITH EXTERNAL EVENTS.

7.1. Features to enhance defence in depth in general:

- Critical parameters obtained from the reactor monitoring, control and diagnostic system, the anti-seismic protection system, as well as a loss of electric supply of safety channels cause the operation of the emergency reactor shutdown and of the activating systems of safety facilities.

7.2. Features addressing external events in particular:

- An anti-seismic protection system (active system) directly indicates the limit peak accelerations induced by external events and causes the operation of the emergency reactor shutdown and of the activating systems of safety facilities;
- Damping devices are installed on the primary loop for the reduction of seismic vibrations.

8. EMERGENCY PLANNING ISSUES:

- Special automatic system unlocks the gates for the access of emergency teams in case of a fire, loss of electric supply, and in other accidents.

5. CAREM-25 (CNEA, Argentina)

1. LIST OF POSTULATED EXTERNAL EVENTS.

Included in the list is every initiating event exceeding a frequency of occurrence of 10^{-7}, namely:

- Explosions (deflagrations and detonations) with or without fire, originated from off-site sources and on-site (but external to safety related buildings);
- Earthquakes;
- Tornadoes
- Lightning.

Others external events, like floods, will be evaluated for a defined specific site.

2. PROTECTION BY STRUCTURAL DESIGN OF BUILDINGS, CONTAINING STRUCTURES, SYSTEMS AND COMPONENTS IMPORTANT TO SAFETY, AGAINST POSTULATED EXTREME EXTERNAL EVENTS:

- The containment is included in the reactor building, which acts as a second confinement and also provides the protection from external event impacts; the nuclear module being compact and small, this considerably reduces the probability of an external missile impact on the containment.

3. SPATIAL SEPARATION OF REDUNDANT SAFETY RELATED SYSTEMS TO SECURE PROTECTION AGAINST LOCALIZED ADVERSE EFFECTS, INCLUDING THOSE RESULTING FROM EXTERNAL EVENTS.

Nothing specifically indicated here.

4. DESIGN FEATURES, IMPLEMENTED WITHIN PROTECTED BUILDINGS, TO MAINTAIN FUEL TEMPERATURE WITHIN ACCEPTANCE LIMITS UNDER POSTULATED EXTREME EXTERNAL EVENTS WHEN ALL SOURCES OF POWER, COOLING WATER SUPPLY, AND COMPRESSED AIR EXTERNAL TO THE PROTECTED BUILDING ARE ASSUMED TO BE LOST, AND NO CREDIT IS GIVEN TO OPERATOR ACTIONS WITHIN A STIPULATED GRACE PERIOD.

4.1. Active safety systems requiring emergency power supply.

Nothing specifically indicated here.

4.2. Passive systems for reactor shutdown and heat removal within protected buildings that remain available to provide safety functions.

4.2.1. Passive systems requiring emergency power supply based instrumentation and electrical signals to get actuated.

- The First Shutdown System (FSS) is designed to shut down the core when an abnormality or a deviation from normal operation occurs, and to maintain the core subcritical during all shutdown states. This function is achieved by dropping a total of 25 neutron-absorbing elements into the core, using the force of gravity.
- The second shutdown system is a gravity-driven device for the injection of borated water at high pressure. It is actuated automatically when the reactor protection system detects the failure of the FSS or in case of LOCA. The 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 from the steam dome to the upper part of the tank, and the other 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 by gravity. The discharge of a single tank produces the complete shutdown of the reactor.
- The Residual Heat Removal System (RHRS) has been designed to reduce the pressure on the primary system and to remove the decay heat in case of Loss of Heat Sink (LOHS). It 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 between 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 in the steam line are always open, while the outlet valves are normally closed therefore, the tube bundles are filled with condensate. When the system is triggered, the outlet valves open automatically. The 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 process, heat is transferred to the water of the pool by a boiling process. This evaporated water is then condensed in the suppression pool of the containment.
- The emergency injection system prevents core exposure in case of a LOCA. The system consists of two redundant accumulators with borated water, connected to the reactor pressure vessel (RPV). The tanks are pressurized; thus, when during a LOCA the pressure in the reactor vessel reaches a relatively low value, rupture disks break and the flooding of the RPV starts, preventing the core uncovery for a long period. The RHRS is also triggered to help to depressurize the primary system, in case the breakage area is small.

Even these systems require an assured-power-supply based instrumentation and electrical signals to get actuated; in case of a loss of assured power supply they are actuated in order to fulfill the safe failure mode criteria.

4.2.2. Passive systems not requiring any electrical signals to get actuated:

- Natural circulation heat removal under normal operating conditions.

4.3. Heat sinks that remain available with loss of external coolant supply:

- CAREM-25 relies on the use of passive safety systems and, once they are operated, they have the autonomy of 48 hours to control and mitigate accidents. During this period, no operator action or external element is needed. From this point of view, many situations like blackout and LOHS that could be induced by external events are easily and reliably handled by the NPP.

- The RHRS removes the heat to two pools filled with cold water inside the containment building. Each pool has a 100% capability for removing the residual heat for at least 48 hours.
- The pressure suppression pool of the containment condenses evaporated water from the RHRS pools or from small LOCAs with the autonomy of at least 48 hours.

4.4. Inherent safety features.

Nothing specifically indicated here.

5. FEATURES FOR PREVENTION AND MITIGATION OF CONSEQUENCES OF HYPOTHETICAL SEVERE ACCIDENTS.

Nothing specifically indicated here.

6. FEATURES FOR PREVENTING UNACCEPTABLE RELEASE OF RADIOACTIVITY FOLLOWING POSTULATED BEYOND DESIGN BASIS ACCIDENTS.

Nothing specifically indicated here.

7. OTHER IMPORTANT SAFETY FEATURES, INCLUDING OTHER SPECIAL FEATURES PROVIDED TO DEAL WITH EXTERNAL EVENTS.

7.1. Features to enhance defence in depth in general:

- The hydraulic Control Rods Drives (CRD) avoid the use of mechanical shafts passing through the RPV, or the extension of the primary pressure boundary, and thus eliminate the possibility of a large LOCA, since the whole device is located inside the RPV.
- Due to the absence of large diameter piping associated with the primary system, no large LOCA has to be handled by the safety systems. The elimination of large LOCAs considerably reduces the need in emergency core cooling system components, AC supply systems, etc.
- Elimination of the primary pumps in CAREM-25 results in the elimination of Loss of Flow Accidents (LOFAs), in lower costs and the advantages in maintenance and availability.
- Large coolant inventory in the primary circuit results in the large thermal inertia and long response time in case of transients or accidents.
- The primary coolant is on the outside of the steam generator tubes and, therefore, the tubes are under compressive loading, which reduces the stress corrosion cracking thus reducing the probability of a tube rupture.

7.2. Features addressing external events in particular.

Nothing specifically indicated here.

8. EMERGENCY PLANNING ISSUES:

- The CAREM-25 allows an important reduction in the emergency planning.

6. IRIS (International consortium lead by Westinghouse, the United States of America)

1. LIST OF POSTULATED EXTERNAL EVENTS:

- Aircraft crashes;
- Electromagnetic interference from off-site (e.g. from communication centres, portable phone antennas) and on-site (e.g. from the activation of high-voltage electric switch gears);

- Earthquakes;
- Extreme meteorological conditions (temperature, snow, hail, frost, subsurface freezing, drought, wind);
- Tornadoes;
- Fire;
- Floods.

2. PROTECTION BY STRUCTURAL DESIGN OF BUILDINGS, CONTAINING STRUCTURES, SYSTEMS AND COMPONENTS IMPORTANT TO SAFETY, AGAINST POSTULATED EXTREME EXTERNAL EVENTS:

- The reactor, containment, passive safety systems, fuel storage, power source, control room and back-up control are all located within the reinforced concrete auxiliary building and are protected from on-site explosions;
- IRIS is designed with a passive habitability system that provides breathing air for operating personnel for an extended period of time. This feature allows the IRIS external air intake to be isolated when/ if hazardous gas is detected;
- 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 farther underground. Also, the IRIS safety features are passive and are contained within the auxiliary building;
- IRIS is designed to survive a hypothetical flood called the Probable Maximal Flood (PMF). The PMF can be based on an estimate made by combining the worst possible values (minmax) of all factors that contribute to producing a flood, rather than being based only on studies of observed flood frequencies. This capability is due to the use of passive features, which are all contained within the auxiliary building and do not require external water or power supplies for at least 7 days.

3. SPATIAL SEPARATION OF REDUNDANT SAFETY RELATED SYSTEMS TO SECURE PROTECTION AGAINST LOCALIZED ADVERSE EFFECTS, INCLUDING THOSE RESULTING FROM EXTERNAL EVENTS.

Nothing specifically indicated here.

4. DESIGN FEATURES, IMPLEMENTED WITHIN PROTECTED BUILDINGS, TO MAINTAIN FUEL TEMPERATURE WITHIN ACCEPTANCE LIMITS UNDER POSTULATED EXTREME EXTERNAL EVENTS WHEN ALL SOURCES OF POWER, COOLING WATER SUPPLY, AND COMPRESSED AIR EXTERNAL TO THE PROTECTED BUILDING ARE ASSUMED TO BE LOST, AND NO CREDIT IS GIVEN TO OPERATOR ACTIONS WITHIN A STIPULATED GRACE PERIOD.

4.1. Active safety systems requiring emergency power supply.

IRIS has no active safety systems.

4.2. Passive systems for reactor shutdown and heat removal within protected buildings that remain available to provide safety functions.

4.2.1. Passive systems requiring emergency power supply based instrumentation and electrical signals to get actuated.

The required power is provided by stored energy (safety grade batteries). No emergency diesel/AC power source is required.

- The Emergency Heat Removal System (EHRS) is designed to perform the following major functions: emergency core decay heat removal, emergency reactor coolant system water inventory control (LOCA mitigation), and emergency containment pressure reduction. The EHRS is designed to maintain the plant in a safe shutdown condition for up to 7 days without any replenishment.
- The Automatic Depressurization System (ADS) is designed to automatically depressurize the reactor coolant system (RCS) following postulated accidents, e.g. LOCA. It also provides operator with the ability to manually depressurize RCS.
- The Emergency Boration System (EBS) provides limited RCS make-up and also provides sufficient borated water for core reactivity control during transients or accidents when the normal RCS make-up supply from the Chemical and Volume Control System (CVCS) is not available or is insufficient.
- The Long-term Gravity Makeup System (LGMS) is designed to perform the following major functions: gravity make-up to the reactor coolant system, containment sump pH control.
- Effective heat removal from inside the vessel is provided by the SG/ EHRS; the primary system is depressurized by condensation and not by loss of mass.

4.2.2. Passive systems not requiring any electrical signals to get actuated.

Nothing specifically indicated here.

4.3. Heat sinks that remain available with loss of external coolant supply:

- Plant safety grade ultimate heat sink for the removal of RCS sensible heat and core decay heat for at least one week, without credit for any water make-up. 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.

4.4. Inherent safety features:

- IRIS implements the “safety by design™” approach, where accidents are by design prevented from occurring, rather than coping with consequences;
- Integral vessel configuration eliminates loop piping and external components, thus enabling compact containment and plant size;
- Integral reactor layout eliminates large primary piping;
- Large, tall vessel contributes to an increased water inventory;
- Increased natural circulation;
- Steam generators are designed for full primary pressure therefore, no over-pressurization is possible;
- Integral pressurizer is used, which ensures a large pressurizer volume relative to the reactor power;
- Small, high design-pressure containment;
- Control Rod Drive Mechanisms (CRDMs) are located within the RV, which eliminates the possibility of a control rod ejection accident;
- The pressure vessel (PV) cavity provides for the cavity flood-up, external vessel cooling and In-Vessel Retention (IVR), thus preventing vessel failure.

5. FEATURES FOR PREVENTION AND MITIGATION OF CONSEQUENCES OF HYPOTHETICAL SEVERE ACCIDENTS:

- IRIS is designed such that a postulated core melt will reliably not result in failure of the reactor vessel, through implementation of the In-Vessel Retention (IVR) strategy, which eliminates ex-vessel steam explosion, direct containment vessel (CV) heating, core-concrete interaction.

- Inerted containment.
- The diverse and redundant automatic depressurization system (ADS) eliminates high-pressure melt scenarios.

6. FEATURES FOR PREVENTING UNACCEPTABLE RELEASE OF RADIOACTIVITY FOLLOWING POSTULATED BEYOND DESIGN BASIS ACCIDENTS:

- Low-leakage thick-steel containment vessel with a reduced number and size of penetrations.
- The IRIS containment is inerted and thus provides protection from the reaction of the Zircaloy in the cladding of the active fuel by ensuring that the released hydrogen cannot detonate in the containment following postulated core damage events.
- A diverse means of containment heat removal (passive containment cooling system, PCCS) is provided so that the probability of containment over-pressure failure, following a small/ medium LOCA and/ or failure to provide core cooling, is essentially eliminated.

7. OTHER IMPORTANT SAFETY FEATURES, INCLUDING OTHER SPECIAL FEATURES PROVIDED TO DEAL WITH EXTERNAL EVENTS.

7.1. Features to enhance defence in depth in general:

- IRIS has non-safety related back-up diesels for normally available active equipment that can bring the plant to cold shutdown conditions; prolonged loss of off-site power is not foreseen to have a major impact on the plant.
- The IRIS Refuelling Water Storage Tank (RWST) is designed to be replenished by alternative water sources such as fire trucks, therefore it is completely independent on the plant power resources. Because of these and other reasons, it is expected that the impact of external events at the site will be lower than that for current plants.

7.2. Features addressing external events in particular.

- Low temperature related effects such as freezing, snowfall and ice cover are addressed in the design process. The safety-grade ultimate heat sink (RWST) and passive systems are located within the auxiliary building and are protected from freezing. The non-safety related heat sink and the related service water and pumps are adequately warmed to prevent icing. Any required remedial action can be taken to ensure the availability of the normal plant cooling, and protection of the instruments, components, and structures whose failure could result in a plant trip or affect the operation of normal plant functions.
- The RWST, which is the plant's ultimate heat sink, will be protected from some external events by locating it inside the reinforced concrete auxiliary building structure.
- All the IRIS safety related equipment, including the batteries that provide emergency power and the passive habitability system, are also located within this structure.
- The normally operating systems and their non-safety, active back-up systems are typically located within substantial structures that can withstand some degree of external event challenges. This equipment includes the back-up diesel generators. However, the service water mechanical draft-cooling tower has no special protection.
- The IRIS plant safety features, once actuated, rely on natural driving forces such as gravity and natural circulation flow for their continued function. These safety systems do not need diesel generators as they are designed to function without safety-grade support systems (such as AC power, component cooling water, or service water for a period of 7 days).

8. EMERGENCY PLANNING ISSUES.

- Reduced or eliminated requirements for emergency response planning.

7. PHWR-540 (NPCIL, India)

1. LIST OF POSTULATED EXTERNAL EVENTS:

- Lightning;
- Earthquake;
- Potential flooding;
- Winds;
- Aircraft crashes;
- Explosions and toxic gas releases from industrial activities.

2. PROTECTION BY STRUCTURAL DESIGN OF BUILDINGS, CONTAINING STRUCTURES, SYSTEMS AND COMPONENTS IMPORTANT TO SAFETY, AGAINST POSTULATED EXTREME EXTERNAL EVENTS:

- Double containment system,
- Use of a protective rock bund up to 7.03 m above mean sea level for the protection against wave run-up.

3. SPATIAL SEPARATION OF REDUNDANT SAFETY RELATED SYSTEMS TO SECURE PROTECTION AGAINST LOCALIZED ADVERSE EFFECTS, INCLUDING THOSE RESULTING FROM EXTERNAL EVENTS:

- Back-up control room is located in the service building; diametrically opposite from the main control building;
- Redundant power supplies (diesel generators, UPS systems, batteries) provided in separate, widely spaced buildings;
- Safety related systems & components grouped and placed in buildings of appropriate seismic categories.

4. DESIGN FEATURES, IMPLEMENTED WITHIN PROTECTED BUILDINGS, TO MAINTAIN FUEL TEMPERATURE WITHIN ACCEPTANCE LIMITS UNDER POSTULATED EXTREME EXTERNAL EVENTS WHEN ALL SOURCES OF POWER, COOLING WATER SUPPLY, AND COMPRESSED AIR EXTERNAL TO THE PROTECTED BUILDING ARE ASSUMED TO BE LOST, AND NO CREDIT IS GIVEN TO OPERATOR ACTIONS WITHIN A STIPULATED GRACE PERIOD.

4.1. Active safety systems requiring emergency power supply:

- Auxiliary boiler feed pumps;
- Shutdown cooling system;
- Back-up water supplies to steam generators and to process water, through diesel-driven firewater pumps, drawing water from a safety grade water reservoir.

4.2. Passive Systems for reactor shutdown and heat removal within protected buildings that remain available to provide safety functions..

4.2.1. Passive systems requiring emergency power supply based instrumentation and electrical signals to get actuated

Nothing specifically indicated here.

4.2.2. Passive systems not requiring any electrical signals to get actuated.

- Reactor shutdown system (gets actuated on a failure of the electric supply).
- Steam Generator Atmosphere Discharge Valves, which open on an instrument air failure.

4.3. Heat sinks that remain available with loss of external coolant supply.

Nothing specifically indicated here.

4.4. Inherent safety features:

- Primary coolant thermo-siphon capability.

5. FEATURES FOR PREVENTION AND MITIGATION OF CONSEQUENCES OF HYPOTHETICAL SEVERE ACCIDENTS:

- Cold moderator surrounding the fuel channels, which can serve as a heat sink;
- Water filled reactor vault.

6. FEATURES FOR PREVENTING UNACCEPTABLE RELEASE OF RADIOACTIVITY FOLLOWING POSTULATED BEYOND DESIGN BASIS ACCIDENTS:

- Primary containment clean-up system (filtration & pump-back system);
- Secondary containment, with purging arrangement to maintain negative pressure in the annular space between primary & secondary containments.

7. OTHER IMPORTANT SAFETY FEATURES, INCLUDING OTHER SPECIAL FEATURES PROVIDED TO DEAL WITH EXTERNAL EVENTS.

7.1. Features to enhance defence in depth in general.

Nothing specifically indicated here.

7.2. Features addressing external events in particular:

- Placing of safety related equipment in the basement is avoided. Also, design provisions are made to ensure that underground tunnels do not constitute paths for water ingress into the basements.
- The cooling water intake structure is designed for a cyclonic storm to ensure decay heat removal capability.
- For performing safety functions, no reliance is placed on off-site electric power supplies, which may get affected by a cyclone/ high wind. On-site emergency power supplies are based on diesel generators and batteries.
- Sites having unacceptable seismic potential are excluded (i.e. those falling in Seismic Zone V as per Indian national standard IS-1893-2000; or those having any capable fault within 5 km).
- The grade elevation is higher than the design basis flood level, based on:
  - For coastal sites: a 1000-year return period of a cyclonic storm surge coincident with the highest astronomical tide and wave run-up effect.
  - For inland sites: probable maximum precipitation and routing of the resultant waters through a river channel, together with failure of the upstream dams.
- Screening distance values are used in siting to protect the plant from aircraft crashes.
- Chemical explosions and toxic gas release from off-site facilities are either:
  - Excluded by distance > 5 km; or
  - Control is taken of locating the hazardous industrial facilities within 5 km radius.

8. EMERGENCY PLANNING ISSUES:

- Measures to ensure easy access of the emergency teams to the site are provided from different directions. For coastal sites, a sea route is also available.
- Emergency drilling is performed on a regular basis.

8. ACR-700 (AECL, Canada)

1. LIST OF POSTULATED EXTERNAL EVENTS:

- Aircraft crashes (assessments made for capability of containment);
- Electromagnetic interference;
- Earthquakes;
- Cyclones (Design Basis Tornado);
- Lightning.

2. PROTECTION BY STRUCTURAL DESIGN OF BUILDINGS, CONTAINING STRUCTURES, SYSTEMS AND COMPONENTS IMPORTANT TO SAFETY, AGAINST POSTULATED EXTREME EXTERNAL EVENTS:

- The containment system includes: a pre-stressed concrete containment structure (the reactor building) with a pre-stressed concrete dome and an internal steel liner; building air coolers for heat removal; a containment isolation system consisting of valves or dampers in the ventilation ducts and certain process lines penetrating the containment envelope; and a hydrogen control system to maintain hydrogen concentration below the deflagration-to-detonation limit for beyond design basis accidents.
- The containment structure is seismically qualified. Other seismically qualified structures are the reactor auxiliary building, the main control building, the raw service water pump-house and the maintenance building.

3. SPATIAL SEPARATION OF REDUNDANT SAFETY RELATED SYSTEMS TO SECURE PROTECTION AGAINST LOCALIZED ADVERSE EFFECTS, INCLUDING THOSE RESULTING FROM EXTERNAL EVENTS:

- The long term cooling system, which assures shutdown heat removal capability in the long term period after a normal shutdown and all design basis events including loss of coolant accidents; this system is arranged in two physically separate and redundant divisions completely independent from one another.
- The safety support systems for cooling water and electrical power are arranged in two physically separate and redundant divisions completely independent from one another.
- Separation and independence also includes the provision of a secondary control area as a back-up to the main control room for certain emergency conditions which may render the main control room uninhabitable.

4. DESIGN FEATURES, IMPLEMENTED WITHIN PROTECTED BUILDINGS, TO MAINTAIN FUEL TEMPERATURE WITHIN ACCEPTANCE LIMITS UNDER POSTULATED EXTREME EXTERNAL EVENTS WHEN ALL SOURCES OF POWER, COOLING WATER SUPPLY, AND COMPRESSED AIR EXTERNAL TO THE PROTECTED BUILDING ARE ASSUMED TO BE LOST, AND NO CREDIT IS GIVEN TO OPERATOR ACTIONS WITHIN A STIPULATED GRACE PERIOD.

4.1. Active safety systems requiring emergency power supply:

- The long term cooling system maintains shutdown heat removal from the reactor in the long-term period for all design basis events. The long term cooling system gives up the reactor decay heat to the safety related cooling water systems: the recirculated cooling water system (intermediate, closed system) and the raw service water system (open system connected to the ultimate heat sink), in this order of heat transfer.

4.2. Passive systems for reactor shutdown and heat removal within protected buildings that remain available to provide safety functions.

4.2.1. Passive systems requiring emergency power supply based instrumentation and electrical signals to get actuated:

- Two fast-acting shutdown systems: one operating with insertion of rods by gravity and the other with injection of soluble neutron absorber into the moderator.
- The emergency feedwater system supplies water to the secondary side of the steam generators by gravity from a reserve water tank located inside the dome of the containment, following certain initiating events and after automatic depressurization of the steam generators.
- The emergency coolant injection system constitutes the high-pressure portion of the emergency core cooling system. The system injects water into the reactor coolant system from normally pressurized tanks, following a loss of coolant accident.

4.2.2. Passive systems not requiring any electrical signals to get actuated.

- Natural circulation capability in the reactor coolant system to cope with transients due to loss of forced flow.

4.3. Heat sinks that remain available with loss of external coolant supply:

- A large tank in the upper part of the reactor building (reserve water tank) can make up water to the secondary side of the steam generators by gravity as part of the emergency feedwater system function, thus allowing decay heat removal for a long time after shutdown without any reliance on cooling water systems located outside the containment.

4.4. Inherent safety features:

- Significantly negative power reactivity coefficient;
- Negative full-core void reactivity sized to offer a balanced nuclear protection between loss of coolant accidents and fast cooldown accidents;
- All reactivity devices for reactor shutdown and control are located in the low pressure and temperature moderator, eliminating the possibility of accidents such as rod ejection;
- On-power fuelling permits minimizing excess reactivity holdup in the reactor.

5. FEATURES FOR PREVENTION AND MITIGATION OF CONSEQUENCES OF HYPOTHETICAL SEVERE ACCIDENTS:

- Passive thermal capacity of moderator can maintain core coolability for loss of coolant accidents combined with the unavailability of the emergency core cooling system.
- Passive thermal capacity of shield water surrounding the calandria vessel slows down severe core damage progression for the extremely improbable condition of a loss of coolant accident combined with the simultaneous unavailability of the emergency core cooling system and the moderator back-up heat sink. A slower core melt progression after a severe core damage accident means slower containment pressurization and allows the operator to take corrective actions before the containment failure and consequential large release of radioactivity can occur.

- Passive make-up from the reserve water tank to moderator and shield water increases the time duration of the passive heat removal capabilities of these two separate water volumes, thus enhancing mitigation of severe core damage accidents.

6. FEATURES FOR PREVENTING UNACCEPTABLE RELEASE OF RADIOACTIVITY FOLLOWING POSTULATED BEYOND DESIGN BASIS ACCIDENTS:

- Containment structure;
- Containment isolation system;
- Heat removal from the containment atmosphere after an accident is provided by the containment cooling system, comprised of local air coolers suitably distributed inside the reactor building;
- Hydrogen control is provided by passive autocatalytic recombiners;

7. OTHER IMPORTANT SAFETY FEATURES, INCLUDING OTHER SPECIAL FEATURES PROVIDED TO DEAL WITH EXTERNAL EVENTS.

7.1. Features to enhance defence in depth in general:

- A secondary control area backs up the main control room for emergency conditions that may render the main control room uninhabitable.
- The safety support systems in ACR (cooling water systems and electrical power supplies) are provided with greater redundancy and separation of redundant features to increase the resistance to randomly occurring events and common cause events, including external events.

7.2. Features addressing external events in particular:

- The reserve water tank located inside the dome of the reactor building is a major feature addressing external events (see also item 4.3). The tank contains sufficient water to supply the secondary side of the steam generators by gravity and to remove decay heat for a long time after a shutdown. The ensemble of the reserve water tank and the steam generator secondary side (emergency feedwater system) does not depend on cooling water supplies located outside the containment;
- Safety systems and safety support systems are seismically qualified for a Design Basis Earthquake (DBE).

8. EMERGENCY PLANNING ISSUES.

Requirements for emergency planning depend on the regulatory framework and site conditions applicable to each specific project. Therefore, they are outside the scope of the ACR reference design. However, design features that help reducing emergency planning requirements have been strengthened in the ACR-700 reference design. Moderator back-up heat sink (with passive make-up capability from reserve water tank) practically allows excluding large early release for beyond design basis accidents (BDBAs). Shield water heat sink around the calandria vessel (with passive make-up capability from reserve water tank) reduces the probability of containment failure and consequential late large release due to severe core damage. Site-dependent requirements and provisions for emergency planning will be identified for each specific project.

9. AHWR (BARC, India)

1. LIST OF POSTULATED EXTERNAL EVENTS:

- Safe Shutdown Earthquake (SSE), Operation Basis Earthquake (OBE);
- Flooding potential;

  - Inland flooding;
  - Coastal flooding;
  - Dam break;
  - External flooding from events like tsunamis, storm, cyclones;
- Hazards with influence on air and water intake and outfall structures (e.g. floating debris);
- Lightning;
- Winds;
- Aircraft crash;
- Explosions and toxic gas releases from industrial activities (off-site and on-site);
- Internal fire;
- External environmental conditions (temperature and humidity, cooling water temperatures);
- Electromagnetic interference from off-site and on-site activities;
- Loss of ultimate heat sink (for inland sites, e.g. failure of an upstream or a downstream dam);
- Site specific events (slope instability; soil liquefaction, surface collapse or uplift);
- Human-induced events (toxic gas release; chemical explosion, industrial or military accident, surface vehicle impact or explosion).

2. PROTECTION BY STRUCTURAL DESIGN OF BUILDINGS, CONTAINING STRUCTURES, SYSTEMS AND COMPONENTS IMPORTANT TO SAFETY, AGAINST POSTULATED EXTREME EXTERNAL EVENTS:

- The reactor is provided with an inner pre-stressed concrete containment designed to provide leak-tightness under a large break LOCA, and an outer secondary containment that protects the inner containment from external events including aircraft impacts.
- Layout of civil structures is such that less important structures would protect the more important ones.
- The effect of flood-related events is avoided by providing a high-grade elevation level to take care of probable maximum precipitation and maximum possible sea level etc. in extreme environmental conditions.
- Safety-related structures, components, and systems are designed for the SSE.
- Protection against seismic events (SSE and OBE) is achieved through proper layout of the plant buildings considering factors like avoiding structural connections between different safety class structures and seismic category structures, sufficient gap for seismic isolation or shake space, symmetrical layout of structures, etc.
- 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, as well as minimizing the inventory of combustible material.
- Damages related to lightning are avoided by grounding.
- Closing dampers in the ventilation systems provides detection of poisonous gases and minimizing their ingress into structures and air intakes. Air bottles of 30 minutes capacity are provided for the supply of fresh air to operating personnel.
- Important nuclear auxiliary systems are located inside the reactor building and in the basement, to the extent possible.

3. SPATIAL SEPARATION OF REDUNDANT SAFETY RELATED SYSTEMS TO SECURE PROTECTION AGAINST LOCALIZED ADVERSE EFFECTS, INCLUDING THOSE RESULTING FROM EXTERNAL EVENTS:

- In keeping with normal practice for Indian PHWRs, the separation and redundancy of safety related systems is provided in the layout.

- Two separate control rooms, main control room and supplementary control room are provided. The latter has redundant functions to shut down the reactor in the event of the main control room becoming uninhabitable.
- 4×50 % redundancy philosophy adopted for safety related systems;
- As far as possible, the safety related systems and components of similar safety class/ seismic category are located and placed suitably in buildings/ structures of appropriate classifications.
- Four independent emergency core cooling system (ECCS) trains are provided;
- Reactor shutdown and decay heat removal systems, control systems, instrumentation and power supplies are redundant and diverse;
- Safety systems are grouped into two groups, which are functionally and physically independent and supported by the diverse and independent support systems;
- Redundant power supplies (UPS systems, batteries) are located in separate, widely spaced buildings.
- 3 × 100% capacity diesel generators are provided at segregated locations.

4. DESIGN FEATURES, IMPLEMENTED WITHIN PROTECTED BUILDINGS, TO MAINTAIN FUEL TEMPERATURE WITHIN ACCEPTANCE LIMITS UNDER POSTULATED EXTREME EXTERNAL EVENTS WHEN ALL SOURCES OF POWER, COOLING WATER SUPPLY, AND COMPRESSED AIR EXTERNAL TO THE PROTECTED BUILDING ARE ASSUMED TO BE LOST, AND NO CREDIT IS GIVEN TO OPERATOR ACTIONS WITHIN A STIPULATED GRACE PERIOD.

4.1. Active safety systems requiring emergency power supply (class III and class II):

- Active shutdown cooling system for long-term decay heat removal;
- Auxiliary feedwater pump;
- Back-up water supplies through diesel-driven firewater pumps, drawing water from a safety grade water reservoir;
- Control and instrumentation channels;
- Primary containment and secondary containment ventilation systems;
- Active process water system;
- Service water system;
- Moderator cooling system;
- End-shield cooling system;
- Fire water system.

4.2. Passive systems for reactor shutdown and heat removal within protected buildings that remain available to provide safety functions.

4.2.1. Passive systems requiring emergency power supply based instrumentation and electrical signals to get actuated:

- Mechanical shut-off rods;
- Liquid poison injection based secondary shut down system.

4.2.2. Passive systems not requiring any electrical signals to get actuated:

- Use of steam pressure to passively drive decay heat removal;
- Use of steam pressure to passively enable shutdown in the extremely low probability case of a failure of both mechanical shut-off rods and liquid poison shut off system;
- Heat removal from the core under normal full power operating conditions is performed by natural circulation of coolant;

- Decay heat removal from the core, in case of non-availability of main steam condenser, is accomplished by natural circulation;
- Passive injection of ECCS water, initially from accumulator and later from the overhead Gravity Driven Water Pool (GDWP), is performed with four independent trains directly into the fuel cluster, without the need for operation of a valve or availability of instrumentation signal;
- Submergence of the reactor core under water before exhaustion of the ECCS inventory;
- Passive containment cooling system;
- Passive removal of moderator heat in case cooling medium (feedwater) is not available.

4.3. Heat sinks that remain available with loss of external coolant supply:

- GDWP with 6000 cubic meter storage capacity provides a three-day grace period for decay heat removal and during large break LOCAs;
- Fire water storage provides cooling of the important auxiliary systems for eight hours;
- Moderator acts as an ultimate heat sink;
- Emergency water reservoir is provided.

4.4. Inherent safety features:

- Negative void coefficient of reactivity;
- Low excess reactivity in the core;
- Reactivity devices are located in low pressure moderator;
- Low burn-up reactivity swing;
- Low xenon load;
- Low core power density;
- Large coolant inventory in main heat transport system;
- Natural circulation driven heat removal during normal operation and hot shutdown condition.

5. FEATURES FOR PREVENTION AND MITIGATION OF CONSEQUENCES OF HYPOTHETICAL SEVERE ACCIDENTS:

- Availability of moderator as heat sink;
- Availability of water in the calandria vault as an additional heat sink;
- Flooding of the reactor cavity following LOCA.

6. FEATURES FOR PREVENTING UNACCEPTABLE RELEASE OF RADIOACTIVITY FOLLOWING POSTULATED BEYOND DESIGN BASIS ACCIDENTS:

- Passive containment isolation through establishment of a water seal;
- Passive containment cooling;
- Vapour suppression in GDWP;
- Double containment;
- Direct injection of ECCS water into the fuel cluster;
- Use of light water as a coolant and absence of high-pressure heavy water in primary coolant system will result in a reduced tritium activity for AHWR;
- Primary Containment Cleanup System and Primary Containment Controlled Discharge System (PCCD) are provided to minimise release of radioactivity after postulated BDBAs;
- Passive containment isolation system.

7. OTHER IMPORTANT SAFETY FEATURES, INCLUDING OTHER SPECIAL FEATURES PROVIDED TO DEAL WITH EXTERNAL EVENTS

7.1. Features to enhance defence in depth in general:

- Diesel generators with 3 x 100 % capacity located at different locations;
- Double containment;
- Supplementary control building.

7.2. Features addressing external events in particular:

- Double layered plant security system and separation of nuclear island from administrative area;
- Underground tunnels and trenches do not constitute paths for water ingress into plant buildings;
- Cooling water intake structure is designed for a cyclonic storm;
- For performing safety functions, no reliance is placed on off-site electric power supplies, which may get affected by cyclone /high wind. On-site emergency power supplies based on diesel generators, and batteries are relied upon;
- Sites having unacceptable seismic potential are excluded (i.e. those falling in Seismic Zone V as per Indian national standard IS-1893-2000; or those having any capable fault within 5 km);
- Grade elevation is higher than the design basis flood level, based on:
  - For coastal sites: a 1000-year return period of a cyclonic storm surge coincident with the highest astronomical tide and wave run-up effect,
  - For inland sites: probable maximum precipitation and routing of the resultant waters through a river channel, together with failure of the upstream dams.
- Screening distance values are used in siting to protect the plant from aircraft crashes;
- Chemical explosions and toxic gas release from off-site facilities are either:
  - Excluded by distance > 5 km; or
  - Control is taken of locating the hazardous industrial facilities within 5 km radius.

8. EMERGENCY PLANNING ISSUES:

- No need for emergency planning in public domain.

10. SWR 1000 (AREVA, Europe)

1. LIST OF POSTULATED EXTERNAL EVENTS:

- Safe Shutdown Earthquake (SSE);
- Airplane crash (small sporting aircraft, military aircraft, large passenger aircraft);
- Explosion pressure wave;
- Release of hazardous explosive, toxic, and corrosive gas from off-site and on-site storage;
- Fire generated from off-site sources (mainly for its potential for smoke and toxic gas production);
- Electromagnetic interference from off-site and on-site sources;
- Extreme meteorological conditions (wind, storm, temperature, humidity, snow, hail, frost, subsurface freezing, drought);
- Hazards with potential influence on cooling water intakes and air intakes (e.g. ice frazil, ice debris, seaweed, marine life algae, oil slicks, smoke);

- Floods;
- Landslides;
- Lightning.

2. PROTECTION BY STRUCTURAL DESIGN OF BUILDINGS, CONTAINING STRUCTURES, SYSTEMS AND COMPONENTS IMPORTANT TO SAFETY, AGAINST POSTULATED EXTREME EXTERNAL EVENTS:

- The containment is surrounded by the reactor building with a strong outer shell;
- Sufficiently thick-dimensioned outer building walls designed for protection against large commercial aircraft crash and separated from the inner structures;
- Walls and floors of the inner structures are decoupled from the outer shell in order to reduce the loads induced by an aircraft crash;
- The building is made with watertight reinforced concrete able to withstand sulphate-bearing groundwater up to 3.5 meters above MSL (mean sea level ~ plant grade level) and provided with a ventilation system to maintain the building at a slightly negative pressure relative to the atmosphere;
- The passive safety systems are new features. They are located within the containment, which is surrounded by the protected reactor building. These new systems are designed against all induced vibration loads produced by external event loads;
- The accommodation of the safety related instrumentation and control (I&C) and switch gears within special compartments in the fully protected reactor building avoids spurious signals in case of external events and the destruction of the switch gear building;
- The spent fuel pool is located within the fully protected reactor building; for diesel generators, the same protection philosophy is valid as for the EPR;
- Detection of poisonous gases and prevention of their penetration into compartments in which the personnel stays is possible.

3. SPATIAL SEPARATION OF REDUNDANT SAFETY RELATED SYSTEMS TO SECURE PROTECTION AGAINST LOCALIZED ADVERSE EFFECTS, INCLUDING THOSE RESULTING FROM EXTERNAL EVENTS:

- The passive safety systems have quadrant physical separation. The active safety systems are located at opposite sides within the containment or reactor building.
- The two trains of safety-related service water and component cooling water systems together with the emergency diesel-generator systems and MV-bus bars are arranged physically separated by more than 120 m, accommodated in the buildings protected against wreckage loads.
- The reactor supporting systems building, containing the main control room, is spatially separated from the bunkered emergency control room building.

4. DESIGN FEATURES, IMPLEMENTED WITHIN PROTECTED BUILDINGS, TO MAINTAIN FUEL TEMPERATURE WITHIN ACCEPTANCE LIMITS UNDER POSTULATED EXTREME EXTERNAL EVENTS WHEN ALL SOURCES OF POWER, COOLING WATER SUPPLY, AND COMPRESSED AIR EXTERNAL TO THE PROTECTED BUILDING ARE ASSUMED TO BE LOST, AND NO CREDIT IS GIVEN TO OPERATOR ACTIONS WITHIN A STIPULATED GRACE PERIOD.

4.1. Active safety systems requiring emergency power supply:

- Two trains of the low pressure coolant injection and residual heat removal systems with dedicated essential service water systems and component cooling water systems.

4.2. Passive systems for reactor shutdown and heat removal within protected buildings that remain available to provide safety functions.

4.2.1. Passive systems requiring emergency power supply based instrumentation and electrical signals to get actuated.

- Boron shutdown system (Fast boron injection system).

4.2.2. Passive systems not requiring any electrical signals to get actuated:

- Passive Pressure Pulse Transmitters (PPPT) used to activate control rod drives (CRDs) with scram system**; c**ontainment isolation at main steam lines and feedwater lines; reactor depressurization system;
- Emergency condensers for heat removal from the reactor pressure vessel (RPV);
- Flooding lines for passive core flooding in the event of LOCA;
- Containment cooling condensers for heat removal from the containment;
- Reactor shutdown by control rods via hydraulic scram system;
- Safety relief valves for reactor pressure relief and depressurization;
- Main steam and feedwater isolation valves.

4.3. Heat sinks that remain available with loss of external coolant supply:

- Large water volume in the RPV;
- Large water volumes within the containment;
- Large water volume in the shielding/ storage pool above the containment within the reactor building.

4.4. Inherent safety features.

- Negative Doppler, temperature and void reactivity coefficients of the core.

5. FEATURES FOR PREVENTION AND MITIGATION OF CONSEQUENCES OF HYPOTHETICAL SEVERE ACCIDENTS

- RPV depressurization by highly redundant and diverse safety relief valves (SRVs) to avoid high pressure core melt sequences;
- Passive flooding of the RPV exterior and passive heat removal with large margins to critical heat flux (CHF) to achieve core melt retention within RPV;
- Containment is inerted by nitrogen to avoid hydrogen-oxygen reactions;
- Containment is designed for hydrogen generation corresponding to 100% zirconium oxidation.

6. FEATURES FOR PREVENTING UNACCEPTABLE RELEASE OF RADIOACTIVITY FOLLOWING POSTULATED BEYOND DESIGN BASIS ACCIDENTS:

- Passive heat removal from the containment via containment cooling condensers;
- Containment isolation and integrity, limitation of radioactive releases by filtering of potential releases; the heating, ventilation and air conditioning (HVAC) penetrations are permanently closed during power generation, because the containment is inerted with nitrogen and the main steam lines and feedwater lines can be isolated by passive means (system fluid operated valves activated by passive pressure pulse transmitters).

7. OTHER IMPORTANT SAFETY FEATURES, INCLUDING OTHER SPECIAL FEATURES PROVIDED TO DEAL WITH EXTERNAL EVENTS.

7.1. Features to enhance defence in depth in general:

- SRVs for reactor pressure relief and reactor depressurization;
- No operator actions are required immediately after onset of an external event, because the passive safety systems manage all required safety functions. In case of destruction of the reactor supporting systems building with the main control room by an airplane crash, the operating personnel has to occupy the emergency control room (bunker).

7.2. Features addressing external events in particular.

Nothing specifically indicated here (already covered under items 2 and 3).

8. EMERGENCY PLANNING ISSUES

Off-site emergency response actions, such as evacuation or relocation are not required. Food control is restricted to the immediate vicinity of the plant.

11. VK-300 (NIKIET, the Russian Federation)

1. LIST OF POSTULATED EXTERNAL EVENTS:

- Aircraft crashes: 20 t mass and 200 m/s aircraft velocity;
- Explosions: > 30 kPa overpressure;
- Collision of ships and floating debris (ice, logs, etc.) with the water intakes: > 20 t;
- Earthquakes: > 8 units on the MSK-64;
- Extreme meteorological conditions (temperature, snow, hail, frost, subsurface freezing, drought): snow level growth > 20 mm/h; freezing thickness >25 mm;
- Floods: water level > 1 m; water velocity > 0.7 m/s;
- Cyclones: >50 m/s wind velocity.

2. PROTECTION BY STRUCTURAL DESIGN OF BUILDINGS, CONTAINING STRUCTURES, SYSTEMS AND COMPONENTS IMPORTANT TO SAFETY, AGAINST POSTULATED EXTREME EXTERNAL EVENTS.

- Secondary containment is provided to mitigate severe accidents and external impacts.

3. SPATIAL SEPARATION OF REDUNDANT SAFETY RELATED SYSTEMS TO SECURE PROTECTION AGAINST LOCALIZED ADVERSE EFFECTS, INCLUDING THOSE RESULTING FROM EXTERNAL EVENTS.

Nothing specifically indicated here.

4. DESIGN FEATURES, IMPLEMENTED WITHIN PROTECTED BUILDINGS, TO MAINTAIN FUEL TEMPERATURE WITHIN ACCEPTANCE LIMITS UNDER POSTULATED EXTREME EXTERNAL EVENTS WHEN ALL SOURCES OF POWER, COOLING WATER SUPPLY, AND COMPRESSED AIR EXTERNAL TO THE PROTECTED BUILDING ARE ASSUMED TO BE LOST, AND NO CREDIT IS GIVEN TO OPERATOR ACTIONS WITHIN A STIPULATED GRACE PERIOD.

4.1. Active safety systems requiring emergency power supply.

Nothing specifically indicated here.

4.2. Passive systems for reactor shutdown and heat removal within protected buildings that remain available to provide safety functions.

4.2.1. Passive systems requiring emergency power supply based instrumentation and electrical signals to get actuated:

- Two reactivity control systems:
  - Control rods;
  - Boric acid injection.

4.2.2. Passive systems not requiring any electrical signals to get actuated:

- Natural circulation of coolant in all modes;
- Passive activation of safety systems;
- Passive operation of safety systems.

4.3. Heat sinks that remain available with loss of external coolant supply:

- Emergency cooling tank;
- Atmospheric air is the ultimate heat sink.
- Emergency heat sinks outside the pre-stressed concrete vessel (PCV), i.e. emergency tanks & heat exchangers.

4.4. Inherent safety features:

- Self-regulation and self-limitation of power (negative reactivity effects and coefficients).

5. FEATURES FOR PREVENTION AND MITIGATION OF CONSEQUENCES OF HYPOTHETICAL SEVERE ACCIDENTS:

- The use of two containments: primary reactor containment and secondary containment.

6. FEATURES FOR PREVENTING UNACCEPTABLE RELEASE OF RADIOACTIVITY FOLLOWING POSTULATED BEYOND DESIGN BASIS ACCIDENTS:

- Secondary containment.

7. OTHER IMPORTANT SAFETY FEATURES, INCLUDING OTHER SPECIAL FEATURES PROVIDED TO DEAL WITH EXTERNAL EVENTS.

7.1. Features to enhance defence in depth in general:

- The use of two containments: primary reactor containment and secondary containment.

7.2. Features addressing external events in particular:

- Secondary containment.

8. EMERGENCY PLANNING ISSUES:

- No off-site emergency planning is needed.

12. ABWR-II (Toshiba Corporation, Japan)

1. LIST OF POSTULATED EXTERNAL EVENTS:

- Earthquakes;
- Extreme meteorological conditions (snow)
- Cyclones (Typhoon)
- Lightning.

2. PROTECTION BY STRUCTURAL DESIGN OF BUILDINGS, CONTAINING STRUCTURES, SYSTEMS AND COMPONENTS IMPORTANT TO SAFETY, AGAINST POSTULATED EXTREME EXTERNAL EVENTS:

- Aircraft crashes (optional).

3. SPATIAL SEPARATION OF REDUNDANT SAFETY RELATED SYSTEMS TO SECURE PROTECTION AGAINST LOCALIZED ADVERSE EFFECTS, INCLUDING THOSE RESULTING FROM EXTERNAL EVENTS:

- Four divisions of emergency core cooling system (ECCS);
- Redundant/ diverse power supply with four emergency generators (2 diesel, 2 gas turbine).

4. DESIGN FEATURES, IMPLEMENTED WITHIN PROTECTED BUILDINGS, TO MAINTAIN FUEL TEMPERATURE WITHIN ACCEPTANCE LIMITS UNDER POSTULATED EXTREME EXTERNAL EVENTS WHEN ALL SOURCES OF POWER, COOLING WATER SUPPLY, AND COMPRESSED AIR EXTERNAL TO THE PROTECTED BUILDING ARE ASSUMED TO BE LOST, AND NO CREDIT IS GIVEN TO OPERATOR ACTIONS WITHIN A STIPULATED GRACE PERIOD.

4.1. Active safety systems requiring no emergency power supply:

- Advanced reactor core isolation cooling system (ARCIC) with the capability of self-standing operation and power supply under station blackout conditions (SBO) beyond the battery capacity; ARCIC is operated by a reactor-steam driven turbine with small generator.

4.2. Passive systems for reactor shutdown and heat removal within protected buildings that remain available to provide safety functions.

4.2.1. Passive systems requiring emergency power supply based instrumentation and electrical signals to get actuated:

- Passive reactor cooling system (PRCS).

4.2.2. Passive systems not requiring any electrical signals to get actuated:

- Passive containment cooling system (PCCS).

4.3. Heat sinks that remain available with loss of external coolant supply:

- Passive heat removal system (PRCS, PCCS) cooling pool;
- Suppression pool.

4.4. Inherent safety features:

- Passive containment cooling system (PCCS) can keep its heat removal (steam condensation) performance via venting a non-condensable gas (such as nitrogen or hydrogen) utilizing pressure difference between the drywell and the wetwell.

5. FEATURES FOR PREVENTION AND MITIGATION OF CONSEQUENCES OF HYPOTHETICAL SEVERE ACCIDENTS:

- Advanced reactor core isolation cooling system (ARCIC) which has a capability of self-standing operation and power supply under station blackout conditions (SBO) beyond the battery capacity;
- Passive heat removal systems for the reactor and containment (PRCS, PCCS);
- Passive autocatalytic recombiner (PAR) to avoid hydrogen burning.

6. FEATURES FOR PREVENTING UNACCEPTABLE RELEASE OF RADIOACTIVITY FOLLOWING POSTULATED BEYOND DESIGN BASIS ACCIDENTS:

- Passive containment cooling system (PCCS) prevents containment failure or venting for overpressure protection and the associated radioactivity release to the environment following postulated beyond design basis accidents (BDBAs).

7. OTHER IMPORTANT SAFETY FEATURES, INCLUDING OTHER SPECIAL FEATURES PROVIDED TO DEAL WITH EXTERNAL EVENTS.

7.1. Features to enhance defence in depth in general.

Nothing specifically indicated here.

7.2. Features addressing external events in particular.

Nothing specifically indicated here.

8. EMERGENCY PLANNING ISSUES:

- The ABWR-II design provides more emphasis on BDBA capability in order to achieve a higher level of safety, such as to attain practical exclusion of the probability of the emergency evacuation/ resettlement.

13. BN-800 (Sankt-Peterburg Atomenergoproekt, the Russian Federation)

1. LIST OF POSTULATED EXTERNAL EVENTS:

- Aircraft crashes;
- Earthquakes;
- Extreme meteorological conditions,
- Cyclones
- Explosions,
- Electromagnetic interference from off-site,
- Internal hazard loads.

2. PROTECTION BY STRUCTURAL DESIGN OF BUILDINGS, CONTAINING STRUCTURES, SYSTEMS AND COMPONENTS IMPORTANT TO SAFETY, AGAINST POSTULATED EXTREME EXTERNAL EVENTS:

- Shear walls and shell dome are reinforced concrete structures capable of withstanding external hazards;
- Structural and component design takes into account all postulated external events;
- Outer building structures are designed to protect safety-related systems and components from external events.

3. SPATIAL SEPARATION OF REDUNDANT SAFETY RELATED SYSTEMS TO SECURE PROTECTION AGAINST LOCALIZED ADVERSE EFFECTS, INCLUDING THOSE RESULTING FROM EXTERNAL EVENTS:

- Layout separation and redundancy of safety channels and systems; the goal is to achieve a safe shutdown of the plant in case of an aircraft crash.

4. DESIGN FEATURES, IMPLEMENTED WITHIN PROTECTED BUILDINGS, TO MAINTAIN FUEL TEMPERATURE WITHIN ACCEPTANCE LIMITS UNDER POSTULATED EXTREME EXTERNAL EVENTS WHEN ALL SOURCES OF POWER, COOLING WATER SUPPLY, AND COMPRESSED AIR EXTERNAL TO THE PROTECTED BUILDING ARE ASSUMED TO BE LOST, AND NO CREDIT IS GIVEN TO OPERATOR ACTIONS WITHIN A STIPULATED GRACE PERIOD.

4.1. Active safety systems requiring emergency power supply.

Nothing specifically indicated here.

4.2. Passive systems for reactor shutdown and heat removal within protected buildings that remain available to provide safety functions.

4.2.1. Passive systems requiring emergency power supply based instrumentation and electrical signals to get actuated:

- The shutdown system and activating systems of safety facilities operate automatically, with no operator actions required;
- Loss of electric supply of the safety channels causes the operation of the emergency reactor shutdown and of the activating systems of safety facilities.

4.2.2. Passive systems not requiring any electrical signals to get actuated.

Nothing specifically indicated here.

4.3. Heat sinks that remain available with loss of external coolant supply.

Nothing specifically indicated here.

4.4. Inherent safety features.

Nothing specifically indicated here.

5. FEATURES FOR PREVENTION AND MITIGATION OF CONSEQUENCES OF HYPOTHETICAL SEVERE ACCIDENTS.

Nothing specifically indicated here.

6. FEATURES FOR PREVENTING UNACCEPTABLE RELEASE OF RADIOACTIVITY FOLLOWING POSTULATED BEYOND DESIGN BASIS ACCIDENTS.

Nothing specifically indicated here.

7. OTHER IMPORTANT SAFETY FEATURES, INCLUDING OTHER SPECIAL FEATURES PROVIDED TO DEAL WITH EXTERNAL EVENTS.

7.1. Features to enhance defence in depth in general.

Nothing specifically indicated here.

7.2. Features addressing external events in particular.

Nothing specifically indicated here.

8. EMERGENCY PLANNING ISSUES:

- Special automatic system unlocks the gates for the access of emergency teams in case of a fire, loss of electric supply, and in other accidents.

14. CHTR (BARC, India)

1. LIST OF POSTULATED EXTERNAL EVENTS:

- Aircraft crashes;
- Cyclones;
- Flooding potential;
- Earthquake.

2. PROTECTION BY STRUCTURAL DESIGN OF BUILDINGS, CONTAINING STRUCTURES, SYSTEMS AND COMPONENTS IMPORTANT TO SAFETY, AGAINST POSTULATED EXTREME EXTERNAL EVENTS:

- Various structures, systems and equipment for the CHTR are being designed for high level and low probability seismic events such as operating basis earthquake (OBE) and safe shutdown earthquake (SSE). Seismic instrumentation is also planned.

3. SPATIAL SEPARATION OF REDUNDANT SAFETY RELATED SYSTEMS TO SECURE PROTECTION AGAINST LOCALIZED ADVERSE EFFECTS, INCLUDING THOSE RESULTING FROM EXTERNAL EVENTS:

- Two different and independent passive systems are provided consisting of multiple independent trains for reactor shutdown;
- Two different sets of heat pipes from different locations are provided for passive heat dissipation to the environment during postulated accidental conditions;
- An additional passive heat dissipation system is provided to dissipate heat by the conduction to a heat sink; the system is compartmentalized.

4. DESIGN FEATURES, IMPLEMENTED WITHIN PROTECTED BUILDINGS, TO MAINTAIN FUEL TEMPERATURE WITHIN ACCEPTANCE LIMITS UNDER POSTULATED EXTREME EXTERNAL EVENTS WHEN ALL SOURCES OF POWER, COOLING WATER SUPPLY, AND COMPRESSED AIR EXTERNAL TO THE PROTECTED BUILDING ARE ASSUMED TO BE LOST, AND NO CREDIT IS GIVEN TO OPERATOR ACTIONS WITHIN A STIPULATED GRACE PERIOD.

4.1. Active safety systems requiring emergency power supply:

- All safety and heat removal systems are passive, requiring no power supply.

4.2. Passive systems for reactor shutdown and heat removal within protected buildings that remain available to provide safety functions.

4.2.1. Passive systems requiring emergency power supply based instrumentation and electrical signals to get actuated:

- All safety and heat removal systems are passive, requiring no power supply;
- Loss of electric supply of the secondary shutdown system causes reactor shutdown.

4.2.2. Passive systems not requiring any electrical signals to get actuated:

- Passive core heat removal by natural circulation of liquid heavy metal coolant;
- Three independent systems capable of dissipating the neutronically limited power to the environment by passive means under postulated accidental conditions are provided;
- Passive power regulation system;
- Two independent passive systems for reactor shutdown.

4.3. Heat sinks that remain available with loss of external coolant supply:

- The all-ceramic core has a large heat capacity, ensuring slow temperature rise in fuel under postulated accidental conditions;
- The reactor core is surrounded by a large heat sink.

4.4. Inherent safety features:

- Excellent high temperature (up to 1873 K) performance of TRISO fuel; the probability of release of fission products and gases is very low;
- Large negative Doppler coefficient of the fuel for any state within the irradiation cycle;
- The all-ceramic core has a large heat capacity, ensuring slow temperature rise in fuel under postulated accidental conditions;
- Low core power density;
- Small excess reactivity of the reactor core, facilitated by the use of burnable poison;
- Negative moderator temperature coefficient;
- Low-pressure operation of the coolant; due to very high boiling point (1943 K) of Pb-Bi coolant, there is very large thermal margin available. In addition to this, there is no over-pressurization and no chance of reactor thermal explosion due to coolant emergency overheating, as there is no rise in coolant pressure in any operating or accidental condition;
- Negligible thermal energy is stored in the coolant that is available for release in the event of a leak or accident;
- Chemical inertness of Pb-Bi coolant at high temperatures ensures that in case of a contact with air or water the coolant does not react violently with explosions or fires;
- Low induced long-lived gamma activity of the coolant; in case of a leakage the coolant is capable of retaining iodine and other radionuclides;
- For Pb-Bi coolant, the reactivity effects (void, power, temperature, etc.) are negative.

5. FEATURES FOR PREVENTION AND MITIGATION OF CONSEQUENCES OF HYPOTHETICAL SEVERE ACCIDENTS:

- Excellent high temperature (up to 1873 K) performance of TRISO fuel; the probability of release of fission products and gases is very low;
- Large heat capacity ceramic core — Slow temperature rise of fuel in case of postulated accident condition, resulting in large span of time available for corrective action even in case all heat sinks are lost. The all-ceramic core has a large heat capacity, ensuring slow temperature rise in fuel under postulated accidental conditions, resulting in a large time span available for corrective action even in case all heat sinks are lost;
- A large heat sink is available outside the outer shell of the reactor.

6. FEATURES FOR PREVENTING UNACCEPTABLE RELEASE OF RADIOACTIVITY FOLLOWING POSTULATED BEYOND DESIGN BASIS ACCIDENTS:

- Very high temperature capability of fuel enables heat dissipation to the surroundings before any large-scale fission product release can occur.

7. OTHER IMPORTANT SAFETY FEATURES, INCLUDING OTHER SPECIAL FEATURES PROVIDED TO DEAL WITH EXTERNAL EVENTS.

7.1. Features to enhance defence in depth in general:

- Increased shutdown reliability provided by two independent passive shutdown systems requiring no operator intervention;
- Three independent and redundant passive heat removal systems for the removal of heat under postulated accidental conditions;
- Inherent safety features of the reactor, such as all-ceramic core, excellent high temperature performance of TRISO coated particle fuel, large negative Doppler coefficient of fuel, negative void coefficient and high boiling point of the inert coolant.

7.2. Features addressing external events in particular:

- Chemical inertness of the Pb-Bi coolant prevents fires in case of its accidental exposure to air or water;
- In case of coolant leakage due to an external event, the induced long-lived gamma activity of the coolant is low and the coolant is capable of retaining iodine and other radionuclides.

8. EMERGENCY PLANNING ISSUES:

- No impact in public domain is anticipated.

ANNEXES
I — VI

ANNEX I

SEISMIC PROBABILISTIC SAFETY ASSESSMENT OF NUCLEAR POWER PLANTS

M.K. RAVINDRA
ABSG Consulting Inc., Irvine, CA, United States of America

Abstract

This paper presents an extended summary of the methodology for seismic probabilistic safety assessments (SPSAs) of nuclear power plants, which has been established as a US national standard (ANS, 2003) on external event PSA. A comprehensive list of publications on SPSA is included.

1. INTRODUCTION

1.1. Overview of methodology

Seismic probabilistic safety assessments (PSA) have been conducted for over 50 nuclear power plants worldwide in the last 25 years. The methodology has been well established and the necessary data on the parameters of the PSA models have been generally collected. Detailed description of the procedures used in seismic PSA is given in several published reports [I-1 to I-6]. In response to the need for risk-informed decisions, a US national standard [I-7] on external event PSA has been developed which prescribes the standard requirements for different elements of a seismic PSA.

The seismic PSA method addresses each of the following questions:

- What is the seismic risk to the plant (e.g. core damage frequency (CDF) and large early release frequency (LERF))?
- What range of ground motion levels dominates the seismic risk?
- What are the plant vulnerabilities and components that are the dominant contributors to seismic risk?
- What are the potential improvements which can be made to reduce risk?

The key elements of a seismic PSA used to address the above questions are:

- ***Seismic hazard analysis***: to develop frequencies of occurrence of different levels of ground motion (e.g. peak ground acceleration and average spectral acceleration) at the site;
- ***Systems/Accident sequence analysis***: modelling of the various combinations of structural and equipment failures as well as human errors that could initiate and propagate a seismic core damage sequence;
- ***Seismic fragility evaluation***: to estimate the conditional probability of failure of important structures and equipment whose failure may contribute to the frequency of unacceptable damage to the plant (e.g. core damage);
- ***Risk quantification***: assembly of the results of the seismic hazard, fragility, and systems analyses to estimate the frequencies of core damage, and severe radiological releases. Assessment of the impact of seismic events on the containment and consequence analyses, and integration of these results with core damage analysis to obtain estimates of seismic risk in terms of effects on public health (e.g. early deaths and latent cancer fatalities).

The starting point for PSA analysis is the occurrence of an event which perturbs the normal heat removal process to the extent that a reactor shutdown is required and alternative methods of heat removal are required. In the case of equipment failure within the plant, the identification of the event and subsequent requirements is relatively straightforward. In the case of an earthquake, the situation is much more complex. This results in the necessity to do a considerable amount of analysis of the effects of varying size earthquakes on the plant and equipment. This information is used to identify the condition of the plant immediately after the earthquake and, hence, the equipment available to provide the decay heat removal and maintain the core in a stable state. Thus, the first three tasks above equate to the initiating fault evaluation in the internal events PSA.

Since there are many uncertainties in the model parameters that describe the seismic hazard, structural and component fragilities, and systems reliability, it is important to propagate the uncertainties at different stages of the analysis to obtain uncertainty bounds on the overall seismic risk estimates, such as CDF and LERF. Because of the large uncertainties associated with seismic risk estimates, the traditional approach has been to look for insights in a more qualitative way rather than emphasize the "bottom-line numbers". However, the need for developing realistic "bottom-line" numbers has become important in recent times as the industry and regulators are moving towards ensuring and demonstrating quantitatively that ALARA principles are met, and it is feasible to make risk-informed decisions.

1.2. Organization of this Annex

Section 2 describes the probabilistic seismic hazard analysis methods and recent applications. Section 3 discusses the differences between the systems analysis performed for the seismic events and that conducted for internal event initiators. Section 4 describes the methods and databases for seismic fragility evaluation of structures and equipment that are modelled in the systems analysis. Section 5 discusses how the risk quantification is conducted for seismic initiated accidents. The results and insights from recent seismic PSAs are highlighted in Section 6. The final section describes how seismic PSA could be used in the design of new reactors.

2. SEISMIC HAZARD ANALYSIS

Seismic hazard is usually expressed in terms of the frequency distribution of the peak value of a ground motion parameter (e.g. peak ground acceleration, peak spectral acceleration at different dynamic frequencies, etc.) during a specified time interval (e.g., one year). The different steps of this analysis are as follows [I-8 to I-9]:

(1) Identification of the sources of earthquakes, such as faults and seismotectonic provinces;

(2) Evaluation of the earthquake history of the region to assess the frequencies of occurrence of earthquakes of different magnitudes or epicentral intensities;

(3) Development of attenuation relationships to estimate the intensity for earthquake-induced ground motion (e.g. peak ground acceleration) at the site;

(4) Integration of the above information to estimate the frequency of exceedence for the selected ground motion parameter.

The hazard estimate depends on uncertain estimates of attenuation, upper bound magnitudes, and the geometry of the postulated sources. Such uncertainties are included in the hazard analysis by assigning probabilities to alternative hypotheses about these parameters. These are displayed on what is known on a logic tree. A probability distribution for the frequency of exceedance of the ground motion parameter is thereby developed. The annual frequencies for exceeding specified values of the ground motion parameter are displayed as a family of curves with different probabilities (Fig. I-1) assigned to them.

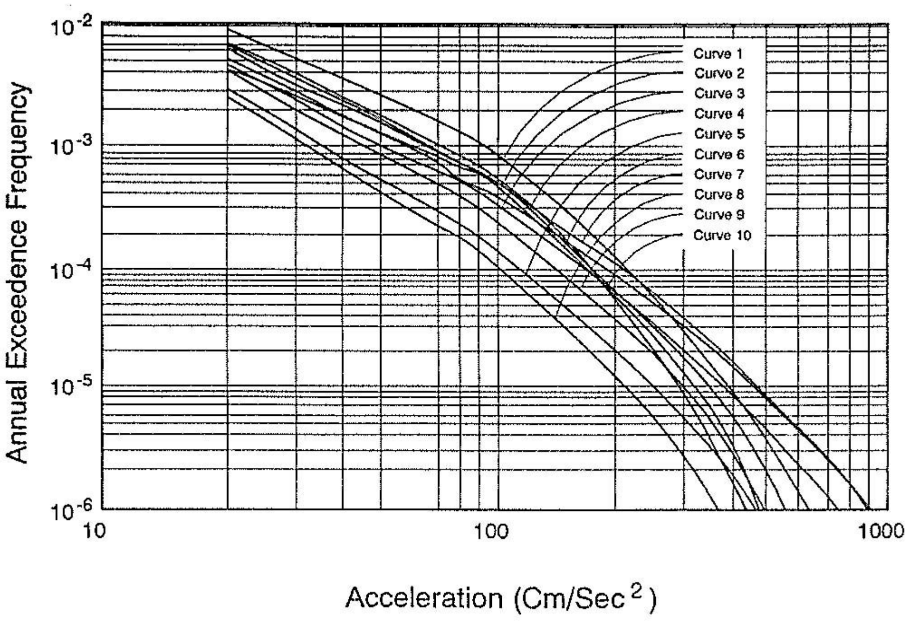


FIG. I-1. Seismic hazard curves for a nuclear plant site.

Another important output of seismic hazard analysis is the shape of ground motion spectrum; this has a major impact on the seismic fragility evaluation.

Probabilistic seismic hazard studies have been done for nuclear power plant sites in the USA since the late 1970s. The need for incorporating different viewpoints on the seismic sources, activity rates, ground motion, etc. was recognized in the 1980s, and several important studies were done for all existing nuclear power plant sites in the USA (Lawrence Livermore National Laboratory and the Electric Power Research Institute). More recently, the methodology for systematically eliciting expert opinions and developing an informed community distribution of uncertainty in seismic hazard has been proposed in the report by the Senior Seismic Hazard Analysis Committee (SSHAC) [I-5]. A full scale application of the SSHAC methodology is being conducted for the Swiss nuclear power plants. This study is the state-of-the-art effort bringing together renowned experts in seismic source modelling, ground motion modelling and hazard computation. It has rigorously followed the guidance given in the SSHAC report and elicited the opinions of experts and combined them to obtain the technical community distribution on the seismic hazard at each site. The numerical results of this study are currently being reviewed by the sponsors.

3. SEISMIC SYSTEMS ANALYSIS

Nuclear power plants have many safety systems to bring the plant into a safe shutdown condition, thereby preventing core damage and mitigating any accident. There are many front-line systems performing these functions; these front-line systems derive support (i.e. water, instrument air, steam, and control power) from supporting systems. Analysis of nuclear power plants composed of multiple trains of redundant safety systems is accomplished using event trees and fault trees [I-1]. This analysis was developed initially for the initiating events induced by operator errors and random failures, the so-called “internal events”.

Reference [I-10] describes approaches to develop a seismic probabilistic risk assessment (SPRA) logic model, quantify the resulting accident sequence frequencies, and present the results. Although the logic model includes both the development of event trees and fault trees, it refers to all of the logic model effort as systems analysis.

The approach offered assumes that there exists an internal events probabilistic risk assessment (PRA) for power operation of the same plant, from which the CDF can be calculated. The internal events

PRA must also include the sequence development sufficient for a Level 2 assessment (i.e. including an assessment of containment systems and containment phenomenology) and thereby enable one to compute the LERF for the internal events. The internal events PRA must be consistent with the ASME PRA standard for internal events [I-11]; i.e. it must have been successfully reviewed against the standard, or otherwise justified that it is acceptable.

If an internal events PRA does not exist, one can build a new one before embarking on the SPRA. However, if this approach is taken, the internal events PRA must adhere to the standard for all the tasks; i.e. initiating events, accident sequences, success criteria, systems modelling, data, human reliability analysis, and use of expert judgment. A peer review must also be performed to ensure that the standard is met.

A seismic PSA (SPSA) has its own requirements, as presented in the ANS standard for external events [I-7]. Development of a SPSA requires expert judgment and extrapolation of knowledge beyond that used to show compliance with design standards. For this and other reasons, a peer review is also required for the SPSA models and quantification.

Further details on systems analysis for seismic initiated events can be found in EPRI [I-10]. This reference discusses:

- The development of a list of structures and equipment to be considered for modelling in the SPSA (this list is used in the seismic walkdown and development of seismic fragilities);
- How to incorporate seismic failure modes into the PRA logic model;
- How to integrate the resulting logic models with the hazard curves and fragility curves to quantify the accident sequences in the model;
- The documentation requirements; and
- Performance of peer review.

Systems analysis for seismic events follows the approach taken for the internal events analysis. However, there are some major differences between the seismic and internal events as below:

- The entire range of earthquake ground motion levels need to be considered as potential initiating events;
- Seismic events may damage passive plant components (e.g. tanks, heat exchangers and piping) and structures that are not typically modelled in the internal event PRA;
- Seismic events may simultaneously damage multiple redundant systems and components at the plant. Mitigation of the event may, therefore, require a combination of plant system responses not considered in the accident sequence models for other initiators;
- Uncertainties in the seismic hazard and fragility are large and should be consistently propagated in order to produce the confidence ranges on seismic CDF and LERF.

4. SEISMIC FRAGILITY EVALUATION

The seismic fragility of a structure or equipment is defined as the conditional probability of its failure at a given value of acceleration (i.e. peak ground acceleration or peak spectral acceleration at different frequencies). The methodology for evaluating seismic fragilities of structures and equipment is documented in the PRA Procedures Guide [I-1] and is more specifically described for application to NPPs in [I-2 and I-3]. This general methodology has been applied in over 50 seismic probabilistic risk assessments of nuclear power plants.

The objective of a fragility evaluation is to estimate the capacity of a given component relative to a ground acceleration parameter, such as peak ground acceleration or spectral acceleration. Typically, the seismic hazard for a plant site is defined by peak ground acceleration (PGA) or spectral accelerations at different structural frequencies; hence, all fragility estimates are referenced to ground acceleration (peak ground or spectral acceleration). Peak ground acceleration is used as an example indicator only. If the seismic hazard curves are available in terms of spectral accelerations at different frequencies they could be used as long as consistency in the hazard and fragility definitions is maintained. In spite of its shortcomings as a damage measure, peak ground acceleration is a familiar term for all analysts involved in seismic PSA (i.e. systems analysts, hazard analysts and fragility analysts). In the Diablo Canyon seismic PSA, sensitivity studies indicated minor change to the core damage frequency calculated using fragilities defined in terms of peak ground acceleration compared to those defined using average spectral acceleration. The important conclusion is proper interface between the analysts (i.e. hazard, fragility and systems) should take place, and it does not matter what parameter the fragility is referenced to as long as the failure mode is properly defined and the seismic response and capacity values are consistently calculated.

The ground acceleration capacities of the components are estimated using information on plant design basis and responses calculated at the design-analysis stage. The ground acceleration capacity is a random variable that can be described completely by its probability distribution. However, there is uncertainty in the estimation of the parameters of this distribution, the exact shape of this distribution, and in the appropriate failure model for the component. For any postulated failure mode and set of parameter values describing the ground acceleration capacity and shape of the probability distribution, a fragility curve depicting the conditional probability of failure as a function of peak ground acceleration can be obtained. Hence, for different models and parameter assumptions, one could obtain different fragility curves. A satisfactory way to consider these uncertainties is to represent the component fragility by means of a family of fragility curves obtained as above. A subjective probability value is assigned to each curve to reflect the analyst's degree of belief in the model that yielded the particular fragility curve.

At any acceleration value, the component fragility (i.e. conditional probability of failure) varies from 0 to 1; this variation is represented by a subjective probability distribution. On this distribution we can find a fragility value (say, 0.01) that corresponds to the cumulative subjective probability of 5%. We have 5% cumulative subjective probability (confidence) that the fragility is less than 0.01. Similarly, we can find a fragility value for which we have a confidence of 95%. Note that these statements can be made without reference to any probability model. Using this procedure, the median and high (95%) and low (5%) confidence fragility curves can be drawn. On the high confidence curve, we can locate the fragility value of 5%; the acceleration corresponding to this fragility on the high confidence curve is the so-called "high-confidence-of-low-probability-of-failure" (HCLPF) capacity of the component. By characterizing the component fragility through a family of fragility curves, the analyst has expressed all his knowledge about the seismic capacity of the component along with the uncertainties. Given the same information, two analysts with similar experience and expertise would produce approximately the same fragility curves. Development of the family of fragility curves using different failure models and parameters for a large number of components in a seismic PRA is impractical if it is done as described above. Hence, a simple model for the fragility was proposed as described in the above-cited references. In the following section this fragility model is described.

4.1. Fragility model

The entire fragility family for an element corresponding to a particular failure mode can be expressed in terms of the best estimate of the median ground acceleration capacity, A_m, and two random variables. Thus, the ground acceleration capacity, A, is given by:

$$A = A_m e_R e_U \tag{1}$$

in which e_R and e_U are random variables with unit medians, representing, respectively, the inherent randomness about the median and the uncertainty in the median value. In this model, we assume that both e_R and e_U are lognormally distributed with logarithmic standard deviations, β_R and β_U, respectively. The formulation for fragility given by equation (1) and the assumption of lognormal distribution allow easy development of the family of fragility curves that appropriately represent fragility uncertainty. For the quantification of fault trees in the plant system and accident sequence analyses, the uncertainty in fragility needs to be expressed in a range of conditional failure probabilities for a given ground acceleration. This is achieved as explained below.

With perfect knowledge of the failure mode and parameters describing the ground acceleration capacity (i.e. only accounting for the random variability, β_R), the conditional probability of failure, f_O , for a given peak ground acceleration level, *a*, is given by:

$$f_0 = \Phi\left[\frac{\ln\left(\frac{a}{A_m}\right)}{\beta_R}\right] \tag{2}$$

where Φ (...) is the standard Gaussian cumulative distribution function. The relationship between f_O and *a* is the median fragility curve plotted in Fig. I-2 for a component with a median ground acceleration capacity A_m = 0.87g and β_R = 0.25. For the median conditional probability of failure range of 5% to 95%, the ground acceleration capacity would range from A_m exp (-1.65 β_R) to A_m exp (1.65 β_R), i.e., 0.58 g to 1.31 g.

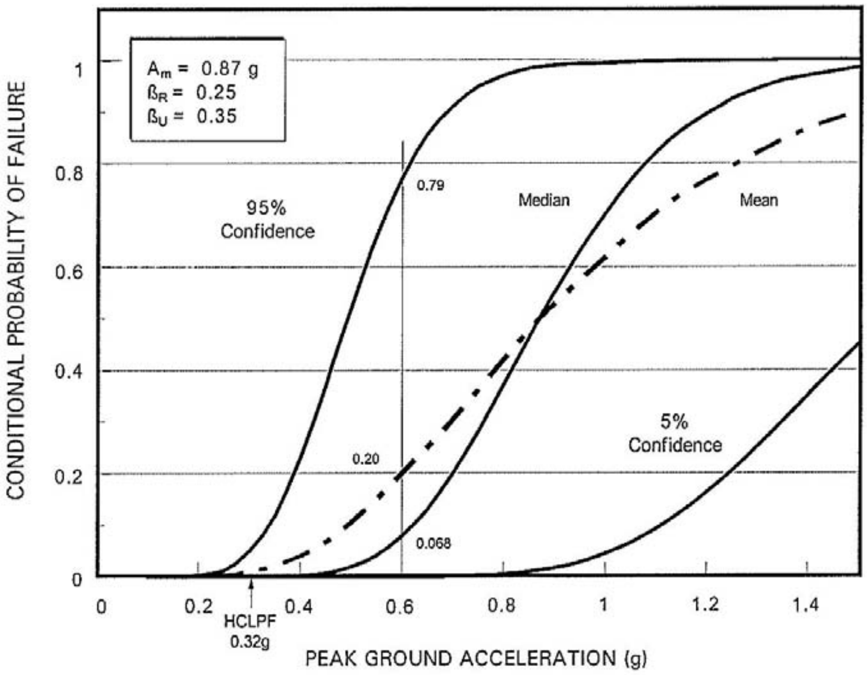


FIG. I-2. Mean, median, 5% non-exceedance, and 95% non-exceedance fragility curves for a component.

When the modelling uncertainty β_U is included, the fragility becomes a random variable (uncertain). At each acceleration value, the fragility f can be represented by a subjective probability density function. The subjective probability, Q (also known as "confidence") not exceeding a fragility f' is related to f' by:

$$f' = \Phi\left[\frac{\ln\left(\frac{a}{A_m}\right)+\beta_U\Phi^{-1}(Q)}{\beta_R}\right] \tag{3}$$

where:

Q = P[f < f' | a]; i.e., the subjective probability (confidence) that the conditional probability of failure, f, is less than f' for a peak ground acceleration a;

$\Phi^{-1}(...)$ = the inverse of the standard Gaussian cumulative distribution function.

For example, the conditional probability of failure f' at acceleration 0.6 g that has a 95% non-exceedance subjective probability (confidence) is obtained from equation (3) as 0.79. The 5% to 95% probability (confidence) interval on the failure at 0.4 g is 0 to 0.79. Subsequent computations in the seismic PSA are made easier by discretizing the random variable probability of failure f into different intervals and deriving probability q_i for each interval (Fig. I-3). Note that the sum of q_i over all the intervals is unity. The process develops a family of fragility curves, each with an associated probability q_i.

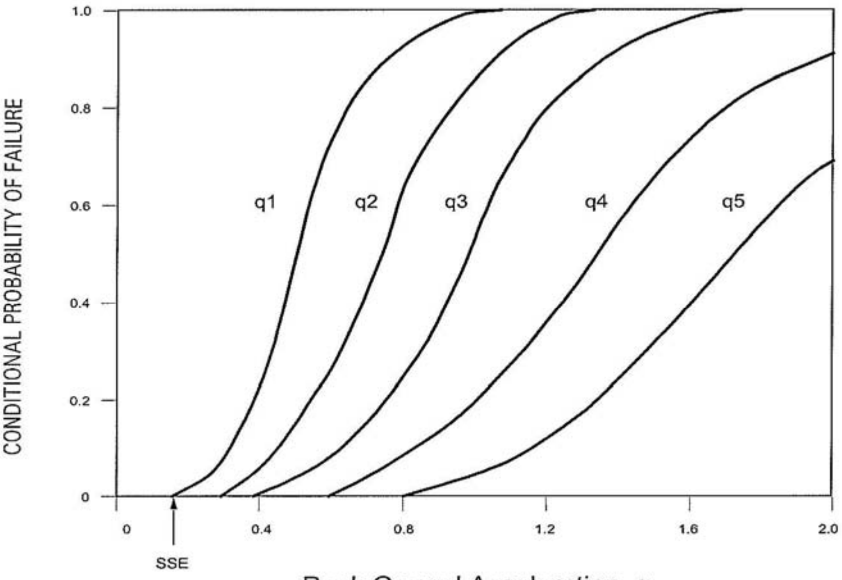


FIG. I-3. Discrete family of fragility curves for a component.

A mean fragility curve is also plotted in Fig. I-2. This is obtained using equation (2) but replacing β_R with the composite variability $\beta_C = (\beta_R^2 + \beta_U^2)^{½}$.

The median ground acceleration capacity A_m, and its variability estimates β_R and β_U are evaluated by taking into account the safety margins inherent in capacity predictions, response analysis, and equipment qualification, as explained below.

4.2. Failure modes

The first step in generating fragility curves such as those in Fig. I-2 is to develop a clear definition of what constitutes failure for each of the critical elements in the plant. This definition of failure must be agreeable to both the structural analyst generating the fragility curves and the systems analyst who must judge the consequences of component failure. Several modes of failure (each with a different consequence) may have to be considered and fragility curves may have to be generated for each of these modes. For example, a motor-actuated valve may fail in any of the following ways:

(1) Failure of power or controls to the valve (typically related to the seismic capacity of such items as cable trays, control panels, and emergency power). Since these failure modes are not related to the specific item of equipment (i.e., motor actuated valve) and are common to all active equipment, such failure modes are most easily handled as failures of separate systems linked in a series to the equipment;

(2) Failure of the motor;

(3) Binding of the valve due to distortion and, thus, failure to operate;

(4) Rupture of the pressure boundary.

It may be possible to identify the failure mode most likely to be caused by the seismic event by observations during the walkdown or by reviewing the equipment design and considering only that mode. Otherwise, fragility curves are developed based on the premise that the component could fail in any one of all potential failure modes.

Identification of the credible modes of failure is largely based on the analyst's experience and judgment. Review of plant design criteria, calculated stress levels in relation to the allowable limits, qualification test results, seismic fragility evaluation studies done on other plants, and reported failures (in past earthquakes, in licensee event reports and fragility tests) are useful in this task.

Structures are considered to have failed functionally when they cannot perform their designated functions. In general, structures have failed functionally when inelastic deformations under seismic load are estimated to be sufficient to potentially interfere with the operability of safety-related equipment attached to the structure, or fractured sufficiently so that equipment attachments fail. These failure modes represent a conservative lower bound of seismic capacity since a larger margin of safety against collapse exists for nuclear structures. Also, a structural failure has been generally assumed to result in a common cause failure of multiple safety systems, if these are housed in the same structure. For example, the service water pumps may be assumed to fail when the enclosure pump house roof collapses. Structures that are susceptible to sliding are considered to have failed when sufficient sliding deformation has occurred to fail buried or interconnecting piping or electrical duct banks.

For piping, failure of the support system and fracture of the pressure boundary are credible failure modes. Failure modes of equipment examined may include structural failure modes (e.g., bending, buckling of supports, anchor bolt pullout, etc.), functional failures (binding of valve, excessive deflection in rotating equipment), and breaker trip or relay chatter.

Consideration should also be given to the potential for soil failure modes (e.g. liquefaction, toe bearing pressure failure, base slab uplift, and slope failures). For buried equipment (i.e. piping and tanks), failure due to lateral soil pressures may be an important mode. Seismically induced failures of structures or equipment under impact of another structure or equipment (e.g. a crane) may also be a consideration. Seismically induced failures of dams, if present, resulting in either flooding or loss-of-cooling-source, should also be investigated.

4.3. Estimation of fragility parameters

In estimating fragility parameters, it is convenient to work in terms of an intermediate random variable called the factor of safety. The factor of safety, F, on ground acceleration capacity above a reference level earthquake specified for design; e.g. the safe shutdown earthquake (SSE) level specified for design, A_{SSE}, is defined as follows:

$$A = FA_{SSE}$$

$$F = \frac{\text{Actual seismic capacity of element}}{\text{Actual response due to SSE}}$$

$$= \frac{\text{Actual capacity}}{\text{Calculated capacity}}$$

$$\times \quad \frac{\text{Calculated capacity}}{\text{Design response due to SSE}}$$

$$\times \quad \frac{\text{Design response due to SSE}}{\text{Actual response due to SSE}}$$

F is further simplified as:

$$F \quad = \quad \frac{\text{Actual capacity}}{\text{Design response due to SSE}}$$

$$\times \quad \frac{\text{Design response due to SSE}}{\text{Actual response due to SSE}}$$

$$F = F_C F_{SR} \tag{4}$$

Note that F can also be defined with reference to a different earthquake such as the operating basis earthquake (OBE) level and Review Level Earthquake (RLE).

The median factor of safety, F_m, can be directly related to the median ground acceleration capacity, A_m, as:

$$F_m = \frac{A_m}{A_{SSE}} \tag{5}$$

The logarithmic standard deviations of F, representing inherent randomness and uncertainty, are identical to those for the ground acceleration capacity A.

4.3.1. Fragility of structures

For structures, the factor of safety can be modelled as the product of three random variables:

$$F = F_S F_\mu F_{SR} \tag{6}$$

The strength factor, F_S, represents the ratio of ultimate strength (or strength at loss-of-function) to the stress calculated for A_{SSE}. In calculating the value of F_S, the non-seismic portion of the total load acting on the structure is subtracted from the strength as follows:

$$F_S = \frac{S - P_N}{P_T - P_N} \tag{7}$$

where S is the strength of the structural element for the specific failure mode, P_N is the normal operating load (i.e. dead load, operating temperature load, etc.) and P_T is the total load on the structure (i.e. sum of the seismic load for A_{SSF} and the normal operating load). For higher earthquake levels, other transients (e.g. safety/ relief valve (SRV) discharge) may have a high probability of occurring simultaneously with the earthquake. The definition of P_N in such cases should be extended to include the loads from these transients.

The inelastic energy absorption factor (ductility factor), F_μ, accounts for the fact that an earthquake represents a limited energy source, and many structures or equipment items are capable of absorbing substantial amounts of energy beyond yield without loss-of-function. A suggested method to determine the de-amplification effect resulting from inelastic energy dissipation involves the use of ductility modified response spectra [I-12]. The de-amplification factor is primarily a function of the ductility ratio μ defined as the ratio of maximum displacement to displacement at yield. More recent analyses [I-13] have shown the de-amplification factor to also be a function of system damping. One might estimate a median value of μ for low-rise concrete shear walls (typical of auxiliary building walls) of 4.0. The corresponding median F_μ, value would be 2.45 at 7 % damping. The variabilities in the inelastic energy absorption factor, F_μ, are both estimated for this case as $\beta_R = 0.21$ and $\beta_U = 0.21$, taking into account the uncertainty in the predicted relationship between F_μ, μ, and system damping.

The structure response factor, F_{SR} is based on recognition that, in the design analyses, structural response was computed using specific (often conservative) deterministic response parameters for the structure. Because many of these parameters are random (often with wide variability) the actual response may differ substantially from the calculated response for a given peak ground acceleration.

The structure response factor, F_{SR}, is modelled as a product of factors influencing the response variability:

$$F_{SR} = F_{SA} F_{GMI} F_{\delta} F_M F_{MC} F_{EC} F_{SSI} \tag{8}$$

where:

F_{SA} = spectral shape factor representing variability in ground motion and associated ground response spectra;

F_{GMI} = ground motion incoherence factor that accounts for the fact that a travelling seismic wave does not excite a large foundation uniformly;

F_{δ} = damping factor representing variability in response due to difference between actual damping and design damping;

F_M = modelling factor accounting for uncertainty in response due to modelling assumptions;

F_{MC} = mode combination factor accounting for variability in response due to the method used in combining dynamic modes of response;

F_{EC} = earthquake component combination factor accounting for variability in response due to the method used in combining earthquake components;

F_{SSI} = factor to account for effect of soil-structure interaction including the reduction of input motion with depth below the surface.

The median and logarithmic standard deviations of F are expressed as:

$$F_m = F_{S\,m} F_{\mu_m} F_{SA\,m} F_{GMI\,m} F_{\delta\,m} F_{M\,m} F_{MC\,m} F_{EC\,m} F_{SSI\,m} \tag{9}$$

and

$$\beta_F = \left(\beta_s^{\,2} + \beta_\mu^{\,2} + \beta_{SA}^{\,2} + \beta_{GMI}^{\,2} + \cdots + \beta_{SSI}^{\,2}\right)^{1/2} \tag{10}$$

The logarithmic standard deviation ßF is further divided into random variability, β_R, and uncertainty, β_U. To obtain the median ground acceleration capacity A_M, the median factor of safety, F_m, is multiplied by the reference earthquake peak ground acceleration.

Fragility of equipment and other components

For equipment and other components, the factor of safety is composed of a capacity factor, F_C; a structure response factor, F_{SR}; and an equipment response (relative to the structure) factor, F_{RE}. Thus, F_{RE}

$$F_{RE} = F_C F_{RE} F_{SR} \tag{11}$$

The capacity factor F_C for the equipment is the ratio of the acceleration level at which the equipment ceases to perform its intended function to the seismic design level. This acceleration level could correspond to a breaker tripping in a switchgear, excessive deflection of the control rod drive tubes, or failure of an equipment support. The capacity factor for the equipment may be calculated as the product of F_S and F_{μ}.. The strength factor, F_S, is calculated using equation (7). The strength, S, of equipment is a function of the failure mode.

Equipment failures can be classified into three categories:

(1) Elastic functional failures;
(2) Brittle failures;
(3) Ductile failures.

Elastic functional failures involve the loss of intended function while the component is stressed below its yield point. Examples of this type of failure include the following:

- Elastic buckling in tank walls and component supports;
- Excessive blade deflection in fans.

The load level at which functional failure occurs is considered the strength of the component.

Brittle failure modes are those that have little or no system inelastic energy absorption capability. Examples include the following:

- Anchor bolt failures;
- Component support weld failures;
- Shear pin failures.

Each of these failure modes has the ability to absorb some inelastic energy on the component level, but the plastic zone is very localized and the system ductility for an anchor bolt or a support weld is very small. The strength of the component failing in a brittle mode is therefore calculated using the ultimate strength of the material.

Ductile failure modes are those in which the structural system can absorb a significant amount of energy through inelastic deformation. Examples include the following:

- Pressure boundary failure of piping or vessel nozzles;
- Structural failure of cable trays and ducting;
- Failure of component support members (plastic bending, plastic buckling).

The strength of the component failing in a ductile mode is calculated using the yield strength of the material for tensile loading. For flexural loading, the strength is defined as the limit load or load to develop a hinge mechanism.

The inelastic energy absorption factor, F_μ, for a piece of equipment is a function of the ductility ratio, μ. The median value of F_μ is considered close to 1.0 for brittle and functional failure modes. For ductile failure modes of equipment that respond in the amplified acceleration region of the design spectrum, the ductility is calculated in a manner similar to structures [I-13].

The equipment response factor F_{RE}, is the ratio of equipment response calculated in the design to the realistic equipment response; both responses being calculated for design floor spectra. F_{RE} is the factor of safety inherent in the computation of equipment response. It depends upon the response characteristics of the equipment and is influenced by some of the variables listed under equation (8). These variables differ according to the seismic qualification procedure. For equipment qualified by dynamic analysis, the important variables that influence response and variability are as follows:

- Qualification method (QM);
- Spectral shape (SA) - including the effects of peak broadening and smoothing, and artificial time history generation;
- Modelling (affects mode shape and frequency results) (M);
- Damping (δ);
- Combination of modal responses (for response spectrum method) (MC);
- Combination of earthquake components (ECC).

For rigid equipment qualified by static analysis, the variables, except the qualification method, and combination of earthquake components are not significant. The equipment response factor is the ratio of the specified static coefficient divided by the zero period acceleration of the floor level where the equipment is mounted. If the equipment is flexible and was designed via the static coefficient method, the dynamic characteristics of the equipment must be considered. This requires estimating the fundamental frequency and damping, if the equipment responds predominantly in one mode. The equipment response factor is the ratio of the static coefficient to the spectral acceleration at the equipment fundamental frequency.

Where testing is conducted for seismic qualification, the response factor must take into account the following:

- Qualification method (QM) ;
- Spectral shape (SA);
- Boundary conditions in the test versus installation (BC) ;
- Damping (δ);
- Spectral test method (sine beat, sine sweep, complex waveform, etc.) (STM);
- Multi-directional effects (MDE).

The overall equipment response factor is the product of these factors of safety corresponding to each of the variables identified above. The median and logarithmic standard deviations for randomness and uncertainty are estimated following equations (9) and (10).

The structural response factor, F_{SR}, is based on the response characteristics of the structure at the location of the component (equipment) support. The variables pertinent to the structural response analyses used to generate floor spectra for equipment design are the only variables of interest to equipment fragility. Time-history analyses using the same structural models used to conduct structural response analysis for structural design are typically used to generate floor spectra. The applicable variables are as follows:

- Spectral shape;
- Ground motion incoherence;
- Damping;
- Modelling;
- Soil-structure interaction, including reduction with depth of seismic input.

For equipment with a seismic capacity level that has been reached while the structure is still within the elastic range, the structural response factors should be calculated using damping values corresponding to less than yield conditions (e.g. about 5% median damping for reinforced concrete). The combination of earthquake components is not included in the structural response, since the variable is to be addressed for specific equipment orientation in the treatment of equipment response. Median F_m and variability β_R and β_U estimates are made for each of the parameters affecting capacity and response factors of safety. These median and variability estimates are then combined using the properties of lognormal distribution in accordance with equations (9) and (10) to obtain the overall median factor of safety F_m and variability β_R and β_U estimates required to define the fragility curves for the structure or equipment. For each variable affecting the factor of safety, the random (β_R) and uncertainty (β_U) variabilities must be separately estimated. The differentiation is somewhat judgmental, but it can be based on general guidelines. Essentially, β_R represents variability due to the randomness of the earthquake characteristics for the same acceleration and to the structural response parameters that relate to these characteristics. The dispersion represented by β_U is due to factors such as the following:

- Our lack of understanding of structural material properties such as strength, inelastic energy absorption, and damping;
- Errors in calculated response due to use of approximate modelling of the structure and inaccuracies in mass and stiffness representations;
- Usage of engineering judgment in lieu of complete plant-specific data on fragility levels of equipment capacities, and responses.

4.4. Information sources

Fragility evaluation utilizes data from various sources — plant specific and generic. Plant specific information would be design analysis and qualification test data. Generic information consists of earthquake experience data [I-14 and I-15], fragility test data [I-16 to I-20], qualification tests of similar components in other plants [I-21] and expert opinion. Fragility parameter values derived for several components in the past seismic probabilistic risk assessments have been compiled in Reference [I-22].

Several sources of information are utilized in developing plant-specific and generic fragilities for equipment. These sources include the following

- Seismic evaluation calculations;
- Plant safety analysis reports;
- Seismic evaluation report summaries;
- Past earthquake experience and expert opinion.

In seismic margin studies, an index of seismic margin is the HCLPF capacity of the component. This quantity considers both the uncertainty and randomness variabilities and is the acceleration value for which we have 95% confidence that the failure probability is less than 5%. That is, it is an acceleration value for the component for which we are highly confident there is only a small chance of failure given this ground acceleration level:

$$\text{HCLPF Capacity} = A_m \exp\{ -1.65 (\beta_R + \beta_U)\} \tag{12}$$

For some applications, a mean point estimate of core damage is considered adequate. In developing a mean point estimate, a composite fragility curve could be used. The composite fragility curve is defined by two parameters A_m and β_C, where A_m is the median capacity as previously described, and β_C is the composite variability.

The HCLPF capacity is then approximately defined as :

$$\text{HCLPF Capacity} = A_m \exp(-2.33\ \beta_C) \qquad (13)$$

4.5. Other fragility models

The lognormal model for fragility has been used in most seismic PSAs conducted to date. However, there have been some attempts to use other probability models to describe the fragility of components. As a sensitivity study, Ravindra et al [I-2] explored the use of Weibull distribution for seismic fragility. Note that the Weibull distribution has two parameters that can be derived from the mean and standard deviation of the variable. It was concluded from this study that Weibull model gives unrealistically high fragilities in the lower tail. The basic information needed is still the mean and standard deviation (equivalently, median, and β_R and β_U). There is not much empirical and analytical data available to justify the use of probability models requiring more than two parameters. The lognormal model is easy to use and could be partly justified by the Central Limit Theorem, since the overall safety factor is a product of several individual safety factors. Ellingwood [I-23] and Reed and Kennedy [I-3] have also arrived at similar conclusions.

4.6. Hybrid method

The fragility methodology of estimating the median and β_R and β_U described in this report is universally applicable. It does, however, require the median factors of safety for different variables affecting the response and capacity to be estimated as well as their logarithmic standard deviations. In the US nuclear industry, seismic margin assessments have been done for a number of nuclear power plants. Seismic margin is defined as the HCLPF capacity of components which are on chosen success path (s) for bringing the plant to a safe shutdown. The HCLPF capacities of components are calculated using a deterministic procedure called "conservative deterministic failure margin (CDFM)" method. EPRI [I-14] describes the CDFM method and provides several examples. In order to simplify the seismic PSA, a hybrid method is suggested in Reed and Kennedy [I-3] and Kennedy [I-6]. The main feature of this method is the development of seismic fragility using the HCLPF capacity. First, the HCLPF capacity of the component is estimated using the CDFM method. Next, the logarithmic standard deviation β_C is estimated using judgement and the following guidance [I-6]. For structures and major passive mechanical components mounted on ground or at low elevations within structures, β_C typically ranges from 0.3 to 0.5. For active components mounted at high elevations in structures the typical β_C range is 0.4 to 0.6. When in doubt, use of β_C of 0.4 is recommended. The median capacity is calculated using equation (13) and an approximate fragility curve for the component is thereby obtained. Reed and Kennedy [I-3] further recommend that this approximate fragility curve be used for each component in the systems analysis to identify the dominant contributors to the seismic risk (e.g. core damage frequency). For a few components that dominate the seismic risk, more accurate fragility parameter values should be obtained and a new quantification done to obtain a more accurate mean core damage frequency and to confirm that the dominant contributors have not changed.

The CDFM method, though being universally applicable in concept, has been derived following the seismic design and qualification practices of the US nuclear industry. The parameters and implied safety factors in the CDFM procedures should be appropriately modified for use in other countries, reflecting the differences in practices. The same caveat would apply to the use of generic β_C values. These generic values have been arrived at using the results and insights of a number of seismic PSAs involving thousands of fragility calculations. Judgement should therefore be exercised in their use for new applications in countries outside the USA.

5. SEISMIC RISK QUANTIFICATION

The procedure for calculating the frequencies of accident sequences induced by seismic events differs from internal event sequence quantification in the way the fragilities of components over the entire range of possible earthquake accelerations are considered and in the way fragility and hazard are integrated. The risk quantification should also account for correlation between component failures and the potential for non-seismic random failures of equipment and operator errors. It should also allow complete propagation of uncertainties throughout the analysis.

Generally, the resulting CDF and LERF are reported for the total of all seismic induced initiating events. Seismic-PRA practitioners possess different tools to accomplish this integration and quantification [I-24]. Analysts usually use an iterative process, in which an interim and approximate seismic model quantification is performed, after which certain parts of the overall systems model may be screened out on the basis that they do not contribute importantly to the results, or the model is augmented to include additional seismic failure modes. The quantification is then finalized.

The numerical schemes for risk quantification fall into two broad, but by no means exclusive categories. The first group, utilizing simulation techniques such as Latin Hypercube Sampling (LHS) and Monte-Carlo Simulation (MCS), involves random sampling from a number of continuous probability density functions (PDFs). The sampling process randomly chooses the specific confidence level of fragility curve families to be combined in the trial. The conditional probability of plant failure at each ground motion level is then computed. The samples are repeated many times and each trial output saved for each ground motion level. This data can then be sorted by CDF (or LERF depending on the output), and then the plant fragility curves are determined. Finally, the sampling process can continue in a second step whereby the plant fragility curves are sampled along with the confidence level of the hazard curve. These curves are then combined to give the CDF (or LERF). Again by repeating the process many times, the uncertainty in CDF (or LERF) is then determined.

The second category involves the discretization of analytical probability density functions (PDF) into discrete probability distributions (DPD) and is referred to as the DPD method. In a discretization scheme, a continuous lognormal density function is approximated by a finite number of $\{<p_i, x_i>\}$ doublets. The quantification steps then proceed along the lines outlined above to determine plant fragility curves and finally the CDF (or LERF) with uncertainties. The difference in this approach is that the probability distributions for failure must be combined just two at a time, and the process repeated for each summation required.

Three quantification methods are described in more detail in the paper [I-24]. For completeness, the existence of a fourth method should be mentioned. This is the Multiple Integration Method, which formed the core of the systems analysis phase in the seismic safety margins research program [I-25]. This method does not strictly belong to either one or the two categories defined earlier; here probabilities of cutsets are represented by multinormal integrals and evaluated numerically using Gaussian quadrature.

In each of the above methods, the proper interpretation of the fragility curves is required. The use of double lognormal distributions to represent the family of fragility curves gives rise to long tails for the individual component failure probabilities towards low ground motion levels. Since there are very many components in a nuclear plant, all subject to seismic failure; the sum of all these low probabilities of failure for so many components may give rise to a finite probability of some equipment failure, even at very low ground motions. It is recognized that the long tails for the assumed representation of the fragility curve families is artificial. In fact, the fragility curves are sometimes derived by choosing a ground motion level at which failure is not expected and conservatively assigning that ground motion level as the HCLPF. Certainly, extrapolation of the fragility curves to ground motion levels well below the HCLPF is not warranted nor intended by the fragility analysts. For this reason, truncation of the fragility curves at some level of ground motion is recommended.

For the base case quantification of CDF and LERF, it is recommended that the fragility curves be truncated at the HCLPF ground motion level on the mean fragility curve. For lower ground motion levels, a failure probability can be assumed. However, a sensitivity case should also be quantified assuming no truncation of the fragility curves explicitly modelled in the SPSA.

6. RESULTS AND INSIGHTS FROM RECENT SEISMIC PSAs

6.1. Results and insights

The output from a seismic PSA (SPSA) consists of:

- Frequencies of occurrence of different levels of ground motion at the site, including a characterization of uncertainties;
- Seismic fragilities for each component failure mode and seismic margins of safety;
- Seismic fragilities of accident sequences and seismic margins of safety;
- Seismic accident sequence frequencies and uncertainty distributions;
- Impact of non-seismic unavailabilities on seismic risk;
- Identification of dominant seismic risk contributors: components, systems, sequences and procedures;
- Determination of conditional probability of core damage for different levels of ground motion input;
- Identification of ranges of ground motion contributing to seismic risk;
- Measures of potential risk reduction as a function of seismic upgrading, to aid in backfitting the decisions.

Over the last 25 years, a number of seismic PSAs have been conducted for nuclear power plants in the USA, Canada, Switzerland, Finland, Hungary, Czech Republic, Slovenia, the Republic of Korea and Taiwan. These studies have been performed to some regulatory needs or to respond to some increased perception of seismic hazard. In the US, about half of the operating plants performed seismic PSA as part of the individual plant examination of external events (IPEEE) during 1990 and 1997. The results and insights from the IPEEE can be found in Rubin et al [I-26]. Some important findings are summarized in the following:

- The mean CDF for seismic events ranged from 1 10-6 to 1 10-5 per year; the uncertainty bounds were about 2 to 4 orders of magnitude (10-1);
- The importance of walkdown to identify seismic vulnerabilities in operating plants cannot be overemphasized;
- Peer review is found to be essential to validate the analyst’s judgments and to assure the reasonableness of the risk results and insights;
- The significant seismic risk contributors are typically electrical equipment, tanks and unreinforced (or lightly reinforced) masonry walls. However, each plant has its own unique features making a detailed seismic PSA useful to identify the risk contributors for any needed seismic upgrading;
- Seismic hazard at the site (both the mean value and the shallow slope of the seismic hazard curve) has a profound influence on the seismic CDF;

The uncertainty in seismic hazard typically drives the uncertainty bounds in the seismic CDF;

- Close interaction between the systems analyst, fragility analyst and hazard analyst is essential to ensure realistic estimate of seismic CDF;
- Sensitivity studies are helpful to identify the need and extent of seismic upgrading of equipment and structures in the plant.

6.2. Maturity of seismic PSA

Although seismic PSA has a long record with over 50 % of the operating nuclear power plants in the US and many nuclear power plants in the UK, the Republic of Korea, Taiwan, Switzerland, Finland, Czech Republic, Hungary and Slovenia, questions on maturity of seismic PSA compared to the internal event PSAs are still often raised. The main reason is that the seismic PSA requires input from and participation of experts in the specialty areas of seismic hazard and fragility. Internal event PSAs have been conducted by larger groups of analysts, and have been more extensively reviewed and debated in public forums.

Seismic hazard analysis is conducted with limited amount of recorded data on earthquake occurrences; this is supplemented by seeking opinions of multiple experts. With each new hazard study, increases in the perceived seismic hazard are observed. Seismic fragility evaluation has been conducted over the years by a small group of specialists; although many engineers have been trained in this area, very few have had the opportunity to perform the fragility analysis. Unlike the internal event PSA, different elements of a seismic PSA have large epistemic uncertainties making the "point estimates of CDF and LERF" meaningless and necessitating uncertainty propagation. Many systems analysts are not familiar with this aspect nor have the software to do a credible job.

Nevertheless, it could be contended that seismic PSA is a very mature activity; databases, methods and standards exist for performing different elements of the seismic PSA. Maturity of seismic PSA in any Member State can only be accomplished by publishing the studies, having peer reviews by international experts and promoting open debates among the practitioners.

7. USE OF SEISMIC PSA IN DESIGN OF NEW REACTORS

Seismic PSA could be used in the design of "new" nuclear power plants. Applications of this use could be seen in the design certification of advanced reactors (e.g., ABWR, AP-1400, etc.), in the seismic assessment of the Kashiwazaki 6 and 7, and the Lungmen nuclear power plant in Taiwan.

Seismic PSA of new nuclear power plants is conducted at different stages of the plant life starting with the conceptual design, detailed design and installation, and operation. The objectives are to ensure that the plant meets the seismic safety goals and to identify any system-level and component-level vulnerabilities that could be overcome early in the plant design. The seismic PSA is therefore to be treated as a living PSA. It is also important to establish realistic and plant-specific baseline CDF and LERF in order to facilitate any risk-informed applications in the future. It is useful that this seismic PSA be conducted to meet the industry standard on external event PSA, such as ANS 58.21-2003.

The three stages of seismic PSA are described in the following. Each succeeding stage makes use of the information collected and models developed in the previous stage(s).

7.1. Stage 1: Preliminary Safety Analysis Report (PSAR)

- Select the plant SSE (or design basis earthquake) — may not meet R.G. 1.165;
- Conduct a probabilistic seismic hazard analysis for the site using the state of the art methodology (at least meeting the Capability Category II of the ANS Standard ANSI/ANS-58.21-2003 [I-7]);
- Select seismic design basis (design criteria and qualification criteria) — this may be standard review plan;
- Based on the preliminary design of safety systems, develop a seismic PSA model (i.e. event trees and fault trees) and derive the seismic equipment list for seismic PSA;
- For each item on seismic evaluation list (SEL), develop seismic fragility assuming that the component will be seismically qualified to meet IEEE requirements, and the anchorage will meet the design codes like ACI –349, 359 and ASME. This is called "reasonably achievable fragility". One may use EPRI ALWR Utility Requirements Document;
- Quantify the system model and estimate CDF and LERF using the seismic hazard at the site and the seismic fragilities; develop the complete probability distributions on CDF and LERF;
- Compare with seismic portion of the safety goals to verify acceptability;
- Identify system level seismic vulnerabilities that could be resolved in this stage (e.g. adding redundant sources of water, etc.) and examine if certain systems/ components could be made

stronger by changing the design criteria (e.g. raising the test level for some important electrical components).

7.2. Stage 2: Full Safety Analysis Report (FSAR)

- Revise the fragilities using “as designed and tested” information;
- Recalculate CDF and LERF and uncertainties;
- Identify dominant seismic risk contributors;
- Examine the risk benefits of selective upgrading, since the installation is still ongoing.

7.3. Stage 3: Plant is about to start operation

- Perform a walkdown to confirm installation is proper and that there are no potential interaction concerns;
- Recalculate the seismic fragilities if needed;
- Establish a baseline seismic CDF and LERF along with uncertainties for future risk-informed applications and risk management.

8. CONCLUSION

Seismic probabilistic safety assessments (PSA) have been conducted for over 50 nuclear power plants worldwide in the last 25 years. The methodology has been well established and the necessary data on the parameters of the PSA models have been generally collected. In response to the need for risk-informed decisions, a US national standard (ANS, 2003) on external event PSA has been developed which prescribes the standard requirements for different elements of a seismic PSA.

Although seismic PSA has a long record with over 50% of the operating nuclear power plants in the US and many nuclear power plants in the UK, the Republic of Korea, Taiwan, Switzerland, Finland, Czech Republic, Hungary and Slovenia, questions on maturity of seismic PSA compared to the internal event PSAs are still often raised. The main reason is that the seismic PSA requires input from and participation of experts in the specialty areas of seismic hazard and fragility. Internal event PSAs have been conducted by larger groups of analysts, and have been more extensively reviewed and debated in public forums.

Nevertheless, it could be contended that seismic PSA is a very mature activity; databases, methods and standards exist for performing different elements of the seismic PSA. Maturity of seismic PSA in any Member State can only be accomplished by publishing the studies, having peer reviews by international experts and promoting open debates among the practitioners.

REFERENCES

[I-1] Nuclear Regulatory Commission, PRA Procedures Guide Vol. 2. NUREG/CR-2300 Washington D.C. (1983).

[I-2] KENNEDY, R.P. RAVINDRA, M.K., Seismic fragilities for nuclear power plant risk studies, Nuclear Engineering and Design, Vol. 79, No. 1 (May 1984) pp 47–68.

[I-3] REED, J.W., KENNEDY, R.P., Methodology for developing seismic fragilities, EPRI TR-103959, Research Project RP2722-23, prepared for Electric Power Research Institute, Palo Alto, California (August 1993).

[I-4] RAVINDRA, M.K., Seismic risk assessment, in Probabilistic Structural Mechanics Handbook — Theory and Industrial Applications, Editor C. (Raj) Sundararajan, Chapman and Hall, Chapter 19, (1995).

[I-5] BUDNITZ, R.J. et al., Recommendations for probabilistic seismic hazard analysis: guidance on uncertainty and use of experts, NUREG/CR-6372, U.S. Nuclear Regulatory Commission, Lawrence Livermore National Laboratory, Livermore, California (1997).

[I-6] KENNEDY, R. P., Overview of methods for seismic PRA and margin analysis including recent innovations, (Paper presented at OECD/NEA/JAERI Workshop on Seismic Risk, Tokyo, Japan, August 1999).

[I-7] External – events PRA methodology, American National Standard, ANSI/ANS-58.21-2003, ANS, La Grange Park, Illinois (2003).

[I-8] CORNELL, C.A., Engineering seismic risk analysis, Bulletin of Seismological Society of America, 58:1583-1606 (1968).

[I-9] REITER, L., Earthquake hazard analysis: issues and insights, Columbia University Press, New York (1990).

[I-10] SPRA implementation guide, Final Report co-authored by D. Wakefield, M. Ravindra, K.L. Merz and G.S. Hardy (ABS Consulting) for the Electric Power Research Institute (December 2003) Electric Power Research Institute (EPRI), Palo Alto, California (2003).

[I-11] Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME 2002, New York, ASME RA-S-2002.

[I-12] NEWMARK, N.M., Inelastic design of nuclear reactor structures and its implications on design of critical equipment, SMiRT Conference (Paper presented at Int. Conf., San Francisco, California, August 1997) SMiRT Paper K 4/1.

[I-13] RIDDELL, R., NEWMARK,N.M., Statistical analysis of the response of non-linear systems subjected to earthquakes, Department of Civil Engineering, Report UILU 79-2016, University of Illinois, Urbana, Illinois (August 1979).

[I-14] A Methodology for assessment of nuclear power plant seismic margin, Electric Power Research Institute, Palo Alto, California, EPRI NP-6041-SL, Rev. 1 (August 1991).

[I-15] Generic implementation procedures (GIP) for seismic verification of nuclear plant equipment, Rev. 2, Seismic Qualifications Utility Group (SQUQ, Washington, D.C. February 4, 1992).

[I-16] BANDYOPADHYAY, K.K. et al., Seismic fragility of nuclear power plant components (Phase II) motor control center, Switchboard, Panel Board and Power Supply, NUREG/CR-4659, Vol. 2, Brookhaven National Laboratory, Upton, New York (December 1987).

[I-17] BANDYOPADHYAY, K.K. et al., Seismic fragility of nuclear power plant components (Phase II) switchgear, I&C panels (NSSS) and Relays, NUREG/CR-4659, Vol. 3, Brookhaven National Laboratory, Upton, New York (February 1990).

[I-18] HOLMAN, G.S., CHOU, C.K., Component fragility research program: Phase I component prioritization, NUREG/CR-4899, Lawrence Livermore National Laboratory, Livermore, California (1986).

[I-19] HOLMAN, G.S., CHOU, C.K. Component fragility research program: Phase I demonstration tests, NUREG/CR-4900, Lawrence Livermore National Laboratory, Livermore, California (1986).

[I-20] HOLMAN, G.S., CHOU, C.K. Using component test data to develop failure probabilities and improve seismic performance, 3rd Symposium on Current Issues Related to Nuclear Power Plant Structures, Equipment, and Piping (Paper presented at Int. Conf , Orlando, Florida, December 1990).

[I-21] MERZ, K.L., Generic seismic ruggedness of power plant equipment, EPRI NP-5223 (Prepared by ANCO Engineers for the Electric Power Research Institute), EPRI NP-5223, Palo Alto, California.

[I-22] CAMPBELL, R.D., RAVINDRA, M.K., MURRAY R.C. Compilation of fragility information from available probabilistic risk assessments, UCID-20571 Rev. 1, Lawrence Livermore National Laboratory, Livermore California (1988).

[I-23] ELLINGWOOD, B. Validation of seismic probabilistic risk assessments of nuclear power plants, NUREG/GR-0008, The Johns Hopkins University, Baltimore, Maryland (January 1994).

[I-24] RUBIN, A.M., et al., An update of preliminary perspectives gained from individual plant examination of external events (IPEEE) (Submittal reviews presented at the ASME Conference, San Diego, California, July 1998).

[I-25] RAVINDRA, M.K., TIONG, L.W., Comparison of methods for seismic risk quantification, Proc. of 10th International Structural Mechanics in Reactor Technology Conference, Anaheim, California (August 1989).

[I-26] WELLS, J.E., CUMMINGS, G.E. AND GEORGE L.L., Seismic safety margins research program, Phase I final report, Systems analysis (project VII), NUREG/CR-2015, vol. 8, Lawrence Livermore National Laboratory, Livermore, California (1981).

ANNEX II

CONSIDERATION OF EXTERNAL HAZARDS AND UNCERTAINTIES IN THE DESIGN OF AN NPP

A.K. GHOSH, H.S. KUSHWAHA
Bhabha Atomic Research Centre, Mumbai, India

Abstract

This paper is dedicated to advances in seismic hazard analysis. In line with the recent US NRC Regulatory Guide, it presents the uniform hazard response spectra (UHRS), i.e. the response spectra having the same mean recurrence interval (MRI), or equivalently, the same probability of exceedence (P) in a specified span of time at all frequencies for the Tarapur Atomic Power Station Site. The present paper develops these spectra considering linear and point sources of earthquakes. The approaches to some other external events are outlined also.

Key words: Earthquakes; Seismic hazard; Faults; Lineaments; Line and point sources; Peak ground acceleration; Response spectrum; Mean recurrence interval; Probability of exceedence; Seismic risk; Magnitude-frequency relationship; Uniform hazard response spectrum.

1. INTRODUCTION

Safety of a nuclear power plant has to be ensured against various events of internal or external origin. The external events may be human-induced or natural. Earthquake is one of the important external events. The design basis earthquake ground motion is generally specified by normalized response spectra (also known as response spectral shapes or the dynamic amplifications factors, DAFs) for a peak ground acceleration (PGA) and various values of damping, as dictated by the local geological and tectonic features and data on past earthquakes. The design basis earthquake ground motion is obtained by a statistical analysis of a large number of records having earthquake parameters in the range of interest and selecting a shape with an acceptable value of the probability of exceedence.

Various uncertainties and randomness associated with the occurrence of earthquakes and the consequences of their effects on NPP components and structures call for a probabilistic seismic risk assessment (PSRA). Seismic hazard analysis for the site is a key element of the PSRA [II-1].

In the traditionally adopted approach [II-2, II-3], the probability of exceedence of the spectral shape is with respect to the database from which it has been derived and is not related with the temporal or spatial distribution of earthquakes. The probability of exceedence of the PGA is, however, evaluated considering the spatial and temporal distribution of earthquakes.

The new Standard Review Plan (SRP) [II-4] and Regulatory Guide [II-5] of the US NRC recommend development of the unnormalized response spectra. The US NRC [II-5] further proposes to carry out a probabilistic seismic hazard analysis (PSHA) based on uniform hazard response spectra (UHRS).

The present work aims to develop the UHRS, i.e. the response spectra having the same mean recurrence interval (MRI), or equivalently, the same probability of exceedence (P) in a specified span of time at all frequencies for the Tarapur Atomic Power Station Site.

2. THEORY

Ghosh et al. [II-6, II-7] extended the method of Cornell [II-2] to spectral acceleration for line and point sources of earthquakes considering a generalized form of correlation. This methodology is applied to determine a uniform hazard response spectrum.

3. SEISMIC HAZARD ANALYSIS

The seismic hazard is presented in the form of UHRS for specified values of MRI and/ or P. The analysis requires development of a frequency-dependent attenuation relation for spectral acceleration, a magnitude-frequency relation, an earthquake arrival model and the evaluation of MRI and P considering all seismogenic sources in the area under consideration.

4. ATTENUATION RELATIONSHIP FOR SPECTRAL ACCELERATION

The present regulatory documents [II-4, II-5] require the ground motion to be presented as the unnormalized response spectrum itself, without scaling it to PGA. Attenuation relation has been developed for the unnormalized response spectrum [II-6].

The response spectral acceleration is assumed to be of the same form as given by equation (1), i.e.:

$$S = S(M, R, \zeta,.T) = b_1 \exp(b_2 M)\ (R+D)^{-b}3, \qquad (1)$$

where: M is the magnitude and R is the hypo-central distance; D is a distance correction factor; ζ is the value of damping; and T is the period for which the response spectrum is being evaluated. The constants, b_1, b_2, and b_3 depend on ζ and T.

Magnitude –frequency relation

The number of earthquakes of the magnitude greater than or equal to M occurring annually is given by the Richter's equation:

$$\log_{10} N_M = a - bM, \qquad (2)$$

where *a* and *b* for a given region are determined from the earthquake occurrence records of that region.

Line source model

Earthquakes occur along faults, which are generally linear features or represented as linear features (lineaments). It is assumed that earthquakes are equally likely to occur anywhere along the length of a fault (lineament).

Considering the effect of all possible values of the focal distances, the cumulative probability $P[S \geq S_d]$ is obtained:

$$P(S \geq S_d) = \int_d^{r_0} P[S \geq S_d | R = r] f(r) dr$$

$$= C\ S_d^{\frac{-\beta}{b_2}}\ G \qquad (3)$$

where $f_R(r)$ is the probability density function of finding an earthquake at a radius *r*; the G values for various types of fault orientations are presented in [II-6];

$$C = e^{\beta M_0} b_1^{\frac{\beta}{b_2}}$$

and β = b ln10.

Equation (3) yields the probability that the spectral acceleration (for given values of damping and period) at a site, S will exceed a certain value, S_d, given that an event of interest ($M \geq M_0$) occurs anywhere on the fault:

If certain events are Poisson arrivals with average arrival rate ν, and if each of these events is independently, with probability P, a special event, then these special events are the Poisson arrivals with average annual arrival rate (p ν). The probability, $P_{i,}$ that any event of interest $M \geq M_0$ will be a special event is given by equation (3).

The annual probability of exceedence of $S_{max} > S_d$ is:

$$1-F_{ap}=1-\exp(-C\nu\, G\, S_d^{\;-\beta/b_2})$$

$$=C\nu\; G\; S_d^{\;-\beta/b_2} \qquad (4)$$

The mean recurrence interval (T_y) of the spectral acceleration S_d is then the reciprocal of (1 - F_{ap}), i.e.

$$T_y = \frac{1}{C\nu G}\; S_d^{\frac{\beta}{b_2}} \qquad (5)$$

The probability of exceedence of S_d in a given span of *t* years is:

$$P=1-\exp(-t/T_y) \qquad (6)$$

The seismic hazard at a site is quantified by the probability (P/S >S_d) and the T_y, and the uncertainties in these quantities due to variations in the correlations for spectral acceleration and uncertainties in the seismic source and occurrence models, i.e. *a* and *b*, depth of focus, *h*.

Point source model

When there are clusters of earthquakes away from the site, each cluster could be modelled as a point source of earthquakes. In case of a single point source, there is no randomness with respect to the location of the earthquake, hence, for a specified value of spectral acceleration, the magnitude is also fixed by the chosen correlation for spectral acceleration. The probability of exceedence of the specified value of spectral acceleration is therefore decided by the temporal distribution of earthquakes. The results for a point source are presented in [II-6].

Multiple line and point sources

When there are a number of line or point sources, the probability of non-exceedence of a specified value of spectral acceleration is obtained by multiplying the probability of non-exceedence of the specified value of spectral acceleration from each of the sources, i.e.,

$$p[S_{\max} \leq S_d] \;=\; \prod_{i=1}^{NS} p[S_{\max} \leq S_d]_{from\,the\,ith\,source}$$

$$=\exp[-\sum_{i=1}^{NS} C_i\; S_d^{\frac{-\beta_i}{b_{2i}}}\; G_i\;\; \nu_i] \qquad (7)$$

5. PRESENT STUDY

Base case

The geological, tectonic and seismic study for the site was earlier carried out to develop the design basis ground motion [II-9]. The lineament map is presented in Fig. II-1. Each of the lineaments shown in the circle of 300-km radius around the site has been considered as a line source. The lengths of the lineaments and their distance from the site have been obtained from this map. Figure II-1 also shows some of the epicentres of earthquakes.

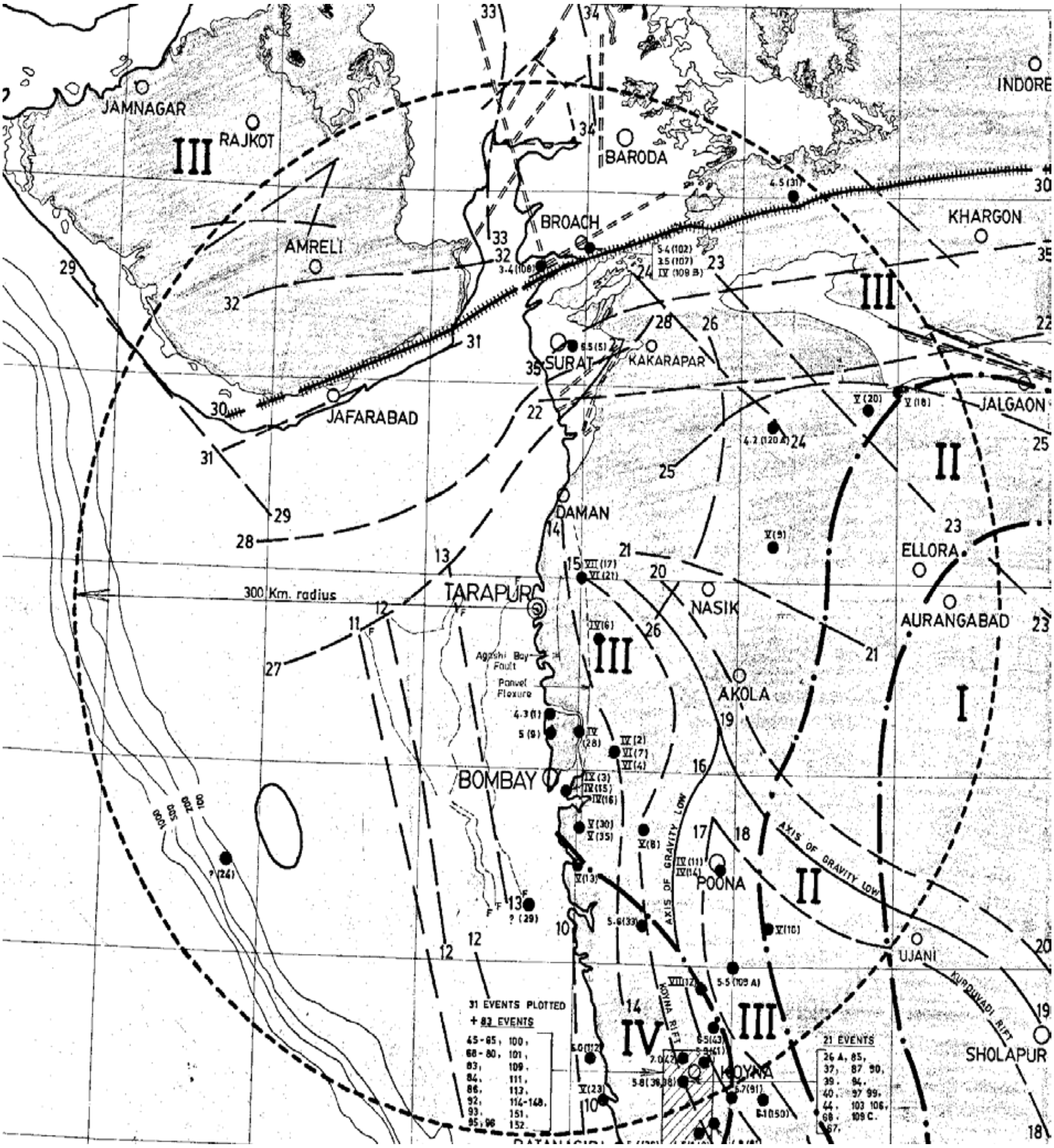


FIG.II-1. Tectonic map of the Tarapur site.

The present study uses 144 horizontal acceleration records from rock sites to develop attenuation relation for the response spectral acceleration [II-6]. The range of magnitude is generally from 4.1 to 8.1, and there are few records of magnitude lower than 4.1. The distance from the fault varies generally about from about 6 km to 125 km. The salient features of the accelerograms are given in [II-6]. The digitized accelerograms were obtained on magnetic tapes from the World Data Center [II-8]. In these data, the original accelerograms have been band-pass filtered between 0.07 Hz and 25 Hz, and base line corrections have been made. Analysis has been carried out with the recorded accelerograms representing the free-field conditions. The geological conditions of the recording sites, identified by the name and number of the recording stations, were verified from published sources.

The attenuation relations thus developed were used for the development of uniform hazard response spectra.

Earthquake data for the period 1504-2001 AD have been obtained from various catalogues available as published literature (global sources). Data have also been obtained from the Gauribidanur Seismic Array (GBA) of Bhabha Atomic Research Centre for the period 1977-1995 AD. Broadly, the data from both sources can be viewed as: (i) those for the Koyna area (Fig. II-1) and (ii) those for other areas. The first recorded earthquake from Koyna is in the year 1965. The magnitude –frequency relationships for the earthquake data from global sources are presented in Figs. II-2a and II-2b. The figures include the observed data and results of an earlier study by Ravi Kumar et al. [II-10]. A least a square fit of the data was carried out (see equation (3)) and the constant of the equation (‘a’ value) was increased to obtain a modified fit to envelope the observed data which is also included in the figures.

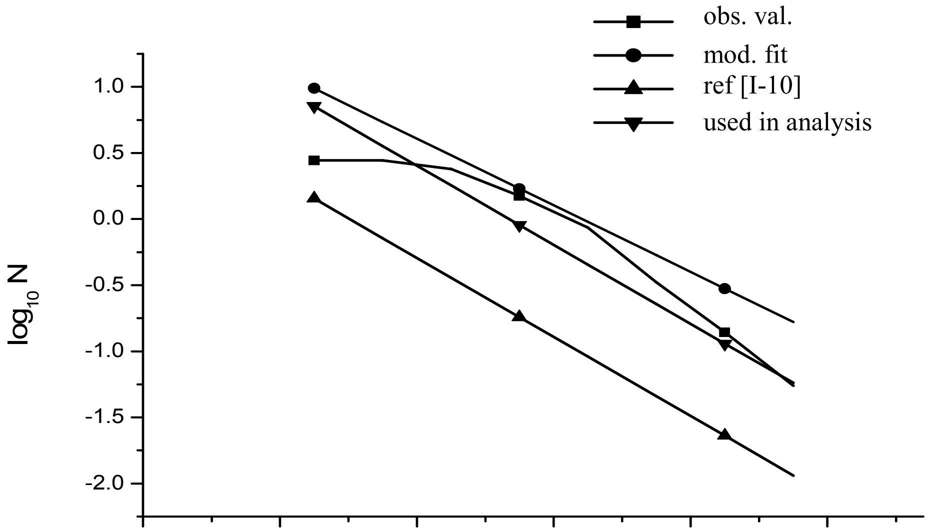


FIG. II-2a. Magnitude-frequency relationship: Koyna data (global sources).

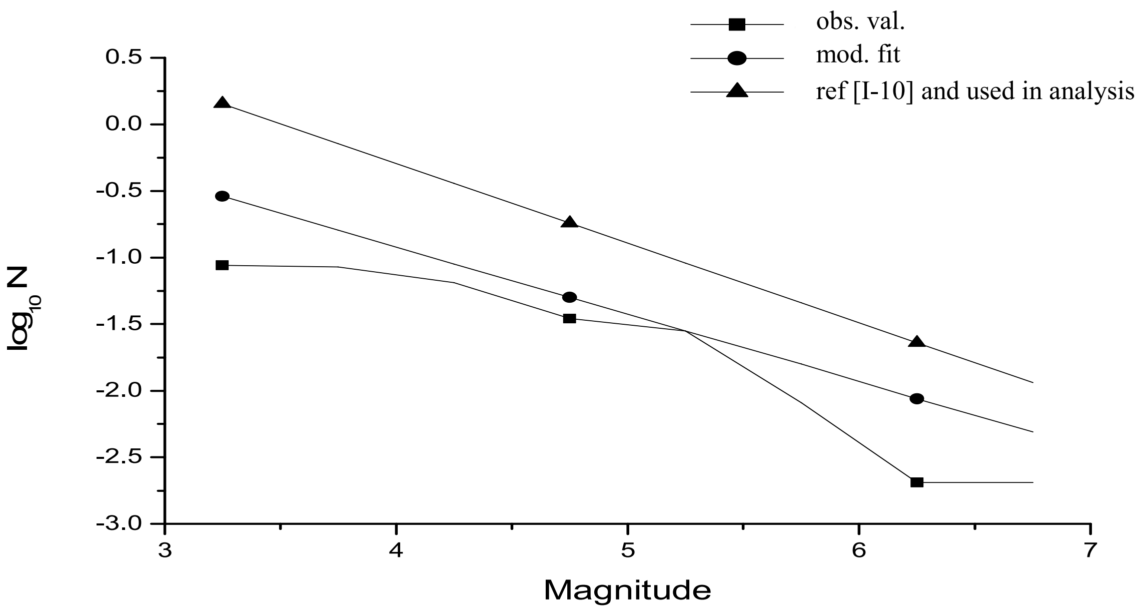


FIG. II-2b. Magnitude-frequency relationship: other data (global sources).

The 'a' and 'b' values obtained from [II-10] yield a rather non-conservative value of the occurrence rates of earthquakes in the Koyna region. Based on all the data, a realistic set of values have been used for obtaining the UHRS which is close to the least square fit and conservative for the magnitude range M > 6, which produces acceleration in the range of interest for design. The least square analysis showed a large variation of 'a' values obtained from the earthquake data from global sources and GBA (see Table II-1). The variation of 'a' for Koyna earthquakes was, however, not significantly large. The 'a' and 'b' values obtained from various studies are presented in Table II-1.

TABLE II-1. MAGNITUDE–FREQUENCY RELATIONSHIPS

Data	KOYNA AREA		OTHER AREAS		REMARKS
	a	b	a	b	
Global	2.63	0.505	1.10	0.505	Least square fit data modified to envelope the observed values
GBA	2.794	0.505	1.785	0.505	Least square fit data modified to envelope the observed values
Ref. [II-10]	2.1016	0.5989	2.1016	0.5989	
Base values	2.8	0.5989	2.1016	0.5989	Base values used in the analysis (see Fig. II-2)

The Koyna earthquakes occur in a small cluster. These earthquakes are assumed to be generated from a point source. The 'a' and 'b' values for all line sources are assumed to be the same.

The analysis has been carried out considering a maximum magnitude of 6.5 (reference value) for earthquakes occurring in the region under study [II-10].

Sensitivity study

Uniform hazard response spectra (UHRS) have been generated for the reference values of the various parameters mentioned in the foregoing. A sensitivity study has been carried out to account for uncertainties or variations in these parameters. UHRS have been generated by considering ± 10% variation in the values of *a* and *b*, the distance of the lineament/point source from the site, depth of focus and the length of the lineaments. While one parameter was varied, the other parameters were held at their reference values. UHRS were generated considering a maximum magnitude of 7.

6. NUMERICAL RESULTS

The design response spectra developed in the traditional way will have different values of MRI (or P) at various frequencies. Figures II-3a and II-3b show the variation of MRI of the spectral acceleration for an operating basis earthquake (OBE) and safe shutdown earthquake (SSE) as a function of frequency.

Figures II-4 (a-f) show the variation of MRI and the probability of exceedence in 50 years as a function of PGA. When one parameter is varied, all other parameters are held at their reference values.

Figure II-4a presents the variation of MRI and P with PGA for the maximum magnitudes of 6.5 (reference case) and 7. As the maximum magnitude increases, the value of PGA for the same MRI also increases.

Figure II-4b considers the effect of depth of focus. Results are presented for the depth of focus of 20 km (reference case) and 18 km (90% of the reference value) for all sources.

Figure II-4c results presents results for the reference values of the distance of the seismic sources from the site, as well as those assuming each source distance is reduced by 10%. Again, the value of PGA for the same MRI increases with the reduction in depth of focus or the distance from the site.

Figure II-4d shows the results of variation in the length of the lineaments. It may be noted that the asymptotic value of PGA remains unaffected by the length of the lineament as long as the maximum magnitude, depth of focus and the shortest distance from the site are unchanged.

Figures II-4e and II-4f present the sensitivity of results to the variations in *a* and *b*. A variation of 10% is considered on either side of the reference values of *a* and *b*.

Figures II-5a and II-5b present the UHRS for various values of MRI and the probability of exceedence, with all other parameters being kept at their base values. The spectral acceleration at any frequency increases with a decrease of the probability of exceedence. From the earlier studies [II-6] it has been observed that for a single source, as the distance from the fault (Δ) increases, the value of the spectral acceleration for a fixed MRI decreases. Similarly, for a fixed MRI, the spectral acceleration decreases with an increase of l, the length of the fault. At smaller values of l, all earthquakes are concentrated in a small zone around the site, so that for a given value of MRI, the spectral acceleration will be higher than that when earthquakes are likely to occur over a wider range of distances. As l increases, the results tend to become asymptotic. Distant earthquakes affect motion in a 0.5 s – 2 s range of periods. As one moves away from the site, an earthquake of a higher magnitude would be required to generate the same spectral acceleration at the site. Thus, the value of MRI for the specified spectral acceleration will be higher.

A higher value of '*a*' or a lower value of '*b*', with other parameters remaining unchanged, would imply a higher value of '*M*', leading to a higher value of spectral acceleration.

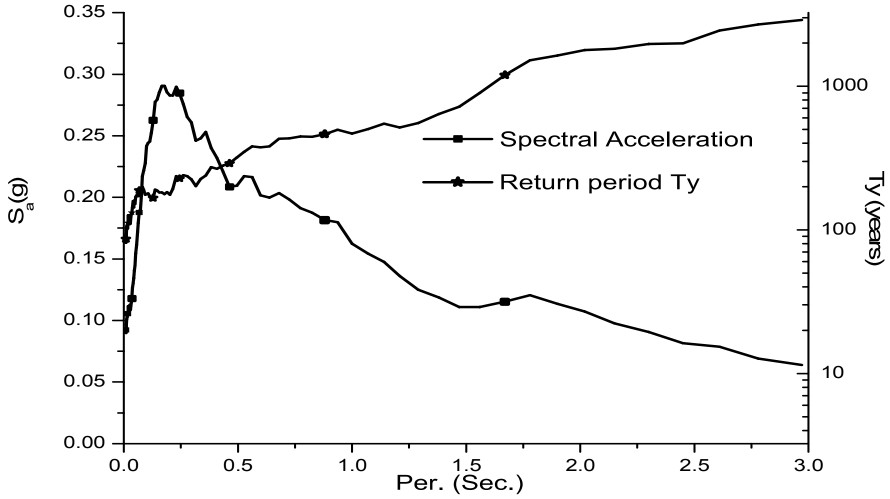


FIG. II-3a. Return period at various frequencies (periods) for the OBE design response spectrum; 5% damping; horizontal.

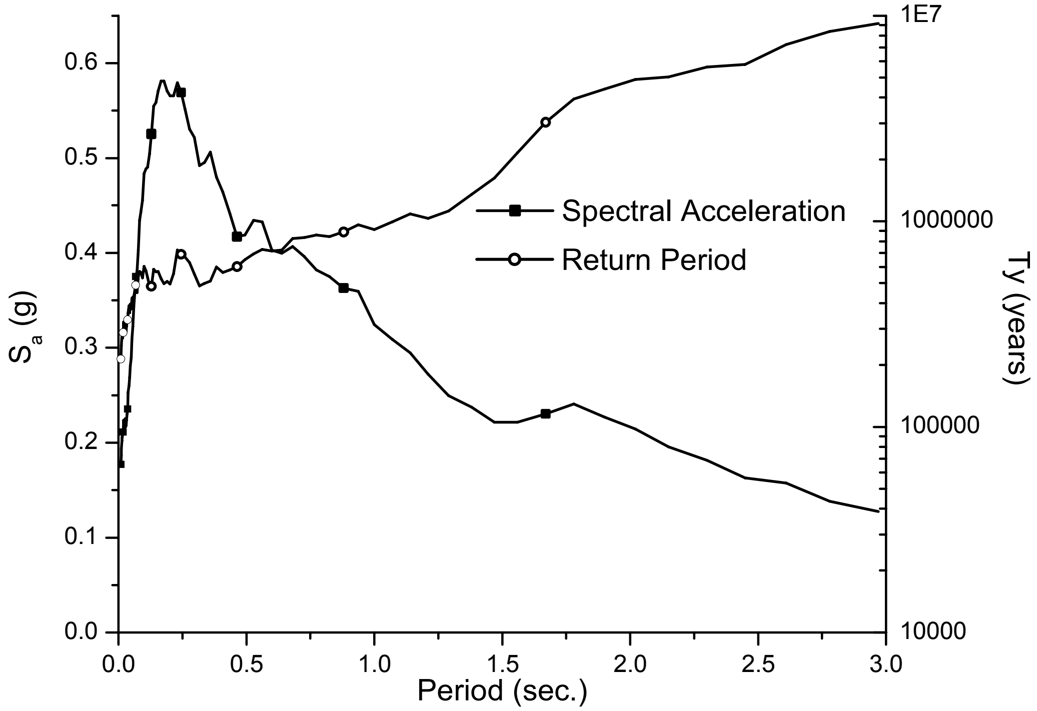


FIG. II-3b. Return period at various frequencies (periods) for the SSE design response spectrum; 5% damping; horizontal.

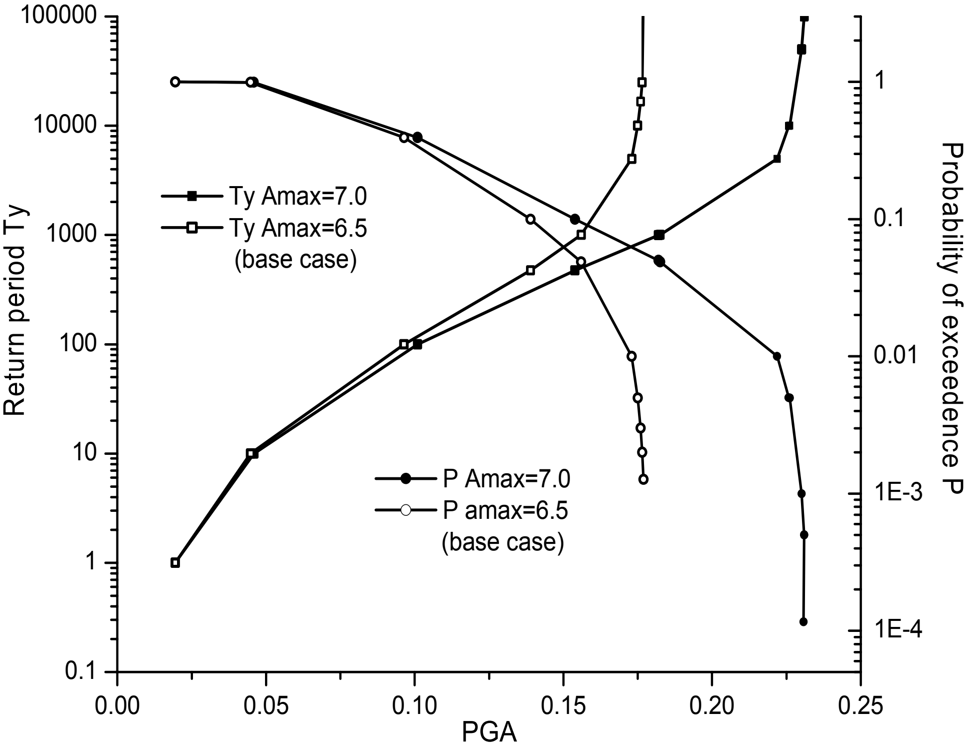


FIG. II-4a. Return period and probability of exceedence vs. PGA for M_{max}=7.0 and M_{max}=6.5 at the Tarapur site.

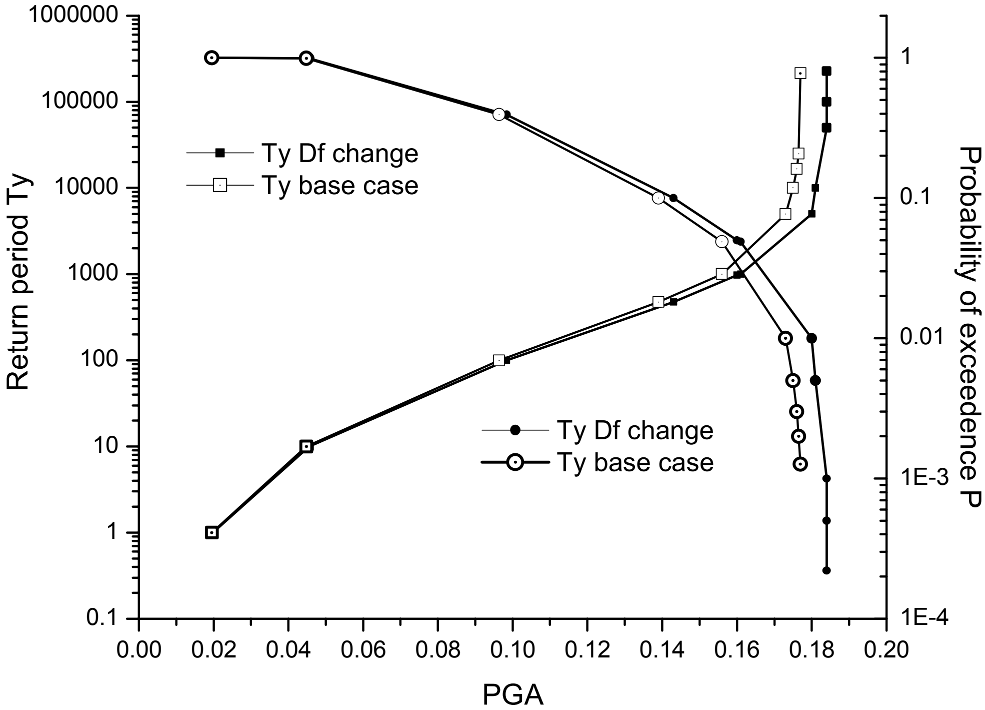


FIG.II-4b. Return period and probability of exceedence vs. PGA for different depth-of-focus values at the Tarapur site ('Df change' means that the depth of focus value is 0.9 of that in the reference case).

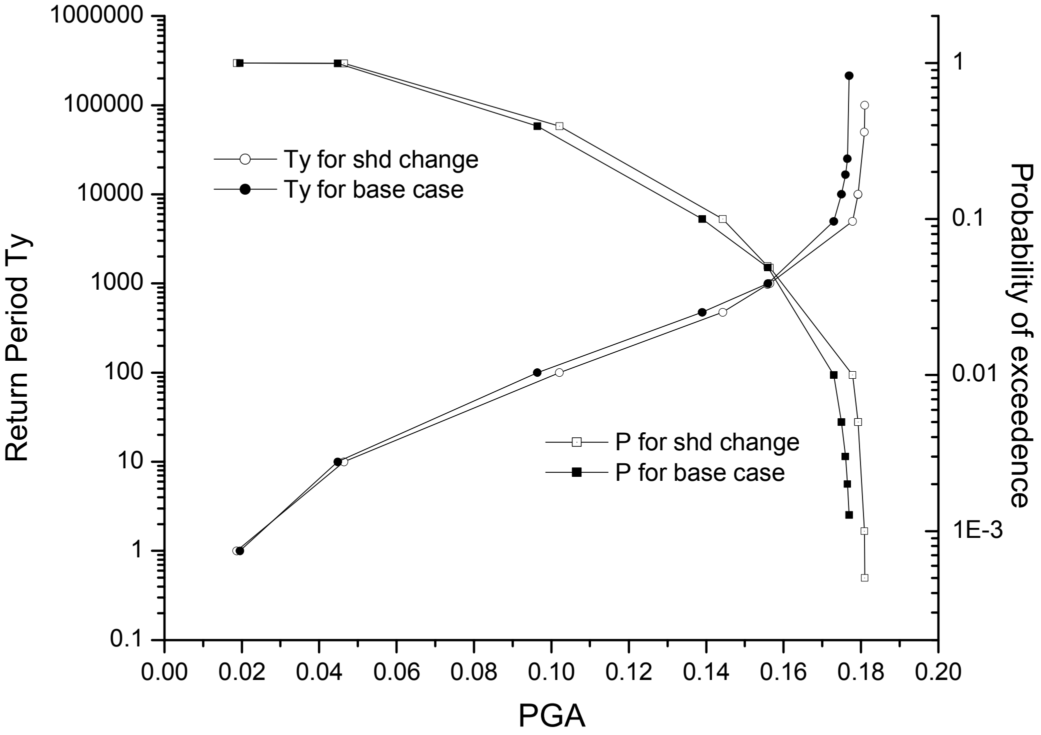


FIG.II-4c. Return period and probability of exceedence vs. PGA for the reference ('base case') and the reduced (by 10%; 'shd change') values of the distance of the seismic sources from the Tarapur site.

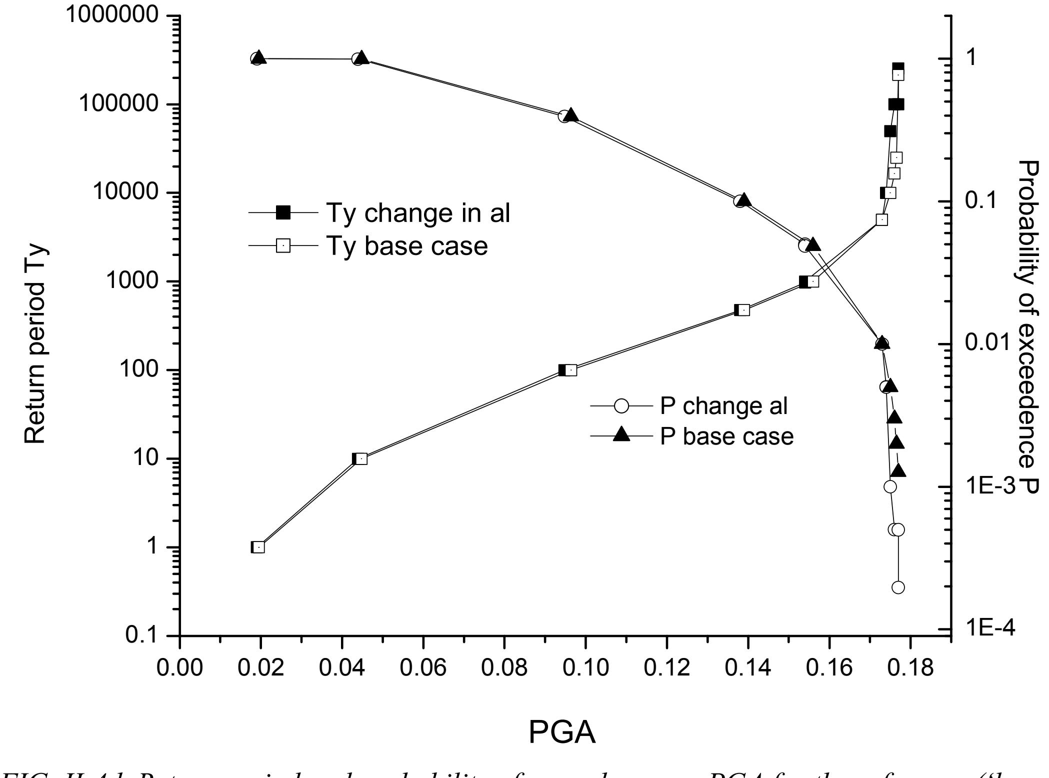


FIG. II-4d. Return period and probability of exceedence vs. PGA for the reference ('base case') and changed ('change al') lengths of lineaments; the Tarapur site.

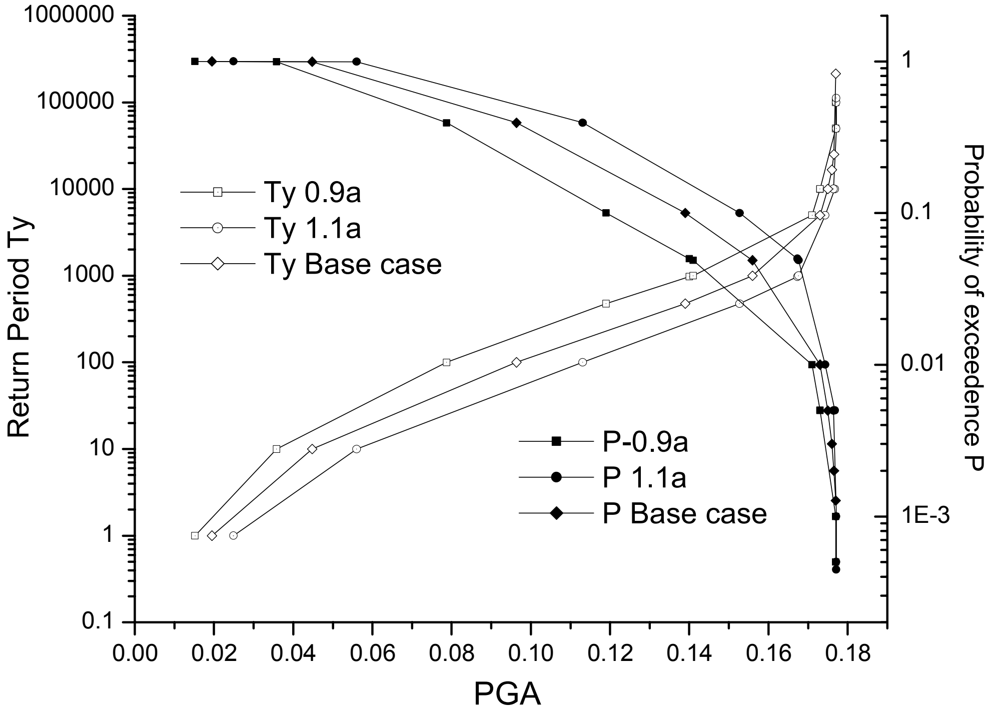


FIG. II-4e. Return period and probability of exceedence vs. PGA for different 'a' values; the Tarapur site.

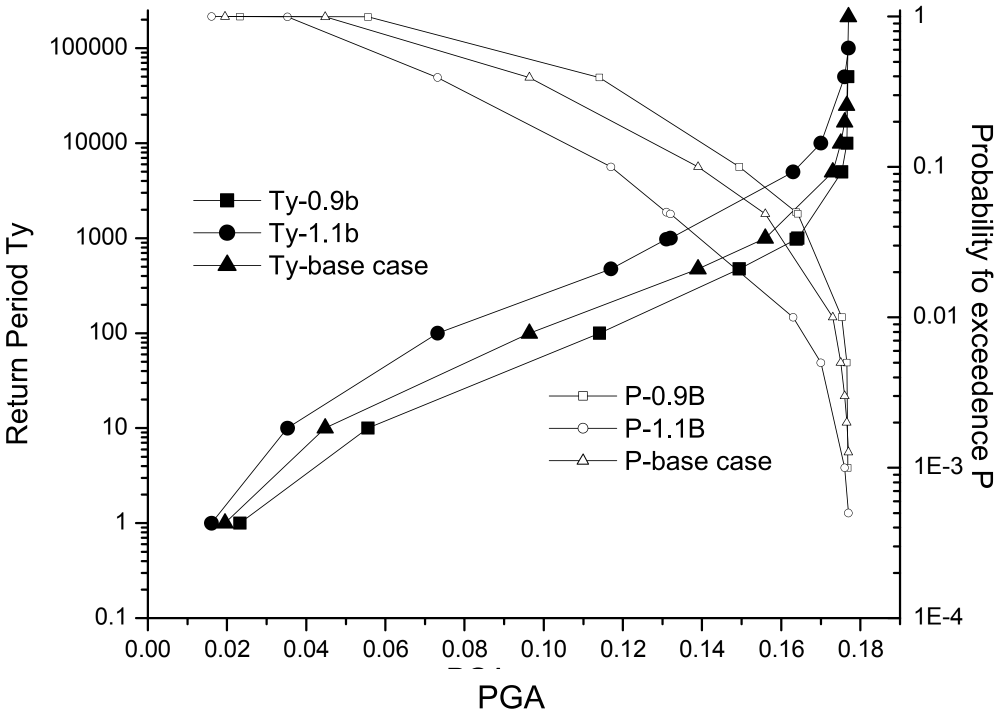


FIG. II-4f. Return period and probability of exceedence vs. PGA for different 'b' values; the Tarapur site.

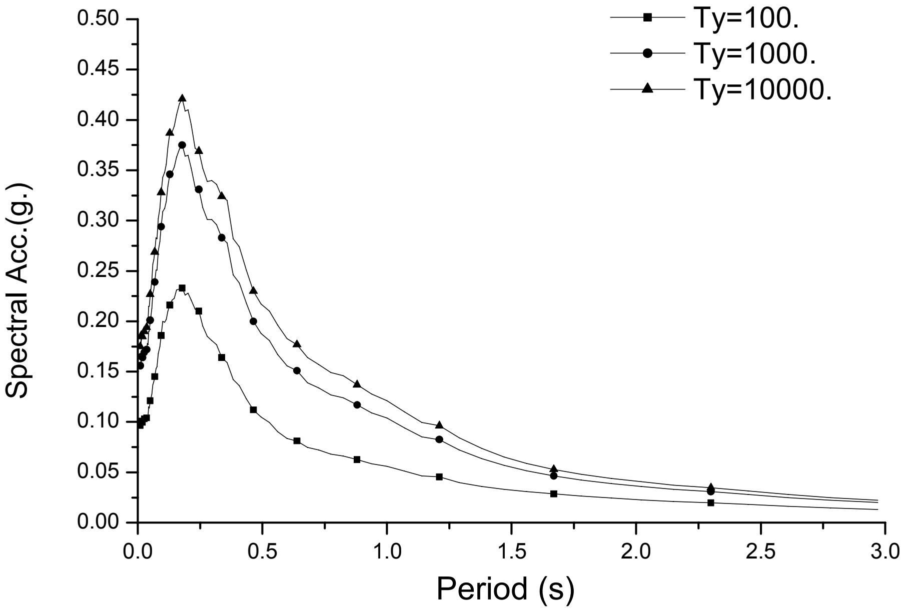


FIG. II-5a. UHRS vs. frequency (period) for different values of MRI.

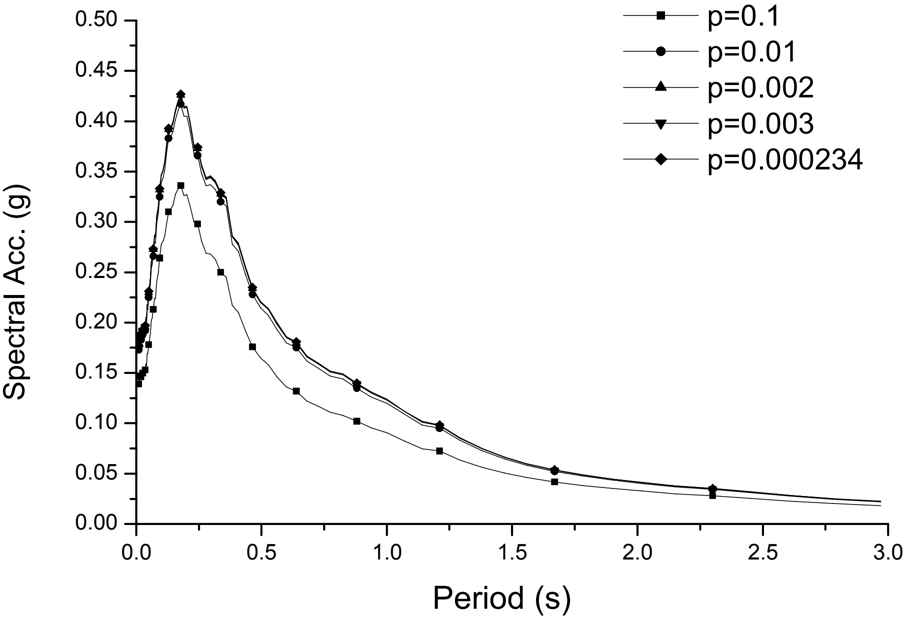


FIG.II-5b. UHRS vs. frequency (period) for different values of P.

7. AIRCRAFT CRASH HAZARD

In view of possible significant impact on NPP safety, the potential for aircraft crashes in the region of a proposed NPP should be considered in site evaluation [II-11]. In the initial stage of site selection, a simple screening based on Screening Distance Value (SDV) can be applied. SDV may be arrived at for events so that the probability of adverse impact on the NPP on account of events taking place beyond such distances will be less than the screening probability level (SPL). Events having a probability of occurrence less than the SPL need not be considered. A value of 10^{-7} per year is considered for SPL. A probabilistic evaluation of a spectrum of aircraft hazards is carried out, and a conservative SDV is arrived at by considering the following parameters: (i) distance from the airport to the site; (ii) types and frequency of air traffic corridors and air route crossings; and (iii) existing crash statistics. The SDVs adopted in India with respect to an aircraft crash hazard are given in Table II-2, with reference [II-12] being the source of these data.

TABLE II-2. SCREENING DISTANCE VALUES (SDVs) FOR AIRCRAFT CRASH HAZARD

INSTALLATION	SDV (km)
Large airport	8
Small airport	5
Military airfield	15

At the same time, as part of safety evaluation programme, Indian containment structures have also been assessed for beyond design basis accidents such as an aircraft impact load. The analysis of an external missile impact can be performed by uncoupling the problem, in which the missile is assumed to crash on a rigid surface, as recommended in the Agency guidelines. The procedure assumes uncoupling the missile and the target structure therefore the impact load is generated from the impact energy and crushing strength of the missile. The influence of target deformation is assumed to be small as this assumption is conservative for the evaluation of load time history. The loading time history is generated for various categories of aircrafts, such as Boeing 707-320, 707-720, 737, and Airbus family A300B2-200, A300B2-100, A300B4-200, and A310-202. A summary of the results obtained is presented in [II-13].

8. CONCLUSION

The paper presents a methodology and calculation results of the uniform hazard response spectra (UHRS), i.e. the response spectra having the same mean recurrence interval (MRI), or equivalently, the same probability of exceedence (P) in a specified span of time at all frequencies, for the Tarapur Atomic Power Station Site. These spectra have been produced considering linear and point sources of earthquakes. It is further recognized that the predicted seismic hazard can vary with various parameters involved. Numerical results are presented to show this variability. These results will help determine the seismic hazard and associated uncertainties at the considered site.

REFERENCES

[II-1] KENNEDY, R.P., RAVINDRA M.P. Seismic fragilities for nuclear power plant hazard studies, Nuclear Engineering and Design, 79 (1984) pp 47–68.

[II-2] CORNELL, C.A. Engineering seismic hazard analysis, Bulletin of the Seismological Society of America, 59, 5 (1968) pp 1583–1606.

[II-3] GHOSH A.K., RAO K.S., KUSHWAHA H.S. Development of response spectral shapes and attenuation relations from accelerograms recorded on rock and soil sites, Report BARC/1998/016, Bhabha Atomic Research Centre, Government of India (1998).

[II-4] U.S.N.R.C. Vibratory Ground Motion, Standard Review Plan 2.5.2, NUREG- 800, Rev.3 (1997).

[II-5] U.S.N.R.C. Identification and Characterisation of Seismic Sources and Determination of Safe Shutdown Earthquake Ground Motion, Regulatory Guide 1.165 (1997).

[II-6] GHOSH AK, KUSHWAHA, HS. Development of Uniform Hazard Response Spectra for Rock Sites Considering Line and Point Sources of Earthquakes, Report BARC/2001/E/031, Bhabha Atomic Research Centre, Government of India, 2001.

[II-7] GHOSH A.K., RAO K.S., KUSHWAHA H.S. Development of uniform hazard response spectra for Tarapur, Trombay and Kakrapar sites. Report BARC/2003/E/019, Bhabha Atomic Research Centre, Government of India (2003).

[II-8] World Data Centre. Catalogue of eismographs and Strong Motion Records, Report SE-6, Solid Earth Geophysics Division, Environmental Data Service, Boulder, Colorado, U.S.A. (1985).

[II-9] GHOSH AK, BANERJEE, D.C. Earthquake Design Basis for Tarapur Site, Internal Report, Bhabha Atomic Research Centre (March 1990)

[II-10] RAVI KUMAR, M. BHATIA, S.C. A New seismic hazard map for the Indian plate region under the global seismic hazard assessment programme, Current Science, 999, 77(3), pp 447–453.

[II-11] INTERNATIONAL ATOMIC ENERGY AGENCY, External Human-Induced Events in Site Evaluation for Nuclear Power Plants, IAEA Safety Guide No. NS-G-3.1, Vienna (2002).

[II-12] AERB, Code of Practice on Safety in Nuclear Power Plant Siting, AERB/SC/S, Atomic Energy Regulatory Board, Government of India (1990).

[II-13] MUKESH KUKREJA, SINGH, RK, VAZE, K.K., KUSHWAHA, HS Damage evaluation of 500 MW(e) Indian pressurized heavy water reactor nuclear containment for air craft impact, 17th International Conference on Structural Mechanics in Reactor Technology (SMiRT-17), Paper No. J003, Prague (2003).

ANNEX III

DESIGN FOR PROTECTION AGAINST EXTERNAL EVENTS IN INDIAN NPPS

S.S. BAJAJ
Nuclear Power Corporation of India Ltd, Mumbai, India

Abstract

This paper presents the approaches applied in design and siting of the Indian pressurized heavy water reactor plants (PHWR) to ensure protection from external events, including earthquakes, floods and cyclones and wind, with reference to the current Indian regulatory requirements. A flooding incident that occurred at the Kakrapar Atomic Power Station (KAPS) in June 1994 is described. An outline of the advanced approaches developed for seismic qualification of future NPPs is given.

1. INTRODUCTION

Potential external events, both human-induced & natural, constitute important consideration in siting and design of Indian NPPs. Attempts are made at siting stage to exclude or minimize the threats from external events. For threats that remain, the preferred coping means are inherent and/ or passive features. External natural events considered include earthquakes, flooding potential, and winds, while human-induced events addressed include hazard from aircraft crashes, explosions and toxic gas releases from industrial activities.

This paper discusses the approaches for protection against external event impacts used in Indian NPPs.

2. SITING

The current siting practices follow several requirements with regard to external events [III-1] as brought out below.

For seismicity:

- The criteria for site disqualification address sites having high seismic potential, i.e., those falling in seismic zone V as per Indian Standard classification (IS-1893);
- The sites with a history of earthquakes of magnitude greater than 6.5 are excluded; as well as
- The sites having any capable fault within 5 km; and
- The sites with unacceptable liquefaction potential.

For aircraft crashes, the screening distance values are applied as follows:

▪ Small airfields	-	5 km;
▪ Major airports	-	8 km;
▪ Military airfields	-	15 km.

For other human-induced events:

- The screening distance value of 5 km is applied for activities involving manufacture, storage and transportation of toxic/ inflammable explosive chemicals, or for mining/ blasting activities;
- The screening distance value of 10 km is used for military installations, such as ammunitions storages, etc.
- Provision are made of a `sterilized zone' of 5 km around the NPP, in which there is administrative control on development activities including prohibition of the location of hazardous industrial facilities.

For flooding at coastal sites:

- A minimum grade elevation above the astronomical tide level must be 4.0 m on the Eastern coast and 3.0 m on the Western coast.

3. LAYOUT

Physical separation of the redundant systems/components performing safety functions provides a protection from the impacts of localized adverse effects, including those resulting from external events. In this respect, the following features provided in the current PHWRs of 540 MW(e) are relevant.

- Back-up control room for each unit is located in the Service Building, diametrically opposite to the main control building.
- Emergency power supply systems such as diesel generators, UPS systems and batteries are separately housed in safety related structure, with two such buildings for each unit (station auxiliary buildings, A and B).
- Safety related systems and components are grouped and placed in buildings of appropriate safety classification and seismic category.

4. PROTECTION FROM EARTHQUAKES

4.1. Methodology for defining earthquake design parameters

4.1.1. Current approach

In the current methodology for arriving at earthquake design parameters, smoothened mean + sigma (m + σ) response spectral shapes for different values of damping are generated from a number of acceleration time histories, having similar geological and seismotectonic conditions, by normalizing each acceleration time history to 1g peak ground acceleration (PGA). The normalized m + σ response spectral shape is further multiplied by the safe shutdown earthquake (SSE) and operating basis earthquake (OBE) level PGA using suitable attenuation correlation for a SSE and OBE PGA to get the design ground response spectra (DGRS) for different values of damping.

The SSE PGA is based on the maximum potential of the region within 300 km radius being moved on to a capable fault, which is closest to the plant, having a capacity to generate an earthquake of the maximum potential derived above. The maximum potential is generally derived by adding unit intensity equivalent magnitude (about 0.7) to the maximum recorded earthquake within 300 km radius. The OBE PGA is the maximum of the PGA for the magnitudes of actual events assigned to all the faults in the region of 300 km radius.

For seismic design of the 2×540 MW(e) PHWR NPP at Tarapur (TAPP-3,4), one objective was to develop standard designs of buildings/ structures, which could be adopted for different sites. Accordingly, site-specific ground response spectra were derived for rocky sites at three locations (Nagarjunasagar, Tarapur & Kakrapar), and from the above three site spectra, envelope ground response spectrum was worked out for a 5% damping value.

For seismic design purposes, the above combined enveloped spectrum for 5% critical damping was chosen as standard spectrum, and three statistically independent time histories, compatible with this ground response spectrum were developed. Based on these time histories, the other curves of spectra for various values of damping were developed, smoothened and used for design.

4.1.2. Approach proposed for the future

The drawback of the present approach for arriving at earthquake design parameters is that the (m+ σ) spectrum does not have uniform confidence (84.1 %) at all frequencies and has a 50% confidence at higher frequency (33 Hz, where the spectrum is anchored to the PGA).

To address this and other drawbacks, new approaches are being considered for future plants, viz. the 700 MW(e) PHWR currently in the design stage. In one proposed approach, instead of generating attenuation correlation only for PGA, the attenuation correlations are generated for different frequencies based on data available for similar sites. From these frequency-dependent attenuation correlations, the (m + σ) spectra are generated for any combinations of magnitude and distance for design earthquake(s), by deterministic approach. These frequency-dependent attenuation correlations are used in generating site-specific deterministic response spectra.

Another approach under consideration is a probabilistic one, wherein, along with the use of frequency-dependent attenuation coefficients mentioned above, all faults in 300 km radius are considered for their possible earthquake generating magnitude, and are treated with probabilistic methods to arrive at seismic hazard curves for various frequencies of interest. These hazard curves are used to generate uniform hazard response spectra.

5. SEISMIC DESIGN

For seismic design of various NPP items, well established standard methodologies [III-2] are followed, which involve defining three levels of earthquake, viz. SL2 (SSE), SL1 (OBE) and a code level earthquake (as defined by the Indian Standard IS-1893 [III-3] for conventional structures). The NPP items are categorized with respect to the seismic loads based on their importance and relevance to safety, into three categories. Appendix A, which is an excerpt from the Indian Regulatory Guide [III-2] on the subject, gives the details in this regard.

Some relevant points pertaining to design for earthquakes are highlighted below:

- While designing items for SL1 and SL2 earthquakes, the damping values used are median minus one standard deviation;
- As a special combination requirement for the design of primary containment structure, loads from SSE are combined with loss-of-coolant accident (LOCA) loads. Table III-1 details the load combinations and design acceptance criteria;
- High energy piping systems, not qualified for leak-before-break (LBB) criteria for applicable loads, including earthquake loads, are provided with pipe whip restraints and barriers to protect safety related equipment and containment boundary in their vicinity;
- Possible interactive effects of lower seismic category items adversely affecting higher category items due to collapse, falling or other spatial interaction are addressed by either upgrading the category of the offending, lower category item, or by other suitable protective measures.
- Any dams in the vicinity of the plant, not qualified to SSE level, are considered to burst, and their implication on design basis flood level as well as availability of ultimate heat sink is taken into account;
- No credit is taken for off-site power supplies for performing essential safety functions;
- Although reactor systems whose failure could constitute design basis accidents (DBAs) are designed for SSE, the mitigating safety system such as emergency core cooling system (ECCS) are still designed for SSE as a conservative approach;
- Plant operating procedures require that in the event of ground motion exceeding the peak ground acceleration for OBE level earthquake, the plant is to be shut down and the restart is to be done only after specified inspections. To monitor the ground motion, strong motion earthquake recorders are provided at the site. Micro-earthquake stations are also provided around each site to monitor the seismic status of site continually over the years.

TABLE III-1. LOAD COMBINATIONS AND ACCEPTANCE CRITERIA*

CONDITION	STRENGTH CHECK		SERVICEABILITY CHECK	
	LOAD COMBINATION	PARTIAL SAFETY FACTOR CONCRETE/STEEL	LOAD COMBINATION	ACCEPTANCE CRITERIA
Abnormal + extreme environment	DL+P_a+0.5T_a+(1,0.4) E_s+ PS	1.15/1	DL+P_a+0.6T_a+(1,0.4) E_s+ PS	No tension in current section
Extreme environment	1.35DL+LL+0.8T+(1,0.4)E_s+1.35PS	1.15/1	DL+LL+0.6T+(1,0.4) E_s+ PS	No tension in current section
Severe environment	1.35DL+LL+0.8T+(1,0.4)E_o+1.35PS	1.5/1.15	DL+LL+0.6T+(0.4,1) E_o+ PS	Covering section in compression
Abnormal	1.35DL+1.5LL+1.35P_a+0.66T_a+1.35PS	1.5/1.15	DL+LL+P_a+T_a+PS	– No cracking in inner face $\sigma_c \leq 0.5f_c$ – Covering section in compression – Average compression in current section = 1MPa
Test	1.35DL+1.5LL+1.35P_T+0.8T_T+1.35PS	1.5/1.15	DL+LL+P_T+0.6T_T+PS	Done
Normal operation	1.35DL+1.5LL+0.8T+1.35PS+1.3WL	1.5/1.15	DL+LL+0.6T+PS+WL	– $\sigma_c \leq 0.5f_c$ – Covering section in compression
Construction	1.35DL+1.5LL+1.35PS+1.3WL	1.5/1.15	DL+CLL/LL+PS+WL	– Uncracked section – $\sigma_c \leq 0.67f_c$ – $\sigma_t \leq 0.67f_t$

* The acronyms used in Table III-1 are: DL - dead load; LL - live load; CLL - construction live load; PS – pre-stress load; P_a, T_a - accident based pressure and temperature loads (e.g., for LOCA or steam line break inside the containment building); P_T,T_T - pressure and temperature respectively during test conditions; E_s - earthquake, SL2 (SSE) load; E_o – earthquake, SL1 (OBE) load; T - ambient temperature load (extreme summer/ winter); WL - design wind load (return period 1000 years); (1,0.4) - denotes factors for combination of a vertical and the two components of a horizontal seismic load.

6. PROTECTION AGAINST FLOOD

6.1. Design basis flood; level and flood protection in design [III-4, III-5]

Basic protection against external floods is provided by specifying finished grade level for the main plant buildings/ structures above the design basis flood (DBF) level or the safe grade elevation.

For coastal sites, the DBF level is arrived at considering maximum level based on 1000-year return period of a cyclonic storm surge coincident with the highest astronomical high tide and wave run-up effect.

As an example, by applying the abovementioned requirement to the TAPP-3,4, the safe grade elevation was assessed to be 6.03 m above the mean sea level (MSL), see Table III-2. Accordingly, all site areas are levelled to this elevation. Further, the grade floor level (plinth levels) of plant buildings, including switchyard and the CW pump house are at 6.33 m above the MSL, i.e. 0.3 m above the safe grade elevation.

TAPP-3, 4 has also been provided with a protective rock bund along the coast, which extends to a height of 7.03 m above the MSL as further protection against waves.

Additional consideration regarding protection against external floods relates to (a) provision of an efficient network of surface drainage system to cater to the maximum design basis precipitation intensity, and (b) protection of the basements from possible ingress of floodwaters through pipe/ cable tunnels. The latter is further discussed in the following section.

For inland sites, the estimation of design basis flood is based on probable maximum precipitation (PMP) and routing of the resulting waters through the river channel to arrive at the maximum water level at the site. Also considered are failures of the upstream dams.

TABLE III-2. DESIGN BASIS FLOOD (DBF) LEVEL FOR TAPP-3, 4

EXTERNAL EVENT/ DESIGN BASIS	LEVEL ABOVE MSL
Highest astronomical high tide level (based on the analysis of data for the period 1970-1989, for return period of 1000 years)	2.84 m
Storm surge (inverted barometer effect + uniform wind field effect); based on the analysis of worst tropical cyclones and resulting storm surges from the data of the last 110 years	2.30 m
Wave run-up	0.89 m
Safe grade elevation (DBF level)	6.03 m

6.2. Flooding incident at KAPS [III-6, III-7]

A flooding incident was experienced at the Kakrapar Atomic Power Station (KAPS) in June 1994 due to heavy unprecedented rains, along with the failure of flood control provisions. KAPS is located on the left bank of a canal fed from river Tapi. The design basis flood (DBF) level for the plant is based on the postulation of floodwater discharges from an upstream dam to the river together with heavy precipitation, according to which the river level (RL) of 50 m was designated as the DBF level. Accordingly, the main plant grade is kept at 51.0 m, while the pump house and other plant buildings are at 50.0 m, although these are some low-lying areas (below 50 m) in the vicinity. Also, there are underground tunnels and trenches (for pipes and cables) located below grade level and connected to the basement areas of the turbine building. The plant surface drainage system is designed for a rainfall intensity of 100mm/hr for a maximum duration of 1 hour, with drain discharge points going down to invert the level of the RL= 47 m into the pond associated with the canal. Thus, the pond level needs to be regulated (by control of downstream discharge gates) such that the back-flows from these drains are avoided.

During the incident, when there was heavy rain over a 15-hour period, with peak intensity of 90mm/ hr, Unit 1 was under shutdown and Unit 2 was under commissioning. The water level in the pond started rising; the weir gates at the discharge from the pond could not be fully opened as they were blocked by huge chunks of grass with roots and clay mounds. The rising level in the pond caused a back-flow of water through the plant water pump house tunnel connected to the turbine-building basement. Further, there was water logging in low-lying areas of the plant site. This water also entered the turbine-building basement through a pipe tunnel, the cover of which had been removed for some maintenance job and was not replaced.

The ingress of water into the turbine building flooded three basement areas and submerged the equipment like process water pumps, boiler feed pumps, etc. 220-kV switchyard had failed due to a failure of the bus support insulator, and this resulted in a Class IV power supply failure.

Dewatering of the turbine building was performed, and during the 9 hours of the Class IV unavailability core cooling was maintained using the station emergency electric power supply and the firewater back-up cooling water supply to shutdown cooling heat exchangers. For the entire duration of flooding at the site, the reactor was under a safe shutdown condition and there were no radiological consequences of this event.

After the incident, a number of corrective actions were taken at KAPS and at other NPPs having similar vulnerability. These actions included:

- Sealing of the pipe and cable tunnels and trenches and checking them before every monsoon. As a defence-in-depth, it is ensured that all tunnels and trenches leading to the basement of the safety related buildings have more than one flood barrier to avoid flood/ seepage water reaching the buildings. Additionally, dewatering provisions were made in the tunnels. All manhole covers /ventilation openings were raised above DBF level;
- All safety related equipment/ devices/ instrument/ junction boxes in basements were raised above the DBF level to the extent possible.

The actions taken by the State authorities included:

- Converting the manual gates at pond discharge weir into the electrically operated ones;
- Maintaining the pond level between the defined minimum and maximum level as a normal practice;
- Augmentation of the communication between the NPP control room and the State authorities.

While the above actions ensure that the adverse effects of such flooding are avoided, a detailed safety analysis of the flooding event was carried out and it was ensured that, with certain identified manual actions, the safety functions of tripping the operating units, maintaining the core cooling and containing the radioactivity are ensured. These manual actions are defined with reference to water level in the pond and in the turbine building (assuming some leak paths), and form a part of the emergency operating procedures. To facilitate these actions, instrumentation was provided in the control room to indicate water level in these areas.

In new NPPs, e.g. TAPP-3,4, placing of the safety related equipment in a basement is avoided. Also, design provisions are made to ensure that the underground tunnels do not constitute paths for water ingress into the basements.

7. CYCLONE/ WIND

The design of civil structures considers wind pressure as one of the design loads. For this purpose, wind speed with a return period of 1000 years is considered as basis.

The Indian Meteorological Department (IMD) issues cyclone warnings and has arrangements for a widespread dissemination of this information through various media. Before actual hitting of a cyclone, the advance warning will be available to activate emergency preparedness.

In the worst case, a complete Class IV power supply failure may occur during cyclones. Class III power supply is ensured in this case as the emergency diesel generators are located inside the qualified station auxiliary buildings, which are qualified for the external events such as SSE & wind loads.

In the event of a damage of surface telecommunications facilities, essential communication can be maintained by other means (like satellite and wireless).

As cyclone will invariably be associated with strong winds, it is possible that loosely lying objects within the plant area or outside may act as missiles, hitting the plant structures and buildings. With an advance warning available, preventive measures can be taken so as to put the material lying outside in the covered areas.

The safe grade elevation has taken into account the effect of cyclone (i.e., storm surge). Depending upon availability of power evacuation, operation of the reactor units at rated power may continue during a cyclone. If reactor shutdown is called for, the decay heat removal capability for extended duration will be available. Cooling water intake structure is designed for a cyclonic storm and, therefore, the ultimate heat sink remains available. Handling of the situation caused by a cyclone is performed via administrative actions, which are activated whenever a cyclonic storm is forecasted.

8. CONCLUSION

For Indian PHWR NPPs, natural external events considered include earthquakes, flooding potential, and winds, while human-induced events addressed include hazard from aircraft crashes, explosions and toxic gas releases from industrial activities. For all of these events, the regulatory requirements are available. The application of seismic requirements is illustrated in this paper for the 2×540 MW(e) PHWR nuclear power plant at Tarapur (TAPP-3,4).

A flooding incident that occurred at the Kakrapar Atomic Power Station (KAPS) in June 1994 due to heavy unprecedented rains, along with the failure of flood control provisions is described. For the entire duration of flooding at the site, the reactor was under a safe shutdown condition and there were no radiological consequences of this event. Corrective measures to prevent such incidents in the future were implemented.

REFERENCES

[III-1] ATOMIC ENERGY REGULATORY BOARD, Code of practice on safety in nuclear power plant siting AERB Code No. AERB/SC/S, Mumbai, India (1990).

[III-2] ATOMIC ENERGY REGULATORY BOARD, Safety classification and seismic categorisation for structures, systems and components of PHWRs', Safety Guide No. AERB/SG/D-1, Mumbai, India (2003).

[III-3] CRITERIA FOR EARTHQUAKE RESISTANT DESIGN OF STRUCTURES, (BIS Standard IS-1893) Bureau of Indian Standards, New Delhi, India (2002).

[III-4] ATOMIC ENERGY REGULATORY BOARD, Design basis flood for nuclear power plants on inland sites, Safety Guide No. AERB/SG/S-6A, Mumbai, India (1998).

[III-5] ATOMIC ENERGY REGULATORY BOARD, Design basis flood for nuclear power plants at coastal sites, Safety Guide AERB/SG/S-6B; Mumbai, India (2002).

[III-6] HAJELA, S., BAJAJ, S.S. Reactor safety under design basis flood condition for inland sites, (paper presented at 1st Nat. Conf. on Nuclear Reactor Safety, Mumbai, India, Nov.2002).

[III-7] MANDOWARA, S.L. et al `KAPS flooding incident experience feedback, (paper presented at DAE Symposium on Cyclone Emergency Preparedness, Kalpakkam, India, Jan. 2002).

Appendix A

EXCERPT FROM AERB SAFETY GUIDE SG/D-1

III-A.1. SEISMIC CATEGORIZATION

III-A.1.1 General

AERB Code of Practice on Safety in Nuclear Power Plant Siting (AERB/SC/S) stipulates that 'structures, systems and components necessary to assure capability for shutdown, decay heat removal and confinement of radioactive material shall be designed to remain functional throughout the plant life in the event of natural phenomenon such as earthquakes, cyclones and floods.' This section explains the basis of seismic categorization.

III-A.1.2 Earthquake Levels

As per the siting code AERB/SC/S, following two earthquake levels have been defined:

(1) S1 level earthquake; and

(2) S2 level earthquake.

The S1 level is the maximum ground motion, which can be reasonably expected to be experienced at the site area once during the operating life of the nuclear power plant with an estimated return period of about 100 years. In the design, the S1 level ground motion corresponds to Operating Basis Earthquake (OBE).

The S2 level is the level of ground motion that has a very low probability of being exceeded. It represents the maximum level of ground motion to be used for design of structure, systems and components (SSCs) important to safety. In the design, the S2 level ground motion corresponds to the Safe Shutdown Earthquake (SSE).

III-A.1.3 Categorization

SSCs are to be categorized in three seismic categories.

III-A.1.3.1 Seismic category-1

Seismic category-1 shall include all SSCs:

(i). whose failure could directly or indirectly cause accident conditions; or

(ii). which are required for shutting down the reactor, monitoring critical parameters, maintaining it in a safe shutdown condition and removing decay heat on a long term basis; or

(iii) which are required to prevent radioactive release or to maintain release below limits established by AERB for accident conditions (e.g., containment system).

As a conservative measure, it is recommended to include those items in category-1, which are designed to mitigate the consequences of design basis accidents resulting from failure in primary pressure boundary, despite the fact that the latter is designed to withstand earthquake loads.

The mean return period is estimated to be typically, 10 000 years.

All seismic category-1 structures, systems and components should be designed or qualified for both S1 (OBE) and S2 (SSE) (ref. AERB safety guide AERB/SG/D-23 on 'Seismic Qualification').

III-A.1.3.2. Seismic Category-2

Seismic category-2 shall include all SSCs which are required to:

(i) prevent the escape of radioactivity beyond the limits prescribed for normal operation and not covered in category-1; or

(ii) mitigate those accident conditions which last for such long periods that there is a reasonable likelihood of an earthquake of the defined severity occurring during this period and not covered in category-1.

All seismic category-2 structures, systems, and components shall have demonstrated capability to withstand the effects of S1 (OBE).

III-A.1.3.3 Seismic Category-3

Seismic category-3 includes SSCs which are not important to safety and those not covered in category-1 or 2. Items under this category may follow national practice; for example, the civil structures under this category can be designed and built as per IS-1893.

ANNEX IV

ADVANCED CANDU REACTOR (ACR) SAFETY DESIGN APPROACH

M. BONECHI
Atomic Energy of Canada Limited, Mississauga, Ontario, Canada

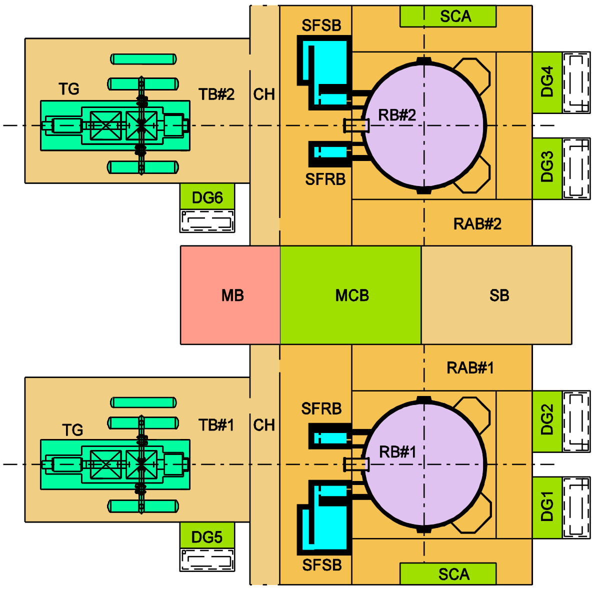
Abstract

This paper outlines the basic features of the reference Advanced CANDU Reactor (ACR) design and the safety design approach to protection against internal and external events with emphasis on the latter type of events. The paper was provided to the IAEA for the purpose of the Technical Meeting on Definition of Plant Safety Design Options to Cope with External Events held in Vienna on 14–19 November 2005.

1. INTRODUCTION

The Advanced CANDU Reactor (ACR) design is based on the modular concept of horizontal fuel channels surrounded by a heavy water moderator, the same as with all CANDU reactors. The major innovation in the ACR is the use of slightly enriched uranium as fuel and of light water as coolant circulating in the fuel channels. This results in a more compact reactor design and a reduction of heavy water inventory, both contributing to a significant decrease in cost compared to CANDU reactors that employ natural uranium as fuel and heavy water as coolant.

The ACR design is built on the proven technology of the CANDU 6 and incorporates advances from CANDU 9 and lessons learned from operating units. Key traditional characteristics of the CANDU system that are maintained in the ACR include: simple, economical fuel bundle design; on-power fuelling; and separate cool, low-pressure moderator with back-up heat sink capability. The ACR-700 version of the ACR design, which is used as reference in this paper, is a two-unit integrated plant with each unit having a gross output of 753 MW(e). A schematic of the general plant layout is given in Fig. IV-1.



Legend:

CH	Crane hall
DG	Diesel generator
MCB	Main control building
MB	Maintenance building
RAB	Reactor auxiliary building
RB	Reactor building
SB	Service building
SCA	Secondary control area
SFRB	Spent fuel receiving bay
SFSB	Spent fuel storage bay
TB	Turbine building
TG	Turbine-generator

FIG. IV-1. General plant layout.

The design also features higher pressures and temperatures of reactor coolant and main steam, thus providing a larger thermal efficiency than the existing CANDU plants. These thermal-hydraulic characteristics further emphasize the ACR drive toward improved economics. The safety enhancements made in ACR encompass safety margins, performance, reliability and separation of safety related systems, and increased resistance to severe accidents. Passive features additional to those already present in the operating CANDU plants have also been built into the design.

AECL is presently undertaking upfront licensing efforts for the review of the ACR design with the Canadian Nuclear Safety Commission (CNSC) to obtain a statement of licensability of the design, and with the US Nuclear Regulatory Commission (USNRC) for a pre-licensing review leading to the application for standard design certification.

2. REACTOR DESIGN

The use of slightly enriched uranium (SEU) with light water coolant flowing through the horizontal fuel channels allows a smaller D_2O-moderated lattice and results in a more compact reactor core and a smaller calandria vessel containing the moderator. The more compact core sharply reduces the inventory of heavy water in the moderator, giving a major cost reduction.

The reactor core design adopted for ACR also has some important effects that have a bearing on inherent safety. The core has a very flat power distribution that minimizes the demands on the reactor control system during operation. The core also has a significantly negative power coefficient and a small negative full-core void reactivity providing a good balance of nuclear protection between loss-of-coolant accidents and fast cooldown accidents. Moreover, the use of 43-element CANFLEX fuel bundles in lieu of the traditional 37-element fuel bundle increases the operating margins of fuel. In addition, the CANFLEX fuel design increases the critical heat flux of the fuel elements, therefore the margin to fuel sheath dry-out during transients and accidents.

The use of SEU allows increasing the thickness of both the Zr-2.5%Nb pressure tubes and the Zircaloy calandria tubes, thus improving their capability to withstand loads during normal operation and upset conditions. The thickness of the pressure tube also extends the pressure tube design lifetime, with respect to limits determined by both creep and corrosion. The use of SEU fuel enables increasing fuel burn-up to about three times the burn-up in CANDU reactors employing natural uranium. Figure IV-2 provides a 3-D representation of the ACR reactor assembly.

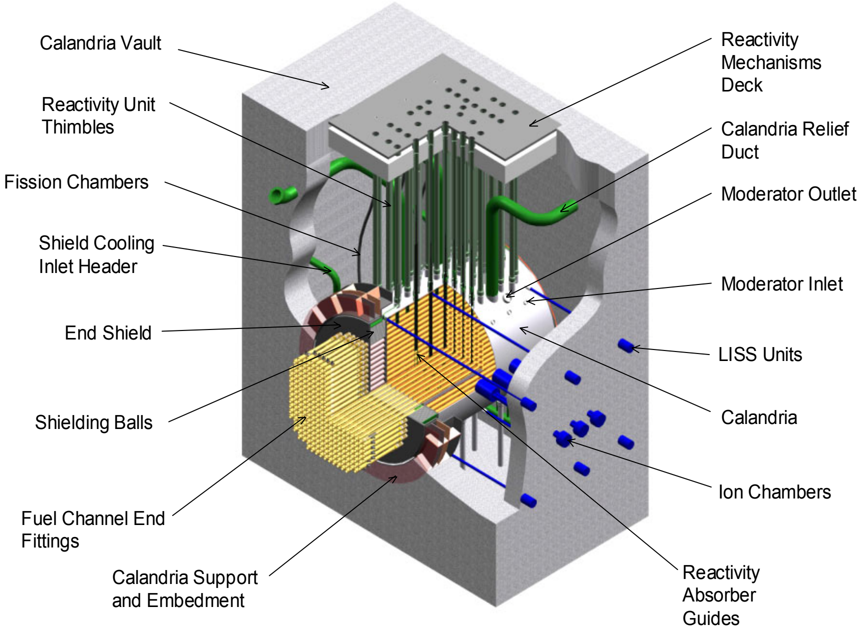


FIG. IV-2. Reactor assembly.

3. SAFETY DESIGN FEATURES

Several improvements in performance and reliability of safety related systems and in protection against common cause events have been made in ACR. These improvements were identified from the insights gained from preliminary probabilistic safety assessments, the results of preliminary safety analyses and operating feedback from existing plants.

Separation, reliability and diversity of the safety systems for shutdown, emergency core cooling and containment, which are the fundamental safety design requirements of CANDU reactors, remain the pillars of the ACR design as well. Separation and independence also includes the provision of a secondary control area as a backup to the main control room for certain emergency conditions.

The same as in the existing CANDU plants, two separate, fast acting shutdown systems are provided, operating on different physical principles. Because of the smaller core size, the two shutdown systems can introduce negative reactivity into the core more quickly. The gravity driven shut-off rods of Shutdown System 1 (SDS1) have a smaller distance to travel into the core, while the liquid poison injected by Shutdown System 2 (SDS2) has to mix with a smaller moderator volume to render the reactor subcritical. All reactivity devices for reactor shutdown and control are located in the low pressure and temperature moderator, eliminating the possibility of accidents such as rod ejection. A simplified representation of the two shutdown systems is provided in Fig. IV-3.

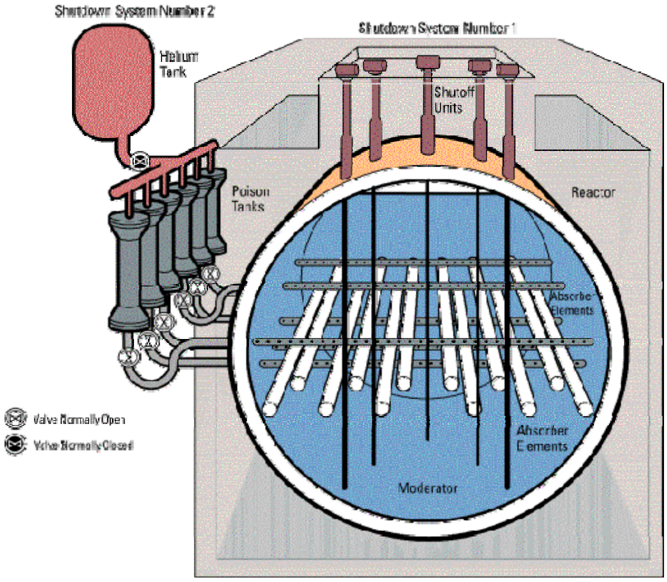


FIG. IV-3. Shutdown systems.

The reliability of the emergency core cooling (ECC) system, which supplies light water coolant to the reactor and maintains fuel cooling in the event of a loss-of-coolant accident, is significantly increased by simplifying the interface between the ECC and the reactor coolant system (RCS) since they are both light water systems. The ECC system consists of a high-pressure injection system with pressurized tanks (emergency coolant injection system) and a system (long term cooling system) that re-circulates water from the floor of the containment back into the RCS by means of pumps. Figure IV-4 provides a 3-D picture of the RCS; a schematic of the emergency coolant injection system is given in Fig. IV-5.

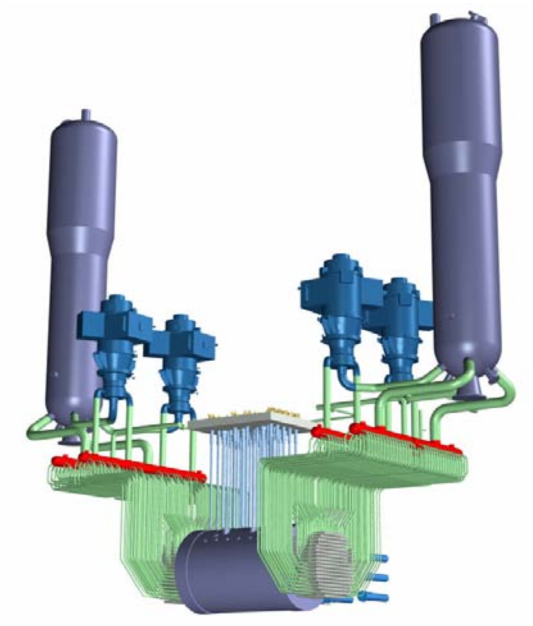


FIG. IV-4. Reactor coolant system.

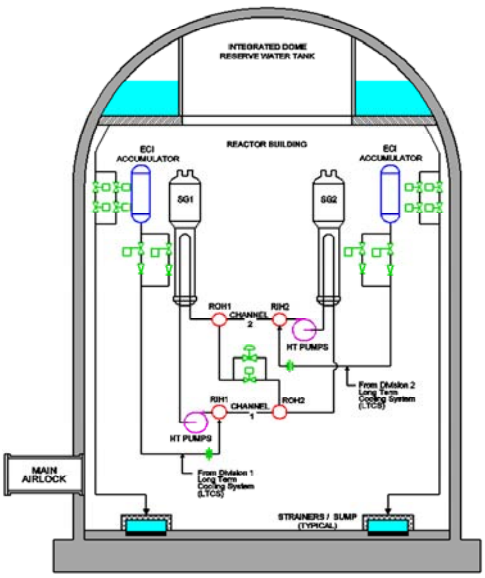
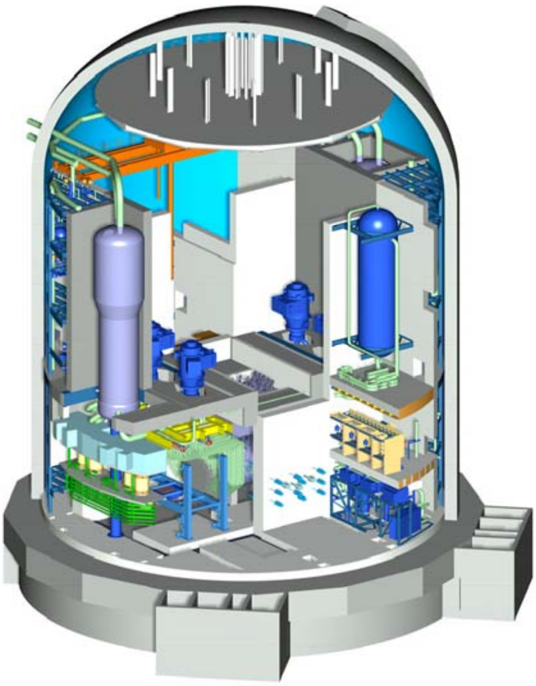


FIG. IV-5. Emergency coolant injection system.

Like all CANDU reactors, ACR also features the inherent ability of the cool, low-pressure moderator to act as an emergency heat sink for a beyond design basis event resulting from a loss-of-coolant accident coincident with postulated complete failure of the ECC system. In ACR, the robustness of the design against this type of improbable accidents, as well as against even more improbable severe core damage accidents where also the moderator back-up heat sink is postulated to be unavailable, is enhanced by passive (gravity) water make-up to the moderator and the shield water surrounding the calandria vessel from a large water tank located at a high elevation in the containment.

The containment system includes a pre-stressed concrete containment structure (the reactor building) with a pre-stressed concrete dome and an internal steel liner, building air coolers for heat removal and a containment isolation system consisting of valves or dampers in the ventilation ducts and certain process lines penetrating the containment envelope. Hydrogen recombiners are included to limit hydrogen content to below the deflagration-to-detonation limit following beyond-design-basis events. A schematic of the containment building is provided in Fig. IV-6.

FIG. IV-6. Containment building.



To achieve a high degree of redundancy and separation, key safety related systems, including the safety support systems, are provided with two independent divisions each of which acting alone is sufficient to fulfill the safety function of the system. The two divisions in a system, as well as redundant components within each division, are separated from each other by distance or physical barriers or combinations of both. The application of this design approach has an impact particularly on the safety support systems, such as the safety related cooling water and electrical power supplies, which extend over large areas of the nuclear steam plant.

Of particular importance among the safety support systems is the reserve water system (RWS). The system consists of a tank located at a high elevation inside containment, which can supply water by gravity to several users inside the containment. This system enhances the defence-in-depth against both design basis events, including external events, and beyond-design-basis events as described later.

4. DESIGN FOR INTERNAL EVENTS

Key to the ACR safety basis is the definition and classification of events to be analyzed. Using the risk-informed approach, the ACR safety basis applies the following principles:

(1) The initiating events should cover the entire spectrum of potential challenges to the safety of the plant from the more frequent events that are anticipated to occur during the lifetime of the plant to the extremely improbable events that are beyond the design basis of the plant;
(2) The safety requirements should be commensurate with the likelihood of the events so that more stringent requirements are applied to more probable events; and
(3) Assumptions and methods for safety analysis should provide a good balance between the need for conservatism at higher event frequencies and the reasonableness of a design-centred assessment at lower event frequencies.

Consistent with international standards and practices, and to take into account the pressure-tube design of the ACR, the safety basis uses three categories of events: design basis events (DEs), limited core damage accidents (LCDAs), and severe core damage accidents (SCDAs).

DEs are events that must be accommodated within specified radiological dose limits and with suitable margins to the breach of the physical barriers (fuel, reactor coolant pressure boundary and containment) against radioactivity release to the environment. The design basis events set the design requirements for the engineered safety features.

LCDAs are lower probability, beyond-design-basis events for which core coolability is maintained. They include: (i) those high temperature accidents which require the moderator as a back-up heat sink; and (ii) severe single channel events which may result in small quantities of molten material in the affected channel. Limited core damage accidents must be coped with within specified dose limits at the exclusion area boundary.

SCDAs are those beyond-design-basis events which result in widespread loss of core and channel geometry, and are directly equivalent to severe accidents in other reactor systems and licensing jurisdictions. Dose limits are not set for severe core damage accidents. Targets are rather set for the cumulative frequencies of severe core damage and large release, which are 10^{-5} and 10^{-6} per year respectively.

As noted above, design basis events are events, which must be accommodated within specified radiological dose limits and with suitable margins to the breach of the physical barriers against the release of radioactivity to the environment. Design basis events include Class 1 through 3 events. A Class 1 event is an event of moderate frequency (anticipated operational occurrence) that may typically occur during a calendar year for a particular plant. A Class 2 event is an infrequent event that may typically occur during the lifetime of a particular plant. A Class 3 event is a limiting event that is not expected to occur but is postulated because of its potentially significant consequences.

Internal events are identified by means of a systematic review of the plant design. Operating experience is used to confirm and supplement the internal events identified through the systematic review. Internal events are then classified according to their likelihood of occurrence along with other considerations, such as quality of design, supporting analyses, testing and inspections.

Examples of the design basis events are:

- Class 1: Events of moderate frequency or anticipated operational occurrences
  - Failure of pressure or inventory control in the RCS;
  - Failure of secondary circuit pressure control;
  - Failure of reactor power control;
  - Loss of Class IV power (station normal AC power supply);
  - Single RCS pump trip;
  - Active failures of the moderator system;
  - Loss of normal steam generator feedwater flow.
- Class 2: Infrequent events
  - Small loss-of-coolant accident (LOCA);
  - Pressure tube failure (calandria tube intact);
  - Off-stagnation feeder break;
  - Partial single channel flow blockage;
  - Main steam line break (outside containment);
  - Steam generator tube rupture;
  - Passive failures of the moderator system.
- Class 3: Limiting events
  - Large LOCA;
  - Pressure tube/ calandria tube rupture;
  - Main steam line break (inside containment);
  - RCS pump seizure.

As stated above, limited core damage accidents are improbable events beyond the design basis for which core coolability is maintained. They comprise two types of accidents, which are strictly connected to the pressure tube reactor design of the ACR with separate fuel channels surrounded by the low-pressure moderator. One type includes accidents initiated in a single fuel channel with significant overheating of fuel material in the channel: severe flow blockage and feeder stagnation break. These accidents involve heat-up at high power and high pressure. The affected fuel channel fails before fuel melting but there is no propagation of the damage to neighbouring channels; hence, damage remains localized to the affected channel. The other type includes accidents with widespread overheating of the fuel in the core but not compromising core coolability. Accidents of this type are loss-of-coolant accidents (LOCA) with loss of emergency core cooling. These accidents involve heat-up at decay power and low pressure. No channel failure and no fuel melting are expected to occur owing to the heat transfer from the fuel to the cool moderator surrounding the fuel channels.

Severe core damage accidents are even more improbable beyond-design-basis events for which core coolability cannot be maintained. SCDAs consist basically of the combinations of LOCA with the loss of both the emergency core cooling system and the moderator heat sink. This accident leads to core disassembly and fuel melting. The core melt progression is slowed down by the large volume of shield water surrounding the calandria vessel containing the moderator. This reduces the rate of energy release into the containment and allows time for the operator to take corrective actions before a large release of radioactivity can occur.

The ACR has strengthened the resistance to core damage challenges by providing means to make up water to the moderator and the shield water system so as to extend the duration of their heat sink capabilities for beyond-design-basis events.

5. DESIGN FOR EXTERNAL EVENTS

5.1. Generic site characteristics for external events

The reference ACR design is based on a set of generic site characteristics, which are considered enveloping a number of potential sites where an ACR plant may be built. Some of the generic site characteristics have been taken from industry or regulatory guides and information documents where recommended values of design parameters were defined based on historical data.

The major external events covered in the reference ACR design are the design basis earthquake and the design basis tornado. A PSA based seismic margin assessment is also performed to evaluate the robustness of the design against high intensity earthquakes. Other external events will be taken into account as applicable for project and site specific applications of the reference ACR design.

5.2. Human-induced events

Most human-induced events are dependent on site-specific conditions, which can be factored in only at the time of an actual project implementation. If applicable, they can be designed against by means of limited modifications to the reference design. Also, experience and practice are that a good number of human-induced events can be excluded through proper site selection and provisions (e.g. distance from the source of the hazard or physical barriers).

A limited number of human-induced events are considered in the ACR reference design when their applicability and impact are likely to affect a large spectrum of potential sites.

Assessments are made to determine the capability of the containment building to withstand the impact of an aircraft crash for various types of aircrafts. The aim is to envelope a spectrum of commercial aircraft sizes within the resistance capability of the containment building structural design.

Electromagnetic interference is dealt with in the reference ACR design through shielding of control signals and separation by distance from power sources.

5.3. Natural events

The major natural events factored in the reference ACR design are a design basis earthquake and a design basis tornado. The Design Basis Earthquake (DBE) has been selected with peak ground acceleration (PGA) of 0.3 g. The reference design ground response spectra (DGRS) are based on the Canadian CSA standard N289.3 and modified to account for Eastern North American earthquakes that are characterized with high frequency vibrations. For the intended site of the ACR plant, it should be demonstrated that the ground response spectra at the foundation level in the free field is enveloped by the reference DGRS. The reference ACR design also uses a Design Basis Tornado (DBT) defined by a maximum wind speed of 530 km/h and by a maximum air pressure drop of 14 kPa.

The reference ACR design includes protection against lightning in accordance with electrical code requirements. Typical means of protection include provision of high-elevation protective cables in the grid, high lightning posts around the switchyard and lightning rods on the top of each building.

Most natural events are dependent on site-specific conditions, which can be factored in only at the time of an actual project implementation. Therefore, they are outside the scope of the reference ACR design. If applicable, they can be designed against by means of limited modifications to the reference design. Also, a good number of these events are generally excluded through proper site selection and provisions.

5.4. Combinations of events

The loads due to external causes (such as wind and precipitations) normally expected during the operation of the plant are combined with the loads of extreme external events unless they are mutually exclusive or the normal loads are bounded by the extreme loads. The focus of any combination of normal external loads with extreme external loads is the assurance that the reactor can be safely shut down and cooled after the extreme event. This sets the determination and selection of the plant features that must be designed to withstand the effects of the load combinations.

The reference ACR design does not combine extreme external events with each other to apply the combinations to design. These events have very low likelihood of occurrence and the probabilities of their combinations, even within a relatively large time interval, are negligible.

The loads due to internal accidents are combined with the external loads that are normally expected to be present during the operation of the plant unless the two sets of loads are mutually exclusive or the normal external loads are bounded by the accident loads. The principle is similar to that used for combining normal external loads and loads due to extreme external events. Again the focus of any combination of normal external loads with accident loads is the assurance that the reactor can be safely shut down and cooled after the accident.

Another type of combination of loads due to external events with loads from internal events is for the situations in which an external event is the initiating cause of the internal event. This is, for example, the case of a loss of the station normal AC power supplies (off-site power and on-site power from the main generator) following a design basis earthquake. In this case, the components and piping of the reactor coolant system (as an example of a major safety related system) are designed to withstand the combined loads due to the design basis earthquake and the pressure-temperature transient experienced as a result of the loss of power to the reactor coolant pumps (reactor coolant system under natural circulation).

The Canadian seismic design approach also applies a lower level earthquake (SL-1 level as per terminology of the IAEA Safety Guide NS-G-1.6 [IV-1]) to the qualification of structures, systems and components that are required in the long term of a LOCA. This earthquake, called site design earthquake (SDE), is postulated to occur 24 hours after a LOCA.

The Canadian seismic design approach does not require the combination of LOCA and design basis earthquake (DBE) loads because the reactor coolant pressure boundary is designed to withstand SL-2 (i.e. DBE) loads within Service Limits C of the ASME Code Section III. The practice in other countries and jurisdictions is to seismically qualify the reactor coolant pressure boundary to the less stringent Service Limits D. However, if required by the practices and regulatory requirements in countries where an ACR plant would be built, the design can be implemented to include the combination of DBE and LOCA loads for the relevant safety related structures, systems and components. In this case Service Limits D would be applied to the design of the reactor coolant pressure boundary for the loading combination.

5.5. Classification of structures, systems and components for external events

Three types of structures, systems and components (SSC) are considered in the context of the protection against design basis external events for the purpose of ensuring nuclear safety:

(1) Structures, systems and components which are essential to maintain the key functions of reactor shutdown, heat removal and containment during and following each design basis external event;
(2) Structures, systems and components which, although not required to perform the key functions of type 1 above, could however fail following a design basis external event in such a manner as to endanger the essential structures, systems and components or to generate potential radiological accidents due to radioactive materials normally stored outside containment;
(3) Structures, systems and components which are neither essential to cope with the design basis external event nor subject to failures which could endanger the capability of the essential structures, systems and components or cause potential radiological accidents due to radioactive materials normally stored outside the containment.

Structures, systems and components of type 1 are designed to maintain their functionality under the relevant design basis external events. Structures, systems and components of type 2 are designed for the relevant design basis external events to the extent of preventing their failure from affecting the essential structures, systems and components, or from generating potential radiological accidents from the storage of radioactive materials outside the containment. Structures, systems and components of type 3 do not need to be designed against design basis external events.

5.6. Methods of plant protection against external events

Plant protection from external events is based on the objective of assuring reactor shutdown and cooling, and (if required) containment of radioactive releases for each design basis external event. The objective is implemented by three means for the essential systems of type 1 as defined above: (i) separation of redundant divisions within an essential system so that the external event can disable only one division at most; (ii) protection of an essential system by suitable physical barriers that prevent the effects of the event from affecting the system; and (iii) qualification of an essential system or a system required to prevent radiological accidents from storage of radioactive material outside containment, to withstand the effects of the event.

The reference ACR design can accommodate external events of high intensity, including a design basis earthquake and a design basis tornado. Engineered passive means of protection are primarily provided by the buildings and structures enclosing essential systems or systems containing radioactive materials whose failure could lead to radiological accidents. Examples are the containment, reactor auxiliary building and maintenance building. Another means of passive protection is provided by physical separation of redundant divisions in the safety support systems including the safety related cooling water systems and electrical power supply systems. Passive protection can also be provided by modifying site features (if needed), such as raising plant elevation or building dikes to protect the plant from floods. The necessity for these features will be evaluated for site-specific projects.

Qualification to remain functional during and following a design basis external event is the primary means of protection for active systems required to cope with the event. For example, all the essential systems and components are qualified to withstand the effects of a design basis earthquake without loss of safety function. Active components include safety related pumps, valves, electrical generators and motors, control systems and actuators.

5.7. Design features for protection against external events

The external events used for the reference ACR design are similar to those applied for the existing CANDU reactors. There are, however, some differences in the intensity of the design basis events used for the design, and in the design features provided to cope with the events.

The seismic resistance has been increased in the ACR: the peak ground acceleration is 0.3 g, higher than in the operating CANDU reactors.

The safety support systems in the ACR are provided with greater redundancy and separation of redundant features to increase the resistance to random occurring events and common cause events, including external events. In particular, the safety support systems for cooling water and electrical power are arranged in two separate divisions completely independent from one another. Each division alone is sufficient to provide the required services to ensure the safe shutdown and cooling of the reactor. Physical separation between the two divisions is provided by a combination of distance and barriers.

A reserve water system (RWS) provides passive water make-up to a number of systems located inside the containment. The RWS consists of a large tank located in the upper part of the containment and connected to the reactor coolant system, secondary side of the steam generators, moderator system and shield water system. Water make-up from the reserve water tank to the supported systems is by gravity. In particular, the water make-up to the secondary side of the steam generators (emergency feedwater system) allows maintaining heat removal from the reactor for a long time without relying on the cooling water supplies located outside the containment. This capability enhances the defence-in-depth for the external events: the containment is designed to be very robust and immune to all design basis external events with a large margin, and safe shutdown and cooling of the reactor can be assured even for extreme situations which may disable the heat removal systems located outside the containment. The make-up provision to the moderator system and the shield water systems are important to enhance the resistance against beyond-design-basis internal events: make-up to the moderator increases the passive thermal capacity of the moderator inside the calandria vessel for limited core damage accidents which involve the use of moderator as a back-up heat sink; and make-up to the shield water surrounding the calandria vessel increases the passive thermal capacity of the shield water for severe core damage accidents which involve the shield water system as a heat sink to slow down the progression of core melt. A schematic of the RWS is provided in Fig. IV-7.

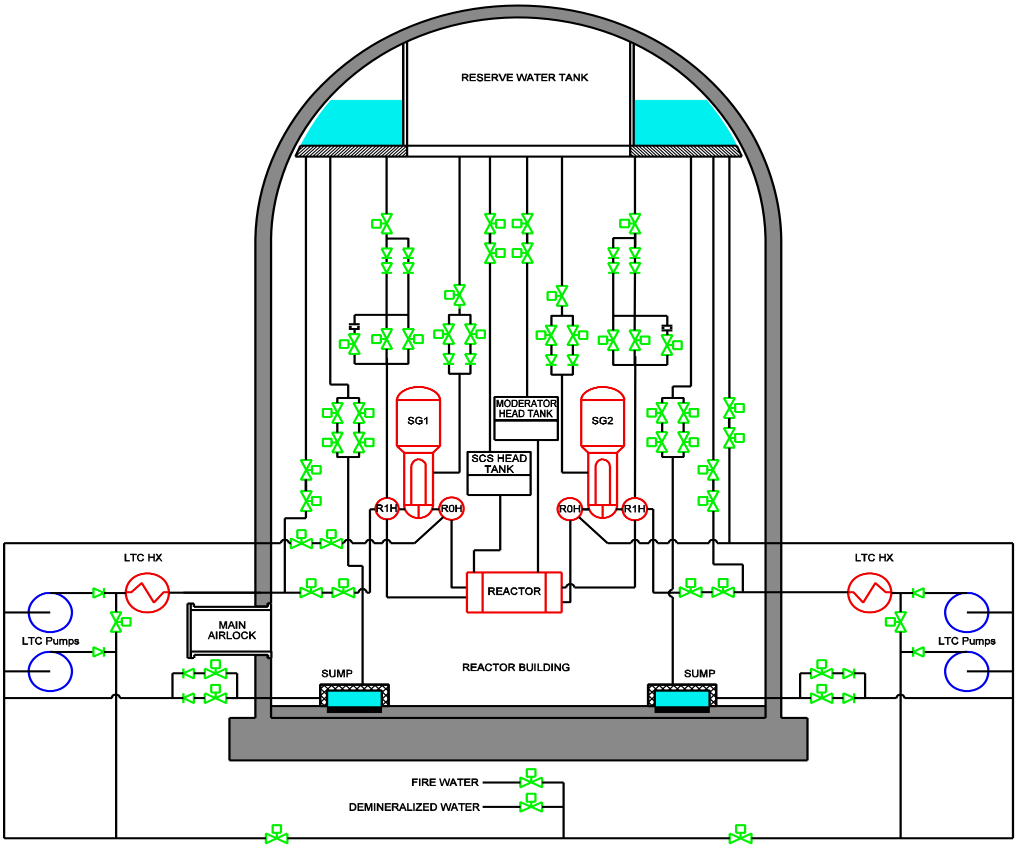


FIG. IV-7: Reserve water system (RWS).

Two separate control centres are provided to monitor plant conditions during and following design basis events. The main control room is used for normal operations but it also contains all the necessary monitoring, control and safety actuation features required to cope with abnormal events. The main control room of the two units is located in a shared building (main control building). However, separate control panels, displays and shift controls are provided for each unit. The control equipment rooms of the two units are physically separate as well. The building and the main control room are seismically qualified and protected against tornadoes. A separate secondary control area is included in each unit and is equipped with monitoring and control features sufficient for the safe shutdown and cooling of the reactor following events that may render the main control room unavailable. Also the secondary control area is seismically qualified and protected from tornadoes. For maximum separation, the secondary control area and the main control room of each unit are located on opposite sides of the containment structure.

Operator actions are performed from the main control room and, in the unlikely event that the main control room becomes unavailable, from the secondary control area. The reference ACR is designed so that all the safety actions to be taken in the short term after an initiating event are automatic. Only long-term actions may require operator intervention.

There are systems in the reference ACR design that can be considered largely passive in the sense that they function with components that have no moving parts or require at most a one-time, irreversible movement (reference is made to the IAEA safety glossary). From the standpoint of the protection from external events, the most prominent of such systems is the reserve water system described above. Other passive systems are the two fast-acting shutdown systems, one operating with insertion of rods by gravity and the other with injection of soluble neutron absorber into the moderator. Both systems are protected from external events either by qualification (e.g. for earthquakes) or by location inside the robust containment structure (e.g. for tornadoes). A further example of passive system is the Emergency Coolant Injection System, which is completely located inside the containment.

5.8. Use of IAEA publications

The key IAEA safety standards used in the design of the reference ACR include the safety guides in the design series. The safety guides in the siting series are also considered for those selected aspects and parameters, which are set as inputs to the reference design. TECDOC publications are consulted for information on good practices.

6. CONCLUSION

This paper has outlined the key features of the ACR design and has reviewed the principles and means used in the design to cope with internal and external events.

The major design features from a safety standpoint include inherent safety characteristics, reliable safety systems and safety support systems, and resistance to beyond-design-basis events.

The ACR safety basis uses a risk-informed approach for identifying and classifying internal events. Safety margins are established so that they are greater as the likelihood of the events in a class increases.

Protection against external events is accomplished through separation and qualification of the safety related systems required to cope with the events. Load combinations applied to the design of structures, systems and components take into account the potential for consequential failures of internal plant processes as a result of an external event.

REFERENCE

[IV-1] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, IAEA Safety Guide No. NS-G-1.6, IAEA, Vienna (2003).

ANNEX V

EXTERNAL EVENTS CONSIDERED IN CAREM DESIGN

D.F. DELMASTRO, S.I. LAYRAL
CNEA, Argentina

Abstract

CAREM is an Argentinean project to achieve the development, design and construction of an innovative, simple and small Nuclear Power Plant (NPP). This NPP has an indirect cycle reactor with some distinctive and characteristic features that greatly simplify the design and also contribute to a high safety level. In this paper, characteristics of the CAREM prototype and the external events considered in its design are presented. Due to the extensive use of passive safety systems with autonomy of 48 hours and the inclusion of the containment in a reactor building (which then that acts as a second containment), the CAREM NPP is shown well suited to cope with external events and their consequences.

1. INTRODUCTION

The CAREM concept was first presented in March 1984 in Lima, Peru, during an Agency conference on small and medium sized reactors. The CAREM design criteria or similar ones have been later adopted by other plant designers, originating a new generation of the integral pressurized water reactor (PWR) designs. The first step of this project is the construction of a prototype of about 27 MW(e), CAREM-25.

2. CAREM-25

CAREM-25 is an indirect cycle reactor with some distinctive features that greatly simplify the design and also contribute to a high safety level. Some of the high-level design characteristics are [V-1]:

- Integrated primary cooling system;
- Primary cooling by natural circulation;
- Self-pressurization of primary cooling system;
- Reliance on passive safety features.

2.1. Safety systems

The CAREM safety systems are passive and designed to guarantee no need of active interventions to mitigate accidents during a period of at least 48 hours. They are duplicated to fulfil the redundancy criteria. The shutdown systems are designed diverse to meet regulatory requirements.

The first shutdown system (FSS) is designed to shut down the reactor core when a deviation from normal operation occurs, and to maintain the core subcritical during all shutdown states. This function is achieved by dropping a total of 25 neutron-absorbing elements into the core, using the force of gravity.

The hydraulic control rods drives (CRDs) avoid the use of mechanical shafts passing through a reactor pressure vessel (RPV), or the extension of the primary pressure boundary, and thus eliminate the possibility of rod ejection accidents, since the whole device is located inside the RPV.

The second shutdown system is a gravity-driven injection device of borated water at high pressure. It actuates automatically when the reactor protection system (RPS) detects a failure of the FSS, or in case of a loss of coolant accident (LOCA). The 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 from the steam dome to the upper part of the tank, and the other one 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.

The residual heat removal system has been designed to reduce the pressure in the primary system and to remove the decay heat in case of a loss of heat sink (LOHS). It is a simple and reliable system that operates condensing steam from the primary system in the emergency condensers.

The emergency injection system prevents the core from being uncovered in case of a LOCA. In the event of such accident, the primary system is depressurized to less than 15 bar, using the emergency condensers, with the water level remaining over the top of the core. At the pressure below15 bar, the low pressure water injection system comes into operation. This system consists of two tanks with borated water connected to the RPV. The tanks are pressurized, so that when during a LOCA the pressure in the reactor vessel reaches 15 bar, the rupture disks break and the flooding of the RPV starts.

Three safety relief valves protect the integrity of the RPV in case of a strong misbalance between the core power and the power removed from the RPV, which would result in an overpressure. Each valve is capable of providing 100% of the necessary relief. The blow-down pipes of the safety valves are routed to the suppression pool.

2.2. Plant layout

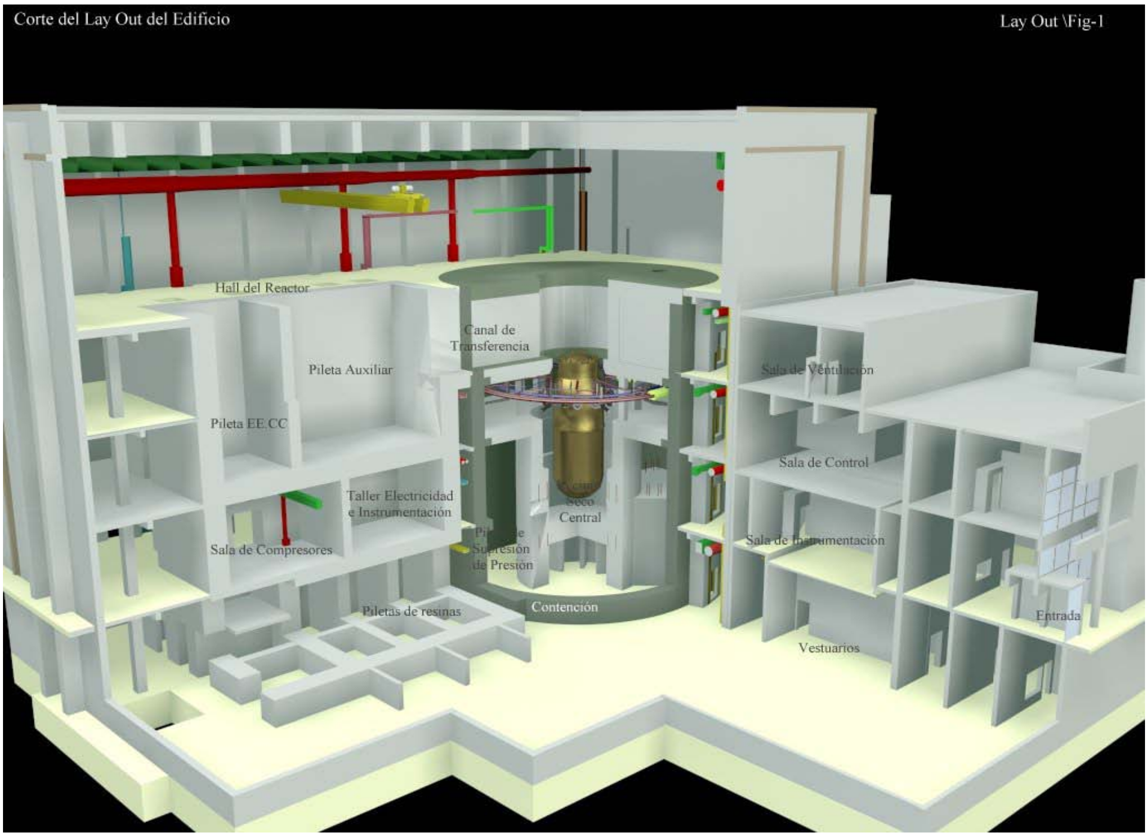


FIG. V-1. Plant layout [V-2].

The CAREM nuclear island is placed inside a pressure suppression containment system, which confines the energy and prevents fission product releases in accidents.

The building that surrounds the containment is placed in a single reinforced concrete foundation mat. It supports all structures belonging to the same seismic classification, which allows integrating the

RPV, the safety and reactor auxiliary systems, the fuel elements pool and other related systems in a single block of the reactor building (Fig. V-1).

In this way, the reactor building acts as a secondary containment. The containment itself is a freestanding, vertical, cylindrical reinforced concrete structure with flat head and bottom, designed to support pressure and temperature conditions and act as a barrier to prevent fission product release to the secondary containment in accidents.

The nuclear module has another relevant structural component shaped as a box surrounded by 5 levels. In the upper part of this box accommodated are the fuel elements pool and the auxiliary pool; the lower part hosts the liquid effluent pool and the spent resin pool.

2.3. Protection from external events

CAREM-25 relies on passive safety systems and, once they are operated, they have autonomy of 48 hours to control and mitigate accidents. During this period no operator action or external element are needed. From this point of view, many situations like NPP blackout and LOHS that could be induced by external events are easily and reliably coped with by the NPP.

The containment is included in the reactor building, which acts as a second containment and also protects the plant from external events. Together with the nuclear module being compact and small, this considerably reduces the probability of an external missile impact on the containment.

3. EXTERNAL EVENTS CONSIDERED IN CAREM-25 DESIGN

3.1. Earthquakes

Seismic features of the CAREM were defined at the basic engineering level to ensure that a single design of the structures, systems and components could be qualified for a variety of siting options.

The philosophy and terminology of the Argentinean Regulatory rules is adopted. The applicable regulation is AR 3.10.1 “Protección contra terremotos en reactores nucleares de potencia”. This norm defines the following two seismic levels for design purposes:

(1) “Severe earthquake” is similar to the safe shutdown earthquake defined by the USNRC and to the L-S2 earthquake level of the Agency guides;

(2) “Probable earthquake” is similar to the operating basis earthquake defined by the USNRC and to the L-S1 earthquake level of the Agency guides.

Since most of the targeted sites are in a moderate seismic zone, the effective acceleration of a severe earthquake was defined as 0.4 g.

The recommendations of the Agency safety guides are used as comes to the methods and detailed definitions.

3.2. Winds

The structures of the NPP will be designed to resist wind loads as indicated in Table V-1

TABLE V-1. DESIGN BASIS WIND PARAMETERS

HEIGHT (M)	WIND DESIGN SPEED (m/s)	EFFECTIVE PRESSURE (kP/m^2)
≤ 8	28.3	50
8 – 20	35.8	80
20 – 100	42.0	110
> 100	45.6	130

The wind design speed is converted to static loads according to the DIN 1055 recommendations with a gust factor of 1.0.

3.3. Tornados

The design basis tornado adopted for the CAREM is classified as F3 on the Fujita scale (corresponds to the region of Argentina with the most severe and frequent tornadoes). The design basis tornado parameters are shown in Table V-2.

TABLE V-2. DESIGN BASIS TORNADO PARAMETERS

Maximum wind speed	92 m/s
Affected width	170 –450 m
Affected length	16-50 m
Maximum rotational speed	75 m/s
Maximum rotational speed radius	45 m
Advancing speed:	
- Maximum	18.6 m/s
- Minimum	1.9 m/s
Pressure reduction	0.1 bar
Pressure reduction coefficient	0.4 bar/s
Vertical speeds	80% of horizontal speeds

Common engineering practices are adopted in the CAREM-25 design. Table V-3 shows the design basis for missiles generated by the tornadoes.

The vibrations produced as a consequence of the tornado are not considered. The considered loads associated with the tornado are:

* W_w: wind pressure
* W_p: differential pressure due to atmospheric pressure change;
* W_m: impact force of the tornado generated missiles.

The tornado loads (W_t) are obtained as different combinations of the considered loads during different phases of the tornado. For example, in phase 6 of the passage of the tornado the load is $W_{t6} = W_w+0.5W_p+W_m$.

TABLE V-3. DESIGN BASIS FOR TORNADO-GENERATED MISSILES

ITEM	MISSILE TYPE	DIMENSIONS (cm)	WEIGHT (kg)	SPEED (RELATIVE TO THE WIND SPEED)
1	Wooden table	10×30×370	90	0.8
2	Steel rod	2.5 (diameter) × 170 (length)	4	0.6
3	Steel pipe	7.6 (diameter) × 300 (length)	35	0.4
4	Steel pipe	15 (diameter) ×450 (length)	130	0.4
5	Steel pipe	30 (diameter) × 450 (length)	335	0.4
6	Light tower	35 (diameter) × 1000 (length)	675	0.4
7	Car	1.86 m^2 (frontal area)	1800	0.2

In the design of the ventilation system of the containment, the effects of tornado will be considered. The buildings protected against tornadoes are the same buildings that are seismically protected. The loss of external electric supply is assumed in the tornado design.

As an administrative measure, it is foreseen that the operational staff will receive a tornado warning from the corresponding meteorological station.

3.4. Explosions

Several buildings and structures of the CAREM are protected against pressure waves produced by explosions. A pressure vs. time function is used to consider the excess pressure impact on the protected buildings. It is assumed that the design measures used for seismic protection are sufficient to protect the NPP also against the impacts of explosions.

3.5. Ingress of gases

If possible, such events are excluded at the siting stage, by screening our sites located in the proximity of installations or transportation routes for toxic or asphyxiant gases.

In case of an eventual presence of off-site toxic gas sources, the administrative measures are foreseen for plant protection. Specifically:

- The operational staff will be informed of the presence of hazardous gases;
- A procedure will be established to close the system for air injection and extraction, and to commute the ventilation to recirculation in case of a hazardous gas warning.

Such warning will not result in a need of auxiliary diesel generators operation.

3.6. Lightning

For the design of the protection system against atmospheric discharges, standards like the NFPA-1980 and IEEE Std. 142-1972 will be taken into account. Table V-4 shows the design basis parameters to be used.

TABLE V-4. DESIGN BASIS LIGHTNING PARAMETERS

Maximum current per lightning	100 kA
Impulse period	1/50 μs

Additional measures will be taken for the building containing the control and instrumentation systems.

3.7. Fire generated from off-site sources

In this phase of the CAREM project, the design of the protection against fires is focussed on internal fires and is based on deterministic criteria. The criteria are mainly taken from the Agency NS-G-1.7 [V-3].

If possible, the proximity of zones with fire risk (forests, transportation routes for fuel and inflammables, etc.) will be avoided at a site selection stage. Devices for early detection of smoke and fires will be used in the inputs of ventilation systems.

The design will take into account measures to avoid the spill of fuel at the site due to other external events, such as earthquakes or explosions. The feasibility of off-site human-induced fires is site-specific and will be evaluated for defined sites.

3.8. Flooding

The impacts of floods will be evaluated later, for a defined site. In general the Agency's NS-G-1.2 [V-4] will be followed.

3.9. Extreme meteorological conditions

The impacts of extreme meteorological conditions will be evaluated later, for a defined site, following the recommendations of the Agency's NS-G-3.4 [V-5].

3.10. Aircraft crashes

Aircraft crashes are not considered in the CAREM-25 design. An appropriate site selection (far away from the airports or airfields) and/ or the adoption of the administrative measures (moving air corridors away) are expected to secure the values of probability of occurrence for aircraft crashes as low as required.

If this goal is not achieved, the characteristics of a plane for the design basis aircraft crash will be defined, and the loads derived from its impact will be calculated. These results will be used in structural design of the containment and other buildings relevant for reactor safety.

3.11. Event combination criteria

The external events were combined using deterministic criteria, in order to obtain the combined loads more exigent than those corresponding to a single event. For example, design basis tornado was combined with the impact of an external missile generated by the tornado.

Combinations with internal events were applied also. For example, the design basis accident for the containment is LOCA (rupture of the largest diameter primary pipe) coupled with the NPP blackout and the probable earthquake (OBE).

4. CONCLUSIONS

At its current stage, the CAREM-25 takes into account many external events and event combinations. Other, site-specific external events will be evaluated later, when a certain site for the NPP is selected.

Due to the extensive use of passive safety systems with autonomy of 48 hours and the inclusion of the containment in a reactor building (which then that acts as a second containment), the CAREM NPP is shown well suited to cope with external events and their consequences.

REFERENCES

[V-1] DELMASTRO, D., et al., CAREM: An advanced integrated PWR, Status and Prospects for Small and Medium Size Reactors (Proc. Int. Seminar, Cairo, Egypt May 2001) IAEA-CSP-14/P, IAEA, Vienna (2002).

[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, Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants, Safety Standards Series No. NS-G-1.7, IAEA, IAEA, Vienna (2004).

[V-4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001).

[V-5] INTERNATIONAL ATOMIC ENERGY AGENCY, Meteorological Events in Site Evaluation for Nuclear Power Plants, Safety Standards Series No. NS-G-3.4, IAEA, Vienna (2003).

ANNEX VI

IRIS SAFETY-BY-DESIGN™ AND ITS IMPLICATION TO LESSEN EMERGENCY PLANNING REQUIREMENTS

M. D. CARELLI, B. PETROVIC[1], P. FERRONI[2],
[1]Westinghouse Electric Co., United States of America,
[2]Politecnico di Torino, Italy, currently MIT, United States of America

Abstract

IRIS (International Reactor Innovative and Secure) is an integral configuration pressurized light water reactor being developed since late 1999 by an international consortium. Its design and safety characteristics have been amply reported. In this paper the safety-by-design™ IRIS philosophy is reviewed to show how the projected safety performance (most accidents either eliminated or inherently mitigated, core damage frequency due to internal events of the order of 10^{-8} events/year) exceeds the current norm of nuclear reactors. The IRIS project plans to use this enhanced safety response to explore the possibility of lessening, or even eliminating, the off-site emergency planning requirements. A review is given of previous attempts to attain this relaxation of licensing regulations and of current goals for advanced reactors. Finally, the proposed methodology is outlined. It consists of a combined deterministic and probabilistic approach, including a review of the defence in depth, and a risk informed analysis of a wide spectrum of accidents, rather than an evaluation of a few design basis accidents.

1. THE IRIS SAFETY-BY-DESIGN™ APPROACH

IRIS (International Reactor Innovative and Secure) is a modular 1000 MW(th) (~ 335 MW(e)) light water reactor with an integral configuration (see Fig. VI-1).

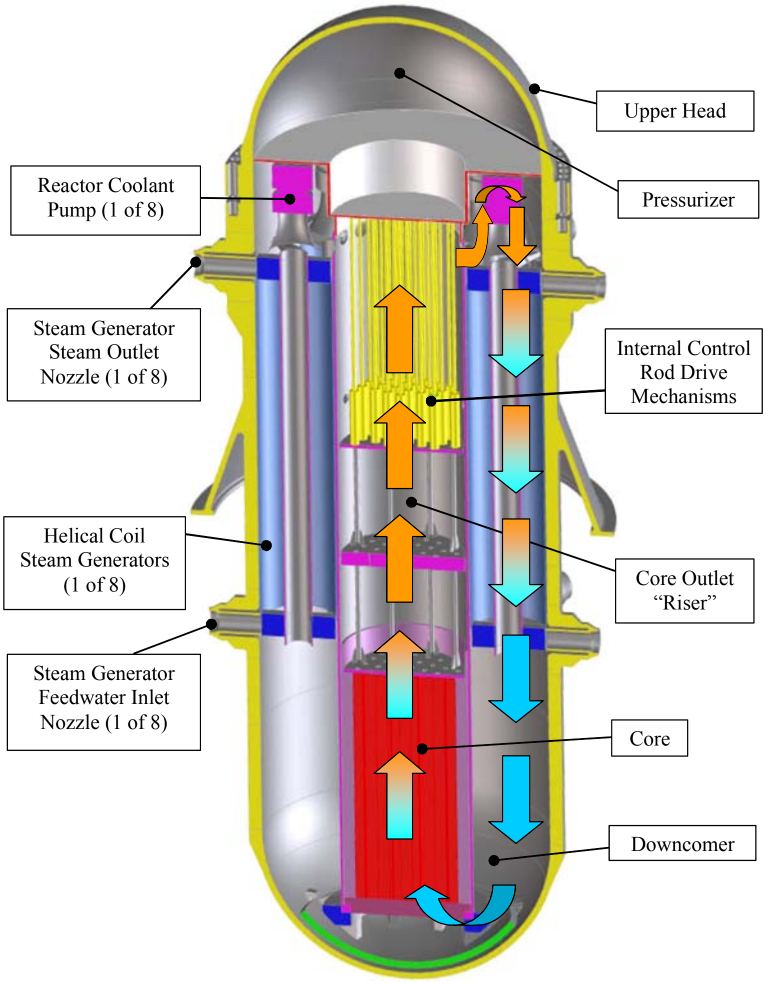

Upper Head
Reactor Coolant Pump (1 of 8)
Pressurizer
Steam Generator Steam Outlet Nozzle (1 of 8)
Internal Control Rod Drive Mechanisms
Helical Coil Steam Generators (1 of 8)
Core Outlet “Riser”
Steam Generator Feedwater Inlet Nozzle (1 of 8)
Core
Downcomer

FIG. VI-1. IRIS integral system.

IRIS has been under development since October 1999 by an international consortium led by Westinghouse Electric Co. and currently comprises 21 organizations from ten countries over four continents. The IRIS design characteristics have been reported in several prior publications (see, e.g. [VI-1 to VI-2]) and are therefore not repeated here.

IRIS is presently undergoing pre-application licensing [VI-3] with the USNRC with the goal of attaining final design approval by 2010 on the road to deployment of the first IRIS module by 2015 or even slightly earlier.

Currently being reviewed with the NRC is the safety approach that is the most unique feature of IRIS and which has been embodied in its safety-by-design™. The underlying feature is just good engineering, which is essential to all designs, i.e. it is to design the reactor such to (i) physically eliminate the possibility for some accidents to occur; (ii) decrease the possibility of occurrence of most remaining accident scenarios; and, (iii) lessen consequences if an accident occurs.

However, the integral configuration offers intrinsically unique possibilities to attain the above goals, which are not achievable with current loop type LWRs, such as elimination of large LOCAs since in an integral configuration there is no external piping. With respect to other integral designs, IRIS has from day one designed the NSSS according to the above safety-by-design™ precepts and found new solutions like the patented vessel-containment coupling which essentially controls the consequences of small and medium LOCAs. In fact, IRIS employs a small, spherical steel containment (see Fig. VI-2) where the design pressure is several times higher than in traditional large cylindrical PWR's containments (still at the same stress limit). During a small/ medium LOCA, the outside-the-break pressure (containment pressure) is thus allowed to rise, while the inside-the-break pressure (vessel pressure) decreases because of the condensation and heat removal in the internal steam generators. Thus, early in the transient (depending on the LOCA conditions, one-half to one hour after occurrence of the break) the differential pressure across the break equalizes and the loss of coolant stops. There is no need for high pressure water injection and, in fact, IRIS does not have a dedicated emergency core cooling injection system. Analyses for a variety of postulated break sizes and locations have shown that in all cases the core remains comfortably covered (see Fig. VI-3, which conservatively refers to the collapsed liquid level, while in reality the vessel contains a vapour-liquid mixture whose level is significantly higher).

Table VI-1 summarizes the implementation of the safety-by-design™. The possibilities offered by the integral configuration have been exploited in IRIS to “design in” the best safety characteristics. In fact, all accidents are affected positively with the lone exception of the feed line break, where the once-through steam generators void quickly. Even in this case however, the large water inventory in the vessel is such to overshadow the quick voiding, and the ultimate response to this accident is better in IRIS than in loop PWRs.

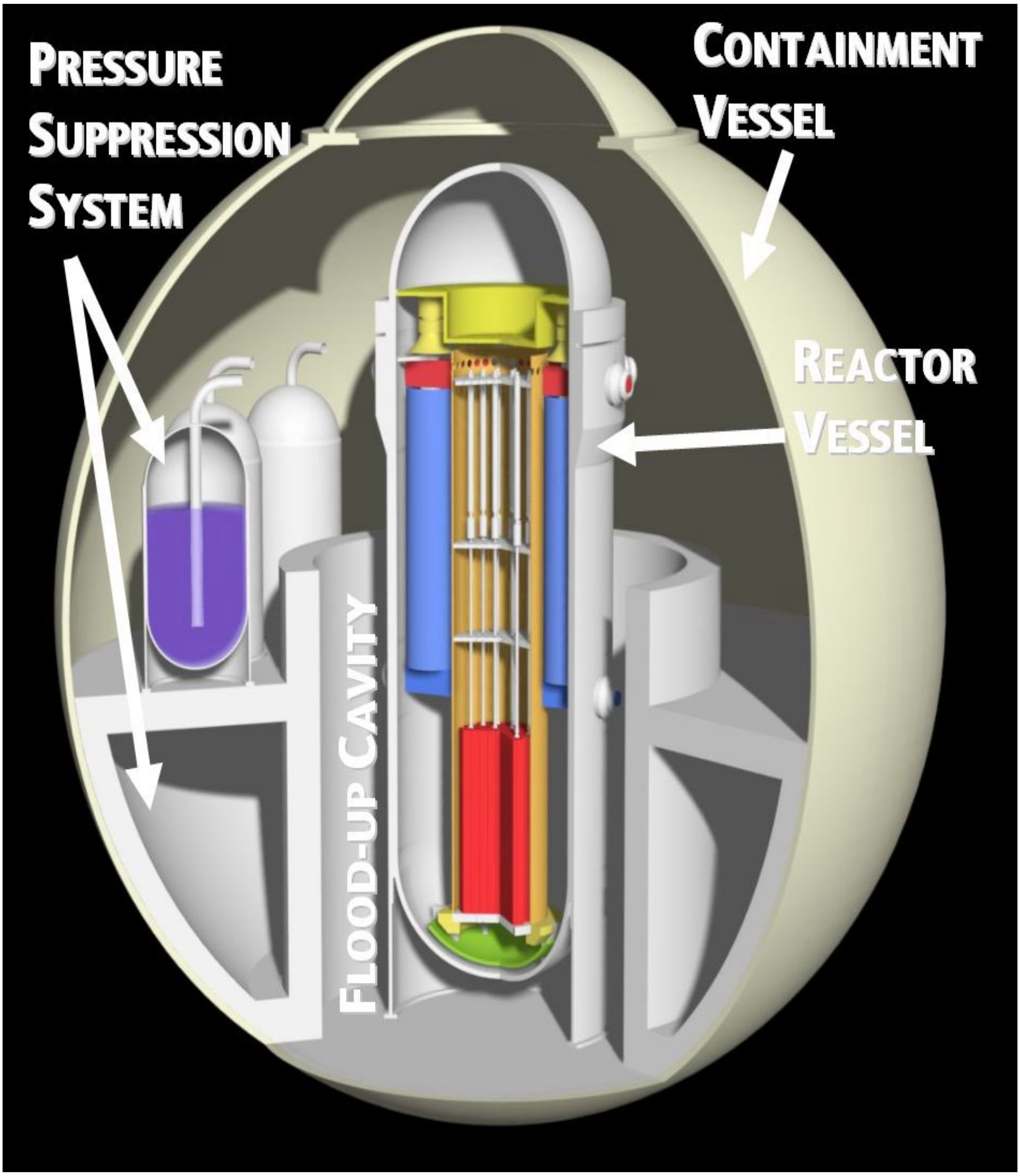
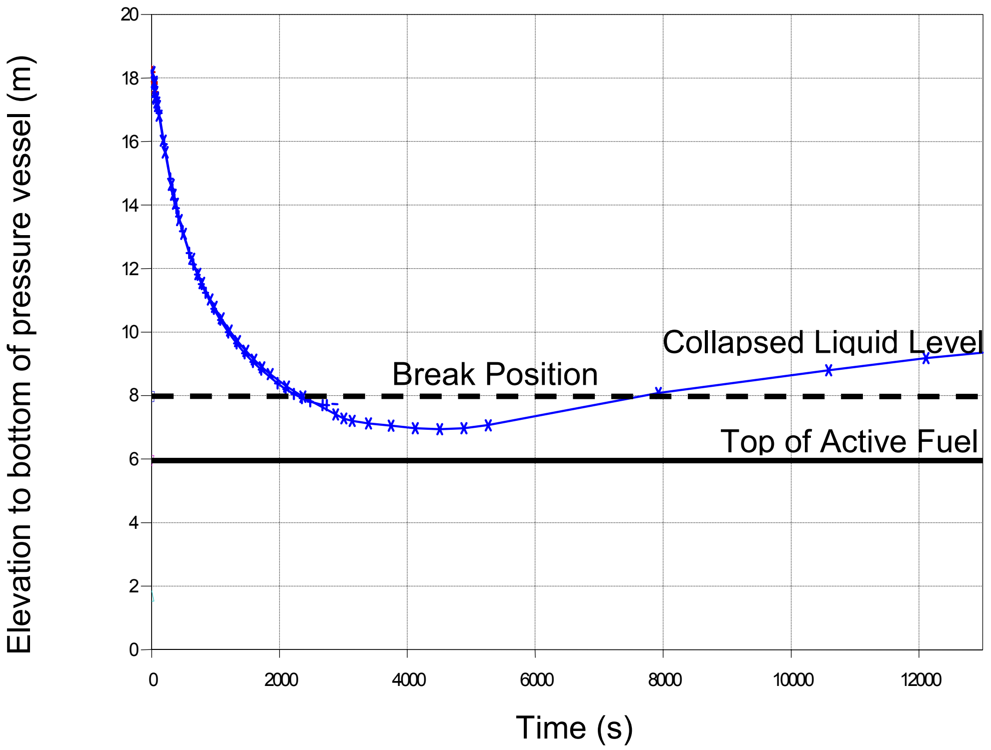


FIG. VI-2. IRIS containment.



Double ended break in the 2" direct vessel injection (DVI) line

- Collapsed liquid level very conservative, mixture significantly higher
- Conservatively assumed containment chocked full with heat structures

FIG. VI-3. Small break LOCAs in IRIS.

One of the effects of the safety-by-design™ is reported in Table VI-2: of the typical eight PWR Class IV accidents (the ones with potential core damage and radiation release to the environment), three are eliminated outright and an additional four have their probability and consequences reduced so that they are downgraded to a lower severity class. Only one accident (fuel handling) remains unaffected as a Class IV.

In parallel to the safety-by-design™, probabilistic risk analysis (PRA) has been performed [VI-4 to VI-5] and iterated with the design to identify and implement design modifications such to minimize the core damage frequency (CDF) due to postulated accidents. The estimated CDF due to internal events attained through this approach is of the order of 10^{-8} and the large early release frequency (LERF) is of the order of 10^{-9}. Both values are significantly lower than estimates for current advanced reactors; they do not mean per se that IRIS is safer, because probabilities of that magnitude, similar to that of a meteorite coming through the dining room window at a family reunion, are rather metaphysical. A more physical prospective is offered in Table VI-3. The NRC recently updated [VI-6] the five most severe accident precursors since the three mile island accident; none of these can occur in IRIS, and similar ones are intrinsically mitigated.

The IRIS project has therefore decided to take advantage of these unequalled safety characteristics and to investigate the possibility of leveraging them to attain "next level licensing", i.e. to reduce, or even eliminate, the current requirement for off-site emergency response planning (for short, referred to in the rest of this paper as "no emergency response").

TABLE VI-1. IMPLEMENTATION OF SAFETY-BY-DESIGN™

IRIS DESIGN CHARACTERISTIC	SAFETY IMPLICATION	ACCIDENTS AFFECTED
Integral layout	No large primary piping	▪ Large break LOCAs
Large, tall vessel	Increased water inventory Increased natural circulation Accommodates internal control rod drive mechanisms (CRDMs)	▪ Other LOCAs ▪ Decrease in heat removal ▪ Various events ▪ RCCA ejection, head penetrations failure
Heat removal from inside the vessel	Depressurizes primary system by condensation and not by loss of mass Effective heat removal by SG/EHRS	▪ LOCAs ▪ All events for which effective cooldown is required ▪ ATWS
Reduced size, higher design pressure containment	Reduced driving force through primary opening	▪ LOCAs
Multiple coolant pumps	Decreased importance of single pump failure	▪ Locked rotor, shaft seizure/ break
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 cooling system pressure reduces piping failure probability	▪ Steam generator tube rupture ▪ Steam line break ▪ Feed line break
Once-through steam generators	Limited water inventory	▪ Steam line break ▪ Feed line break
Integral pressurizer	Large ratio of pressurizer volume to reactor power	▪ Overheating events, including feed line break. ▪ ATWS

TABLE VI-2. TYPICAL PWR CLASS IV ACCIDENTS AND THEIR RESOLUTION IN IRIS DESIGN

CONDITIONS IV DESIGN BASIS EVENTS		IRIS DESIGN CHARACTERISTIC	RESULTS OF IRIS SAFETY-BY-DESIGN™
1	Large break LOCA	Integral reactor vessel layout – no loop piping	Eliminated by design
2	Steam generator (SG) tube rupture	High design pressure once-through SGs, piping, and isolation valves	Reduced consequences, simplified mitigation
3	Steam system piping failure	High design pressure SGs, piping, and isolation valves. SGs have small water inventory	Reduced probability, reduced (limited containment effect, limited cooldown) or eliminated (no potential for return to critical power) consequences
4	Feedwater system pipe break	High design pressure SGs, piping, and isolation valves. Integral RV has large primary water heat capacity.	Reduced probability, reduced consequences (no high pressure relief from reactor coolant system)
5	Reactor coolant pump shaft break	Spool pumps have no shaft	Eliminated by design
6	Reactor coolant pump seizure	No departure from nucleate boiling (DNB) for failure of 1 out of 8 reactor coolant pumps (RCPs)	Reduced consequences
7	Spectrum of control rod ejection accidents	With internal CRDMs there is no ejection driving force	Eliminated by design
8	Design basis fuel handling accidents	No IRIS specific design feature	No impact

TABLE VI-3. IMPLICATIONS OF THE IRIS SAFETY-BY-DESIGN™ ON THE 5 MOST SEVERE ACCIDENT PRECURSORS SINCE 1979 AS RANKED BY NRC

RANK	YEAR	PLANT	ACCIDENT PRECURSOR	IRIS
1	1979	Three Mile Island	Pressurizer power operated relief valve stuck open Partial core meltdown occurred	Same accident cannot occur: IRIS has integral pressurizer and no power operated relief valve. Similar accidents (any small break LOCA) have intrinsic mitigation (core always covered)
2	1985	Davis Besse	Total loss of feedwater (main and auxiliary) Core damage probability = $7*10^{-2}$	Cannot occur: IRIS safety grade decay heat removal system (EHRS) does not require any source of water injection to the steam generators; also, increased primary side thermal inertia inherently mitigate loss of main feedwater events
3	1981	Brunswick	Residual heat removal (RHR) U-tubes heat exchanger failure due to blockage (oyster shells) Core damage probability = $9*10^{-3}$	A BWR event; eliminated by design and operational procedures for RHR, inherent mitigating features
4	1991	Shearon Harris	Unavailability of high pressure safety injection (HPSI) pump Core damage probability = $6*10^{-3}$	Cannot occur: IRIS does not need, thus does not have safety related HPSI pumps
5	2002	Davis Besse	Degraded vessel head; unqualified coatings and debris in containment; potential HPSI pump failure during recirculation Core damage probability = 6*10-3	Cannot occur: IRIS has no vessel head penetrations by adoption of internal CRDMs and has no HPSI pumps

One important consideration, however, is that while, thanks to the safety-by-design™ approach and the PRA guided design, a CDF of the order of 10^{-8} was obtained for internal events, a similar effort has not been performed for the external events. Historically, reactor designers have focused on accident initiators from the nuclear system and thus have driven down the CDF due to internal events. In advanced light water reactors adopting passive safety, the internal events CDF was reduced to the 10^{-6} to 10^{-7} range. External events CDF has also benefited in the new designs, but only to some extent, so that their contribution to the total CDF is equal to or greater than for internal events. The IRIS safety-by-design™ has eliminated many initiators of internal events and consequently the internal events CDF has decreased by at least another decade when compared to passive light water reactors. Still, the external events initiators have not yet been addressed and thus at least for now, the CDF due to external events, such as seismic, is the preponderant factor in the total CDF for IRIS. Consequently, plans have already been made to apply both the safety-by-design™ philosophy and the PRA guided design approach to design the plant such to minimize the external events contribution to CDF to a level lower or at most comparable to that of internal events. This procedure, while developed for IRIS, is of course applicable to any other reactor still in the design stage.

2. NO EMERGENCY RESPONSE: BACKGROUND

2.1. Motivation

The advantages of licensing without the requirement for off-site emergency response planning are substantial, from both the economic and social points of view.

Economically, the most immediate advantage is that there is no need for new infrastructure to facilitate rapid evacuation. This point was stressed by a member of the IRIS consortium who recalled the very expensive (several tens of million dollars) building of new roads. The most cogent experience was the Shoreham saga where the completed plant was never operated because its location in Long Island, New York, did not allow implementing a satisfactory (from the legal viewpoint) evacuation plan.

Regardless of the wiseness in the location choice, the fact remains that a 2 billion dollars plant was sold for US $1 without ever producing one spark of electricity.

If the emergency response requirements are reduced or eliminated, the plant can be located near the user, not requiring the cost of extended transmission lines and allowing co-generation, like desalination, district heating and industrial steam. Also, there will be no a priori impediment to further development and settlements in areas around the plant.

In terms of operating costs, there will be no need for special training of personnel and for periodic evacuation drills.

The economic considerations have also a corresponding social effect, which might prove to be even more important. Elimination of the emergency response requirement basically means that any nuclear power plant is going to be treated no differently than any other power producing facility (to paraphrase the Agency's INPRO goal as will be seen later in Section 2.3). Removing the red flag stigma from a nuclear plant and eliminating the most visible plant characteristics which leads to the NIMBY (not in my back yard) syndrome would significantly increase the public acceptance.

2.2. Previous Attempts and Studies

The concept of the emergency planning zone (EPZ) has been with nuclear power since the very beginning and was eventually codified in the U.S. with the regulatory guide NUREG-0396 [VI-7] and defined in the 10CFR 50.47 as a ten-mile radius for the Plume Exposure Pathway area. It was not long before revisions and modifications were sought. In 1985 the licensee for the Calvert Cliffs plant requested the EPZ reduction from ten to two miles and in 1986 the Seabrook plant requested a reduction to one mile [VI-8]. Both petitions were rejected by the NRC, the former because severe accident issues were still under study by NRC and the latter because the supporting documentation did not contain sufficient justification.

After these two early failures, there were no more licensee petitions, but rather studies and investigations were performed by various organizations, fuelled by the excellent safety record of operating plants and the enhanced safety characteristics of advanced reactors, which were later called Generation III and III+.

The NRC staff in 1993 raised the issue "should advanced reactors with passive advanced design safety features be able to reduce emergency planning zone and requirements?"[VI-9]. No changes were actually proposed but it indicated that a revision of the EPZ was not an impossibility, should a cogent case be made. Later on, an evaluation of emergency planning for advanced reactors was conducted by the NRC in SECY-97-020 [VI-8] reaching the conclusion that the existing NUREG-0396 approach was also appropriate for the new plants, which were on the drawing boards. At the same time, however, it was recognized that "changes to EP requirements might be warranted to account for the lower probability of severe accidents and the longer time period between accident initiation and release of radioactive material for most severe accidents associated with evolutionary and passive advanced LWRs". In order to justify these types of changes, three main issues had to be addressed:

(1) Probability level below which accidents will not be considered for emergency planning (the so-called "cut-off probability" or "cut-off frequency");
(2) Use of increased safety in one level of defence in depth to justify reducing requirements in another level;
(3) Acceptance by federal, state and local authorities.

As it will be seen in Section 3, the methodology proposed by the IRIS project addresses the above issues.

In 1999 EPRI conducted a review of emergency planning for the three US ALWRs, i.e. AP600, ABWR and System 80+[VI-10]. A very comprehensive evaluation was conducted to assess how the ALWR did actually "stack up" against regulations. The EPRI study did (a) confirm conformance with the utility requirement document (URD) criteria; (b) quantify ALWR performance and find that

ALWR doses at 0.5 miles were less than the NUREG doses at ten miles; and, (c) define a cost effective ALWR specific emergency planning.

Of particular relevance to the IRIS proposed methodology is the EPRI approach to actually factor the ALWR performance and the emphasis posed on a probabilistic, risk analysis. Steps recommended for tempering the current emergency planning criteria were:

- Use as a starting point the complete set of accident sequences in the ALWR specific PRA;
- Identify those sequences, which have probability so low that it would not be meaningful to include them, or for which the time before a significant release occurs is large enough to provide adequate warning. Remaining sequences are to be included in a NUREG-0396 type assessment.
- Review the design to confirm the existence of design features and capabilities, which support the low probability of occurrence and long time delay;

EPRI recommended a cut-off probability value of 2×10^{-9}, i.e., three decades below the average ALWR CDF of 2×10^{-6}. For the release time delay, a value of 24 hours or longer would qualify a sequence for being eliminated.

The most recent study in the U.S. was by the Nuclear Energy Institute [VI-11], which focused on a risk-informed, performance-based regulatory framework. The document resulted in a set of regulations for a new 10CFR Part 53, intended to be an alternative to the 10CFR50. NEI 02-02 addresses the issue of how to blend the traditional defence in depth approach with the proposed risk informed regulation. Strategic areas were identified: reactor safety; radiation safety; safeguards; and, administrative. Each area was divided in specific cornerstones. For the reactor safety area, the cornerstones were: initiating events; mitigation; functional barriers to radionuclide release; and, emergency preparedness. It is not required that part 53 and part 50 have the same strength at each level of the defence in depth, but only that the whole strength of the defence in depth be equivalent. Thus, a higher safety degree at some level can compensate for a lower value at others. This is along the lines of issue 2 discussed by the NRC in SECY 93-092 [VI-9].

The third issue of SECY-93-092 was in a sense addressed in a recent study [VI-12] conducted in the Republic of Korea in 2003 to investigate reduction of the EPZ for APR 1400. A key topic of this study was public acceptance. While the technical evaluation indicated that the EPZ radius could be reduced to as low as 700 m instead of the 8 to 10 km required by the Korean regulations, the public was against such a drastic reduction. This applied to both neighbouring residents and occupational workers at the Kori site. Even though the workers were overall more favourable, as one would expect, the message from the public was loud and clear that a technical justification is not enough, but a deep understanding and trust by the public is necessary.

2.3. Current positions and goals

The two major initiatives worldwide on development of next generation reactors are the U.S. led Generation IV initiative and the Agency INPRO (International Project on Innovative Nuclear Reactors and Fuel Cycles).

Both initiatives require that next generation advanced reactors have superior attributes in the areas of economy, safety, sustainability and waste minimization. For each area several goals are stated which must be attained by the advanced reactors of the future. One of the goals in the safety area is the elimination of emergency response planning.

For the Generation IV program this goal is stated [VI-13] as “no credible scenario should exist for release of radioactivity requiring offsite response to ensure public safety.” In elaborating on the rationale and implementation of this goal it is stated: “this goal is not to be construed as zero possibility of any accidental release rather, the focus of this goal is to eliminate the need for formal emergency planning”; a reasonable measure of this goal could be expressed as “no credible accident scenarios that could result in off-site release of radiation exceeding U.S. protection action guidelines; these guidelines may change as improved radiation dose-response models are developed.” The above clearly states that the goal is reached through a combination of intrinsic safety performance of the advanced reactor and a corresponding modification of the regulatory guidelines prompted by an improved technology.

The INPRO goal is stated [VI-14] as that the Innovative Nuclear Energy Systems (INS) “shall not need relocation and evacuation measures outside the plant site, apart from those generic emergency measures developed for any industrial facility”. INPRO is thus the first to state clearly that next generation reactors should be able to be treated no differently than any other industrial facility. It is in fact further declared that “the end point should be to make the risk of INS comparable to that of industrial facilities used for similar purposes, so that for INS there will be no need for relocation or evacuation measures outside the plant site.” Some criteria to satisfy this goal are specified, and they are significantly less conservative than in other studies. It is also suggested that “safety analyses will involve a combination of deterministic and probabilistic assessments, including best estimate plus uncertainty analysis.”

After the publication of the INPRO document, the Agency has reiterated that attainment of the no emergency response is a primary goal and within a recent Coordinated Research Project (CRP) dedicated to small reactors without on-site refuelling it has granted agreements/ contracts to five IRIS organizations (Westinghouse, USA; Polytechnic of Milan, Italy; Eletronuclear, Brazil; University of Zagreb, Croatia; Lithuanian Energy Institute, Lithuania) to investigate aspects of a methodology to obtain such goal. This methodology will be briefly outlined in the next section.

3. PROPOSED METHODOLOGY TO RE-EVALUATE EMERGENCY REQUIREMENTS

The methodology proposed by the IRIS project to investigate modifications to the emergency response regulations includes many of the suggestions and recommendations of previous studies examined in Section 2, within a comprehensive framework anchored on the fact that IRIS has indeed excellent safety characteristics. This methodology is however not exclusive for IRIS and can be adapted to other designs as well, provided that they offer a level of safety comparable to IRIS.

The proposed approach is articulated over the following tenets:

- Combine deterministic and probabilistic assessments;
- “Trade-off” barriers in the defence-in-depth;
- Consider the whole gamut of accidents;
- Do not postulate a priori accidents’ sequences and characteristics;
- Evaluate accident consequences along with their probability of occurring.

They will be briefly discussed in the following.

All the most recent studies emphasize the need for a risk informed, probabilistic approach. There is no question that a probabilistic risk assessment is necessary because any human endeavour has an associated risk and a certain level of risk is generally non-controversial and tacitly accepted. This is not the case, however, for nuclear power and an illogical zero risk policy is requested by a segment of the population. A strictly deterministic approach caters to this position, but it leads to a self-fulfilling prophecy because almost any accident sequence, if followed through a series of unrealistic assumptions, will eventually lead to core damage and radiation release.

The IRIS position is that its safety-by-design™ — by eliminating accidents — offers the deterministic “safety blanket” sought by the public. Table VI-3 is a most powerful exhibit in this respect. Once the large “bad” accidents (loss of coolant, pump stoppage, control rod ejection, etc. as in Table VI-2) are out of the way, the probability/ risk argument should have a better chance of being accepted by the general public.

Implementing previous suggestions, as by NRC itself and NEI, IRIS recommends an exchange in the barriers of the defence in depth, the total effect of course not being compromised. Currently, the defence in depth against radiation release is articulated through material barriers (fuel; cladding; vessel and piping; containment) and a legislative barrier (off-site emergency response). In IRIS a new barrier is provided by the safety-by-design™, which eliminates upfront many severe accidents. The materials barriers are retained and actually a new one is added: the large coolant inventory in the vessel, which is a powerful contributor to the long time delay following an accident (Section 2.2., EPRI study). In addition, the transient response in IRIS is very relaxed; e.g., the coolant transit time from the exit of the steam generators to the core exit is of the order of 20 seconds, giving ample room for corrective action. Thus, the intent of this methodology is to demonstrate that an equivalent or better overall defence in depth is maintained when the legislative barrier is substituted with the safety-by-design™ barrier.

Current licensing is based on evaluation of selected design basis (and beyond design basis) accidents with pre-determined characteristics in keeping with the deterministic approach. In this approach there is also the pre-ordained conclusion that there will be consequences leading to and eventually needing an emergency response. The IRIS approach is to consider the gamut of possible accidents, not just a few selected basis accidents. This is quite a challenging endeavour, but still manageable because a number of accidents are not existent in IRIS and because of the great improvements over the last decade in analytical and computational methods accuracy and speed.

Rather than postulate a priori the accident consequences (e.g. "there shall be a core melting") or its characteristics (e.g. a specified time of release for radiation), the accident sequence will be followed through, without pre-conceived limitations. Obviously, assumptions have to be made as the sequence progresses. "Realistic conservatism" will be used in modelling assumptions; by this it is meant that conservative assumptions will be selected, as long as they do have a physical meaning. When assuming failure of a component or any other path necessary to proceed deeper in the accident, such paths will be tagged with their probability value. The sequence will be followed through to its eventual conclusion, quantifying the amount of radioactive release, if any, to the environment and its probability (cumulative probability of the events' paths through the sequence). Thus, each accident sequence is characterized quantitatively by its consequences and its probability. The released dose from each accident and its probability are calculated as a function of site distance. In this site evaluation, the recommendations from the regulatory guides will be used in order to assess only the effect introduced by IRIS, not by the particular site. Finally, the obtained results will be compared with the regulatory guides recommendations and with the dose thresholds for activation of emergency planning response.

A source of controversial debate is expected to be what is the level of probability for accident consequences in a "regular" plant to be considered "acceptable" and whether such value would also be acceptable for the same consequences when originated by a nuclear plant. The international nature of the IRIS consortium will be an asset in answering these questions as data on the nuclear regulatory climate and public acceptance will be collected worldwide.

4. CONCLUSIONS

The effort proposed here could be of momentous consequence for the nuclear power industry. It is not new, since, as it has been seen, most of the elements of the IRIS proposed technology have already been authoritatively presented and examined. However, this is the first attempt ever to plainly assert and implement that a nuclear power plant should be considered and treated no differently than any other similar purpose facility, period.

There is no question that this is a monumental endeavour, which is by no means guaranteed to succeed. Apart from the intrinsic technical difficulties (while the IRIS project believes that analyses will show the capability to eliminate the off-site emergency response requirement, it has to be proven), "political" difficulties may be overcoming. An off-site emergency, no-population zone, has been a characteristic of nuclear plants since Day One. There will be resistance from regulatory bodies and there is public mistrust (see, e.g. the Korean study). The U.S. utilities are not terribly interested for now, because already licensed sites exist for future new build. And, previous attempts have failed.

Still, now is the appropriate time to pursue this goal. There is a combination of events, which may not occur again. Nuclear power has been in the doldrums for the last almost thirty years and the slide into what its opponents hope to see as the road to oblivion has been accelerated by the hostile attitude of some governments of Western Europe with the mandated present and future closure of existing plants, as well as the prohibition of building new ones. But, this time there has been the beginning of a backlash, both in the political and public attitude areas. A few, rational thinking environmentalists have dared to say that nuclear must be considered if one wants to fight against global warming. At the same time, a new breed of nuclear reactor designs have come out, with simpler, more economic design and greatly enhanced safety. We do have now a new product in a new environment; a moment which must be seized. On the specific subject of reviewing the emergency response requirement, there is at least an "intellectual pursuit" in the U.S. and strong support overseas, with the Agency offering high visibility.

There is no question that this "first try" is exceedingly important. If failed, the momentum will be gone and it will be very difficult in the future to overcome the precedent of this failed attempt. Thus, the case must be well prepared and supported. Because of all the considerations previously discussed, it needs well more than a "necessary and sufficient" justification. More than anything else, a credible proponent and a solid design must anchor it. IRIS provides a positive answer to both. Westinghouse does not need any introduction and leads an international consortium of twenty-one organizations from ten nations, which comprise some of the best known names in industry, academia and research establishments. The IRIS project through its safety-by-design™ provides the most cogent case of enhanced safety.

Another consideration is that IRIS is a PWR, the most widely used and licensed technology in the world with well understood potential accident sequences. Thus, it requires the least "leap", because a straight comparison is possible with current practice, without introducing additional uncertainties which will inevitably arise if this new regulation is applied to reactor technologies different from water coolant, which are unfamiliar and have a limited, if any, data base. This said, it must be emphasized that while it is recommended that the IRIS project be the trailblazer in this effort, the methodology exposed here is essentially technology neutral and, thus, this effort can provide the basis for similar efforts by other advanced reactors. The IRIS consortium is open, by its very nature, to collaboration and joint efforts. Of particular importance is the role of the Agency, which is proactively pursuing the re-evaluation of the emergency response requirements for advanced reactors. As mentioned, five IRIS consortium organizations are participating in an Agency sponsored effort, which will provide the first test bed of the programme here outlined.

REFERENCES

[VI-1] CARELLI, M.D., IRIS: A global approach to nuclear power renaissance, Nuclear News, 46**,** No. 10 (Sep. 2003), pp. 32–42.

[VI-2] CARELLI, M.D., et al., The design and safety features of the IRIS reactor, Nuclear Engineering Design, 230, (2004), pp. 151–167.

[VI-3] CARELLI, M.D., KLING, C.L., RITTERBUSCH, S.E., IRIS Pre-application licensing, GLOBAL 2003 (Proc. Int. Conf., November 16–20, 2003, New Orleans, LA, USA), ANS/ENS.

[VI-4] FINNICUM, D., et al., 2003. IRIS Preliminary PRA analysis, GLOBAL 2003 (Proc. Int. Conf., November 16–20, 2003, New Orleans, LA, USA), ANS/ENS.

[VI-5] MAIOLI, A., FINNICUM, D. J., KUMAGAI, Y., IRIS Simplified LERF model, ANES 2004 (Proc. Int. Conf., Miami, FL, October 3–6, 2004).

[VI-6] DAVIS-BESSE Had an extra 0.6 percent chance of core damage, Nuclear News, 47**,** No. 11 (Oct. 2004), p.18.

[VI-7] NUREG-0396: Planning basis for the development of state and local government radiological emergency response plans in support of light water nuclear power plants (Dec. 1978).

[VI-8] THOMPSON, JR., HUGH L., SECY-97-020: Results of evaluation of emergency planning for evolutionary and advanced reactors (Jan. 1997).

[VI-9] SECY-93-092: Issues pertaining to the advanced reactor (PRISM, MHTGR, and PIUS) and CANDU 3 design and their relationship to current regulatory requirements (April 1993).

[VI-10] EPRI TR 113509, Technical aspects of ALWR emergency planning (September 1999).

[VI-11] NEI 02-02, A risk-informed, performance-based regulatory framework for power reactors (May 2002).

[VI-12] LEE, Y.W., KANG, C.S., MOON, J. H., Reduction of EPZ area for APR1400 and its public acceptance, from progress in nuclear energy, Vol. 44, No. 2 (2004) pp. 75–84.

[VI-13] DOE, A technology roadmap for Generation IV nuclear energy systems. U.S. Department of Energy, GIF-02-00 (Dec. 2002).

[VI-14] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidance for the Evaluation of Innovative Nuclear Reactor and Fuel Cycles — Report of Phase 1A of the International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO), IAEA-TECDOC-1362, Vienna (2003).

ANNEX VII

VBER-300 REACTOR SAFETY UNDER EXTERNAL EVENTS

O.B. SAMOILOV, V.B. KAIDALOV, A.V. KURACHENKOV,
A.N. LEPEKHIN, V.A. PANOV
OKBM, Russian Federation

Abstract

Presented are the design features for plant protection from impacts of external events used in the design of the VBER-300 reactor, a small PWR for land-based and floating co-generation nuclear power plants (NPPs) thoroughly based on the experience in design and operation of marine modular reactors and NPPs with reactors of the VVER type. The VBER-300 reactor unit has a double protective shell (double containments) with spatially separated and redundant penetrations of process system channels and is designed in strict compliance with the Russian Federation regulatory codes and standards defining NPP performance under external events. The analysis of excitation frequencies and load distributions within the reactor unit under extreme external impacts caused by a maximum design earthquake and a maximum postulated aircraft crash provides a proof that the VBER-300 design ensures the implementation of all basic requirements to NPP performance under external event impacts.

1. INTRODUCTION

Construction of small and medium sized (SMR) nuclear power plants (NPPs) for electricity generation, heat supply and potable water production is an important trend of nuclear power development.

Activities on district heating and nuclear co-generation plants equipped with 200-600 MW(e) reactor units have been carried out for more than 20 years.

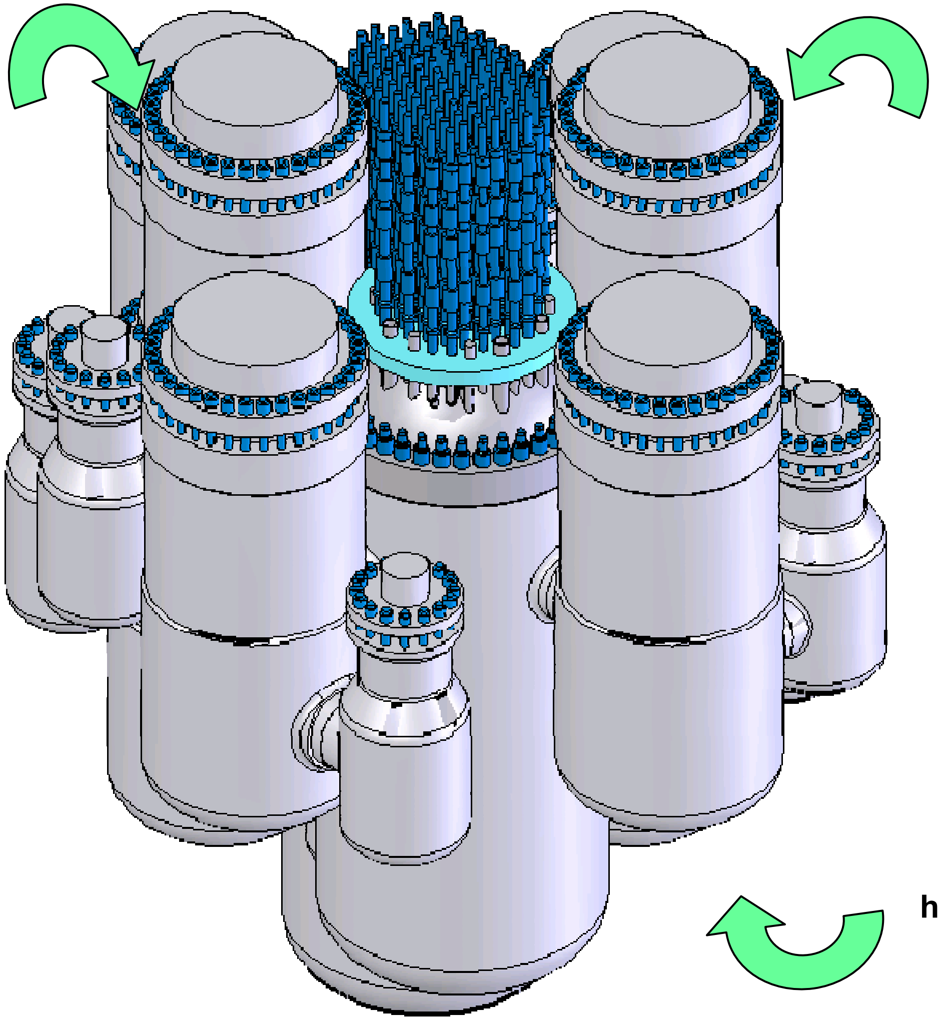
The VBER-300 reactor [VII-1] has been developed on the basis of proven technologies of Russian marine modular reactors, which have accumulated the operating experience of over 6000 reactor-years with 400 reactor units. The VBER-300 design (Fig. VII-1) also borrows from the operating experience of PWR type reactors. Nuclear co-generation plants with the VBER-300 are multi-purpose; they could be used: for heat and electricity supply to cities (Fig. VII-2); within floating NPPs for energy supply to coastal areas (Figs. VII-3, VII-4); and for seawater desalination.

2. DESIGN AND OPERATING CHARACTERISTICS OF VBER-300

The VBER-300 NPP design and operating characteristics are outlined in Table VII-1.

TABLE VII-1. CHARACTERISTICS OF VBER-300

Thermal power, MW	850
Primary pressure, MPa	15.7
Coolant temperature, °C:	
- Core inlet	292
- Core outlet	330
Coolant flow rate, t/h	13160
Steam capacity, t/h	1460
Superheated steam parameters at SG outlet:	
- Pressure, MPa	6.38
- Temperature, oC	305
Number of fuel assemblies	85
Fuel type	Uranium dioxide
Interval between partial refuellings, years	1-2
Effective full power operation per year, hours	minimum 8000
Reactor service life, years	60



USE OF PROVEN TECHNOLOGIES OF MARINE MODULAR REACTORS

- Operating experience of over 6000 reactor-years with 400 reactor units

- Long-term experience in design and fabrication of marine reactors

- Maximum use of previous R&D results

USE OF PWR-TYPE REACTOR OPERATING EXPERIENCE

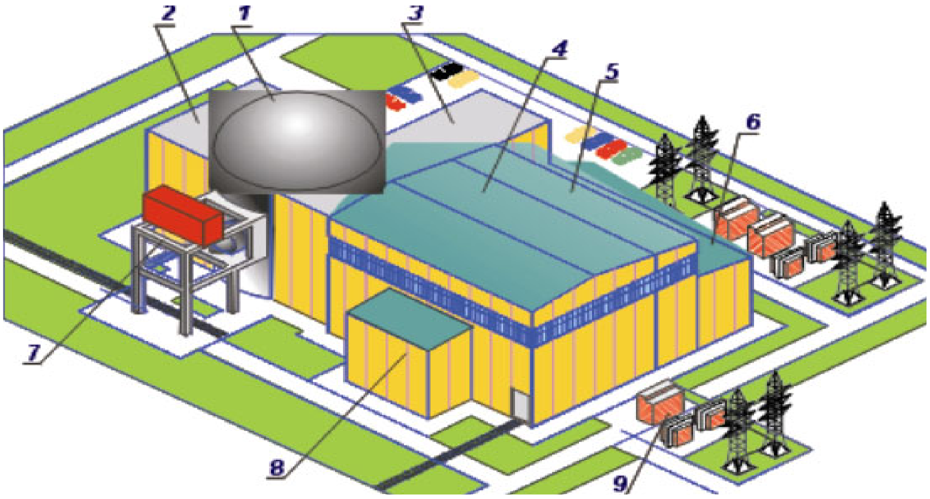
Advanced TVSA fuel assembly has been mastered at the Kalinin NPP

GUARANTEED SAFETY

Use of nuclear district heating plant developments

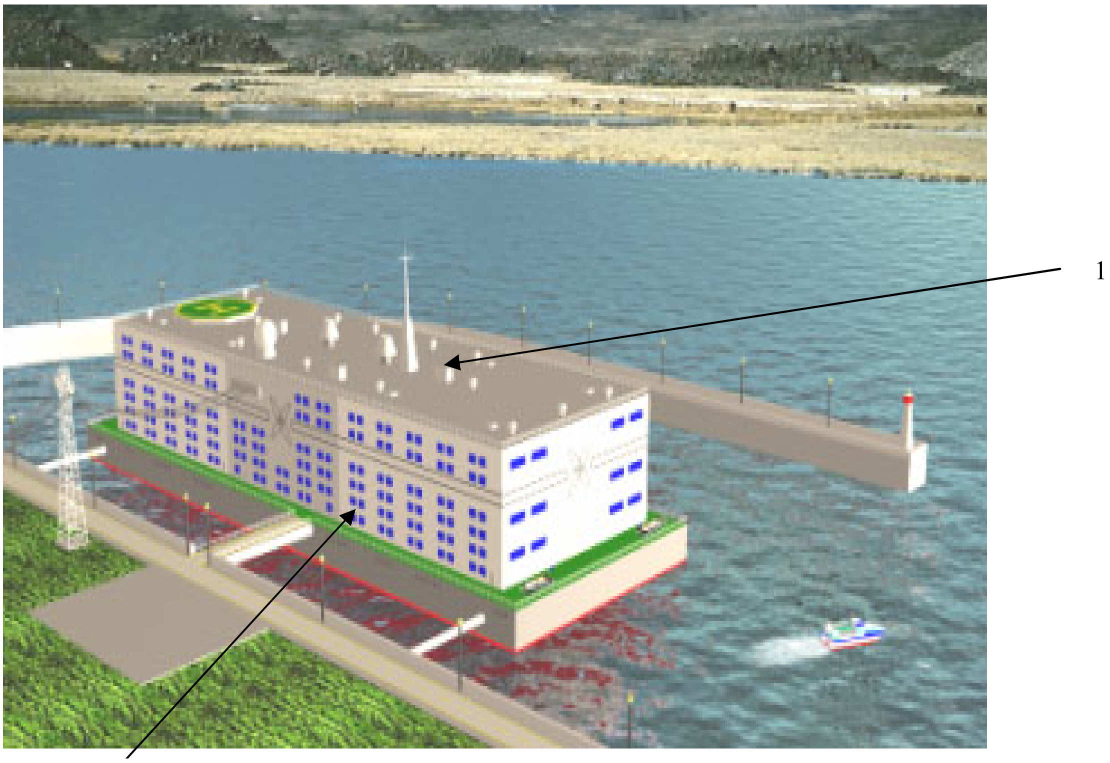
FIG. VII-1. VBER-300 reactor.

Operation of nuclear co-generation plant p	
- Electric power, MW, maximum	295
Operation of nuclear co=-generation plant power unit in heating mode:	
- Electric power, MW, minimum	200
- Heat output, Gcal/h	420
- Temperature of heating system water (supplied/removed), °C	150/70



1– reactor compartment
2- Safety systems rooms
3- Main control room
4- Turbine compartment
5-Deaerator compartment
6- Electric equipment compartment
7-Trestle
8- Auxiliary system compartment
9- Transformer plants

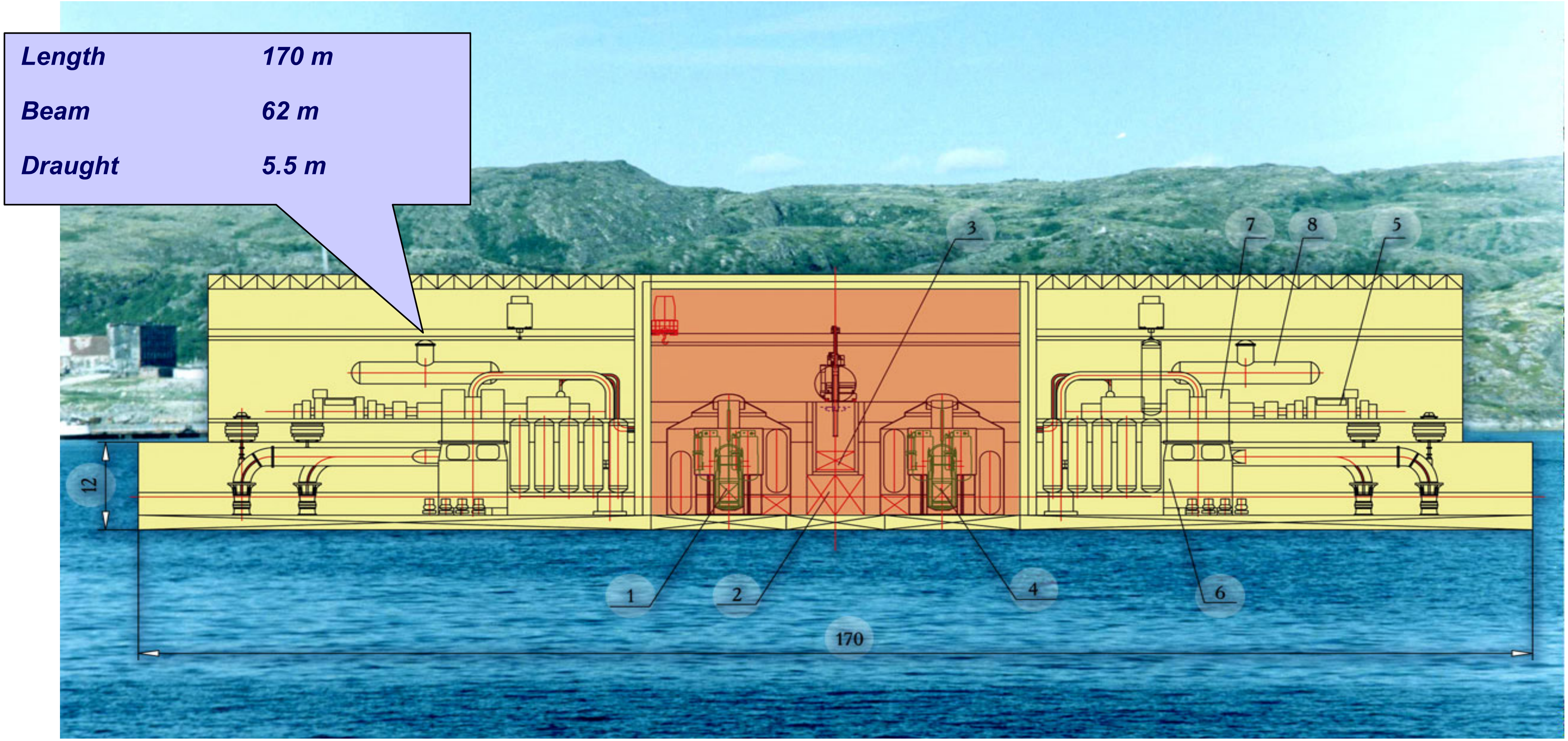
FIG.VII- 2. Land-based nuclear co-generation plant with VBER-300.



1 – Two power units with VBER-300 reactors

2 – Electric power of a floating NPP – 600 MW(e)

FIG.VII- 3. Overview of a floating NPP with VBER-300.



1 Reactor unit No. 1
2 Radioactive waste storage
3 Fresh and spent fuel assembly storage
4 Reactor unit No. 2

5 Electric generator
6 Condenser
7 Steam turbine
8 Deaerator

FIG.VII- 4. Design scheme of a floating NPP with VBER-300.

3. DESIGN FEATURES OF VBER-300 TO COPE WITH EXTERNAL EVENTS

Each nuclear co-generation plant is designed taking into account a variety of external events, as prescribed by the Russian Federation regulatory codes and standards.

Structural design of the NPP with the VBER-300 takes into account the following natural and climatic conditions, which are characteristic of the targeted location site.

- Snow load: S_o=1.0 kPa;
- Wind load: W_o= 0.38 kPa;
- Sleet load for glaze wall thickness of 10 mm;
- Temperature of outdoor air of the coldest five-day week:
  - With 0.98 probability – minus 30°C;
  - With 0.92 probability – minus 28°C.

The reactor equipment with safety systems is located inside the reactor compartment designed as a double – walled containment including inner and outer shells, Fig. VII-5. The inner shell is made of steel; the outer shell is made of ferroconcrete.

The steel shell has a cylindrical shape, 28.0 m in diameter, and is covered by a semi-spherical dome of 14.0 m radius; it has an elliptical bottom of 36.0 m radius, with 4.5 m fillet radii. The shell height is 34 m; the inner volume is 27 000 m^3.

The steel shell is designed for maximum design earthquake parameters: the excess pressure of 0.4 MPa at 150°C.

The steel shell is fabricated of standard construction steels; the wall thickness of the cylindrical part is 28 mm, the dome part - 16 mm and the bottom - 32 mm, which allows welding without any thermal treatment.

The outer shell, which is made of monolithic ferroconcrete without stressed reinforcement, is designed to protect the reactor against the impact of an aircraft crash. Deterministic analysis of load impacts was applied when selecting the design features, such as shell thickness and reinforcement. The outer ferroconcrete shell is of a cylindrical shape (34 m outer diameter and 42.2 m height), with 1.5 m wall thickness, and is covered by 1.5 m thick semi-spherical dome.

The gap between the steel shell and ferroconcrete shell is 1.5 m, which allows monitoring the steel and ferroconcrete conditions, as well as performing the necessary repair and maintenance. The gap accommodates ventilation equipment and filters intended to purify air leaks from the steel shell.

The ventilation systems used to collect air leaks also maintain the reduced pressure in the inter-shell space.

The leak-tightness of the steel shell as adopted in the design is 0.2% per day of air volume in the shell under maximum design basis accident parameters.

The air leaks from ferroconcrete shell, adopted in the design, are not more than 10% per day of the inter-shell space volume.

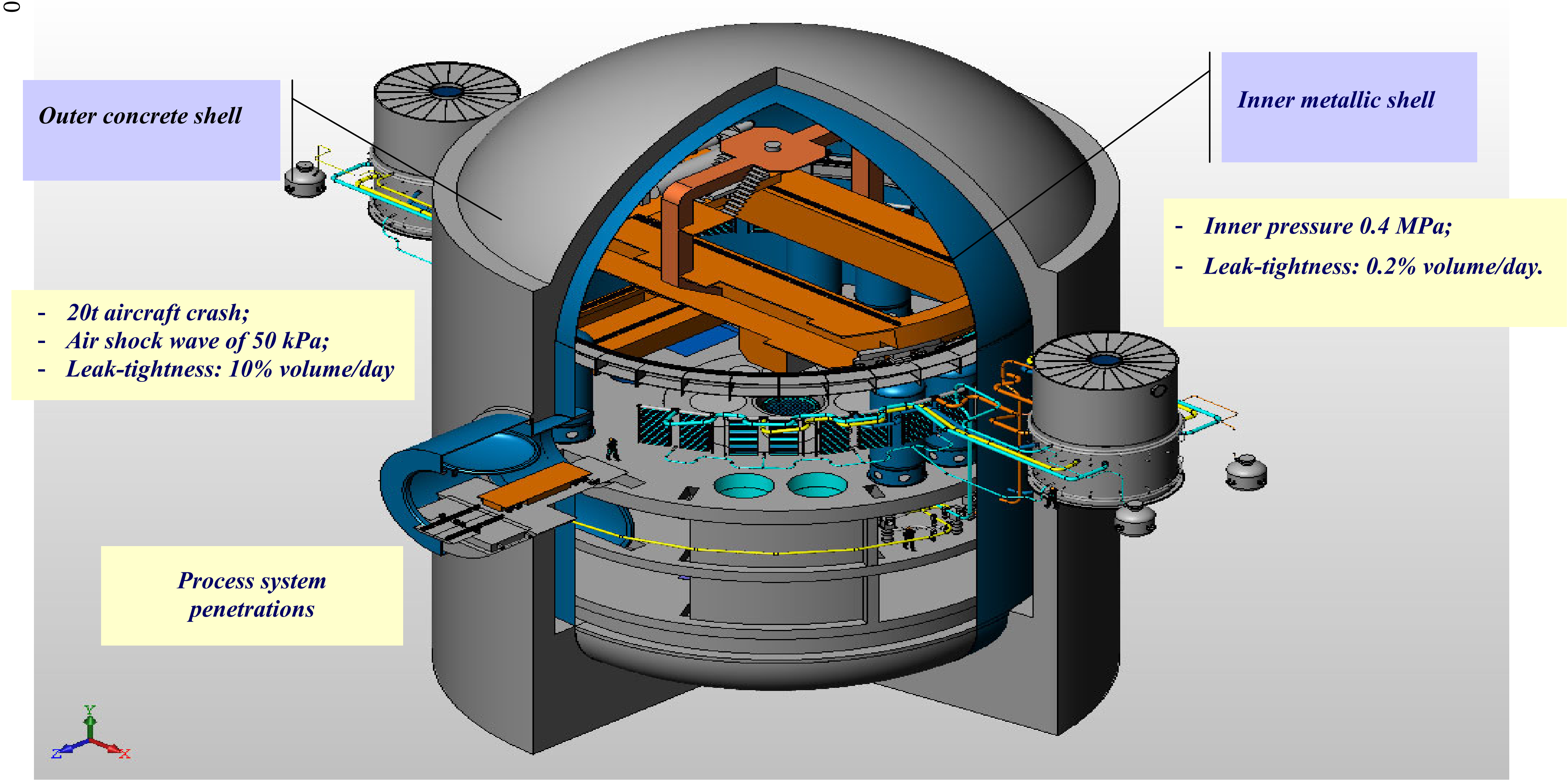

Outer concrete shell
Inner metallic shell
- Inner pressure 0.4 MPa;
- Leak-tightness: 0.2% volume/day.
- 20t aircraft crash;
- Air shock wave of 50 kPa;
- Leak-tightness: 10% volume/day
Process system penetrations
Y
Z
X

FIG. VII- 5. Double-walled containment of VBER-300.

The reactor compartment shells incorporate penetrations of the process safety systems, protection systems and normal operation systems, which are box type structures made of monolithic ferroconcrete with 0.9 m thick outer walls and lining; they are rigidly attached to the ferroconcrete shell from two opposite sides. Such arrangement of the penetrations prevents their simultaneous destruction by a falling plane and also prevents simultaneous failure of the redundant safety systems. The outer walls and lining are designed taking into account the extreme impacts as stipulated in the codes and standards.

The structures, systems and components of a nuclear co-generation plant with the VBER-300 are designed taking into account natural and human-induced external events, providing the possibility of the NPP allocation at any suitable site that meets regulatory requirements.

The external events taken into consideration are: earthquakes; wind loads; low and high temperatures; aircraft crash; shock waves and other events according to the regulatory requirements.

The seismic events considered in the design as per the MSK-64 scale are as follows:

- Maximum design earthquake: 8 points (the horizontal components of acceleration on a free ground are 0.2 g; the vertical component is 2/3 of the horizontal one);
- Design basis earthquake: 7 points (the acceleration components are reduced twice against those in maximum design earthquake).

An aircraft crash is considered with the following parameters:

– Falling plane mass	20 000 kg[1]
– Velocity of a falling plane	200 m/s
– Impact area of a falling plane	7 - 14 m^2
– Shock airwaves are considered with the following parameters:	
– Pressure in the front	50 kPa
– Compression phase duration	Up to 1 s
– Propagation direction	Horizontal

According to the Maritime Register of Shipping, a dynamic effect of 3 g in all directions is considered for the VBER-300 as part of a floating NPP.

The VBER-300 incorporates the following basic design features to ensure plant safety under external events:

- The systems and main equipment are located in the compartments, which are designed to withstand the impacts of external events up to a direct impact of a falling plane or its parts;
- The equipment, devices, safety related system components and their joints are designed with account of possible dynamic loads from external impacts;
- The redundancy of safety system channels and their arrangement is provided in such a way that under external impacts, the remaining channel is capable of 100 % performing the necessary safety function within its design characteristics;
- The use of passive systems to protect the reactor plant and reactor compartment shell;
- Features and measures to prevent simultaneous failure of the main control room and the standby control room, as well as loss of control over the reactor power and cooldown.

The protection system channels that ensure actuation of the reactor shutdown system, core cooling and isolation systems, meet a “safe failure” principle (generate an alarm signal in case of de-energization)

[1] The considered falling plane mass is up to 50 t.

and are redundant. The emergency protection and heat removal systems are put into operation by self-actuating devices.

Under the impacts of extreme external events, the VBER-300 active and passive safety systems remain operable and secure a possibility of an external intervention.

4. ANALYTICAL STUDIES OF VBER-300 PERFORMANCE UNDER EXTERNAL EVENT IMPACTS

The VBER-300 design process included analytical studies of the reactor unit performance under various impacts caused by external events.

In particular, calculations of the reactor unit under a seismic impact of magnitude 8 as per MSK-64 scale were performed. The calculations were carried out using the DANCO code [VII-1] according to the diagram shown in Fig. VII-6.

Obtained from the calculations was an excited frequency spectrum for the VBER-300 in 0-30 Hz range and a stress-strained state load for each excited frequency. The calculations show that the most loaded reactor unit areas are the joints between nozzles and cylindrical shells of the reactor, steam generators and the pump (see Fig. VII-7).

The maximum stresses observed are 100-150 MPa, i.e., is far below the yield strength of nozzle material, which is 390 MPa.

The outer shell strength was calculated for an event of a 20 t aircraft crash using the validated DANCO code [VII-2] within the calculation diagram shown in Fig. VII-8. The shell is fabricated of M400 concrete with the tensile strength of 4 MPa and compression strength of 40 MPa. The bars made of 53GS steel of 400 MPa yield strength reinforce the shell. Cracks appear in the area where the plane contacts the safeguard shell. The cracks propagate to the first reinforcement layer to a 100 mm depth. The deformation intensity on the concrete surface in the plane crash area is ~0.1%, and the stress intensity is 10 MPa (see Fig. VII-9). The overload in the area of the reactor unit attachment to the support platform of the ferroconcrete shell is ~0.6 g, and the excitation frequency of the reactor unit is within 7-10 Hz (see Fig. VII-10).

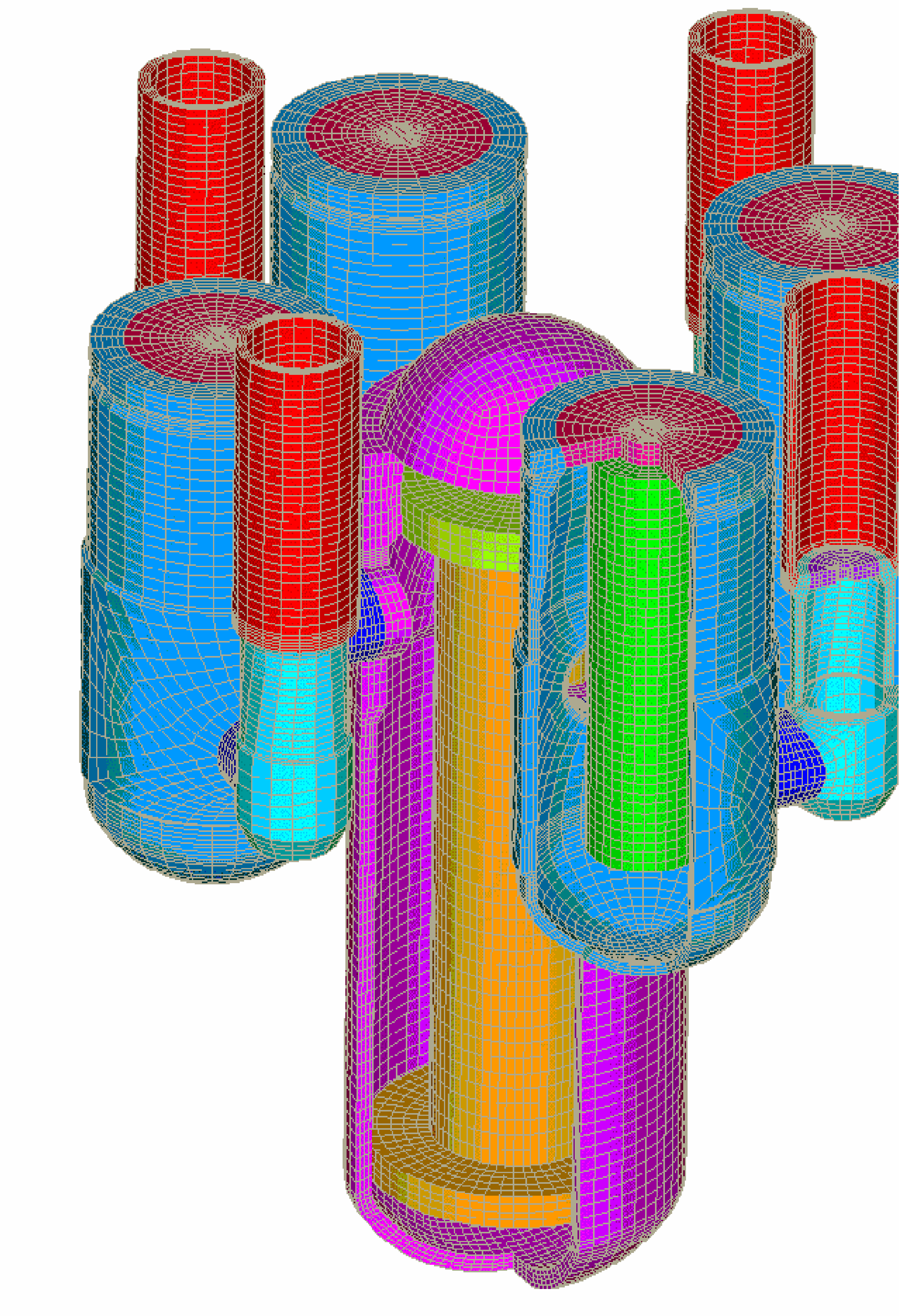


FIG.VII- 6. Calculation diagram of VBER-300 reactor unit for seismic analysis.

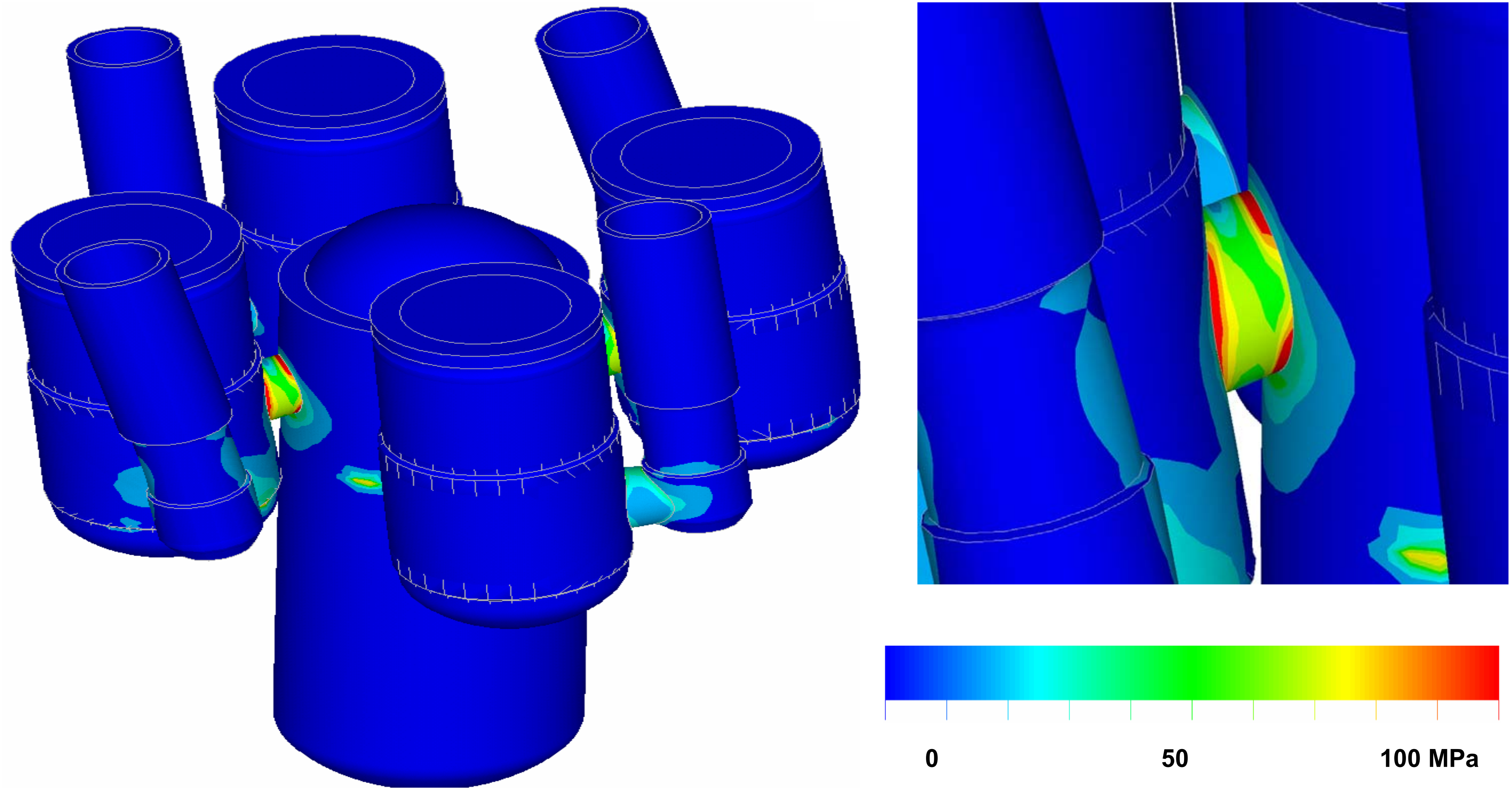


FIG. VII-7. Stress-strained state loads in VBER-300 under a seismic impact.

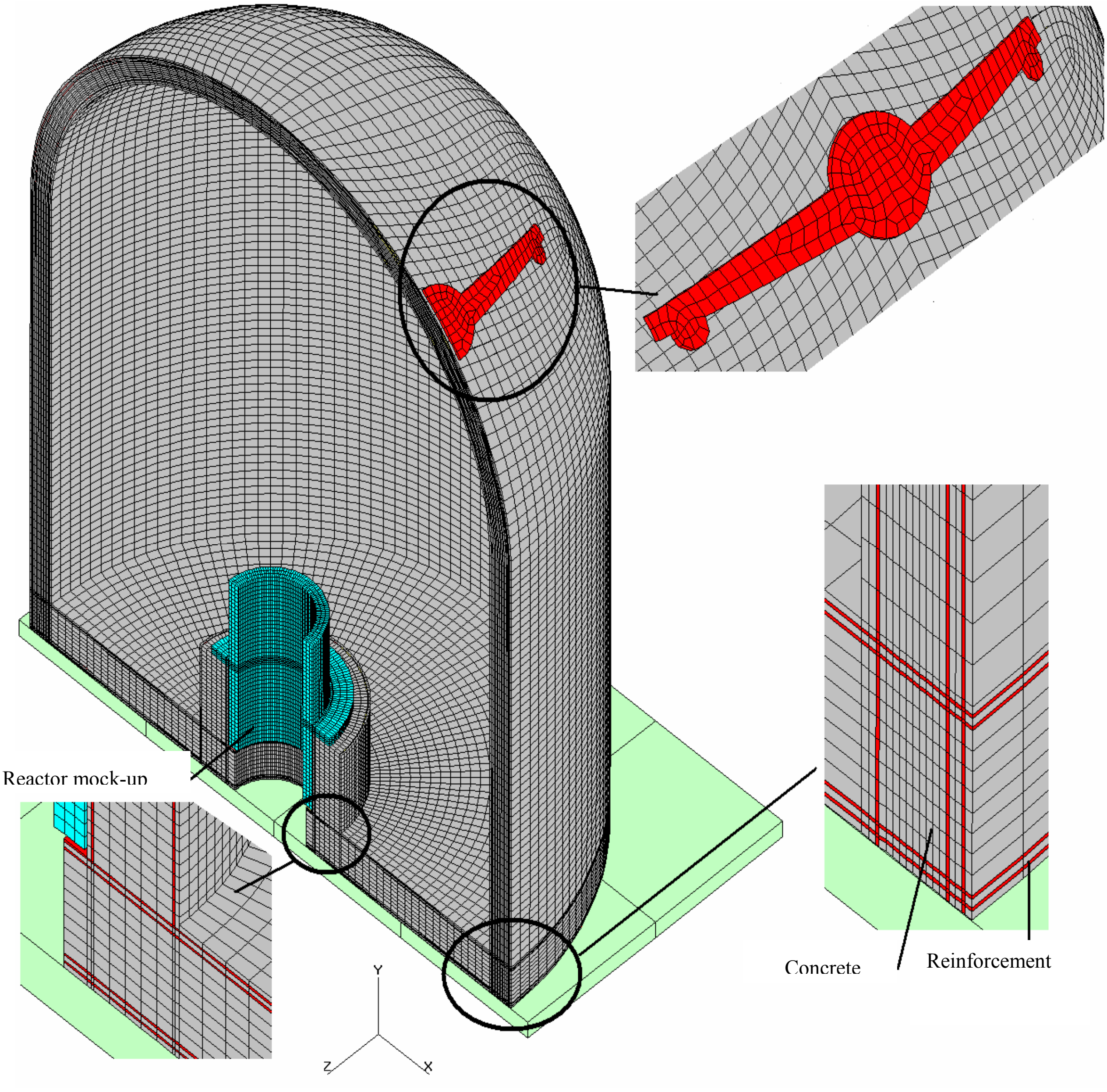


FIG. VII-8. Calculation diagram of VBER-300 reactor unit for aircraft crash analysis.

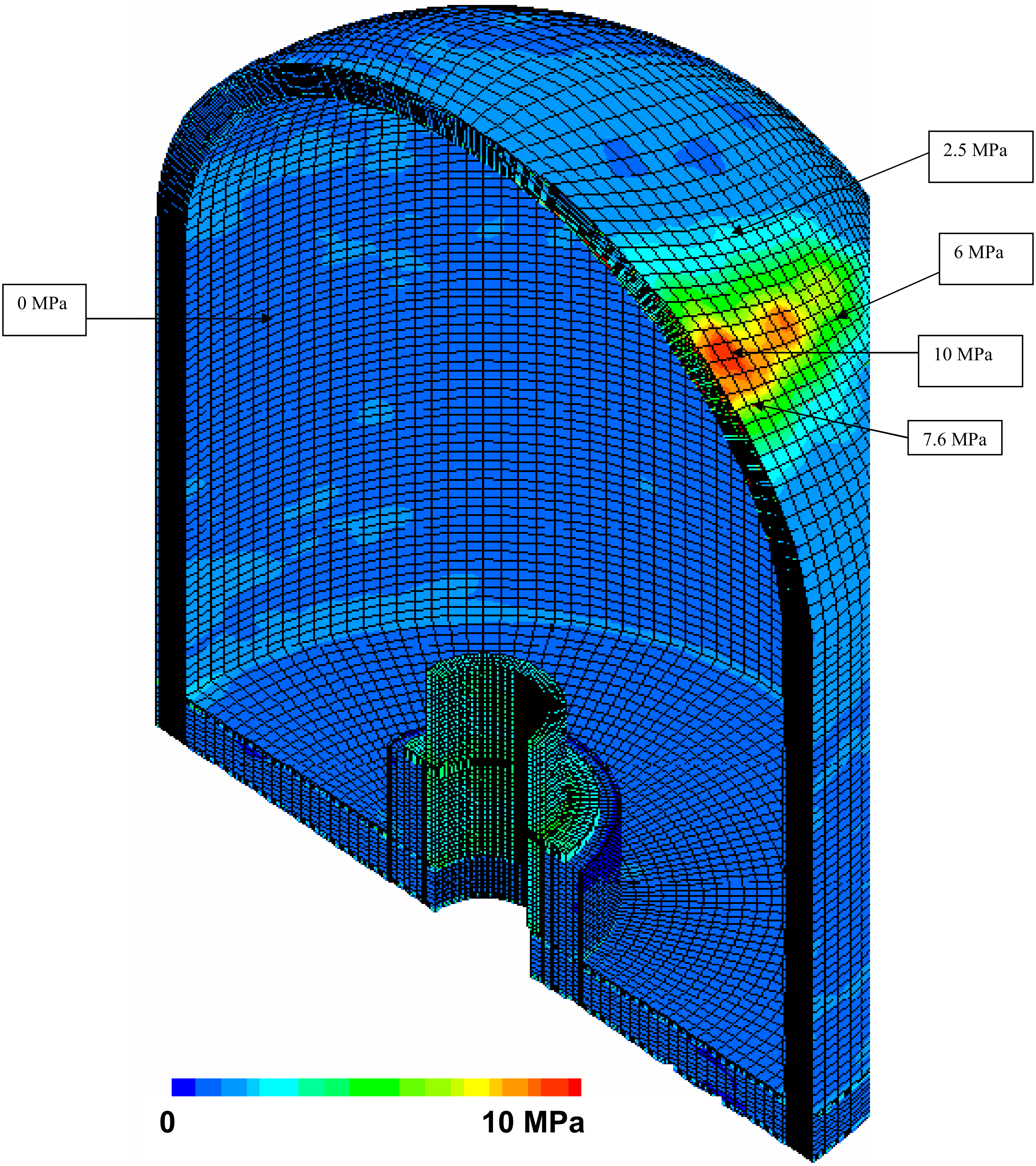


FIG. VII-9. Distribution of stress intensity under the impact of an aircraft crash.

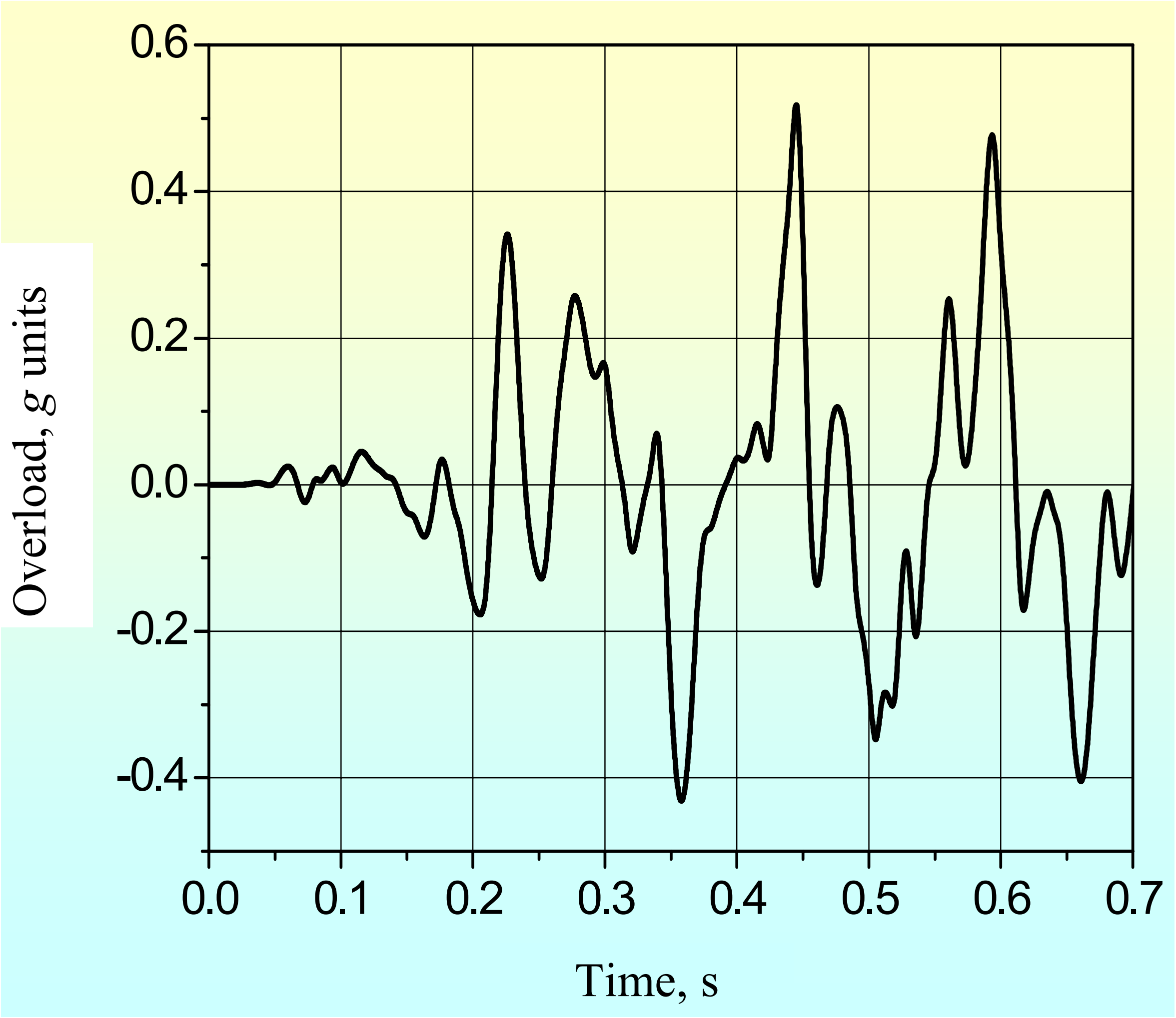


FIG. VII-10. Excitation frequency of the VBER-300 unit under an aircraft crash impact.

5. CONCLUSION

Being based on a combination of proven engineering solutions of the marine reactors and land-based NPPs, and taking into account the state-of-the-art in advanced NPP development, the VBER-300 reactor unit design ensures the implementation of all basic safety requirements to NPP performance under external event impacts.

REFERENCES

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

[VII-2] DANCO code. Qualification certificate No.79 dated December 18, 1997. Gosatomnadzor of Russia, Moscow, Russian Federation.

ANNEX VIII

ABWR-II SAFETY DESIGN AND COPING CAPABILITY FOR EXTERNAL EVENTS

H. OIKAWA
Takashi Sato, Toshiba Corporation, Japan

Abstract

In order to meet utility demands after successful completion of the Advanced Boiling Water Reactor (ABWR) development, the ABWR-II design provides more emphasis on beyond design basis capability to achieve further enhancement of safety such as to ensure practical exclusion of the probability of emergency evacuation/ resettlement. As a result of the ABWR safety design achievement, internal events at power operation are no major concern any longer; therefore, pursuit of comprehensive safety aspects including external evens, e.g., seismic risk, appears to be the next generation design challenge.

To achieve these objectives, the active core and containment cooling system are realized as the rationalized four-division residual heat removal system (RHR) with an emergency power enhancement, and the dedicated passive heat removal system is adopted as an in-depth backup for the reactor and containment cooling. These systems significantly reduce the seismic-induced station blackout risk.

Several types of containment configuration have been studied in addition to the conventional configuration that meets the design target. Aircraft crash is probabilistically excluded from structural consideration for all existing commercial power plants in Japan. However, in order to meet international market needs where relevant utilities' requirements exist, a containment concept with the coping capability against an aircraft crash is also investigated as an optional design extension condition. The containment designs consider other severe accident phenomena on a safety margin basis as well, according to industrial guidelines.

As a result of this design evolution, the ABWR-II achieved distinguished safety features. Both, probabilistic and deterministic consideration of beyond design basis events has been performed at the design stage. The evolutional (passive) system provides not only the defence-in-depth performance for internal events, but also the coping capability for external events.

1. INTRODUCTION

A remarkable evolution of safety system design has been achieved in the course of the ABWR and ABWR-II development from their predecessors. Many safety features have been incorporated into the ABWR design based on the PSA insights. The emergency core cooling system (ECCS) was optimized, and dedicated measures were also provided for accident management.

Keeping ABWR safety advancement, the ABWR-II design provides more emphasis on beyond design basis capability in order to achieve a high level of safety such as to ensure practical exclusion of the probability of emergency evacuation and resettlement. Efforts are made to integrate safety features as well as economic benefits.

2. SAFETY RELATED REQUIREMENTS AND DESIGN PHILOSOPHY

The following safety related requirements have been established during early phases of the ABWR-II development:

- Consideration of severe accidents from the design stage;
- Enhancement of PSA performance (especially for the assessment containment capability);
- Provision of a grace period for both transients and accidents;
- Integration of active and passive systems.

Considering these requirements, the ABWR-II design provides more emphasis on beyond design basis capability in order to achieve a higher level of safety such as to enable practical exclusion of the probability of emergency evacuation/ resettlement. Since, as a result of the ABWR safety design achievement, the internal events at power operation are no longer a major concern, pursuit of comprehensive safety aspects such as shutdown or seismic risk appears to be the next generation design challenge. Optimization of safety and economic aspects is also strongly pursued. Schematics of these new design objectives in application to the emergency core cooling system (ECCS) of a boiling water reactor (BWR) are shown in Fig. VIII-1. To accomplish them, the following design approaches are selected:

- Systems important to safety are incorporated in an integrated manner;
- Hardware increase is minimized for a cost dominant portion of the reactor's structures, systems and components (SSC);
- Additional operational benefits are introduced, to a degree possible.

The safety related system configurations to realize the abovementioned objectives, the performance of safety related systems, and the provisions to cope with external events in the design of the ABWR-II are described in the subsequent sections.

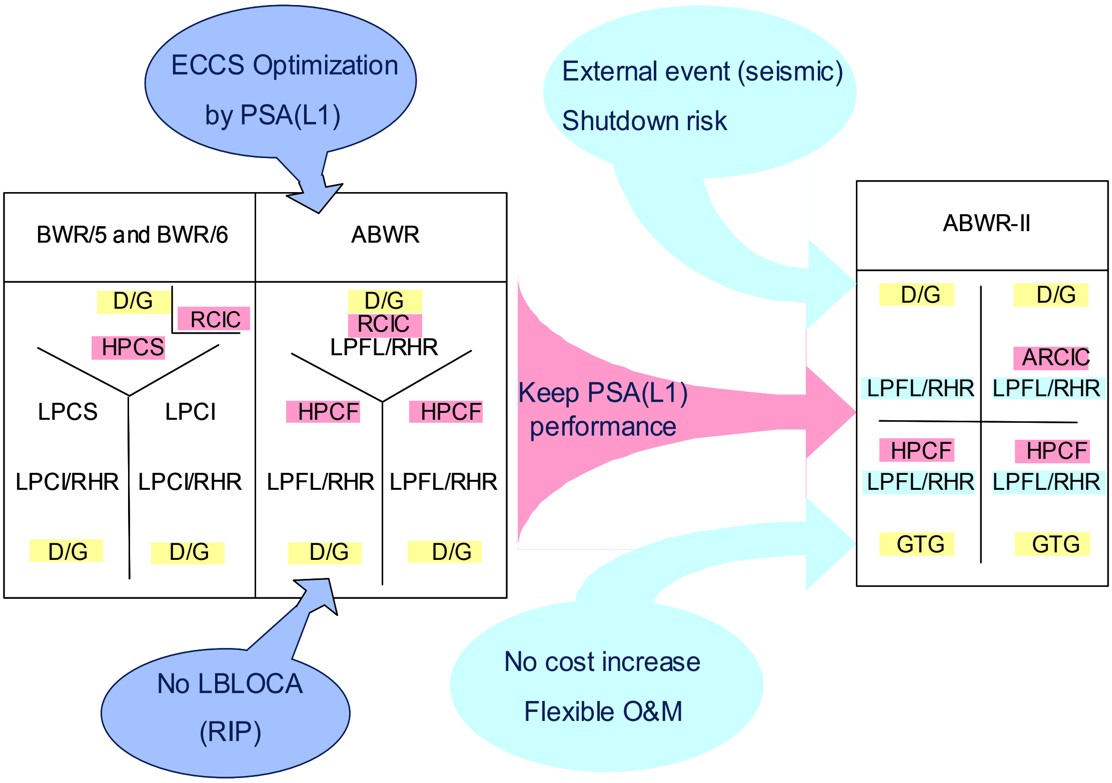


FIG. VIII-1. Evolution of BWR ECCS configuration[1].

3. DESIGN BASIS AND EXTENSION FOR EXTERNAL EVENTS

Typical external events deterministically considered in the existing ABWR-II design are the site-specific earthquake, tsunami, and extreme meteorological conditions (such as typhoon or snow). Lightning as a site-specific event is also considered in the design of the ABWR-II power and control

[1] Acronyms used in Fig. VIII-1 that cannot be found elsewhere are:
Fine motion control rod drive (FMRCD)
Low pressure flooder system (LPFL)
Reactor internal pump (RIP)

system. The design basis for external events is determined on a historical (envelope of records) basis. Specific load combinations and acceptance criteria are defined according to the operational conditions (determined by the category of postulated internal events) and SSC classification.

In addition to a conventional deterministic approach for design basis external events, the concept of design extension condition (DEC), reflecting the capability to cope with beyond design basis events, is more clearly introduced in the ABWR-II. This capability is not necessarily based on a classical design margin, but rather requires a reasonable performance based on a realistic evaluation basis.

As an example, let us consider the suppression pool temperature and the containment pressure increase during a long-term station blackout induced by a seismic event. For the evaluation of a coping capability, a best estimate heat generation and mitigation resource (water/ heat sink) outside the containment might be appropriate, since the event is beyond the design basis. The acceptance criteria for the containment overpressure shall be safety margin basis, such as ASME service level C or factored load category.

Aircraft crashes are probabilistically excluded from structural consideration for all existing commercial power plants in Japan. However, in order to meet international market needs where relevant utilities' requirements exist, a containment concept with the coping capability against an aircraft crash is also investigated as an optional design extension condition.

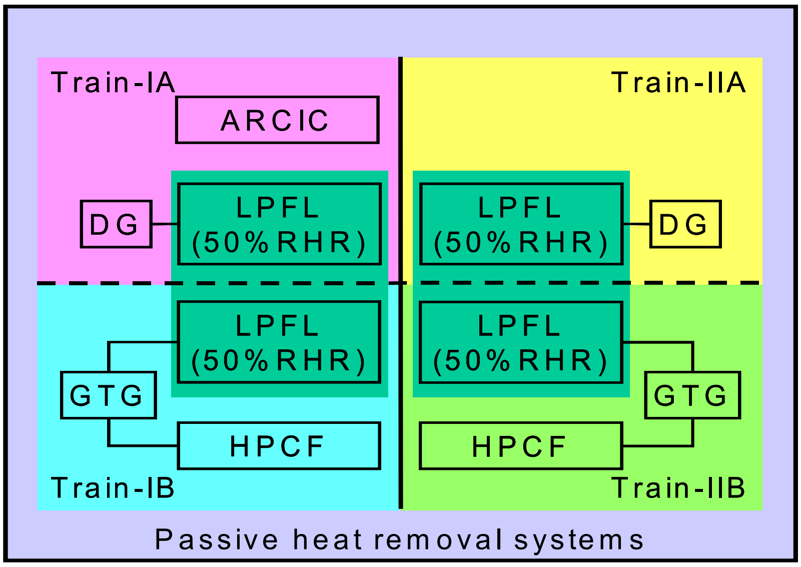
4. SAFETY SYSTEM FEATURES AND DESIGN BASIS PERFORMANCE

The ABWR-II plant configuration incorporates safety related systems with the following design features:

- The reactor core isolation cooling system (RCIC) with a generator (Advanced RCIC, or ARCIC);
- A rationalized four division residual heat removal system (RHR);
- Diversified emergency power supply;
- Passive heat removal systems.

The ABWR-II ECCS configuration [VIII-1] is shown in Fig. VIII-2. The number of high pressure injection systems (one ARCIC and two HPCFs[2]) is the same as that of the ABWR, keeping the redundancy and robustness against transient-initiated events. Design optimization was performed for the low pressure injection system and the RHR system together with its supporting systems for ultimate heat sink, namely, the reactor building closed cooling water (RCW) system and the reactor building seawater (RSW) system. Taking into consideration that the passive heat removal systems of the ABWR-II can be counted as a backup, the basic system configuration of the RCW is two-division (Fig. VIII-3) instead of the three-division in the ABWR. This two-division configuration is expected to reduce equipment cost for the RCW that has a relatively large amount of materials, especially for piping. The RHR, RSW and active components in the RCW in total constitute a four-division configuration that facilitates on-line maintenance and increases reliability and safety. As comes to emergency power sources for active components in the RHR/ RCW/ RSW systems, a four-division configuration consisting of two diesel generators and two gas turbine generators is applied to increase the diversity and to facilitate maintenance. On-line maintenance will be applied to the diesel generators. The gas turbine generators are expected to be practically maintenance-free. In other words, increased reliability and a reduced maintenance outage period in the ABWR-II are achieved with a minimum cost impact by the optimized division configuration of two and four.

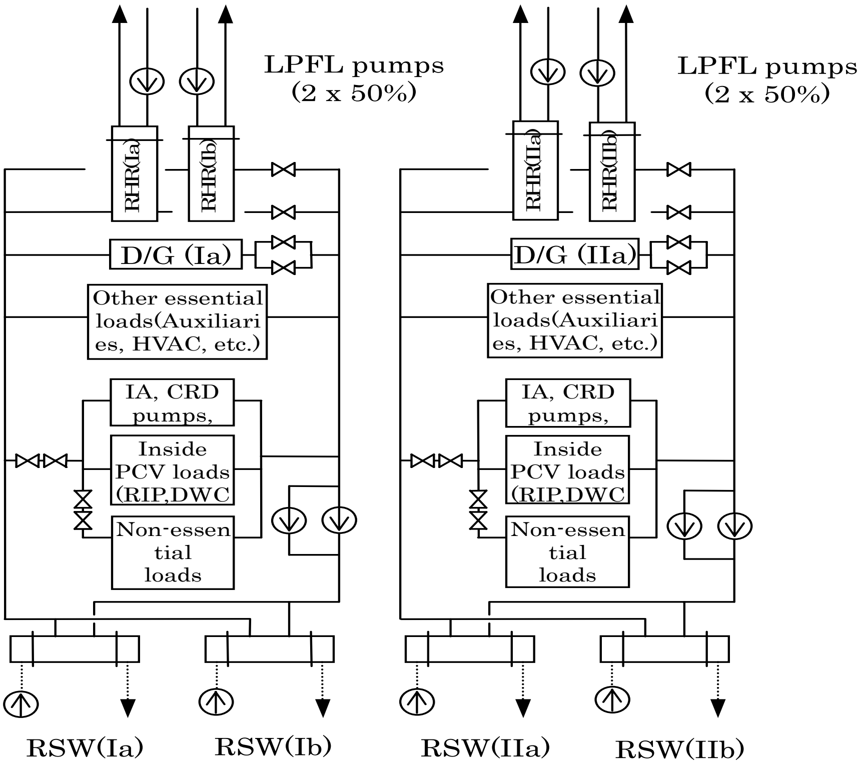
[2] HPCF is high pressure core flooder system.



ARCIC - Advanced reactor core isolation cooling system
HPCF – High pressure core flooder system
LPFL – Low pressure flooder system

DG – Diesel generator
GTG – Gas turbine generator
RHR – Residual heat removal system

FIG. VIII-2. ABWR-II ECCS configuration.



RCW – Reactor building closed cooling water system
HVAC – Heating, ventilation and air conditioning

CRD – Control rod drive
RIP Reactor internal pump

DWC – Drywell cooler
RSW – Reactor building seawater system

FIG. VIII-3. ABWR-II RCW/RSW configuration.

The capacity or size of a safety system is determined as follows. Owing to the fact that, regardless of a fuel bundle design, LOCA is a non-limiting event for ECCS sizing in the ABWR, the capacity and water level set point are determined so that the design basis requirements from a transient event, high level of reliability and an optimum system design balance are satisfied in the same way. Since the system portion that governs the outage period (such as RSW or DG) is provided with N+2 capability, the design basis requirements are fulfilled even assuming an on-line maintenance of this portion.

Containment sizing needs not only deterministic treatment for a conventional design basis LOCA, but also an appropriate consideration for the operational or beyond design basis conditions. For instance, the suppression pool water inventory is determined considering heat sink requirements against the reactor isolation, station blackout or loss of all heat removal functions. Vent pipes and safety/ relief valve (SRV) discharge lines are also affected by increased power. The flow area of pressure suppression vent pipes and the capacity of SRV/ discharge lines are increased against those of the current ABWR. However, a large capacity SRV reduces the number of quenchers and resolves layout restrictions in the suppression pool. Several configurations [VIII-2, VIII-3], which can deal with overpressure due to hydrogen production during a severe accident, have been examined. The features of these containment configurations are discussed in Section 5 below.

Flammable gas control in the containment is performed by the combined use of inerting and passive autocatalytic recombiners (PAR), which ensures the advantages in both safety (automatic start-up and passive operation) and economy (low cost, flexible layout and easy maintenance).

5. BEYOND DESIGN BASIS AND SEVERE ACCIDENT CAPABILITY

The ABWR-II ECCS network has a highly reliable performance achieved by the redundant high pressure injection similar to that of the ABWR, but with extended capability. The advanced reactor core isolation cooling system (ARCIC), Fig. VIII-4, has the capability of a self-standing operation and power supply under long-term station blackout (SBO) conditions beyond the battery capacity.

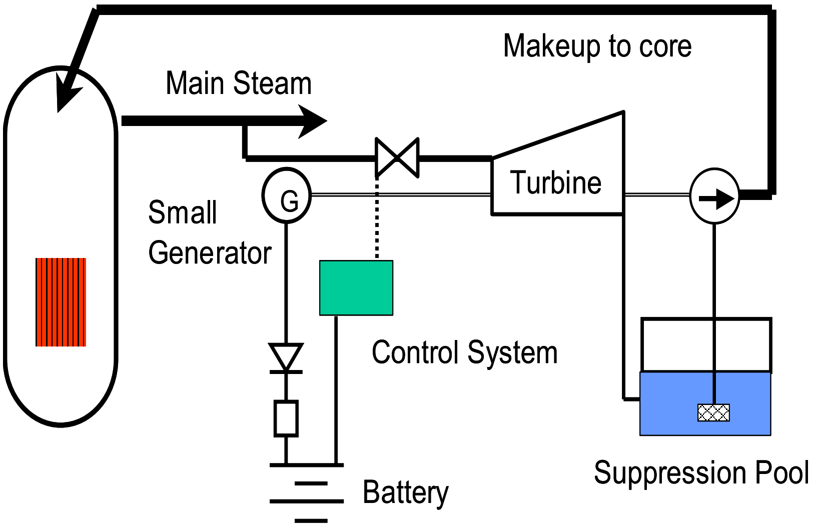


FIG. VIII-4. Advanced reactor core isolation cooling system (ARCIC).

The containment capability to cope with DECs has been focused upon in recent utility requirements. Typical DECs considered in the ABWR-II containment design are: the overpressure protection capability against generation of steam and large amounts of hydrogen (corresponding to 100% active fuel cladding oxidation) without venting; provision of a sufficient (≥ 0.02 m^2/MW(th)) melt spreading floor area, etc.

One of the new safety features to deal with DECs is the passive heat removal system (PHRS). The system consists of two dedicated systems, namely, the passive reactor cooling system (PRCS) and the passive containment cooling system (PCCS), and incorporates a common heat sink pool above the containment allowing for a one-day grace period, Fig. VIII-5. These passive systems are not only to deal with the beyond design basis conditions, but also provide an in-depth heat removal backup for the RHR, and practically eliminate the necessity of the containment venting before and after core damage as a means of overpressure protection. Figure 6 shows the PCCS functional schematic; Fig. VIII-7 gives an example of the containment pressure transient following a typical low pressure core melt scenario.

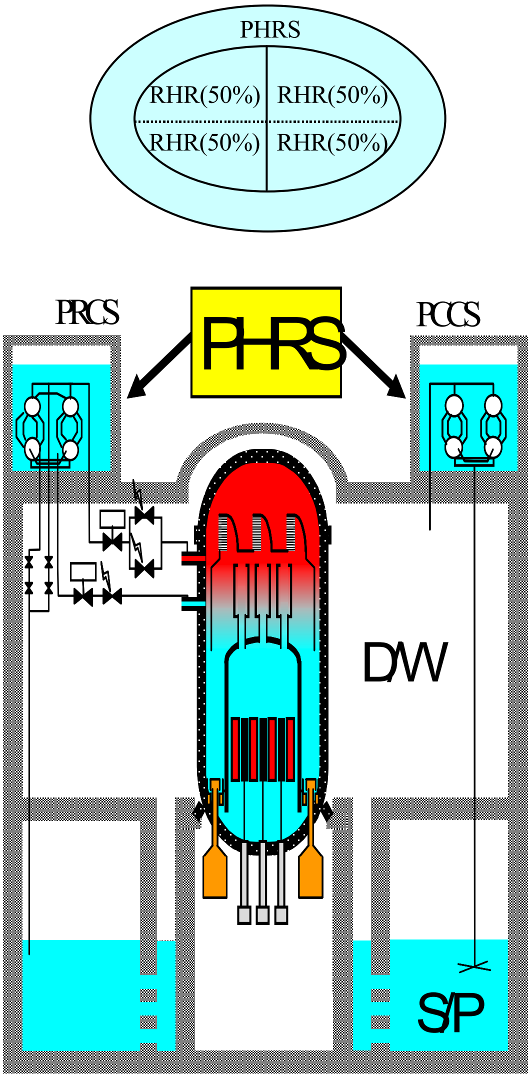


FIG. VIII-5. Passive heat removal system.

The original PCCS is composed of vertical heat exchanger tubes; however, a horizontal U-tube type PCCS has been developed [VIII-4] to enhance the applicability to high seismicity conditions, and to reduce the dead water inventory below the tube for better economy. The optimized tube diameter also provides larger vapour velocity that promotes non-condensable gas venting.

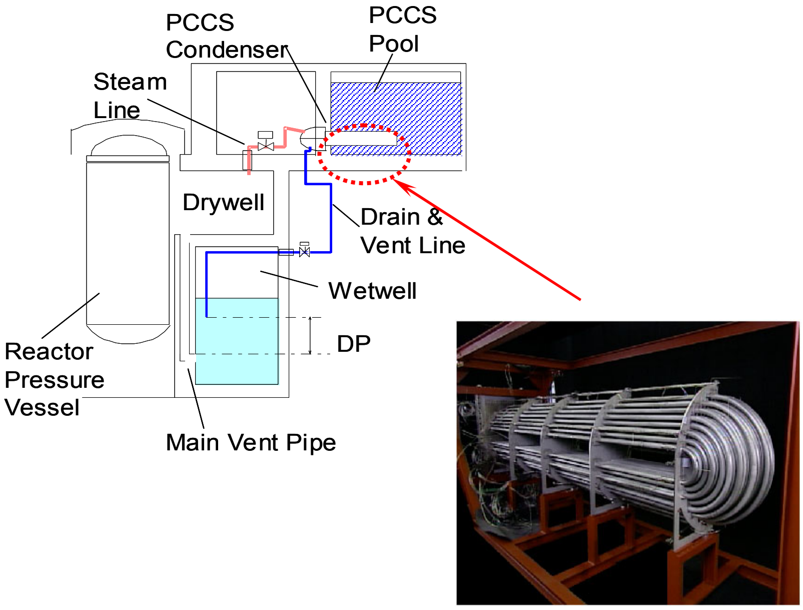


FIG. VIII-6. PCCS configuration and performance.

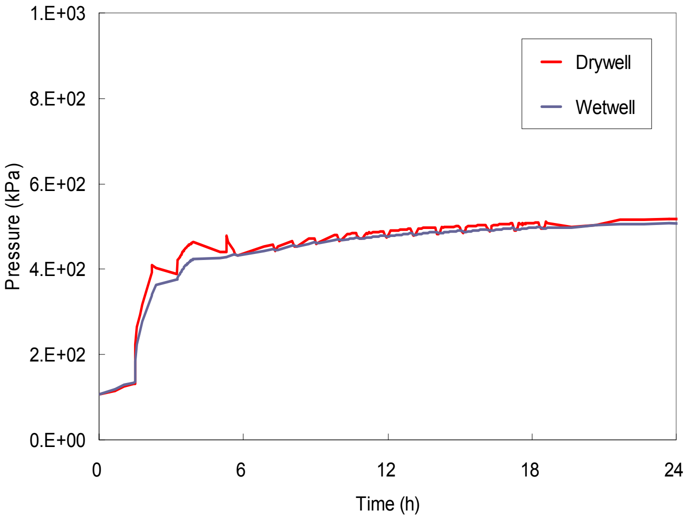


FIG. VIII-7. Containment pressure transient following a typical low pressure core melt scenario.

Although the containment design has not been finalized, several types of configuration have been studied for the ABWR-II in addition to a conventional containment design that meets the design criteria. In a separated drywell concept (Fig. VIII-8), a drywell is separated into the upper and the lower drywell at the reactor pressure vessel (RPV) skirt, and each drywell zone has its own vent pipes and vacuum breakers with the wetwell. This configuration provides larger volume for non-condensable gases as compared to a conventional pressure suppression containment of the same total volume, and reduces the peak pressure during not only the design basis LOCA but also in a severe accident without venting the excessive hydrogen to the atmosphere.

In another concept also aiming to eliminate evacuation beyond the plant boundary, the wetwell area is extended up to the operation floor and to the containment wall, Fig. VIII-9. Rupture disks are installed between this extended area and the wetwell; they are opened when the containment pressure exceeds the design pressure in case of a severe accident.

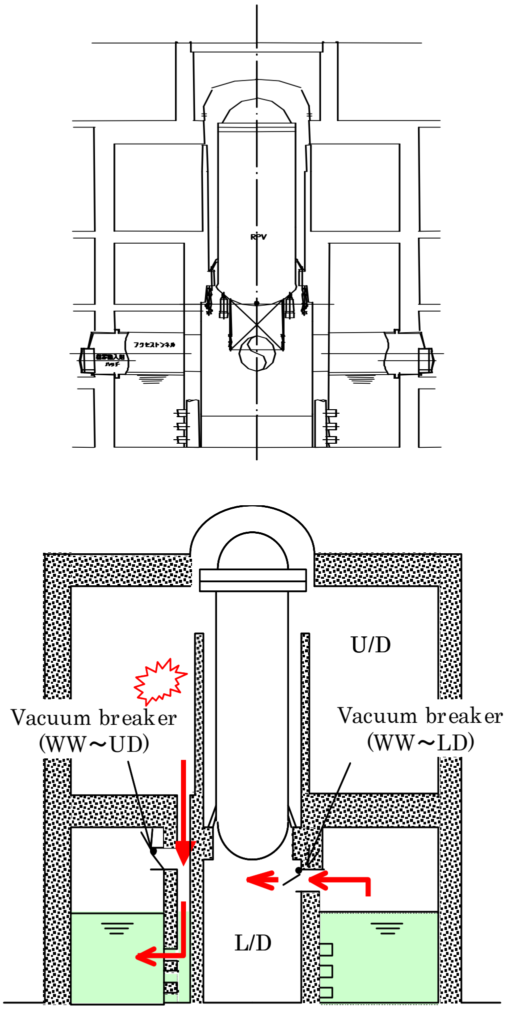


FIG. VIII-8. Separated drywell containment configuration and functional schematic.

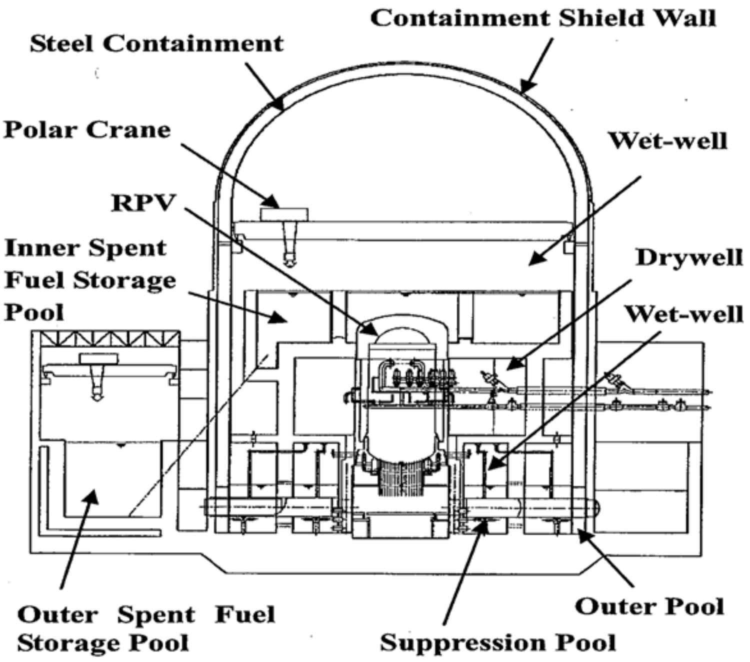


FIG. VIII-9. Containment configuration with wetwell extended to the operation floor.

In addition to the abovementioned, a major design effort has been focused on the external/ shutdown events as described in Section 3. A preliminary PSA evaluation shows that the core damage frequency (CDF) for internal events during power operation has been reduced by about one order of magnitude (see Fig. VIII-10) as a result of the emergency power diversity and redundancy enhancement, the incorporation of a passive cooling system, and the RHR train redundancy enhancement.

A simplified PSA evaluation performed at the design selection stage provided the features of the ABWR-II safety system configuration that secure its robustness even in seismic induced or shutdown events. Figure VIII-11 shows a scoping result with simplified treatment of a seismic event. Due to the emergency power enhancement and the incorporation of a dedicated passive cooling system, the SBO sequence remains a small contributor, even when seismic induced events are taken into consideration.

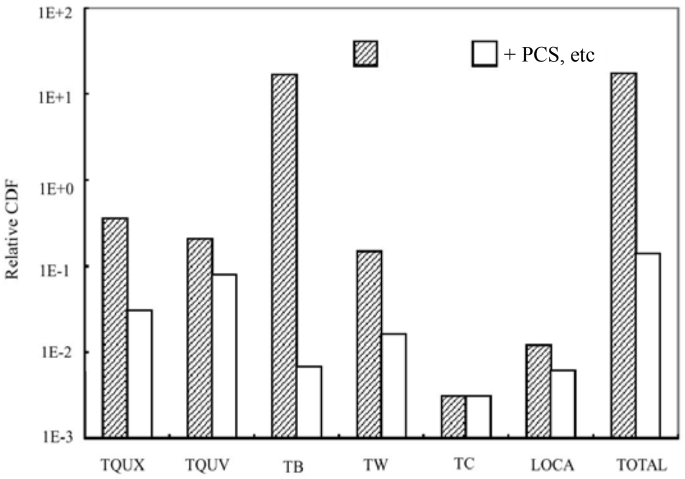


FIG. VIII-10. Core damage frequency (internal events).

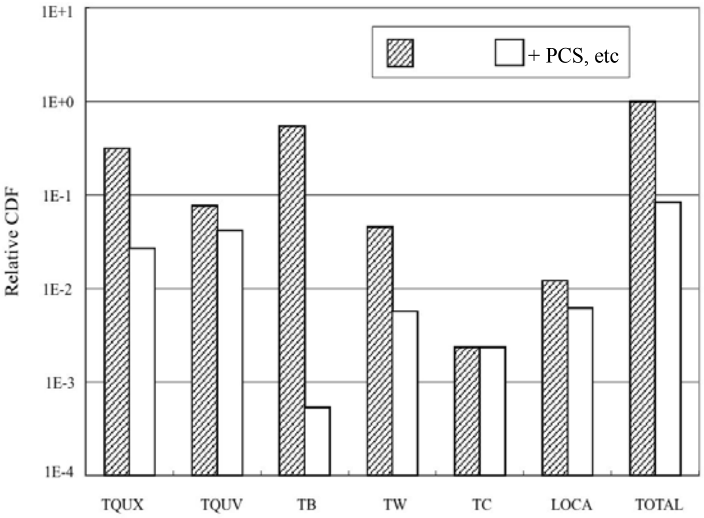


FIG. VIII-11. Effect in CDF with seismic induced station blackout taken into consideration (under TB).

The ABWR-II containment design considers severe accident phenomena such as direct containment heating (DCH), fuel coolant interaction (FCI), and molten core concrete interaction (MCCI) on a safety margin basis. The Japanese industry, collaborating with experts in research organizations, has recently established guidelines for the containment performance design/ evaluation under severe accidents [VIII-5], and a detailed quantitative examination from both phenomenological and probabilistic aspects is being performed [VIII-6].

Figure VII-12 shows the containment failure frequency (CFF) normalized by CDF, and its breakdown by plant damage states (note that the plant damage state, which leads to containment failure prior to core damage, is not included according to the definition of the conditional containment failure probability). The overall conditional containment failure probability is estimated to be well below 0.1 (relative) without any credit of operator action or containment management for recovery.

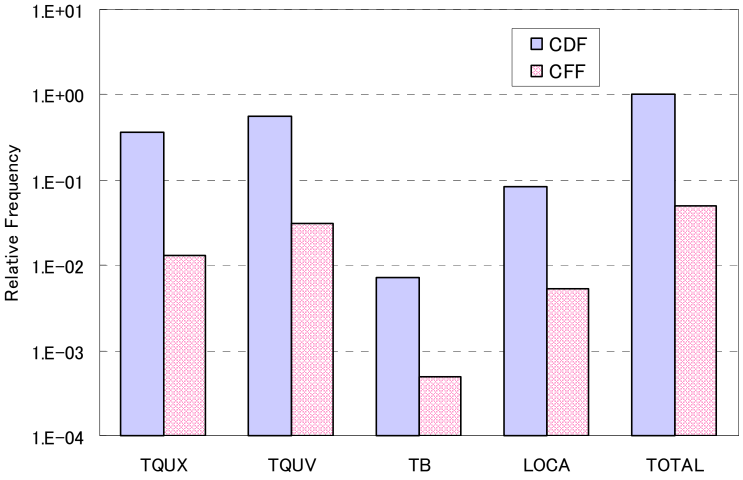


FIG. VIII-12. Containment failure frequency.

Generic research on the key remaining severe accident issues (such as in vessel retention (IVR) or MCCI), currently undertaken in the world, will also contribute to the reduction of the uncertainty of large radioactivity releases [VIII-7].

6. CONCLUSION

The ABWR-II design achieves a distinguished set of safety features via the optimization based on the experience of the preceding designs and on new system technology. Both, probabilistic and deterministic considerations for beyond design basis events have been made at the design stage. The evolutional (passive) system provides not only the defence-in-depth performance for internal events, but also the coping capability for external events. System integration and economic benefits are realized in the ABWR-II simultaneously, so that the utility requirements are met.

ACKNOWLEDGMENTS

The authors wish to acknowledge the support and guidance of Japanese utilities organized by the Tokyo Electric Power Company, and the cooperation of the GE Nuclear Energy and Hitachi, Ltd.

REFERENCES

[VIII-1] SATO, T., et al., Study on advanced ECCS configuration for the next generation boiling water reactors, ICONE7-7331, Tokyo, Japan (1999).

[VIII-2] SATO, T., et al., Study on advanced reinforced concrete containment for the next generation boiling water reactors, ICONE7-7330, Tokyo, Japan (1999).

[VIII-3] KIKUYAMA, T., et al., Conceptual study on the containment design aiming at no evacuation, ICONE11-36589, Tokyo, Japan (2003).

[VIII-4] ARAI, K., et al., Post-test analysis of thermal-hydraulic test using full-scale horizontal PCCS condenser, ICAPP'03-3133, Cordoba (2003).

[VIII-5] Nuclear Safety Research Association, (Guideline for severe accident consideration in future LWR containments (in Japanese)), Japan (1999).

[VIII-6] TERAZU, K., et al., Revamped framework of containment event tree assessment and quantification of branching probabilities for ABWR, (Paper presented at the 7th Korea-Japan PSA Workshop, 2002).

[VIII-7] ANEGAWA, T., et al., Development of ABWR-II and its safety design, Advanced Nuclear Reactor Safety Issues and Research Needs, NEA#03613, ISBN: 92-64-19781-8 (2002).

CONTRIBUTORS TO DRAFTING AND REVIEW

Alzbutas, R.
Lithuanian Energy Institute,
Breslaujos str. 3,
44403 Kaunas, Lithuania

Bajaj, S.S.
Nuclear Power Corp. of India Ltd,
Nabhikiya Urja Bhavan, C-1,
Anushaktinagar,
Mumbai 400094, India

Birbraer, A.N.
SPb AEP,
191036 Suvorovsky proezd 2a,
Sankt Peterburg,
Russian Federation

Bonechi, M.
Atomic Energy of Canada Limited,
2251 Speakman Drive,
Mississauga, Ontario, L5K 1B2
Canada

Brettschuh, W.
FRAMATOME ANP GmbH,
NGPF,
Postfach 10 05 51,
63005 Offenbach/Main,
Germany

Carelli, M.
Westinghouse,
Science and Technology,
1344 Beulah Road,
Pittsburgh, PA 15235-5083
United States of America

Coatsworth, A.
Health and Safety Executive (HSE),
304 The Colonnades, Albert Dock,
Liverpool, L3 4AB,
United Kingdom

Contri, P.
International Atomic Energy Agency
Wagramer Strasse 5, P.O. Box 100,
1400 Vienna, Austria

Delmastro, D.
Comisión Nacional de Energía Atómica (CNEA),
Centro Atómico Bariloche,
Ave. Bustillo Km. 9.5,
8400 – S.C. de Bariloche,
Pcia. Rio Negro, Argentina

Facer, R. I.
International Atomic Energy Agency,
Wagramer Strasse 5, P.O. Box 100,
1400 Vienna, Austria

Ghosh, A.K.
Bhabha Atomic Research Centre (BARC),
Mumbai 400085,
India

Kuznetsov, Yu. N.
Research and Development Institute of Power Engineering (RDIPE – NIKIET),
P.O. Box 788,
Moscow 101000, Russian Federation

Kuznetsov, V.
International Atomic Energy Agency,
Wagramer Strasse 5, P.O. Box 100,
1400 Vienna, Austria

Lee C.-S.
Korea Electric Power Research Institute,
103-16 Munji Dong,
Yusung Gu, Daejeon,
Republic of Korea

Oikawa, H.
Industrial and Power Systems & Services Company,
Toshiba Corporation,
8, Shinsugita, Isogo-ku,
Yokohama, 235-8523, Japan

Panov, V.
OKBM,
603074 Nizhny Novgorod,
Russian Federation

Petrovic, B.
Westinghouse,
Science and Technology,
1344 Beulah Road,
Pittsburgh, PA 15235-5083,
United States of America

Ravindra, M.K.
ABS Consulting Inc,
300 Commerce Drive, Suite 200,
Irvine, CA 92602,
United States of America

Roleder, A.Yu.
SPb AEP,
191036 Suvorovsky proezd 2a,
St. Petersburg,
Russian Federation

Sinha, R.K.
Bhabha Atomic Research Centre,
Mumbai 400085,
India

Stevenson, J.D.
Consulting Engineer,
9217 Midwest Ave.,
Cleveland, Ohio 44125
United States of America