IAEA-TECDOC-1366

Considerations in the development of safety requirements for innovative reactors: Application to modular high temperature gas cooled reactors

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

August 2003

The originating Section of this publication in the IAEA was:

Engineering Safety Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

CONSIDERATIONS IN THE DEVELOPMENT OF SAFETY REQUIREMENTS FOR INNOVATIVE REACTORS: APPLICATION TO MODULAR HIGH TEMPERATURE GAS COOLED REACTORS

IAEA, VIENNA, 2003
IAEA-TECDOC-1366
ISBN 92–0–107203–1
ISSN 1011–4289

Printed by the IAEA in Austria
August 2003

FOREWORD

Member States of the IAEA have frequently requested this organization to assess, at the conceptual stage, the safety of the design of nuclear reactors that rely on a variety of technologies and are of a high degree of innovation. However, to date, for advanced and innovative reactors and for reactors with characteristics that are different from those of existing light water reactors, widely accepted design standards and rules do not exist.

This TECDOC is an outcome of the efforts deployed by the IAEA to develop a general approach for assessing the safety of the design of advanced and innovative reactors, and of all reactors in general including research reactors, with characteristics that differ from those of light water reactors. This publication puts forward a method for safety assessment that is based on the well established and accepted principle of defence in depth.

The need to develop a general approach for assessing the safety of the design of reactors that applies to all kinds of advanced reactors was emphasized by the request to the IAEA by South Africa to review the safety of the South African pebble bed modular reactor. This reactor, as other modular high temperature gas cooled reactors (MHTGRs), adopts very specific design features such as the use of coated particle fuel. The characteristics of the fuel deeply affect the design and the safety of the plant, thereby posing several challenges to traditional safety assessment methods and to the application of existing safety requirements that have been developed primarily for water reactors.

In this TECDOC, the MHTGR has been selected as a case study to demonstrate the viability of the method proposed. The approach presented is based on an extended interpretation of the concept of defence in depth and its link with the general safety objectives and fundamental safety functions as set out in “Safety of Nuclear Power Plants: Design”, IAEA Safety Standards No. NS-R.1, issued by the IAEA in 2000. The present TECDOC is not intended to be exhaustive, but rather suggests a systematic approach to be used in the development of detailed safety requirements.

The IAEA is grateful to the experts who contributed to this publication. The IAEA officer responsible for this publication was M. Gasparini of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

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

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

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

Gas cooled reactors have had a long and varied history which dates back to the very early days of the development of nuclear energy. An IAEA technical report issued in 1990 [1] is a compilation of information on the status of the design and safety for gas cooled reactors at that time. The evolutionary process, along with significant advances in supporting technologies, have culminated in the modular high temperature gas cooled reactor (MHTGR). The MHTGR is expected to achieve the goals of safe, efficient, environmentally acceptable and economic production of energy at high temperature for the generation of electricity and for industrial process heat applications early in the twenty-first century [2].

The MHTGR concept originated in Germany in 1979. There were parallel design variations in the USA and other countries during the 1980s and early 1990s. The specific prismatic block steam cycle design developed in the USA was called an MHTGR, but for the purpose of this report, the term MHTGR is used to indicate a general family of modular HTGRs with common characteristics as defined in Section 2. Design concepts were developed in considerable detail and subjected to review by several regulatory agencies. After several years of limited activity on high temperature gas reactors, a new interest for this technology is appearing in several Member States. A 30 MW(t) reactor (HTTR) was built in Japan and reached the first criticality at the end of 1998. A 10 MW(t) reactor (HTR-10) was constructed in China and the first criticality was achieved in December 2000. A 110 MW(e) pebble bed modular reactor (PBMR) has been proposed by Eskom, the South African Electric Utility, and an international project is under way. The IAEA has been directly involved in the review of the technical and economic feasibility as well as the safety of this reactor. A 270 MW(e) gas turbine modular helium reactor design is being developed in an international project led by the USA and the Russian Federation. Summary descriptions of these concepts as of 2000 are provided in IAEA-TECDOC-1198 [2].

Due to the MHTGR's innovative design approaches, advanced technologies and passive safety features, the safety assessment and the licensing of these reactors may require specific consideration, and the current LWR-based safety requirements may need, special interpretation or adaptation.

The IAEA has a comprehensive programme to update all the IAEA Nuclear Safety Standards (under the oversight of the IAEA Nuclear Safety Standards Committee, NUSSC), and has published some revised reports in particular, the Safety Requirements for Design [3]. These requirements and the derived Safety Guides have been mainly developed for water reactors, and their applicability to MHTGRs is not always straightforward. For example, in MHTGR designs, the fundamental safety functions are achieved with extensive use of passive and/or inherent features. The implementation of defence in depth for MHTGRs is quite different from that of water reactors. These differences can have significant impacts on the licensing approach for plant design, construction and operation.

Today's operating nuclear plants were largely designed following a defence in depth strategy. According to INSAG-10 [4], "Defence in depth consists of a hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between radioactive materials and workers, the public or the environment, in normal operation, anticipated operational occurrences and, for some barriers, in accidents at the plant. Defence in depth is implemented through design and operation to provide a graded protection against a wide variety of transients, including incidents and accidents, equipment failures and human errors within the plant and events initiated outside the plant". This safety approach is reflected in the existing IAEA Safety Standards for the design of nuclear power plants.

To provide guidance in licensing and safety assessments of MHTGRs, there is a need to develop an applicable set of safety requirements derived from the generally accepted principles of nuclear safety. The IAEA has recently developed a methodology for screening the defence in depth of nuclear power plants [5] starting from the basic safety principles as proposed in INSAG-12 [6]. This methodology is used here to develop safety requirements for MHTGR design and operation.

1.2. OBJECTIVE

The objective of the present publication is to propose a technical basis and methodology, based on principles of defence in depth, for conducting design safety assessments and in the long term generating design safety requirements for innovative reactors. The MHTGR is used as an example to illustrate this process. For this purpose, the document provides an overview of the safety related features of current MHTGR technology, examines how the defence in depth principle can be implemented/adopted by the MHTGR design, and how MHTGR designs could satisfy the three fundamental safety objectives:

- general nuclear safety;
- radiation protection;
- technical safety.

A discussion of these objectives and principles in Section 3 provides a framework for development of future IAEA publications related to the MHTGR safety case.

1.3. SCOPE

This report focuses on the MHTGR, as defined in Section 2. The family of designs identified as MHTGRs incorporates some unique features. In particular the coated fuel particles, without metallic cladding, have the potential to retain radionuclides at temperatures well above their normal operating conditions, including the full range of design basis accident conditions. The helium coolant is an inert gas having no possibility of chemical interaction with other materials and no significant reactivity effects. For designs within this family, the decay heat is removed by thermal conduction, convection and radiation, and the design uses simple and reliable passive means that ensure fuel temperatures are maintained within allowable limits even without reliance on the presence of the primary system coolant.

To apply the defence in depth screening approach, this report considered the three fundamental safety functions (control of reactivity, core heat removal, and confinement of radioactive materials), and the challenges to the performance of these functions. Provisions identified are mainly based on design features of current PBMR and GT-MHR concepts, and are identified to illustrate the process for assessing MHTGR concepts.

This report does not consider challenges to the safety functions during various shutdown modes, or fuel storage and radioactive waste issues. A complete analysis, however, should also investigate all plant states and sources of radioactivity.

1.4. STRUCTURE

Section 2 of this TECDOC presents a discussion of specific safety characteristics, particularly inherent safety features that form an integral part of the safety case. This discussion serves to define the family of concepts referred to in this report as MHTGRs.

In Section 3, current general nuclear plant safety principles are addressed. Safety objectives, concepts and principles are described as a framework for design and operation of both current and future reactors. The structure of the IAEA nuclear safety standards is briefly described, identifying the role of the design requirements to ensure safety, and noting the logic underlying their development.

Section 4 introduces a method to prepare design safety requirements for the MHTGR, starting from the current requirements [3] (mostly developed for light water reactors, LWRs), adopting a top-down approach applicable to MHTGRs, and taking credit for recently-developed methodology [5] for screening defence in depth in nuclear reactors.

Section 5 presents a "critical review" of the reference requirements, analysing the defence in depth implemented for advanced reactors. For each level of defence in depth and for each fundamental safety function, the section illustrates the acceptance criteria for a successful achievement of the safety functions. The challenges to this successful behaviour are identified as well as the mechanisms that originate the challenges. Finally the identification of the provisions to cope with these mechanisms create the basis for the definition of the design requirements.

Characteristics of reactor designs considered may be such that established LWR requirements are unnecessary, ineffective or even counterproductive. This requires an analysis of the specific design characteristics and safety features of the family of reactor designs and a full understanding of the role played by these features in achieving a safe design.

Finally, Section 6 summarizes the conclusions from the systematic investigation of the defence in depth of MHTGRs, hopefully contributing to the future work of preparing design requirements for this family of future reactors.

The appendix contributes to this goal by providing a comparison of safety characteristics of LWRs and MHTGRs.

2. MHTGR DESIGN CHARACTERISTICS AND FEATURES RELEVANT TO THE SAFETY CASE

2.1. MHTGR DESIGN SAFETY CONCEPT

The MHTGR's fundamental safety objectives, requirements and design guidelines are based on the specific design characteristics and inherent safety features noted below:

- High quality ceramic coated-particle fuel of proven design, which adequately retains its ability to contain radioactive fission products over the full range of operating and accident conditions.
- A single-phase inert coolant (helium), with no heat transfer limits that would be associated with phase change.
- Post shutdown decay heat removal achievable through conduction, natural convection and radiation heat transfer, limiting maximum temperatures to values consistent with coated fuel particle and structural design limits.
- Combination of low core power density, large reactor core and internals heat capacity, high core thermal conductivity and large fuel thermal margins, resulting in very long times (days) for evolution of response to loss of normal shutdown functions without protective actions.
- Fuel temperature margins and negative temperature-reactivity coefficients sufficient to accommodate any foreseeable reactivity insertions during startup and power operation without damage to the fuel

If successfully developed, the defining safety characteristic of the MHTGR will be that its primary defence against serious accidents is achieved through its inherent design features. Active safety systems or prompt operator actions are not required to prevent significant fuel failure and fission product release. The plant is designed such that its inherent features provide adequate protection despite operational errors or equipment failure. A primary design characteristic is the limitation of rated thermal power to a small fraction (on the order of 6 to 20%) of typical power levels for the large water reactors upon which the existing safety requirements are based. This is necessary to provide for removal of post shutdown decay heat using only passive means. Specific features, characteristics, and related safety issues are discussed in this section.

2.2. COATED FUEL PARTICLE

MHTGR fuel is a ceramic, and is therefore able to withstand much higher temperatures than can fuel elements with metallic cladding. The design of today's coated fuel particle (CFP) has evolved empirically over several decades from a single layer of anisotropic carbon, to BISO (buffered isotropic pyrolytic carbon) to the current TRISO (triple isotropic layers) design. TRISO CFPs are small, typically ~1 mm diameter. In the TRISO design, the fuel kernel (typically LEU-oxide or -oxycarbide or Pu-oxide), is surrounded by a porous buffer layer to absorb fission gasses. Next there is an inner pyrolytic carbon (IPyC) coating; a silicon carbide (SiC) layer (or zirconium carbide – ZrC – in some advanced fuels) layer, and then an outer pyrolytic carbon (OPyC) coating. Variations in CFP design are primarily in fuel type, kernel size, buffer and coating thickness and microstructure, and in methods for fabrication and quality control (QC) screening.

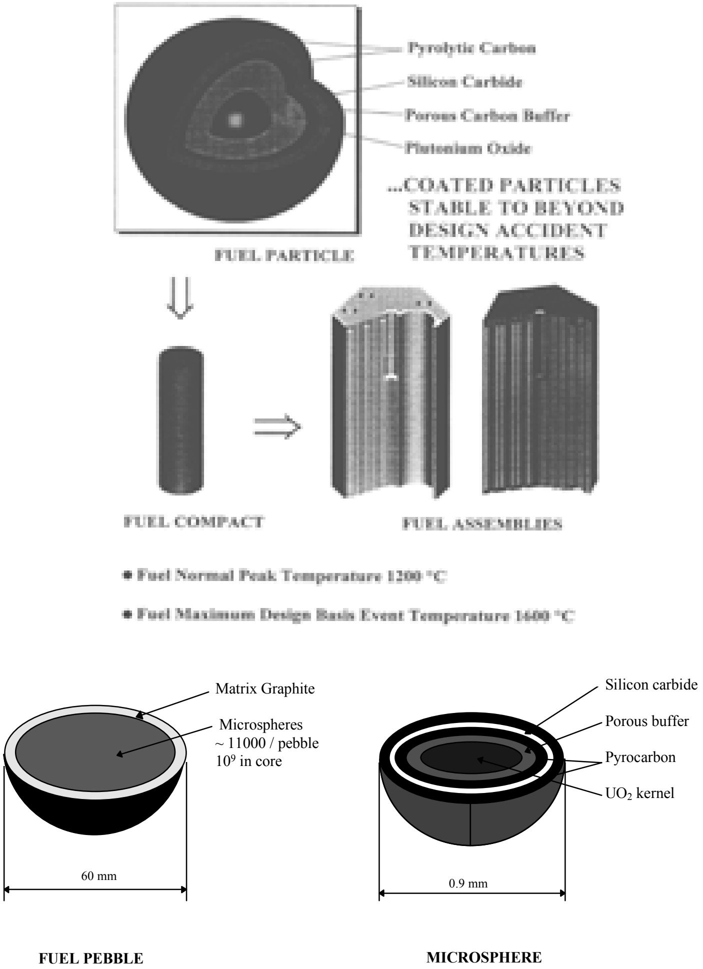


Fig. 1. TRISO fuel for pebble and prism designs.

Since the CFP barriers form the primary line of defence against fission-product release, good performance is essential to the success of the MHTGR design. For the most part, CFP designs have been arrived at empirically. A comprehensive analytical fuel performance model — accurately relating its (statistical) resistance to failure — has not been successfully developed due to the complexity of treating the combined effects of coating microstructure variations, variations in location and characteristics of microscopic imperfections, fission product chemical interactions along grain boundaries, fission gas pressure build-up, long term temperature and irradiation effects, etc. However, the empirical basis for CFP performance, a product of decades of development in many countries, is extensive. An IAEA Co-ordinated Research Project (CRP) on Validation of Predictive Methods for Fuel and Fission Product Behaviour was conducted from 1992 to 1996, with participants from China, France, Germany, Japan, the Russian Federation, the United Kingdom and the USA. The objectives of this CRP were to review and document the status of the experimental data base and of the predictive methods for gascooled reactor (GCR) fuel performance and fission product behaviour, and to verify and validate methodologies for the prediction of fuel performance and fission product transport. The results of this comprehensive international study of CFP performance are reported in IAEA TECDOC-978 [7].

CFP loss-of-function implies inability to retain fission products. Loss-of-function can range from long term diffusion of specific fission products (e.g. caesium) through the coating layers, to sequential or simultaneous coating layer structural failure. There are many factors affecting fission product retention capability of any given CFP, including as-manufactured dimensions, coating layer microstructure, and chemical impurities; irradiation flux and temperature history, and chemical attack. In normal operation a particular concern for gas-turbine (GT) designs is the diffusion of Ag-110m through the intact SiC layer at high operating temperatures. Silver deposition on turbine blades (and elsewhere) could lead to significant personnel exposure during maintenance, and possible material damage problems. Ag-110m precursor fission yields are over 50 times higher for Pu than for U, so it is more of a concern for Pu-burner designs. In accident conditions, CFP time/temperature history during the event tends to dominate the fission product release rate, particularly with regard to diffusion releases. Chemical attack from within (such as Palladium attack on SiC) or from without (such as via air or moisture from ingress events) may also be a factor. CFP compaction methods (prismatic core design compacts or PBR pebble elements) can also affect failure statistics.

Diffusive release of several fission product species appears to begin at about 1600°C, although heating tests of irradiated CFP show very little release in the 1600°C area even for relatively long periods (typical of times at or near the peak in long-term depressurization accidents). Release rates increase markedly for time-dependent exposures in the 1700–2000°C range, and SiC degradation by chemical decomposition begins at approximately 2100°C; hence 1600°C is typically chosen as a conservative limit on peak fuel temperature under accident conditions. It should be noted also that predictions of peak fuel temperatures vs. time analyses often neglect to mention that a relatively small portion of the core fuel is at or near the peak (3-D time-temperature percent-fuel failure models account for this effect in core release predictions).

2.3. HELIUM AS PRIMARY COOLANT

Helium gas pressurized to several MPa is employed as the primary system coolant. Helium is a single phase noble gas with no heat transfer limits associated with phase change. The absence of heat transfer limits (e.g. departure from nucleate boiling — DNB or critical heat flux — CHF) in addition to the core's large thermal inertia may eliminate any safety related need to monitor short term variations in core power and temperature distributions. For the same reason, large local temperature increases during anticipated operational occurrences are less likely to occur. This can offer major operational benefits such as elimination or simplification of safety related monitoring and protection systems, and related surveillance and in-service inspection requirements.

In addition, due to the inert characteristics of helium, no significant chemical attack on fuel and other components would be expected if the contamination levels are kept low. Also, helium has no significant reactivity effects, and a relatively low amount of waste is generated due to activation and/or transmutation of the coolant impurities and corrosion products.

On the other hand, it is relatively easy for helium gas to leak from the primary circuit, especially at the elevated temperatures and pressures (although helium leakage does not cause any important safety issues). Thus for operational purposes, careful consideration is required for the design, fabrication, inspection and maintenance of the primary circuit. A monitoring system to detect the leakage should be able to identify leakage locations.

Helium will not condense if contained in a structure at normal temperatures following depressurization. Thus the pressure would reduce somewhat in accordance with the ideal gas law due to cooling, but would remain relatively high until the helium leaks out of the structure. In contrast, steam released from a water cooled system will condense on structural materials and components, resulting in a relatively rapid decrease in pressure. This characteristic substantially reduces the effectiveness of a conventional containment structure for a helium cooled system relative to a water cooled system. By retaining the helium following a depressurization, the gas leaking from the containment (typically specified as ≤1%/day for existing reactors) can serve as a transport mechanism for radionuclides which would be released from the fuel during a long term heatup. Thus in many important scenarios a conventional containment would result in a higher offsite dose than a filtered vented confinement design.

2.4. DECAY HEAT REMOVAL VIA PASSIVE MEANS

MHTGR designs typically rely on a passive ultimate heat sink system for removal of decay heat in the case of failure or unavailability of all active core cooling mechanisms. Under these conditions, core heat removal is accomplished via heat transfer from the core to the non-insulated reactor pressure vessel via conduction, radiation and (if coolant is present) convection, and from the vessel to the reactor cavity by radiation and convection. A reactor cavity cooling system (RCCS) is necessary to prevent overheating of the reactor cavity concrete during normal operation and to remove core decay heat under accident conditions. The RCCS may not be necessary to prevent overheating of the fuel during accident conditions, as its unavailability would only cause a slight increase in peak fuel temperature. However, it may be necessary to prevent long term overheating of the reactor vessel and possible damage to or failure of reactor cavity structural elements and reactor supports.

In typical designs the RCCS is fully operational during normal reactor operation, and there are no mechanical actions needed for it to function during a loss-of-forced-convection (LOFC) event. However, the operational mode may be different (e.g. transition from forced convection to natural convection RCCS cooling flow). Because of the multiple objectives and wide range of operational conditions, along with its necessarily massive size, the RCCS design and fabrication is challenging as well as crucial. In several instances, the performance of RCCS designs have been found to be difficult to predict with regard to local temperature distributions in the reactor cavity. Due to its location (in the reactor cavity), major repair and/or replacement may be very difficult.

The heat load distributions for depressurized and pressurized LOFC accidents are quite different and may affect RCCS design requirements. For the depressurized case, the peak core temperatures tend to be near the level of the core beltline, while for the pressurized case, peak temperatures and heat loads are near the upper part of the vessel due to convection heating effects.

Additionally, accident analyses of some loss-of-cooling events for some designs have shown that a total functional failure of the RCCS has remarkably little impact on predicted peak fuel temperatures. However, variations among MHTGR designs may significantly affect the functional requirements of the RCCS. For example, analyses have shown that for the higher power designs (~600 MW(t), RCCS operation is required during these accidents to protect the reactor pressure vessel from damage, while its failure does not necessarily lead to vessel damage for the lower power designs (~250 MW(t). Over the past two decades there has been a wide range of experimental and analytical work in this area in support of several MHTGR designs. CRP on Heat Transport and Afterheat Removal for Gas Cooled Reactors Under Accident Conditions was conducted from 1992 to 1997, with participants from China, France, Germany, Japan, Netherlands, the Russian Federation, and the United States of America. The objective of this CRP was to establish sufficient experimental data at realistic conditions, and validated analytical tools to confirm the predicted safe thermal response of MHTGR during accidents. The scope included experimental and analytical investigations of heat transport by natural convection, conduction, and thermal radiation within the core and reactor vessel, and afterheat removal from the reactor vessel. Code-to-code and code-to-experiment benchmarks were performed for verification and validation of the analytical methods. The results of this comprehensive international study of MHTGR passive decay heat removal are reported in IAEA-TECDOC-1163 [8].

2.5. LARGE THERMAL INERTIA, LOW POWER DENSITY, LARGE TEMPERATURE MARGINS

The combination of an MHTGR core's large thermal inertia (high heat capacity and low power density) typically results in long, slow core heatup (and cooldown) transients for loss-of-forced-convection and loss of coolant pressure events. These attributes, coupled with the core's high effective thermal conductivity attributes, tend to delay the occurrence of peak values of fuel temperatures for days, when the magnitude of the afterheat is considerably reduced. Very long response time also allows considerable opportunity for operational corrective measures to be taken.

The thermal response, in combination with the time-at-temperature effect on fuel fission product retention and the helium characteristics noted earlier, fundamentally alters the effectiveness of strategies for fission product containment. For example, in a depressurisation accident, the predicted small fission product release from the fuel occurs long after the depressurization is completed, even for relatively small leaks. At this time, there would be no driving force to transport the fission products. In fact, once the maximum temperature is reached and the system begins to cool, the net flow is inward. However, if the released gas is contained, with a small (e.g. 1%/day) leakage rate, the leakage flow and slowly decreasing pressure would provide a mechanism for fission product transport. Thus attempting to contain the leaking helium can result in a higher fission product release rate for some of the most limiting events. This effect was observed during the safety review of an earlier MHTGR design [9].

For annular core designs, the peak fuel temperatures in the depressurized accident scenarios (for a given total core power and vessel size) are reduced relative to those for a cylindrical active core. Increases in the core graphite conductivity, which can vary widely with irradiation and irradiation-temperature history, can also result in reduced peak fuel temperatures as the core graphite anneals, effectively increasing conductivity with increasing temperature. Thermal radiation (T^4) effects also tend to become the dominating heat transfer mechanism for both prismatic and pebble cores at the very-high (accident-range) temperatures.

2.6. TEMPERATURE MARGINS AND NEGATIVE TEMPERATURE-REACTIVITY COEFFICIENT

A negative temperature-reactivity coefficient can be attained in the MHTGR for the entire fuel cycle and over the full temperature range of concern, as seen in most of the other types of reactors. In combination with the characteristics of large margin between fuel operation and fuel damage temperatures, and relatively low excess reactivity, as discussed below, power control and reactor shutdown can be ensured naturally. These characteristics significantly reduce the safety significance of the reactivity control and reactor shutdown systems.

In the pebble bed reactor, the reactor core can operate with low excess reactivity by adjusting the number of fuel balls introduced during operation. Protection and management of abnormal reactivity insertion conditions could be provided by inherent features, simplifying the design of active/passive protection or mitigation systems to assure safe shutdowns.

For the block type reactor, rather low excess reactivity can be attained by appropriate core design with burnable poison, optimized refuelling programmes, etc. Careful design and quality assurance/control would be required for the reactivity control and shutdown system, as well as countermeasures to the possible control rod housing failure causing rapid reactivity insertion (control rod ejection event).

2.7. FEATURES COMMON TO MHTGRs AND OTHER FUTURE REACTORS

Simplification and use of passive systems

MHTGRs make extensive use of passive characteristics that offer the opportunity to eliminate or simplify active systems that rely on a large number of safety grade support systems by applying the advantages of simple gravity driven or thermal gradient driven safety systems. The challenge is to demonstrate the capability and the reliability of these passive systems, in particular for the long time accident response.

Standardization, prefabrication and modularity

The standardization, prefabrication and modularity of the facilities that will likely be part of the design, construction and operation of MHTGR with evident benefits on the economics of a single unit, will also lead to a simplification of the licensing through a certification procedure, and reduction of the construction time and licensing costs.

Applicability of PSA and risk-informed decision making

Because of the extensive use of passive components, the safety of these reactors is primarily determined by initiating events of very low probability (e.g. structural failures due to extremely rare external events). The consequences of these events are determined by the direct phenomenological response of the plant to these events, rather than by a sequence of failures of systems, which individually have higher probabilities and which can be analyzed and modelled with much less uncertainty. This aspect will pose significant challenges for the development and application of PSA methodologies to address these concepts.

3. GENERAL SAFETY ASPECTS OF NUCLEAR POWER PLANTS

3.1. SAFETY OBJECTIVES

The Safety of Nuclear Power Plants: Design [3], sets out basic objectives, concepts and principles for ensuring safety of nuclear installations in which the stored energy or the energy developed in certain situations could potentially result in the release of radioactive material from its designated location with the consequent risk of radiation exposure of people. The principles are derived from the following three fundamental safety objectives (the following five paragraphs are reproduced from reference [3]):

General Nuclear Safety Objective: *To protect individuals, society and the environment from harm by establishing and maintaining in nuclear installations effective defences against radiological hazards.*

This general nuclear safety objective is supported by two complementary safety objectives dealing with radiation protection and technical aspects. They are interdependent: the technical aspects in conjunction with administrative and procedural measures ensure defence against hazards due to ionizing radiation.

Radiation Protection Objective: *To ensure that in all operational states radiation exposure within the installation or due to any planned release of radioactive material from the installation is kept below prescribed limits and as low as reasonably achievable, and to ensure mitigation of the radiological consequences of any accidents.*

Technical Safety Objective: *To take all reasonably practicable measures to prevent accidents in nuclear installations and to mitigate their consequences should they occur; to ensure with a high level of confidence that, for all possible accidents taken into account in the design of the installation, including those of very low probability, any radiological consequences would be minor and below prescribed limits; and to ensure that the likelihood of accidents with serious radiological consequences is extremely low.*

Safety objectives require that nuclear installations are designed and operated so as to keep all sources of radiation exposure under strict technical and administrative control. However, the radiation protection objective does not preclude limited exposure of people or the release of legally authorized quantities of radioactive materials to the environment from installations in operational states. Such exposures and releases, however, must be strictly controlled and must be in compliance with operational limits and radiation protection standards.

In order to achieve these three safety objectives in the design of a nuclear power plant, comprehensive safety analyses are carried out to identify all sources of exposure and to evaluate radiation doses that could be received by the public and by workers at the installation, as well as potential effects of radiation on the environment. The safety analysis examines: (1) all planned normal operational modes of the plant; (2) plant performance in anticipated operational occurrences; (3) design basis accidents; and (4) selected severe accidents. The design for safety of a nuclear power plant applies the principle that plant states that could result in high radiation doses or radionuclide releases are of very low probability of occurrence, and plant states with significant probability of occurrence have only minor or no potential radiological consequences. An essential objective is that the need for external intervention measures may be limited or even eliminated in technical terms, although such measures may still be required by national authorities.

3.2. THE DEFENCE IN DEPTH STRATEGY

The safety objectives will be achieved through the application of the defence in depth strategy. The strategy for defence in depth [4] is twofold: first, to prevent accidents and, second, if prevention fails, to limit 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's performance generally deteriorates when the status of the plant or a component departs from normal conditions. Thus preventing the degradation of plant status and performance generally will provide the most effective protection of the public and the environment as well as the protection of the investment. Should preventive measures fail, however, control, management and mitigatory measures, in particular the use of a well designed confinement function, can provide the necessary additional protection of the public and the environment.

The concept of defence in depth, as applied to all safety activities, whether organizational, behavioural or design related, ensures that they are subject to functionally redundant provisions, so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures. Application of the concept of defence in depth in the design of a plant provides a series of levels of defence (inherent features, equipment and procedures) aimed at preventing accidents and ensuring appropriate protection in the event that prevention fails. This strategy has been proven to be effective in compensating for human and equipment failures, both potential and actual.

There is no unique way to implement defence in depth (i.e. no unique technical solution to meet the safety objectives), since there are different designs, different safety requirements in different countries, different technical solutions and varying management or cultural approaches. Nevertheless, the strategy represents the best general framework to achieve safety for any type of nuclear power plants.

Generally, several successive physical barriers for the confinement of radioactive material are put in place. Their specific design may vary depending on the activity of the material and on the possible deviations from normal operation that could result in the failure of some barriers. So, the number and type of barriers confining the fission products is dependent on the adopted reactor technology.

Defence in depth is generally structured in five levels. Should one level fail, the subsequent level comes into play. Table I, summarizes the objectives of each one of the five levels and the correspondent primary means of achieving them. The general objective of defence in depth is to ensure that a failure, whether equipment failure or human failure, at one level of defence, and even combinations of failures at more than one level of defence, would not propagate to defeat defence in depth at subsequent levels. The independence of different levels of defence, i.e. the independence of the features implemented to fulfill the requested functions at different levels, is a key element in meeting this objective.

TABLE I. LEVELS OF DEFENCE IN DEPTH (FROM INSAG-10) [9]

Levels of defence	Objective	Essential means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions including prevention of accident progression and mitigation of the consequences of severe accidents (*)	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

* 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 discussed in Section 2, 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 [7] 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.

3.3. THE FUNDAMENTAL SAFETY FUNCTIONS

The objective of the safety approach is to provide adequate means:

- to maintain the plant in a normal operational state;
- to ensure the proper short term response immediately following a postulated initiating event (PIE);

- and to facilitate the management of the plant in and following any design basis accident, and following any plant states beyond the design basis that may occur (i.e. the "severe plant conditions").

To ensure safety (i.e. to meet allowable radiological consequences during all foreseeable plant conditions), the following fundamental safety functions shall be performed in operational states, in and following a design basis accident and in and after the occurrence of severe plant conditions:

- control of the reactivity;
- removal of heat from the core; and
- confinement of radioactive materials and control of operational discharges, as well as limitation of accidental releases.

The possible challenges to the safety functions are dealt with by the provisions (inherent characteristics, safety margins, systems, procedures) of a given level of defence. Combinations of one or more provisions to cope with challenges to levels of defence are often called lines of defence (LOD) (see Section 3.4 for details). The way the fundamental safety functions are achieved and the specific LOD used, are obviously dependent on the specific design.

All mechanisms that can challenge the successful achievement of the safety functions are identified for each level of defence. These mechanisms are used to determine the set of initiating events that encompass the possible initiations of sequences. According to the philosophy of defence in depth, if the evolution of a sequence is not controlled by the provisions of a level of defence it will be by the subsequent level that comes into play (LOD functional redundancy).

Figure 2 shows the logic flow diagram of defence in depth and its correlation to the fundamental safety functions. The objective is always to maintain the plant in a state where the fundamental safety functions (confinement of radioactive products, control of reactivity and heat removal) are successfully fulfilled. Success criteria are defined for each level of defence in depth and for the moment they are expressed only in deterministic terms.

As the objective of the first level of protection is the prevention of abnormal operation and system failures, if it fails, an initiating event comes into play and a sequence of events is potentially initiated. Then the second level of protection will detect the failures or control the abnormal operation. Should the second level fail, the third level ensures that the safety functions are further performed by activating specific LODs (safety systems and other safety features). Should the third level fail, the fourth level limits accident progression through accident management, so as to prevent or mitigate severe accident conditions with external releases of radioactive materials. The last level (fifth level of protection) is the mitigation of the radiological consequences of significant external releases through the off-site emergency response.

Figure 2 shows that some challenges/mechanisms may compromise the effectiveness of the considered level of defence by affecting either the performance of the safety function directly or the reliability of a safety provision. The effectiveness of a level of defence is determined by the ability of the provisions to cope with mechanisms which challenge the performance of safety functions. The probability associated with challenges/mechanisms, the reliability of the demanded safety provisions and the associated potential radiological consequences will define the risk for the considered accident sequence.

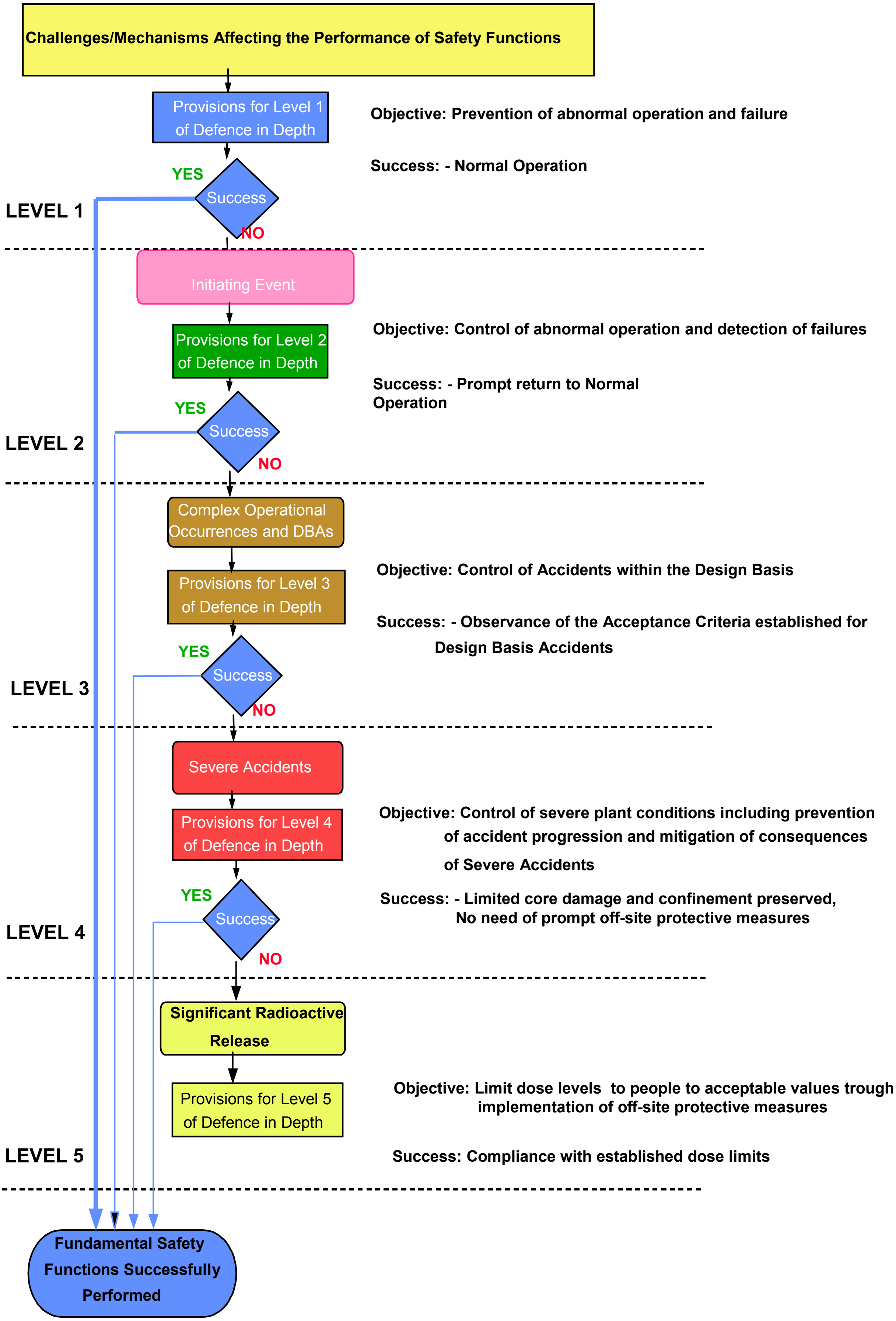

Challenges/Mechanisms Affecting the Performance of Safety Functions
Provisions for Level 1 of Defence in Depth
Objective: Prevention of abnormal operation and failure
Success: - Normal Operation
YES
Success
NO
LEVEL 1
Initiating Event
Provisions for Level 2 of Defence in Depth
Objective: Control of abnormal operation and detection of failures
Success: - Prompt return to Normal Operation
YES
Success
NO
LEVEL 2
Complex Operational Occurrences and DBAs
Provisions for Level 3 of Defence in Depth
Objective: Control of Accidents within the Design Basis
Success: - Observance of the Acceptance Criteria established for Design Basis Accidents
YES
Success
NO
LEVEL 3
Severe Accidents
Provisions for Level 4 of Defence in Depth
Objective: Control of severe plant conditions including prevention of accident progression and mitigation of consequences of Severe Accidents
Success: - Limited core damage and confinement preserved, No need of prompt off-site protective measures
YES
Success
NO
LEVEL 4
Significant Radioactive Release
Provisions for Level 5 of Defence in Depth
Objective: Limit dose levels to people to acceptable values trough implementation of off-site protective measures
Success: Compliance with established dose limits
LEVEL 5
Fundamental Safety Functions Successfully Performed

FIG. 2. Logic flow diagram of defence in depth.

3.4. THE CONCEPT OF LINES OF DEFENCE

To evaluate or compare the implementation of defence in depth by different reactor technologies, it is suggested to adopt a common approach that needs to have the following features:

- the safety objectives should be the same in terms of doses respectively to the operators, the public and the environment (i.e. radiological consequences) for all plant conditions at a given level of defence;
- the safety assessment method should use analogous and comparable approaches based on the integral adoption of defence in depth (all the levels should be considered);
- the approach should be able to integrate the unique characteristics of each type of reactor, with the number and the quality of the required "defences" being a function of the potential internal and external hazards and consequences of failures.

To implement this, it is useful to introduce the concept of lines of defence as any inherent characteristic, equipment or system implemented into the safety related plant architecture, as well as any safety relevant operational procedure, that are necessary to fulfil the safety functions.

The required number and strength of these lines of defence depend on the reactor type, i.e. the implemented LODs shall fulfil the missions requested to prevent abnormal situations or return the plant to a controlled or safe shutdown condition and maintain it in a safe state after a postulated initiating event (PIE). Their design shall take into account simultaneously the needs for performance (to meet the safety criteria), and the safety objectives as well as the recommendations concerning, for example, reliability, redundancy, diversity, in-service inspection requirements, etc.

In this logic, the physical barriers normally considered in LWRs (fuel, cladding, primary circuit and containment) are provisions to confine fission products. Their contribution to safety has to be assessed for each specific concept of reactor and considered in the general safety architecture of the plant.

As lines of defence can rely simultaneously on both active and passive systems as well as on inherent features, the safety assessment approach should consider their correspondent reliabilities to correctly take into account all the potential of the safety related architecture. The LODs can be classified into categories according to their reliability. The number and category of LODs can be used as a tool to assess the adequacy of the implementation of defence in depth.

3.5. CURRENT SAFETY APPROACH

Operating nuclear power plants are largely designed following a safety architecture dictated by the implementation of the strategy of defence in depth (physical barriers and levels of defence) as illustrated in Section 3.2. In the majority of the plants of the current generation the application of defence in depth is mainly based on deterministic considerations. This means that the plant is deterministically designed against a set of normal and postulated accident situations according to well established design criteria in order to meet the radiological targets. The adequacy of the defence in depth is established by the number of barriers and number and quality of systems in each level of defence.

The current design approach has been shown to be a sound foundation for the safety and protection of public health, in particular because of its broad scope of accident sequence considerations, and because of its many conservative assumptions which have the effect of introducing highly conservative margins into the design that, in reality, give the plant the capability of dealing with a large variety of sequences, in some cases well beyond those included in the design basis.

The deterministic approach is complemented by probabilistic evaluations with the main purpose of verifying that the design is well balanced and there are no weak areas or systems that could allow for the possibility of high risk sequences. Probabilistic safety assessment is recognized as a very efficient tool for identifying those sequences and plant vulnerabilities that require specific additional preventive or mitigative design features.

This safety approach is reflected in the current IAEA Safety Standards for the design.

3.6. THE IAEA SAFETY STANDARDS SERIES

Under the terms of its Statute, the IAEA is authorized to establish standards of safety for protection against ionizing radiation. The regulatory related publications are issued in the IAEA Safety Standards Series, covering nuclear safety, radiation safety, transport safety and waste safety. There are three categories within the Safety Standards Series, schematically depicted in Fig. 3:

Safety Fundamentals: present basic objectives, concepts and principles of safety and protection in the development and application of nuclear energy for peaceful purposes.

Safety Requirements: establish the requirements that must be met to ensure safety. These requirements, which are expressed as ‘shall’ statements, are governed by the objectives and principles presented in the Safety Fundamentals.

Safety Guides: recommend actions, conditions or procedures for meeting safety requirements. Recommendations in Safety Guides are expressed as ‘should’ statements, with the implication that it is necessary to take the measures recommended or equivalent alternative measures to comply with the requirements.

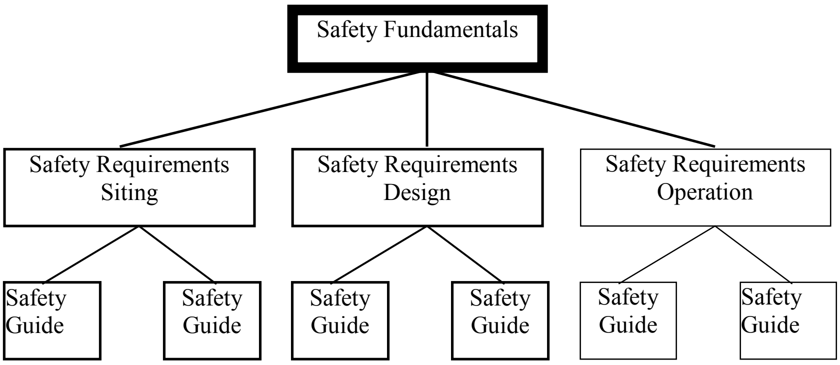


FIG. 3. The IAEA Safety Standards Series.

3.7. DEVELOPMENT OF GENERAL SAFETY DESIGN REQUIREMENTS

Design requirements play an important role in establishing the safety level[1] of the installation and also have great impact on its cost and operating procedures. The general logical process to generate the safety requirements for a reactor plant design is schematically represented in Fig. 4, and briefly described below.

The Safety requirements can be derived from a set of limited safety principles which directly descend from the three well established safety objectives. The safety objectives define the general targets that shall be achieved by a nuclear installation to protect the operators and the population. They are the same for all nuclear installations including nuclear reactors, and are independent of the kind or size of any given installation.

For nuclear reactors, the compliance with the safety objectives is achieved when the three fundamental safety functions *Confinement of radioactive material*, *control of the reactivity* and *removal of the heat from the core* are fulfilled for all the plant operational, accidental and post accidental conditions in accordance with radiological targets.

To ensure that the safety objectives are met with sufficient confidence and the fundamental safety functions are adequately fulfilled, an effective defence in depth should be implemented. For measuring and assessing the adequacy of the defence in depth, success criteria (expressed in deterministic and probabilistic terms) need to be defined for each level of defence.

Defence in depth has been proved to be generally applicable and very effective in assuring safety in NPPs. It can be used as primary guidance for the preparation of safety requirements. As a matter of fact, and as has been shown by INSAG [4], there is correspondence between the five levels of defence in depth and the safety requirements. It is reasonable to assume that this correspondence is maintained for all kind of reactors regardless of their size or specific safety features.

The safety requirements can be obtained by developing, for each fundamental safety function, the corresponding provisions necessary to meet the established success criteria for each level of defence. The correct implementation of the strategy of the defence in depth (i.e. the adoption of an adequate safety architecture) ensures that the fundamental safety functions are reliably achieved and with sufficient margins to compensate for equipment failure and human errors. More demanding success criteria will result in a more effective defence in depth and in more demanding requirements for the provisions for each level of defence.

3.8. INTEGRATION OF DETERMINISTIC AND PROBABILISTIC CONSIDERATIONS IN THE SCHEME OF DEFENCE IN DEPTH

The generalized concept of defence in depth, as outlined in Section 3.2, needs to integrate both deterministic and probabilistic considerations (e.g. system reliability, probabilistic targets, etc.) to provide metrics for assessing the adequacy of the means of each level of defence. The integration of deterministic and probabilistic approaches also provides a basis for additional requirements and to ensure a well balanced design to identify and then

[1] The actual level of safety is determined by the full set of detailed criteria and requirements (deterministic and probabilistic) with which the design complies. In other words, the level of safety depends on the way defence in depth is implemented in the design taking into account the implications of the specific features and technology.

cope with all PIEs. The approach provides general guidance on what is understood to be key engineering judgements about the performance requirements of the plant systems. However, the levels of defence by themselves do not provide the metrics by which to judge adequacy of the implementation of defence in depth. Risk informed approaches which combine deterministic and probabilistic techniques, can be useful tools to assess the contribution of each line of defence to safety with a resulting integrated safety assessment relative to public health and safety.

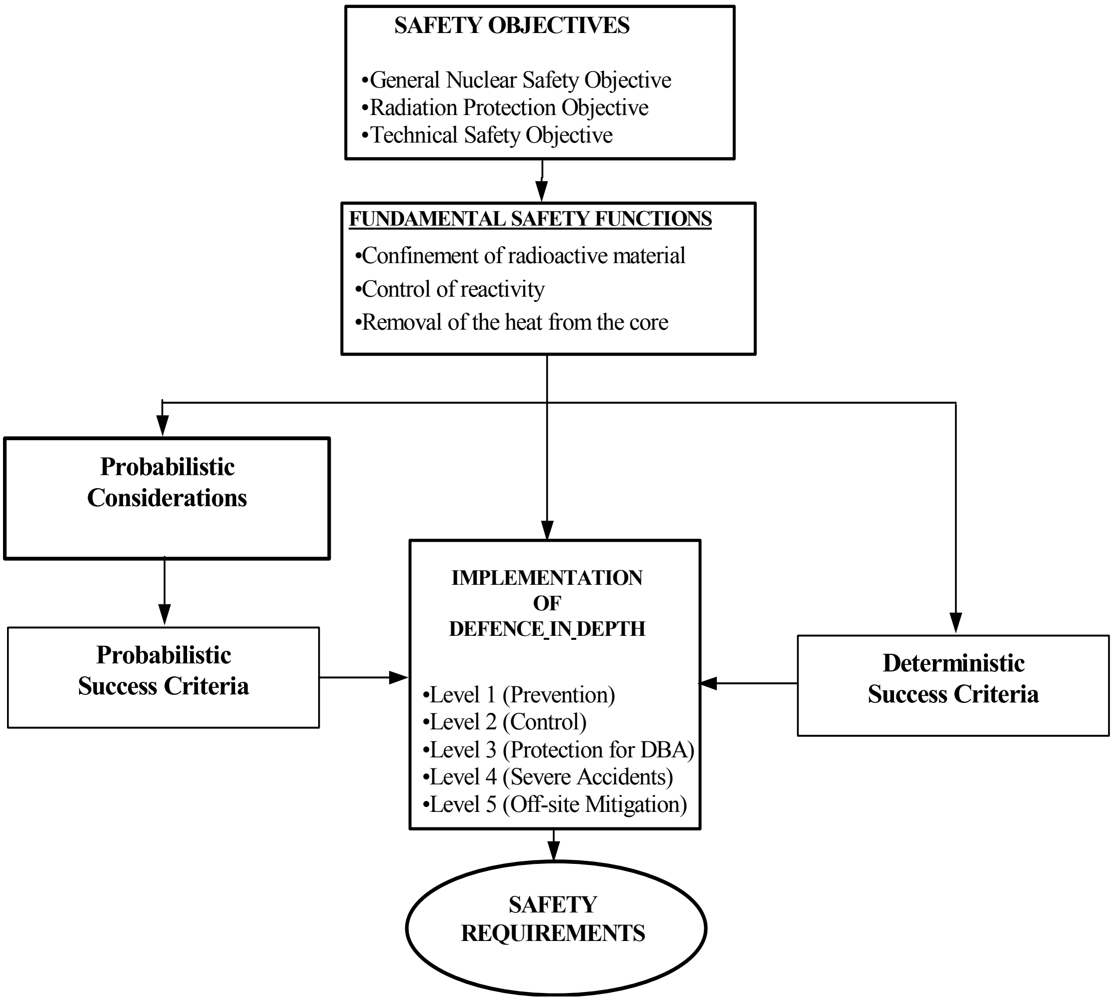

SAFETY OBJECTIVES
•General Nuclear Safety Objective
•Radiation Protection Objective
•Technical Safety Objective
FUNDAMENTAL SAFETY FUNCTIONS
•Confinement of radioactive material
•Control of reactivity
•Removal of the heat from the core
Probabilistic Considerations
Probabilistic Success Criteria
IMPLEMENTATION OF DEFENCE_IN_DEPTH
•Level 1 (Prevention)
•Level 2 (Control)
•Level 3 (Protection for DBA)
•Level 4 (Severe Accidents)
•Level 5 (Off-site Mitigation)
Deterministic Success Criteria
SAFETY REQUIREMENTS

Fig. 4. Logical process for the generation of safety requirements.

The approach that is recommended is the development of a probabilistic safety assessment model of all plant systems without any pre-conceived notion of what is safety related. This model can then be used to determine the importance to safety of systems, structures and components which can then lead to a determination of safety classification. This model can then also be used to assess the contribution of each level of defence to the ultimate safety of the plant as it relates to public health and safety. Should there be barriers or other provisions that need to be strengthened, the value of the improvement can be directly assessed.

A key factor in making safety adequacy assessments is the ability to tie the levels of defence concept to safety goals that are generally accepted for nuclear plants. This linkage provides the integration of safety with technology judgements of adequacy from a public health and safety point of view. The risk informed process can be used in plant design to optimize safety performance and to balance the lines of defence in an overall defence in depth strategy by the quantification possible through the use of probabilistic safety analysis.

One of the key issues in deterministic and probabilistic analysis is how to deal with uncertainties. Traditional deterministic approaches rely on a balance of prevention and mitigation with large design margins and the ultimate final barrier being the 'containment' to cover any unknown phenomenon or event that goes beyond what is generally expected or understood. With advanced reactors, the objective is to design the plant making extensive use of inherent safety features that do not rely on active systems to prevent plant conditions that could lead to fuel failure and fission products release. By employing the risk informed analysis, the contribution to safety of the design features and need for additional features can be assessed. To deal with uncertainties, especially in early deployment of the systems, sensitivity analysis the performance of key systems can be used to provide a measure of the impact of the uncertainty and appropriate design decisions can be made.

Figure 5 shows in a very schematic fashion the curve of the target risk that separates acceptable and unacceptable situations (frequency of the event × consequences) and the integration of the level of defences with the probability associated to each event. The success criterion for each level of defence is represented by the area limited by the maximum acceptable consequence and probability for that level. (e.g. dotted area for Level 2).

An event sequence is initiated (see Fig. 2) if a challenge (internal or external to the plant) breaks the first level of defence (prevention of abnormal operation and failures).

The representation of Fig. 5, with adequate values of consequences and probabilities on the axes of the diagram gives a visual representation of the contribution of each level of defence to the general safety of the plant, provides a metric and allows for comparisons of the safety and implementation of defence in depth in different concepts.

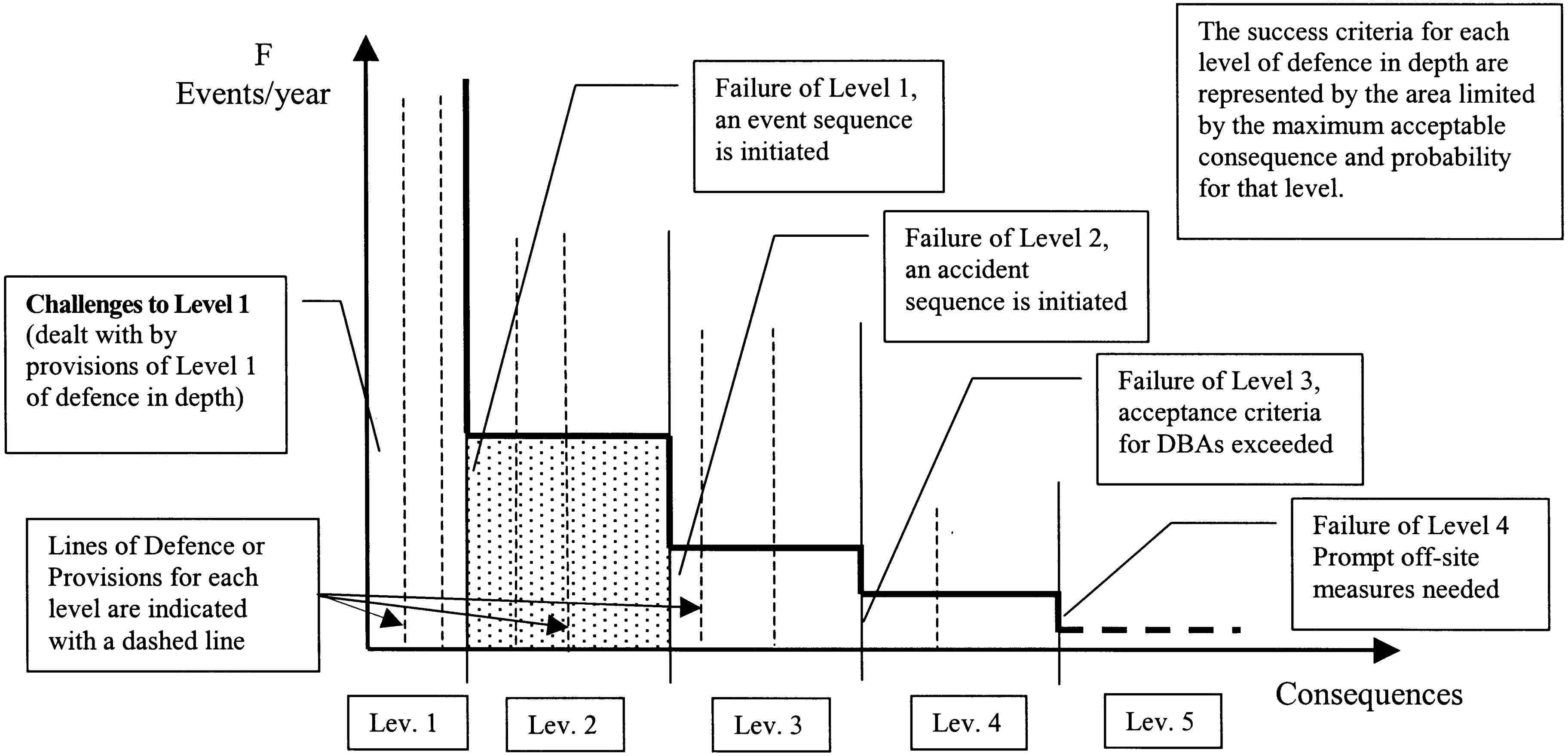

F
Events/year
Failure of Level 1, an event sequence is initiated
The success criteria for each level of defence in depth are represented by the area limited by the maximum acceptable consequence and probability for that level.
Failure of Level 2, an accident sequence is initiated
Challenges to Level 1 (dealt with by provisions of Level 1 of defence in depth)
Failure of Level 3, acceptance criteria for DBAs exceeded
Lines of Defence or Provisions for each level are indicated with a dashed line
Failure of Level 4 Prompt off-site measures needed
Consequences
Lev. 1
Lev. 2
Lev. 3
Lev. 4
Lev. 5

Fig. 5. Correlation of levels of defence and success criteria.

4. PREPARATION OF DESIGN SAFETY REQUIREMENTS FOR THE MHTGR

4.1. THE TOP-DOWN APPROACH

The proposed top-down approach consists of a systematic review of the existing requirements for nuclear power plants [3] starting from the most general (applicable to all nuclear plants) and down to the most specific and more technology dependent. This process is schematically presented in Fig. 6 [5].

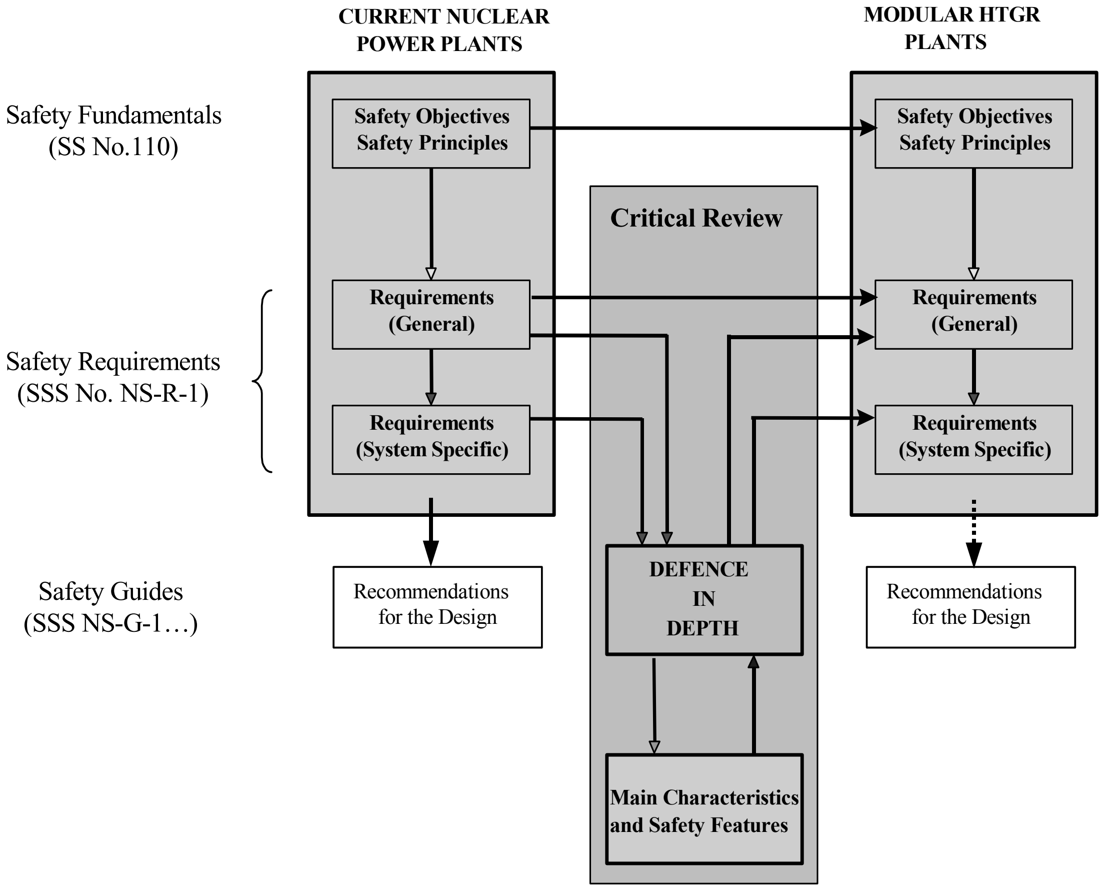

CURRENT NUCLEAR POWER PLANTS
MODULAR HTGR PLANTS
Safety Fundamentals (SS No.110)
Safety Requirements (SSS No. NS-R-1)
Safety Guides (SSS NS-G-1…)
Safety Objectives Safety Principles
Requirements (General)
Requirements (System Specific)
Recommendations for the Design
Critical Review
DEFENCE IN DEPTH
Main Characteristics and Safety Features
Safety Objectives Safety Principles
Requirements (General)
Requirements (System Specific)
Recommendations for the Design

Fig. 6. Generation of Requirements for an MHTGR.

The requirements for a specific type of reactor are generated through a critical interpretation of the objectives, challenges to the objectives, mechanisms posing the challenges and corresponding provisions associated with each level of defence in depth and the full understanding of the safety features of the specific reactor.

The safety requirements for nuclear power plants have reached the current status through a long development process which incorporated the results of the extensive operating experience and the experience gained from the errors of the past. The current safety requirements define the safety approach developed and refined over many years. Although they are mostly developed for water cooled reactors, it is reasonable to assume that they are a good starting point for the preparation of the design requirements for any type of reactors including non-water cooled reactors such as MHTGRs. For these reactors, which make extensive use of inherent safety features, it can be expected that the acceptance criteria of each level of defence could be met using less and simpler safety systems than those for large water reactors.

The mechanism for judging the applicability or adequacy of a requirement for existing NPPs to a MHTGR should be based on the full understanding of its contribution to defence in depth. The 'transfer function' (central box in Fig. 6) that establishes the requirements for a generic nuclear reactor plant from the requirements for existing plants, should not simply be interpreted as a filter to accept or not a requirement but as a mechanism to generate new requirements if they are necessary because of the features of the specific plant. For example, an inherent feature that fulfils a safety function in a very reliable way could allow for a relaxation of the requirements for a safety system or even to the possible elimination of the safety system that performs an equivalent function for water reactors. On the other hand, the designer should be aware that specific features or materials could possibly initiate events for which adequate preventive or mitigative measures could be necessary. This process will lead to the compilation of a consistent set of requirements organised in a hierarchical way with the general requirements at the top and the more specific at the bottom like those existing for current plants.

4.2. APPLICABILITY OF CURRENT DESIGN REQUIREMENTS TO THE MHTGR

The current design requirements [3] and the derived Safety Guides have been mainly developed for water reactors, and their applicability to the design of MHTGR is not always straightforward. In some cases, special interpretation may be necessary. These requirements are applicable to safety functions and the associated structures, systems and components, as well as to procedures important to safety in nuclear power plants (NPPs). They must be met for safe operation of an NPP, and for preventing or mitigating the consequences of events that could jeopardize safety.

Reference [3], which also includes requirements for a comprehensive safety assessment to be carried out in order to identify the potential hazards that may arise from the operation of the plant, under the various plant states, is organized as follows:

Section 2 elaborates on the three safety objectives and the concepts like defence in depth which form the basis for deriving the safety requirements that must be met in the design of any NPP.

Section 3 covers the requirements to be applied by the design organization in the management of the design process, and also the requirements for safety assessment, for quality assurance, and for the use of proven engineering practices and operational experience.

These principal requirements should be applicable to any NPP design independent of the technology adopted.

Section 4 provides the general technical requirements for defence in depth and radiation protection. They should be also independent of the adopted technology.

Section 5 provides the requirements that are applicable to the process of the design itself. It covers safety classification, general design basis, design for reliability, provisions for in-service testing, maintenance and repair, equipment qualification, ageing, human factors, safety analysis and other considerations. Although the implementation of the requirements will conduct to technology dependent solutions (e.g. considered PIEs, in-service inspection solutions, etc.), the requirements are generically stated and, therefore, they are applicable to any type of reactors.

Finally, Section 6 provides design requirements applicable to specific plant systems, such as: the reactor core and associated features, reactor coolant systems, containment systems, instrumentation and control, fuel handling and storage system. These are the most technology-dependent requirements and a deeper investigation should be conducted to determine to what extent they need adaptation or modification for MHTGR designs.

4.3. THE OBJECTIVE-PROVISIONS TREE

The method of the objective-provisions tree, represents a preliminary attempt to systematically address the "critical review" of the implementation of the defence in depth as indicated in the critical review box of Figure 6.

The logical framework of the objective-provisions method is graphically depicted in terms of a tree such as that shown in Figure 7. At the top of this tree is the level of defence in depth of interest, followed by both the objectives to be achieved and the barriers or defences to be protected.

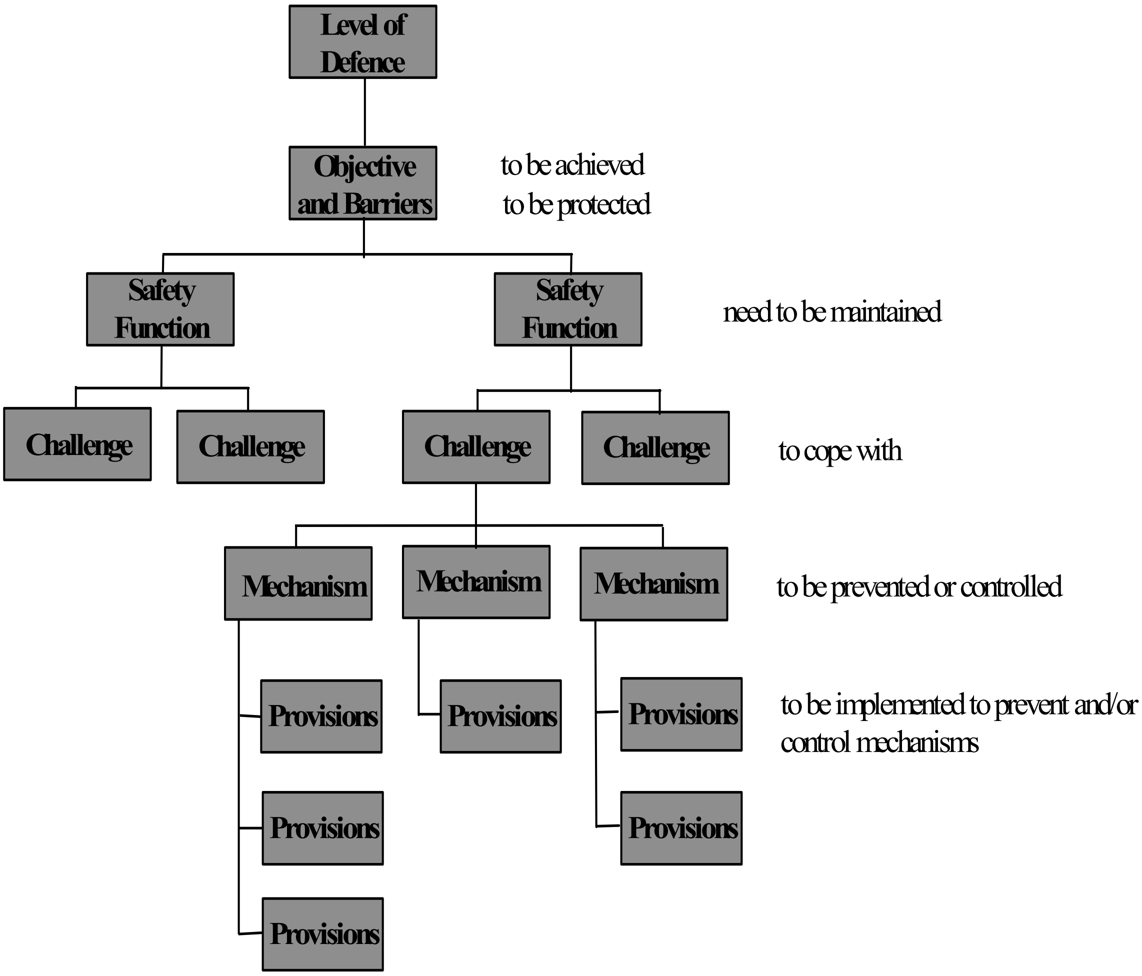


FIG. 7. Defence in depth objective-provisions tree.

The objectives can be directly derived from those of Table I. For example the main objective for Level 3 is to achieve the control of accidents within the design basis. This main objective can be developed and expressed in terms of more specific objectives such as: (a) limit the damage to fuel, (b) avoid any consequential damage to the reactor coolant system, (c) maintain the confinement of radioactive products. For each level of defence, the three fundamental safety functions can be detailed into a consistent group of sub-functions (e.g. reactivity control into shutdown of the reactor, maintain the reactor in safe shutdown conditions…). The specific objectives provide acceptance criteria for the performance of safety functions at each different level of defence.

For each sub-function, the challenges to its fulfilment can be identified. These challenges are general processes or situations that can prevent adequate performance of the safety functions (e.g. reactivity excursions that could damage the fuel before the shutdown). The challenges arise from a variety of mechanisms (or events) which also have to be identified. The identification of the mechanisms (or events) that can challenge the success of a safety function is an essential task in the development of the logical framework for inventorying the defence in depth capabilities of a nuclear power plant. Once the mechanisms are understood, it is possible to determine the provisions necessary to prevent and/or control these mechanisms.

If the set of provisions of a Level N is not sufficient to overcome some mechanisms of a challenge to the safety function or some failures prevent the provisions to perform their function, then additional provisions will come into play to support safety functions to achieve acceptance criteria correspondent to the subsequent Level N+1.

5. IMPLEMENTATION OF DEFENCE IN DEPTH FOR THE MHTGR

In this section, general characteristics of MHTGRs drawn from existing designs and potential provisions based around these characteristics are used to explore the implementation of defence-in-depth using the methods identified in this report. The considerations presented here are intended to illustrate application of the methods and are not intended to be requirements for MHTGRs. However, they can be viewed as a first step in the development of the requirements.

5.1. GENERAL CONSIDERATIONS ON BARRIERS AND LEVELS OF DEFENCE IN DEPTH

The implementation of defence in depth (D.i.D.) for MHTGR differs from that for the traditional LWR strategy to achieve effective defence against radiological hazards. The safety of MHTGR relies strongly on inherent features, with the confinement of radionuclides being accomplished with minimal or no reliance on active systems or operator actions.

Using the definition in INSAG-10 [4], defence in depth consists of a hierarchical deployment of different levels of equipment and procedures (LOD) in order to maintain the effectiveness of physical barriers placed between radioactive materials and workers, the public and the environment in normal operation, anticipated operational occurrences and, for some barriers, in accidents at the plant. Defence in depth is implemented through design and operation to provide a graded approach to defence in a wide variety of transients, incidents and accidents, including equipment failures and human errors within the plant as well as events initiated outside the plant.

The public and the environment are protected primarily by means of these barriers, which may serve both operational and safety purposes or safety purposes only. The defence in depth concept applies to the protection of their integrity against internal and external events that may jeopardize it. Situations in which one or more barriers are breached (such as during shutdown) may require special attention

The description of the “barriers” that can be identified in the MHTGR requires special attention because their importance to safety may vary relative to water reactors. A proposed definition of the barriers is as follows: the kernel (i.e. the fuel material), three particle coating layers, the matrix (i.e. the graphitic material around the particles), the fuel element (i.e. pebble/fuel assembly block), the primary circuit, the plant civil/structural/confinement works, and the filtering system(s). It should be noted that some of these barriers (e.g. pyrocarbon coatings, matrix) are not impervious to all fission products (e.g. caesium), even when intact, and the effectiveness of these barriers in confining radioactive material varies widely, and is dependent on operating (normal/accident) conditions.

In HTGRs, the primary barrier is the silicon carbide layer of the coated fuel particle. There are other “barriers” that reduce the release of fission products into the environment. These other barriers as noted above are effective contributors to the defence in depth of the MHTGR design to limit the release of radioactive materials into the environment and dose to the public.

Concerns have been expressed about the effectiveness of the coated fuel particle (CFP) in providing a containment function, since there are literally billions of them involved in the process. However, for MHTGR designs, the unique characteristics of the technology allow for important complementary considerations that can further enhance the strength and resilience of the robust safety case[2]. The kernel and coating layers of the coated fuel particle (CFP) constitute successive barriers operating **in parallel** among the billions of particles comprising a typical MHTGR core, with each particle containing an insignificant amount of fission products. This population of parallel barriers cannot act in a uniform way in any conceivable circumstance because of the following variations:

- *Variations within a batch* – The nature of the fuel kernel production and fluidized bed coating processes result in a statistical variation of kernel and coating properties such as kernel diameter and coating thickness within a given batch. Mean values and standard deviations in these properties are specified as a part of the fuel product acceptance criteria.
- *Fabrication batches* – the core at any given time will consist of hundreds of combinations of kernel, coating and fuel compact or sphere fabrication batches.
- *Service conditions* – the core at any given time will generally consist of a population of particles with a broad range of service conditions. Spatial variations in temperature and neutron flux, as well as variations in time of service, will produce a broad range of particle histories for the key parameters of temperature history, fluence and burnup.
- *Event conditions* – The extent of the challenge to the containment barriers of a given coated particle is determined by its service conditions as well as by the conditions experienced in a given event. The most important event condition is particle temperature, which will vary over a wide range in any event, with the population mean temperature far below the maximum temperature.

This diversity effectively addresses concerns about fuel that would perform well in normal operation and yet suddenly fail at lower-than-expected temperatures, with the possibility of a sudden onset of barrier failures in a large fraction of the particle population under accident conditions ('weak fuel').

Additional defence in depth considerations involve the preservation of the effectiveness of the barriers and options for dealing with the loss of barrier functions. The current safety practice allows for the loss of some barrier function within the design basis and selected severe accidents of a nuclear plant, with a requirement that at least one of the barriers should remain effective and contain the fission products to ensure compliance with the radiological targets. The safety design of nuclear power plants based on MHTGR technology and operation is consistent with this logic, as discussed further in this section.

Measures relative to defence in depth are ranked in five levels of defence. The first four levels are oriented towards the protection of barriers and mitigation of releases; the last level relates to off-site emergency measures to protect the public in the event of a significant release. Even though implementation of the concept of defence in depth may differ from LWR to MHTGR and may to a certain degree depend on plant design, the main principles are common.

For a consistent implementation of the defence in depth concept, account needs to be taken of the risk represented by the amount and type of radioactive material present in the

[2] These complementary considerations that differentiate the technology of an MHTGR from other kinds of reactors, in particular for the characteristics of the fuel, can be referred to as 'defence in breadth'.

installation; the potential for its dispersion due to the physical and chemical nature of these products; and the possibility of nuclear, chemical or thermal reactions that could occur under normal or abnormal conditions, and the kinetics of such events.

The method of objective-provisions trees is adopted here to systematically conduct the ‘critical review’ of the implementation of defence in depth for MHTGR designs. For each one of the first four levels of defence, three objective-provisions trees are developed correspondent to the three fundamental safety functions. With respect to Level 5, reliance on off-site measures to mitigate consequences of severe accidents should be minimal due to the effectiveness of the previous levels of defence. As provisions of Level 5 of defence in depth do not normally involve design, they are outside of the scope of the present TECDOC.

The adopted strategy to implement defence in depth for MHTGR differs from the traditional LWR philosophy and gives higher priority both to the prevention of accidents through a significant plant architecture simplification that minimizes the number of failures with potential safety significance and to the management of abnormal situations through the implementation of robust LODs (e.g. TRISO particle, passive DHR, etc.). These aspects put strong emphasis on Level 1 and Level 3 of the defence in depth, and considerably enhance the robustness of the overall safety case.

5.2. APPLICATION OF LEVEL 1 DEFENCE IN DEPTH FOR THE MHTGR

The **objective** for Level 1 is the prevention of deviations from normal operation, the prevention of failures, and to ensure that the safety systems would operate reliably if called upon at higher levels of defence. The **essential means** are the provision of the characteristics described in Section 2, conservative design, and high quality in construction and operation. A primary means for preventing accidents is to strive for such high quality in the design that deviations from the normal operation states are well within prescribed design limits.

As for other kind of NPPs, a large number of deviations from normal operation can be avoided through adequate site selection which reduces the likelihood of externally initiating events, either natural or human-induced. Challenges to the safety functions due to unexpected mechanical loads should be compensated by a conservative structural design which takes into consideration loads originated by external events.

Prerequisites for safe operation are careful selection of materials and use of qualified fabrication processes and proven technology, together with extensive testing. In this aspect, MHTGR designs are expected to incorporate well known and proven structural materials, high purity graphite for core internals and high quality ceramic coated particle fuel of proven design, together with recent technological advances in areas like magnetic bearings, compact plate-fin heat exchanger and turbo-machine development.

For MHTGRs, a safety function of the vessel system is to ensure that the core geometry is maintained within acceptable limits under all normal and postulated abnormal conditions. This safety function is derived from two of the fundamental safety functions, named core heat removal and control of reactivity.

During normal operation conditions, with insured core geometry, the heat removal is performed by a helium coolant system using reliable turbo-compressors. An adequate conservative design of core support and barrel structure provides support and alignment for the components that are housed within the reactor vessel. This will avoid insertions of reactivity by preventing changes in core geometry and will also ensure the ability of control rods to insert and safely shut down the reactor.

Support and restraint structures are considered part of the pressure boundary system. The pressure boundary is designed to an international pressure vessel code or standard capable of ensuring that all of the functional, safety and reliability requirements can be met. Provisions can be made for the replacement of some or all of the reactor internals, depending on the degree of confidence in the component lifetimes and reliability. Inspections can be carried out on the ceramic and metallic parts,. These preventive surveillance and maintenance measures are also considered as part of the safety provisions at defence in depth Level 1.

For reactivity induced events, the absence of steam generators for some types of MHTGRs, the higher pressure of helium circuits relative to water cooling systems, and specific design solutions to minimize the presence of water sources, considerably reduce the likelihood of water ingress. Furthermore, unexpected reactivity insertion due to malfunction of the Reactivity Control System is also minimized by seismically designed units which operate under a fail-safe mode. The possibility of operator induced failures is also reduced by design thermal margins, slow thermal response, and other inherent features which minimize or simplify demands for manual intervention.

The MHTGR safety philosophy is based on control of releases primarily by the retention of radionuclides within the coated fuel particle rather than reliance on secondary barriers (such as the primary coolant boundary or the reactor building). Thus, ensuring that the safety criteria are met is the same as ensuring that the retention capability of the coated fuel particles (CFP) is not compromised. There is a considerable design margin between normal operation service conditions and fuel failure temperature.

The importance of the safety function of the pressure boundary system to contain the helium coolant by maintaining vessel integrity is reduced by the ability of the designs to remove decay heat without reliance on the presence of the helium coolant. To ensure fuel integrity under normal operation conditions, design requirements limit chemical and other physical attack on the fuel. The chemically inert helium coolant also minimizes corrosion and eliminates complications associated with internal cladding of the vessel walls. The function of the helium purification system is to remove chemical and particulate contaminants from the primary coolant in order to provide the necessary degree of helium purity during normal operation as well as removing small amounts of fission or activation products present in the coolant in normal operation. Low induced activity of helium is another factor in the low level of radiological consequences expected from leakage during normal operation. The use of magnetic or gas bearings can eliminate coolant contamination by lubricating oil for helium turbo-compressors.

The radiological design objective is that for all pathways any dose received by the operators and the public and releases to the environment in normal operations will not only meet regulatory limits and constraints, but will also be as low as reasonably achievable (ALARA principle). MHTGR designs should minimize the generation of radioactive waste throughout its lifecycle (including decommissioning) and include appropriate processing, conditioning handling and storage systems.

Another typical measure for Level 1 is the provision, as a design attribute, for adequate time for operators and the system to respond to normal events. In an overall sense, the robustness of MHTGR designs is achieved through combination of single phase coolant, low power density, high core heat capacity, and large temperature margins between normal operation and fuel failure temperatures. These Level 1 characteristics provide a more stable operation, and may reduce the requirements for Level 2, which dictate the accuracy, response time, and reliability requirements of the control and protection systems.

Additional typical operating measures corresponding to Level 1, for the safe operation of both LWR and MHTGR, are:

- Comprehensive training of appropriately selected operating personnel whose behavior is consistent with a sound safety culture;
- Adequate operating instructions and reliable monitoring of plant status and operating conditions
- Comprehensive preventive maintenance prioritized in accordance with the safety significance and reliability requirements of systems.

Figure 8 presents the objective-provisions tree for the safety function of control of reactivity where, for the objective of Level 1 of defence in depth, the acceptance criteria are stated as:

1) *to avoid insertion of reactivity which demands countermeasures outside the normal control range*;
2) *ensure the ability to safely shutdown the reactor during normal operation, anticipated operational occurrences and design basis accidents.*

Figure 9 shows the objective-provisions tree for the safety function of core heat removal, with the Level 1 corresponding to acceptance criteria being:

1) *to transfer the power generated in the core to the balance of plant (BOP), repecting allowed temperature ranges on fuel and structures during normal operation*;
2) *ensure the ability to safely remove the decay heat during normal operation, anticipated operational occurences and design basis accidents.*

Figure 10 presents the objective-provisions tree for the safety function of confinement of radioactive material, where the acceptance criteria for Level 1 are:

1) *concentration of radionuclides (including fission products) below the limits established for normal operating conditions in the reactor coolant system and inside the reactor building*;
2) *ensure the ability of maintaining barriers for confining radioactive materials for normal operation, anticipated operational occurences and design basis accidents.*

The provisions identified for Level 1 in the figures address both those which are necessary to support normal operation and those necessary to assure the capability to perform the key safety functions during anticipated operational occurrences and design basis accidents.

5.3. APPLICATION OF LEVEL 2 DEFENCE IN DEPTH FOR THE MHTGR

The **objective** for Level 2 of Defence is the control of abnormal operation and detection of failures. The **essential means** are control, limiting and protection systems and other surveillance features. The successful performance of Level 2 provisions will bring the plant back to normal operating conditions as soon as possible.

Features of Level 2 should come into play whenever a significant deviation from normal operation conditions occurs, implying insufficient safety provisions at Level 1 and the occurrence of a PIE. Monitoring and surveillance measures are typically associated with this level of defence. Level 2 incorporates inherent plant features, such as core stability and thermal inertia, and systems to detect and/or control anticipated operational occurrences, with account taken of phenomena capable of causing further deterioration in the plant status. The systems to mitigate the consequences of such operating occurrences are designed to meet reliability objectives according to specific criteria (such as redundancy, layout and qualification). Diagnostic tools and equipment, such as automatic control systems, may be provided to actuate corrective actions before reactor protection limits are reached.

In MHTGR designs, the reactivity control and shutdown system (RCSS) consists of independent and diverse systems used to control the reactor during normal operation conditions and, when required, to place the reactor in the hot shutdown condition. The control system serves to keep the reactor within normal operating limits, with an independent safety system providing capability to shut down the reactor if normal operating limits are exceeded. The combined use of an additional diverse system provides for maintaining the reactor sub-critical indefinitely in a cold condition. There are limits placed on the depth of insertion of control assemblies to ensure that a sufficient immediate shutdown margin is always available. These systems are supported by a strong negative temperature reactivity coefficient that acts as an effective provision to limit maximum temperature of the fuel.

The vessel system design addresses the requirement for limiting helium leakage at normal operation to (typically) not more than 10% of the helium inventory in the primary circuit per year. In order to monitor and control the state of the vessel system and implement the “leak-before-break” concept, instrumentation may be provided that permits the identification and characterization of defects to be made on-line.

The establishment of limiting conditions for operation (LCOs) for process variables will ensure the fulfillment of design basis accident assumptions, keeping their consequences within prescribed limits. Ongoing surveillance of quality and compliance with the design assumptions by means of in-service inspection and periodic testing of systems and plant components is also necessary to detect any degradation of equipment and systems before it can affect the safety of the plant.

Figure 11 shows the objective-provisions tree for the safety function control of reactivity at Level 2, with the correspondent acceptance criteria being:

> *to limit insertion of reactivity to minimize automatic trips, to keep variables within their operating ranges, and to shutdown the reactor, if necessary.*

Figure 12 presents the objective-provisions tree for the safety function core heat removal, with the acceptance criterion al Level 2 being:

> *to restore the balance between the heat generated and the heat removed, in order to comply with the allowed temperature ranges on fuel and structures established for anticipated operational occurrences.*

In Figure 13, the safety function confinement of radioactive materials has its objective-provisions tree depicted at the Level 2 of defence. The corresponding acceptance criterion is:

> *to keep the concentration of radionuclides in the reactor coolant system and inside containment below the limits established for anticipated operational occurrences.*

5.4. APPLICATION OF LEVEL 3 OF DEFENCE IN DEPTH FOR THE MHTGR

The objective for Level 3 of defence is the control of accidents within the design basis. The essential means are inherent and engineered safety features and accident procedures.

In spite of provisions for prevention and control of abnormal occurrences (failure of Levels 1 and 2), accident conditions may occur. Inherent safety features and protection systems and, if needed, engineered safety features, are provided to prevent evolution toward severe plant conditions and to confine radioactive materials. The measures taken at this level are aimed at preventing fuel damage in particular.

All the safety related features are designed on the basis of postulated accidents representing the limiting loads of sets of similar events. Typical postulated accidents are those originating in the plant, such as the breach of a pipe containing primary coolant (a loss of coolant accident) or loss of control of reactivity (e.g. control rod withdrawal).

Design and operating procedures are aimed at maintaining the effectiveness of the barriers, especially the fuel coating, in the event of such postulated accidents. Inherent features as well as active or passive systems are used. In the short term all these LOD are actuated inherently or by the reactor protection system when needed. If engineered systems (active or passive) are implemented, to ensure them a high reliability, the following design principles are adhered to:

- redundancy (single failure criterion);
- prevention of common mode failure due to internal or external hazards, by physical or spatial separation and structural protection;
- prevention of common mode failure due to design, manufacturing, construction, commissioning, maintenance or other human intervention, by diversity or functional redundancy;
- automation to reduce vulnerability to human failure, at least in the initial phase of an incident or an accident;
- testability to provide clear evidence of LOD availability and performance;
- qualification of LOD for specific environmental conditions that may result from an accident or an external hazard.

The fundamental safety concept for MHTGR designs is aimed at achieving a plant that has no physical process that could cause a radiation induced hazard outside the site boundary. This is mainly achieved by demonstrating that the heat loss from the reactor vessel ultimately exceeds the decay heat production in the post accident condition and that the peak temperature reached in the core during the transient is below the demonstrated fuel degradation point and below the temperature at which the structures are affected. This is intended to preclude any prospect of significant core damage accident. Heat removal from the vessel is to be achieved by passive means.

The main provisions for Level 3 of defence in depth are:

- decay heat removal during accidents by means of passive heat transport mechanisms (heat conduction, radiation, natural convection) to simple surface coolers. Besides dissipating the heat from the reactor cavity during normal operation, including shutdown, the Reactor Cavity Cooling System (RCCS) removes the decay heat during a loss of normal heat transfer functions (loss of coolant, loss of forced cooling). The objective is to prevent the reactor vessel, attachments, supports, instrumentation and the concrete walls from exceeding their design temperature limits. Natural processes, including thermal radiation, conduction and convection, are relied upon to transport the heat from the uninsulated reactor vessel walls (with adequate emissivity) to the cooling panels of the RCCS;
- the strong negative reactivity temperature coefficient, in concert with large fuel power and temperature margins, provides a reliable inherent defence against positive reactivity insertion. The Reactivity Control and Shutdown System (RCSS), consisting of two independent and diverse systems, seismically designed and operated under a single failure criterion mode, provides further defence against reactivity events;
- the passive safety characteristics of the core (negative temperature and high temperature resistance) does not require an intact primary coolant pressure boundary (pipe break) to prevent significant core degradation.

Figures 14 through 16 present the objective-provisions trees, respectively to the safety functions control of reactivity, core heat removal and confinement of radioactive materials. The correspondent acceptance criteria are compatible with the objective for Level 3 of defence, which is the *control of accidents within the design basis*.

Figure 14 shows the objective-provisions tree for the safety function control of reactivity at Level 3, with the correspondent acceptance criteria being:

to limit the consequences of the maximum postulated insertion rate and amount of reactivity into the core, and to achieve and maintain adequate shutdown conditions.

Figure 15 presents the objective-provisions tree for the safety function core heat removal, with the acceptance criterion at Level 3 being:

adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sink(s), ensuring core geometry, and reactor pressure vessel integrity.

In Figure 16, the safety function confinement of radioactive materials has its objective-provisions tree depicted at the Level 3 of defence. The corresponding acceptance criterion is:

concentration of radionuclides (including fission products) below the limits established for design basis accident in the reactor coolant system and inside the reactor building, releases to the environment below the limits established for design basis accidents.

5.5. APPLICATION OF LEVEL 4 OF DEFENCE IN DEPTH FOR THE MHTGR

The objective for Level 4 of defence is the control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents. The essential means are complementary measures and accident management. As noted earlier, severe plant conditions for the MHTGR do not necessarily involve large releases from the fuel, as is generally understood to be the case for existing reactors in "severe accident" conditions. Since fuel melting is eliminated for all practical purposes, severe plant conditions are taken to be conditions that if left unmanaged could challenge the structural integrity of the core and thus the ability to analyse the course of an event.

For the concept of defence in depth, it is assumed that the measures considered at the first three levels will ensure maintenance of structural integrity of the core and limit the potential radiation hazards for members of the public. Nevertheless, additional efforts, if deemed necessary, are made to further reduce the risk[3] and consequences. Accident management is not intended to be used to excuse design deficiencies at prior levels.

The aim of the fourth level of defence is so to ensure that the plant safety related architecture is able to keep the consequences of the considered severe plant conditions within the allowable radiological limits.

Consideration is given to severe plant conditions that were not explicitly addressed in the design (insufficient provisions at Levels 1 to 3) owing to their very low probabilities. Such plant conditions may be caused by multiple failures or by an extremely unlikely event such as a severe earthquake. Some of these conditions (e.g. large air ingress condition) bear a potential that radioactive materials could be released to the environment. The large thermal inertia of the plant and characteristics of the fuel and reactor internal structures will provide considerable time to deal with these conditions. If necessary, additional measures and procedures may be provided. Ancillary and support systems, if employed, would be designed, manufactured, constructed and maintained consistent with the required reliability.

Measures for accident management are also aimed at controlling the course of severe plant conditions and mitigating their consequences.

Essential objectives of accident management are:

- to monitor the plant status;
- to maintain core sub criticality;
- to protect the integrity of the coated fuel particles by ensuring heat removal from the core and preventing excessive loading conditions (both thermo-mechanical and chemical);
- to limit the release of radioactive material to the environment;
- to regain and maintain control of the plant.

The most important objective for mitigation of the consequences of an accident in Level 4 is the protection, to the maximum extent, of the capability of the coated fuel particles

[3] The safety assessment shall also demonstrate that there is no risk for cliff edge effects. For this purpose some sequences must be excluded by design or practically excluded. The methodology to achieve such a demonstration must be defined.

to retain fission products. Inherent features are utilized where possible to attain this objective. Specific measures for accident management would be established on the basis of safety analysis and research results. These measures could utilize existing plant capabilities, including available non-safety classified equipment if they are operable for the accident conditions. Adequate staff preparation and training for such conditions is a prerequisite for effective accident management.

Figures 17 through 19 present the objective-provisions trees, respectively for the safety functions control of reactivity, core heat removal and confinement of radioactive materials. The correspondent acceptance criteria are compatible with the objective for Level 4 of defence, which is the *control of severe plant conditions, preventing accident progression, and mitigating the consequences of severe accidents.*

Figure 17 shows the objective-provisions tree for the safety function control of reactivity at Level 4, with the correspondent acceptance criteria being:

to avoid return to criticality during severe accidents scenarios.

Figure 18 presents the objective-provisions tree for the safety function core heat removal, with the acceptance criterion al Level 4 being:

to transfer the heat generated in the core to the ultimate heat sink without exceeding the maximum allowed fuel temperature in a substantial fraction of the fuel and maintaining the integrity of the vessel and vessel support structures.

In the Figure 19, the safety function confinement of radioactive materials has its objective-provisions tree depicted at the Level 4 of defence. The correspondent acceptance criterion is:

to limit the off-site doses below allowable limits.

5.6. CONSIDERATIONS FOR LEVEL 5 OF DEFENCE IN DEPTH FOR MHTGRS

The objective for Level 5 of defence depth is mitigation of radiological consequences of significant releases of radioactive materials. The essential means are the off-site emergency response.

Even if the efforts described in the foregoing are expected to be effective in limiting the consequences of severe plant conditions, it would be inconsistent with defence in depth to dismiss off-site emergency plans completely. These plans cover the functions of collecting and assessing information about the levels of exposures expected to occur in such very unlikely conditions, and the protective actions that could constitute intervention. The responsible authorities take the corresponding actions on the advice of the operating organization and the regulatory body. The extent of the emergency response plan should be commensurate with the radiological consequences predicted for the accident sequences which have been identified in the safety analysis. The aim is to design a plant for which sheltering and evacuation measures are not necessary.

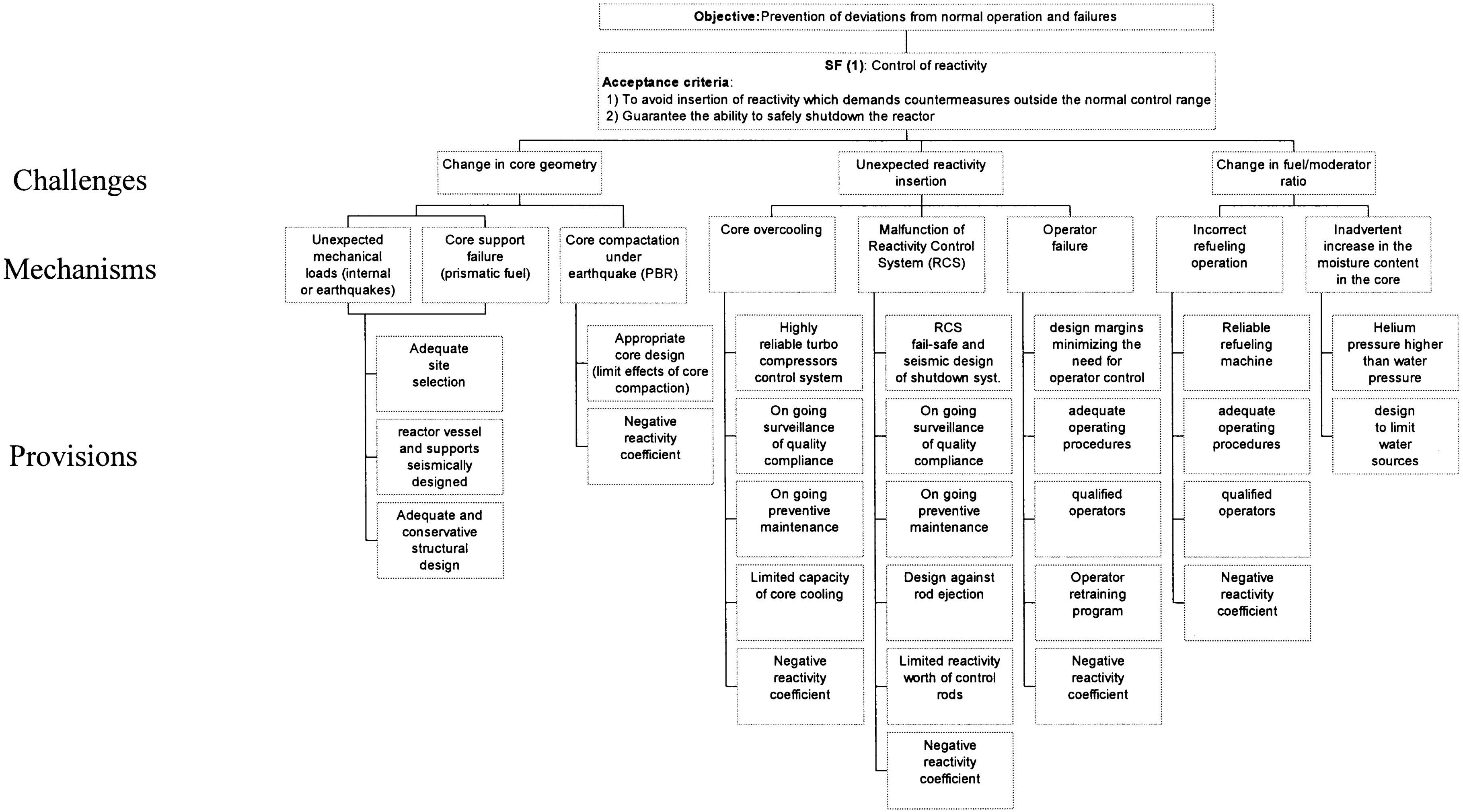

Objective:Prevention of deviations from normal operation and failures
SF (1): Control of reactivity
Acceptance criteria:
1) To avoid insertion of reactivity which demands countermeasures outside the normal control range
2) Guarantee the ability to safely shutdown the reactor
Challenges
Mechanisms
Provisions
Change in core geometry
Unexpected reactivity insertion
Change in fuel/moderator ratio
Unexpected mechanical loads (internal or earthquakes)
Core support failure (prismatic fuel)
Core compactation under earthquake (PBR)
Core overcooling
Malfunction of Reactivity Control System (RCS)
Operator failure
Incorrect refueling operation
Inadvertent increase in the moisture content in the core
Adequate site selection
reactor vessel and supports seismically designed
Adequate and conservative structural design
Appropriate core design (limit effects of core compaction)
Negative reactivity coefficient
Highly reliable turbo compressors control system
On going surveillance of quality compliance
On going preventive maintenance
Limited capacity of core cooling
Negative reactivity coefficient
RCS fail-safe and seismic design of shutdown syst.
On going surveillance of quality compliance
On going preventive maintenance
Design against rod ejection
Limited reactivity worth of control rods
Negative reactivity coefficient
design margins minimizing the need for operator control
adequate operating procedures
qualified operators
Operator retraining program
Negative reactivity coefficient
Reliable refueling machine
adequate operating procedures
qualified operators
Negative reactivity coefficient
Helium pressure higher than water pressure
design to limit water sources

Fig. 8. MHTGR Level 1 of defence in depth: Objective provisions tree for safety function (2) — control of reactivity.

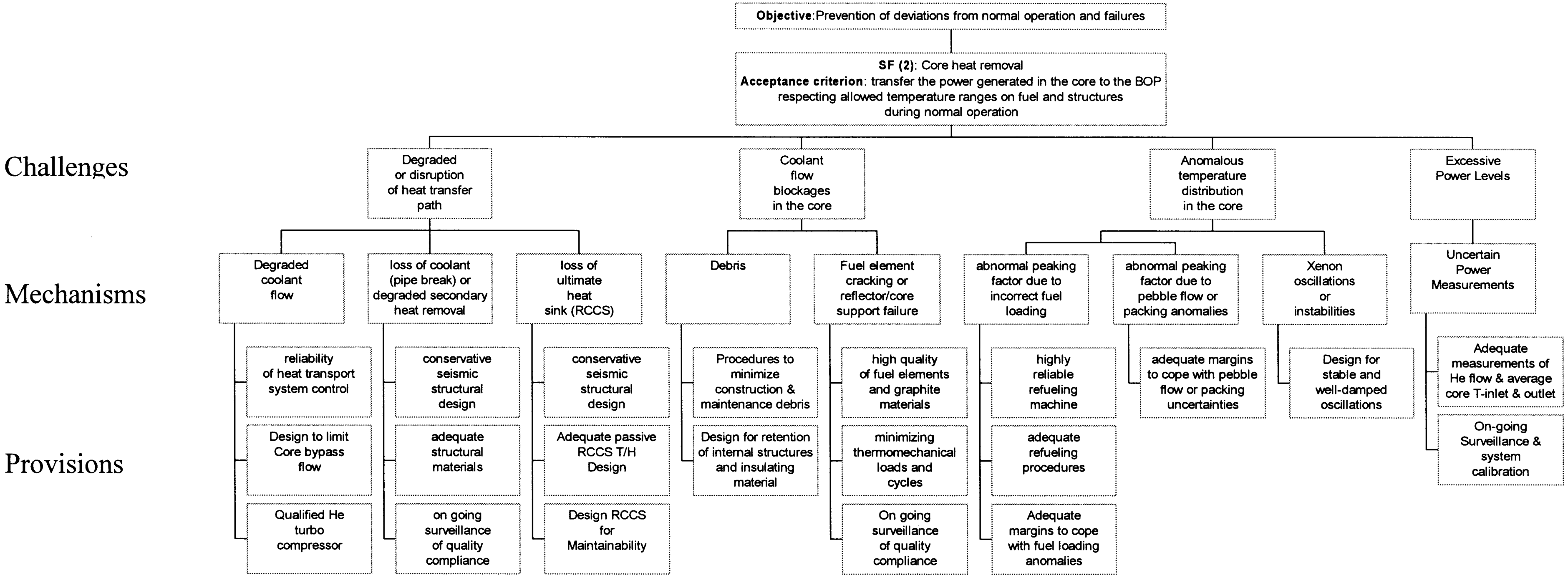

Objective:Prevention of deviations from normal operation and failures
SF (2): Core heat removal
Acceptance criterion: transfer the power generated in the core to the BOP respecting allowed temperature ranges on fuel and structures during normal operation
Challenges
Mechanisms
Provisions
Degraded or disruption of heat transfer path
Coolant flow blockages in the core
Anomalous temperature distribution in the core
Excessive Power Levels
Degraded coolant flow
loss of coolant (pipe break) or degraded secondary heat removal
loss of ultimate heat sink (RCCS)
Debris
Fuel element cracking or reflector/core support failure
abnormal peaking factor due to incorrect fuel loading
abnormal peaking factor due to pebble flow or packing anomalies
Xenon oscillations or instabilities
Uncertain Power Measurements
reliability of heat transport system control
Design to limit Core bypass flow
Qualified He turbo compressor
conservative seismic structural design
adequate structural materials
on going surveillance of quality compliance
conservative seismic structural design
Adequate passive RCCS T/H Design
Design RCCS for Maintainability
Procedures to minimize construction & maintenance debris
Design for retention of internal structures and insulating material
high quality of fuel elements and graphite materials
minimizing thermomechanical loads and cycles
On going surveillance of quality compliance
highly reliable refueling machine
adequate refueling procedures
Adequate margins to cope with fuel loading anomalies
adequate margins to cope with pebble flow or packing uncertainties
Design for stable and well-damped oscillations
Adequate measurements of He flow & average core T-inlet & outlet
On-going Surveillance & system calibration

Fig. 9. MHTGR Level 1 of defence in depth: Objective provisions tree for safety function (2) — core heat removal.

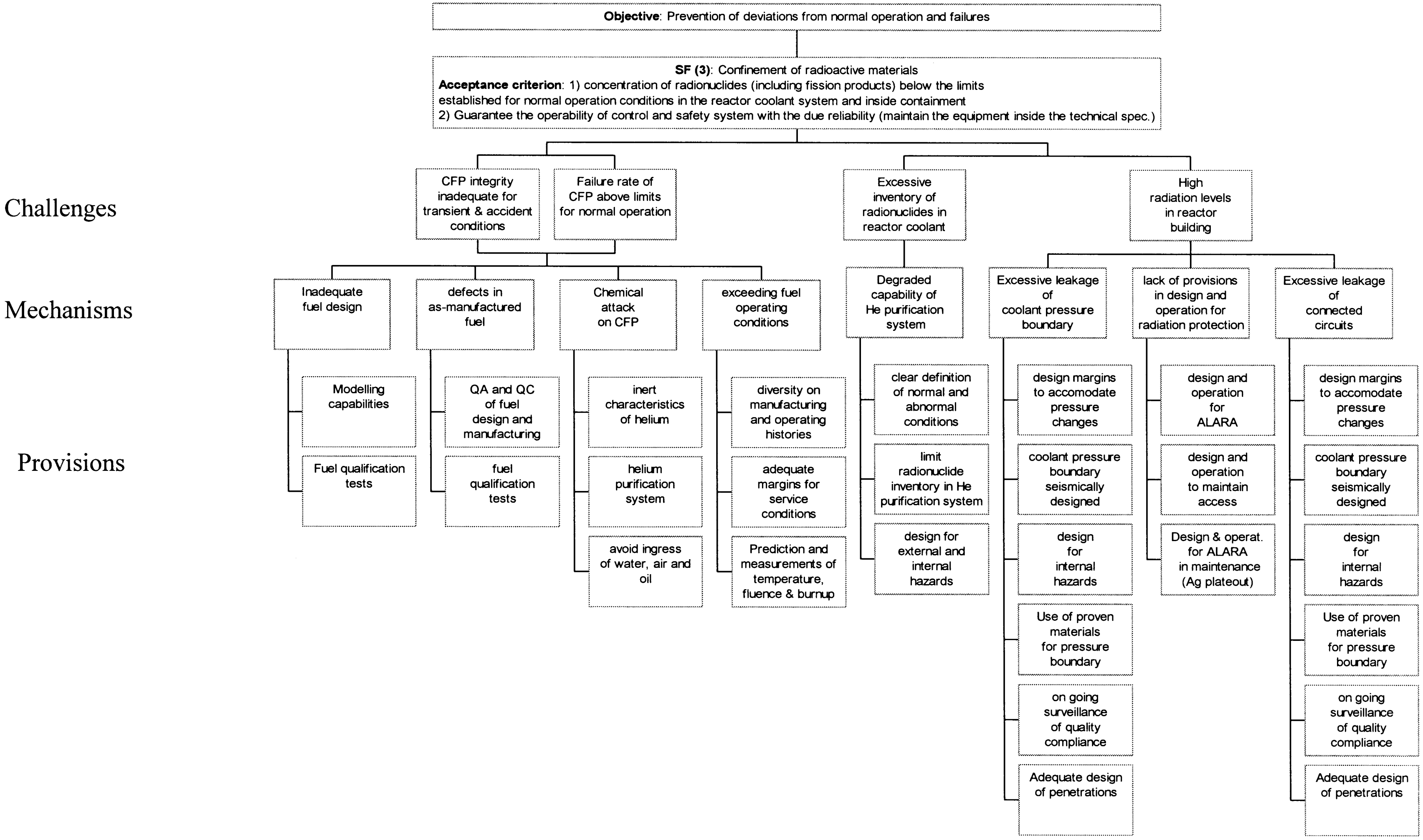

Objective: Prevention of deviations from normal operation and failures
SF (3): Confinement of radioactive materials
Acceptance criterion: 1) concentration of radionuclides (including fission products) below the limits established for normal operation conditions in the reactor coolant system and inside containment
2) Guarantee the operability of control and safety system with the due reliability (maintain the equipment inside the technical spec.)
Challenges
Mechanisms
Provisions
CFP integrity inadequate for transient & accident conditions
Failure rate of CFP above limits for normal operation
Excessive inventory of radionuclides in reactor coolant
High radiation levels in reactor building
Inadequate fuel design
defects in as-manufactured fuel
Chemical attack on CFP
exceeding fuel operating conditions
Degraded capability of He purification system
Excessive leakage of coolant pressure boundary
lack of provisions in design and operation for radiation protection
Excessive leakage of connected circuits
Modelling capabilities
Fuel qualification tests
QA and QC of fuel design and manufacturing
fuel qualification tests
inert characteristics of helium
helium purification system
avoid ingress of water, air and oil
diversity on manufacturing and operating histories
adequate margins for service conditions
Prediction and measurements of temperature, fluence & burnup
clear definition of normal and abnormal conditions
limit radionuclide inventory in He purification system
design for external and internal hazards
design margins to accomodate pressure changes
coolant pressure boundary seismically designed
design for internal hazards
Use of proven materials for pressure boundary
on going surveillance of quality compliance
Adequate design of penetrations
design and operation for ALARA
design and operation to maintain access
Design & operat. for ALARA in maintenance (Ag plateout)
design margins to accomodate pressure changes
coolant pressure boundary seismically designed
design for internal hazards
Use of proven materials for pressure boundary
on going surveillance of quality compliance
Adequate design of penetrations

Fig. 10. MHTGR Level 1 of defence in depth: Objective provisions tree for safety function (3) — confinement of radioactive materials.

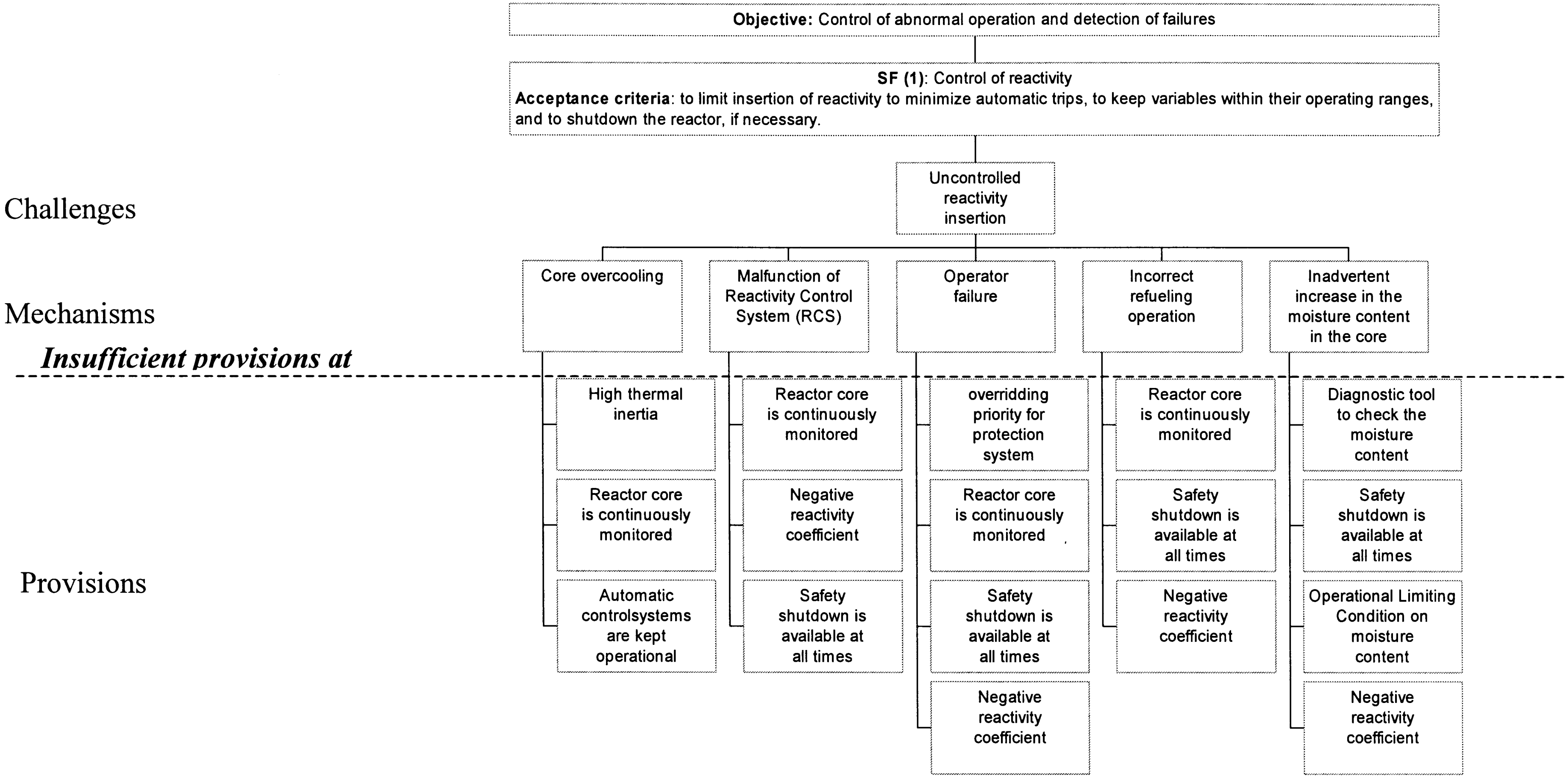

Objective: Control of abnormal operation and detection of failures
SF (1): Control of reactivity
Acceptance criteria: to limit insertion of reactivity to minimize automatic trips, to keep variables within their operating ranges, and to shutdown the reactor, if necessary.
Challenges
Uncontrolled reactivity insertion
Mechanisms
Core overcooling
Malfunction of Reactivity Control System (RCS)
Operator failure
Incorrect refueling operation
Inadvertent increase in the moisture content in the core
Insufficient provisions at
Provisions
High thermal inertia
Reactor core is continuously monitored
Automatic controlsystems are kept operational
Reactor core is continuously monitored
Negative reactivity coefficient
Safety shutdown is available at all times
overridding priority for protection system
Reactor core is continuously monitored
Safety shutdown is available at all times
Negative reactivity coefficient
Reactor core is continuously monitored
Safety shutdown is available at all times
Negative reactivity coefficient
Diagnostic tool to check the moisture content
Safety shutdown is available at all times
Operational Limiting Condition on moisture content
Negative reactivity coefficient

Fig. 11. MHTGR Level 2 of defence in depth: Objective provisions tree for safety function (1) — control of reactivity.

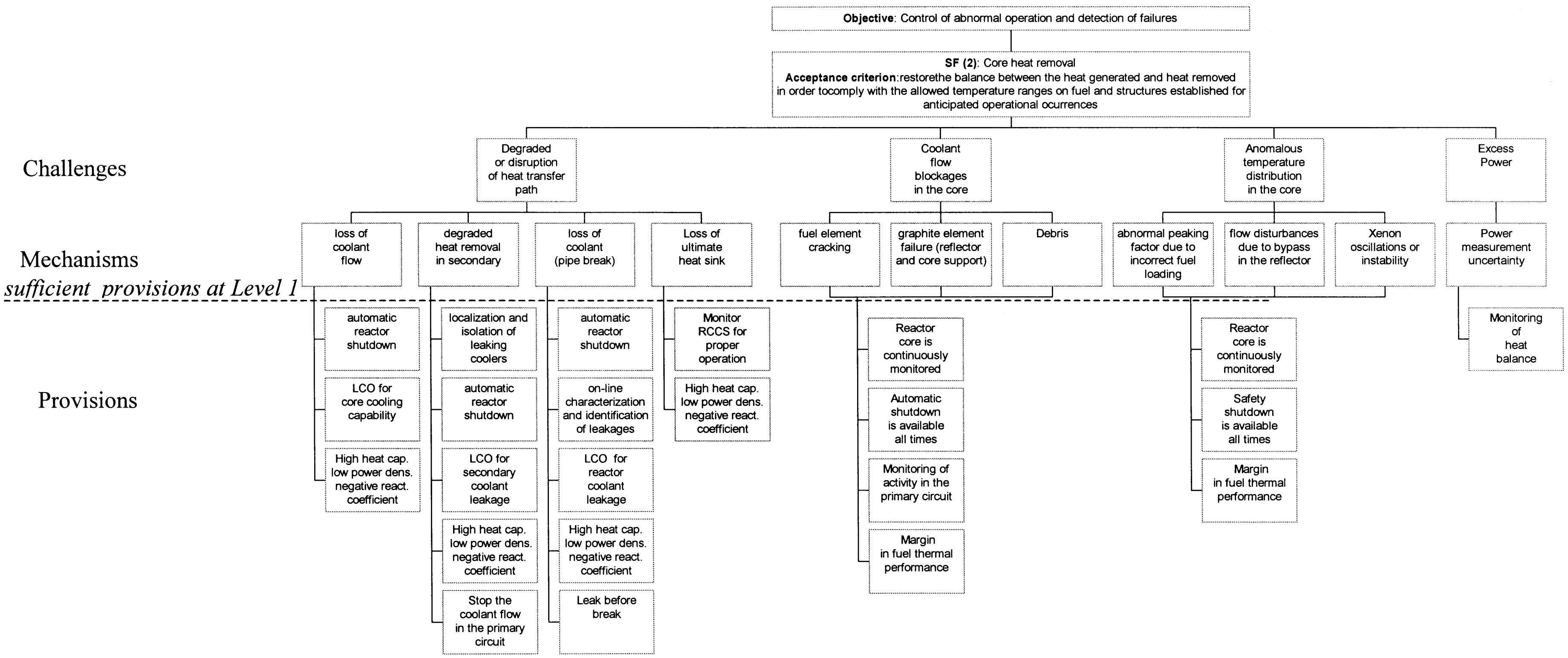

Objective: Control of abnormal operation and detection of failures
SF (2): Core heat removal
Acceptance criterion:restorethe balance between the heat generated and heat removed in order tocomply with the allowed temperature ranges on fuel and structures established for anticipated operational ocurrences
Challenges
Mechanisms
sufficient provisions at Level 1
Provisions
Degraded or disruption of heat transfer path
Coolant flow blockages in the core
Anomalous temperature distribution in the core
Excess Power
loss of coolant flow
degraded heat removal in secondary
loss of coolant (pipe break)
Loss of ultimate heat sink
fuel element cracking
graphite element failure (reflector and core support)
Debris
abnormal peaking factor due to incorrect fuel loading
flow disturbances due to bypass in the reflector
Xenon oscillations or instability
Power measurement uncertainty
automatic reactor shutdown
LCO for core cooling capability
High heat cap. low power dens. negative react. coefficient
localization and isolation of leaking coolers
automatic reactor shutdown
LCO for secondary coolant leakage
High heat cap. low power dens. negative react. coefficient
Stop the coolant flow in the primary circuit
automatic reactor shutdown
on-line characterization and identification of leakages
LCO for reactor coolant leakage
High heat cap. low power dens. negative react. coefficient
Leak before break
Monitor RCCS for proper operation
High heat cap. low power dens. negative react. coefficient
Reactor core is continuously monitored
Automatic shutdown is available all times
Monitoring of activity in the primary circuit
Margin in fuel thermal performance
Reactor core is continuously monitored
Safety shutdown is available all times
Margin in fuel thermal performance
Monitoring of heat balance

Fig. 12. MHTGR Level 2 of defence in depth: Objective provisions tree for safety function (2) — core heat removal.

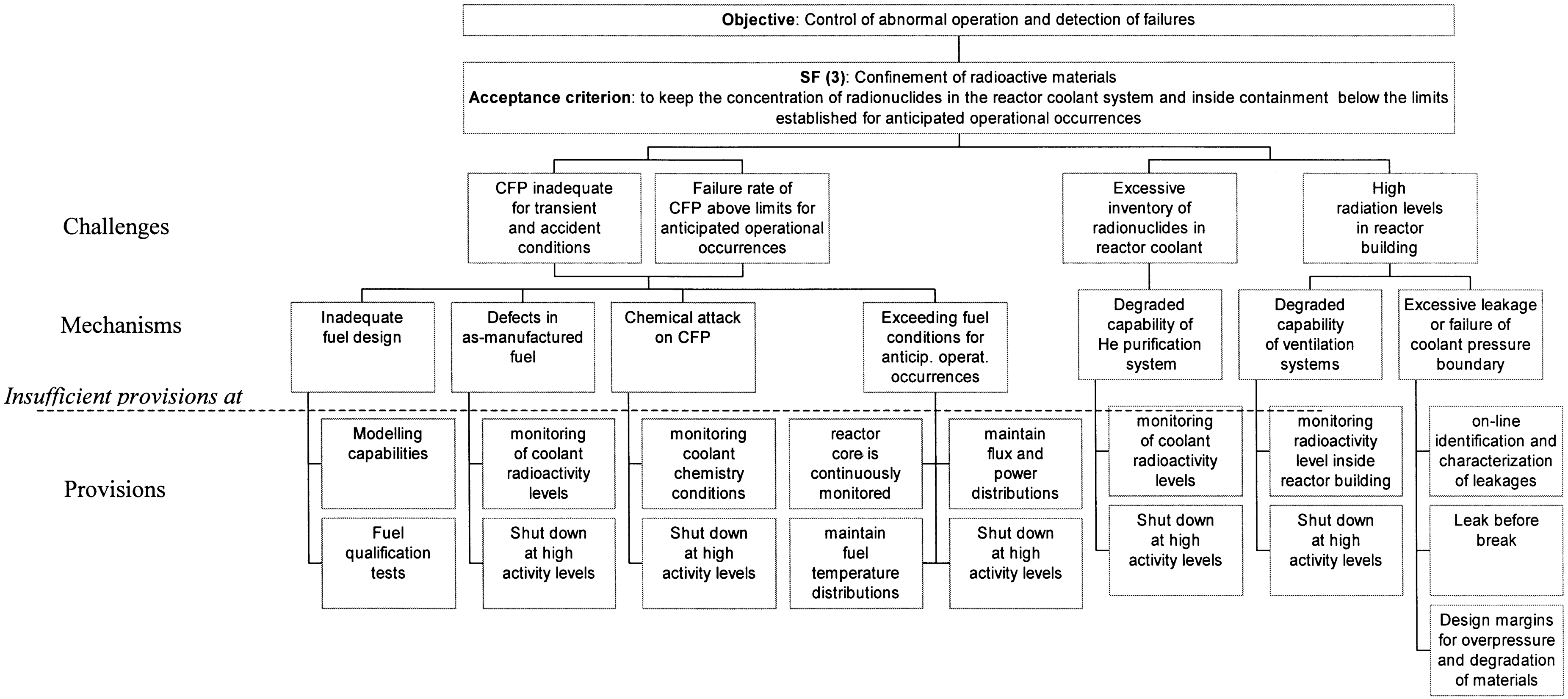
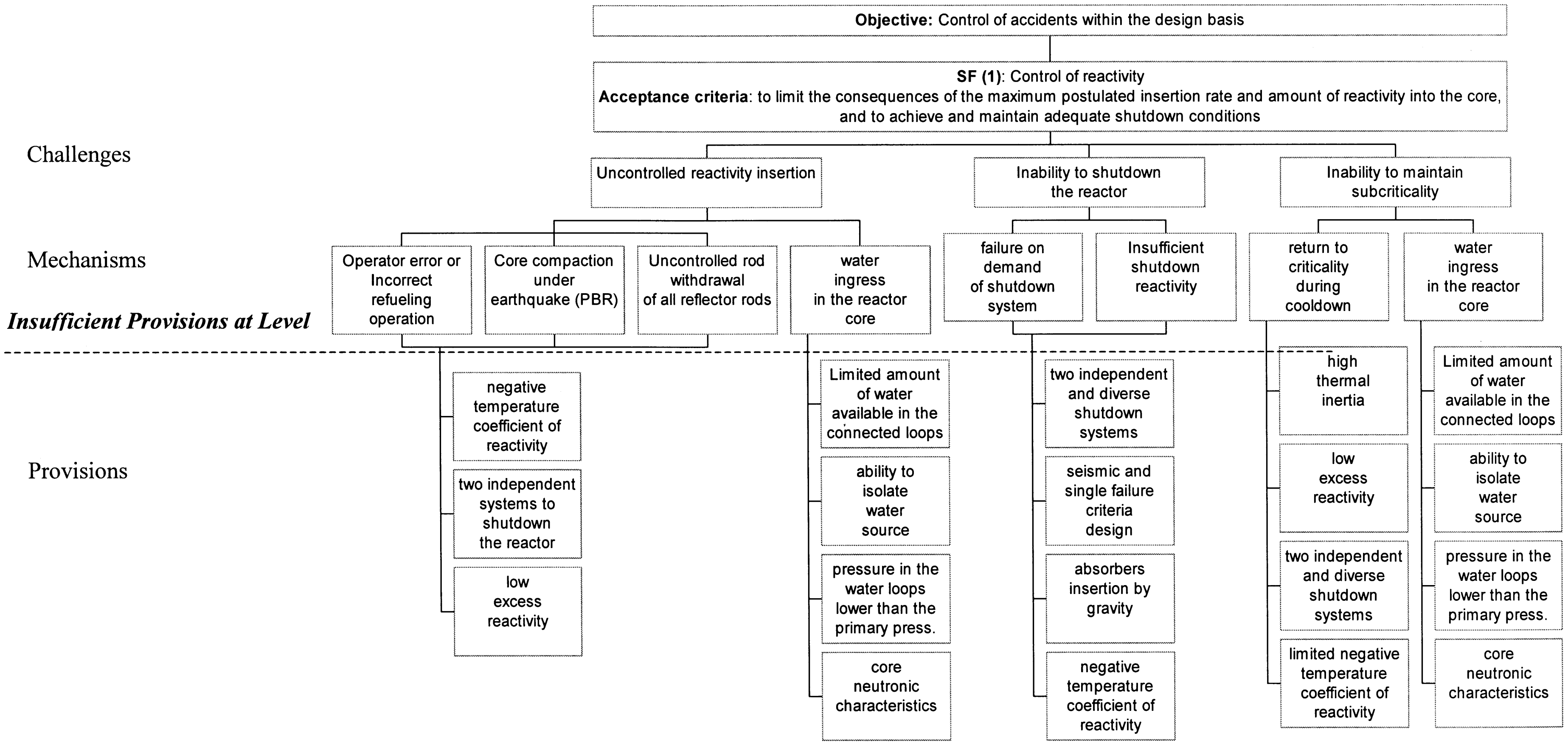

Objective: Control of abnormal operation and detection of failures
SF (3): Confinement of radioactive materials
Acceptance criterion: to keep the concentration of radionuclides in the reactor coolant system and inside containment below the limits established for anticipated operational occurrences
Challenges
CFP inadequate for transient and accident conditions
Failure rate of CFP above limits for anticipated operational occurrences
Excessive inventory of radionuclides in reactor coolant
High radiation levels in reactor building
Mechanisms
Inadequate fuel design
Defects in as-manufactured fuel
Chemical attack on CFP
Exceeding fuel conditions for anticip. operat. occurrences
Degraded capability of He purification system
Degraded capability of ventilation systems
Excessive leakage or failure of coolant pressure boundary
Insufficient provisions at
Provisions
Modelling capabilities
Fuel qualification tests
monitoring of coolant radioactivity levels
Shut down at high activity levels
monitoring coolant chemistry conditions
Shut down at high activity levels
reactor core is continuously monitored
maintain fuel temperature distributions
maintain flux and power distributions
Shut down at high activity levels
monitoring of coolant radioactivity levels
Shut down at high activity levels
monitoring radioactivity level inside reactor building
Shut down at high activity levels
on-line identification and characterization of leakages
Leak before break
Design margins for overpressure and degradation of materials

Fig. 13. MHTGR Level 2 of defence in depth: Objective provisions tree for safety function (3) — confinement of radioactive materials.



Objective: Control of accidents within the design basis
SF (1): Control of reactivity
Acceptance criteria: to limit the consequences of the maximum postulated insertion rate and amount of reactivity into the core, and to achieve and maintain adequate shutdown conditions
Challenges
Uncontrolled reactivity insertion
Inability to shutdown the reactor
Inability to maintain subcriticality
Mechanisms
Operator error or Incorrect refueling operation
Core compaction under earthquake (PBR)
Uncontrolled rod withdrawal of all reflector rods
water ingress in the reactor core
failure on demand of shutdown system
Insufficient shutdown reactivity
return to criticality during cooldown
water ingress in the reactor core
Insufficient Provisions at Level
Provisions
negative temperature coefficient of reactivity
two independent systems to shutdown the reactor
low excess reactivity
Limited amount of water available in the connected loops
ability to isolate water source
pressure in the water loops lower than the primary press.
core neutronic characteristics
two independent and diverse shutdown systems
seismic and single failure criteria design
absorbers insertion by gravity
negative temperature coefficient of reactivity
high thermal inertia
low excess reactivity
two independent and diverse shutdown systems
limited negative temperature coefficient of reactivity
Limited amount of water available in the connected loops
ability to isolate water source
pressure in the water loops lower than the primary press.
core neutronic characteristics

Fig. 14. MHTGR Level 3 of defence in depth: Objective provisions tree for safety function (1) — control of reactivity.

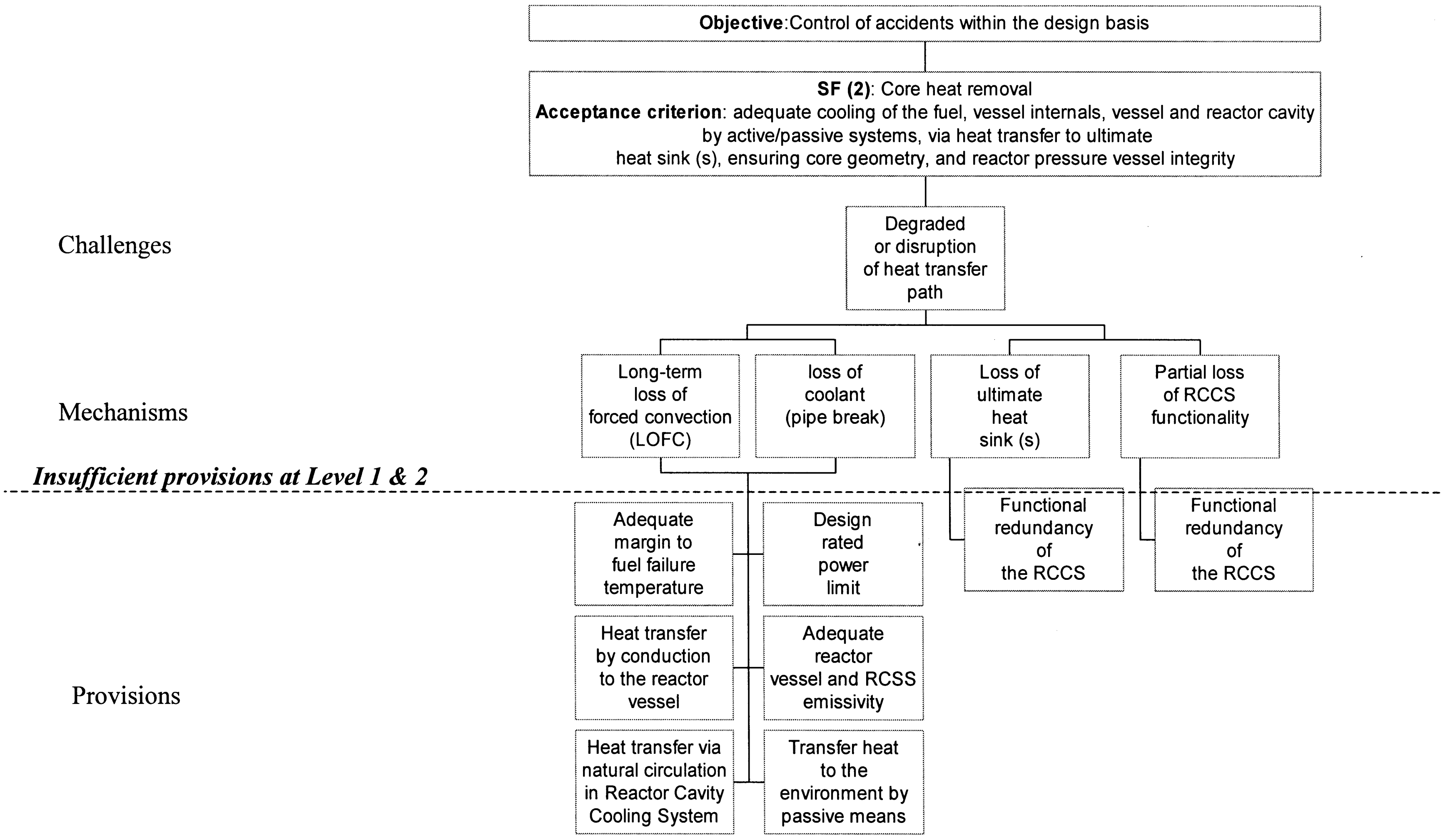

Objective:Control of accidents within the design basis
SF (2): Core heat removal
Acceptance criterion: adequate cooling of the fuel, vessel internals, vessel and reactor cavity by active/passive systems, via heat transfer to ultimate heat sink (s), ensuring core geometry, and reactor pressure vessel integrity
Challenges
Degraded or disruption of heat transfer path
Mechanisms
Long-term loss of forced convection (LOFC)
loss of coolant (pipe break)
Loss of ultimate heat sink (s)
Partial loss of RCCS functionality
Insufficient provisions at Level 1 & 2
Provisions
Adequate margin to fuel failure temperature
Design rated power limit
Heat transfer by conduction to the reactor vessel
Adequate reactor vessel and RCSS emissivity
Heat transfer via natural circulation in Reactor Cavity Cooling System
Transfer heat to the environment by passive means
Functional redundancy of the RCCS
Functional redundancy of the RCCS

Fig. 15. MHTGR Level 3 of defence in depth: Objective provisions tree for safety function (2) — core heat removal.

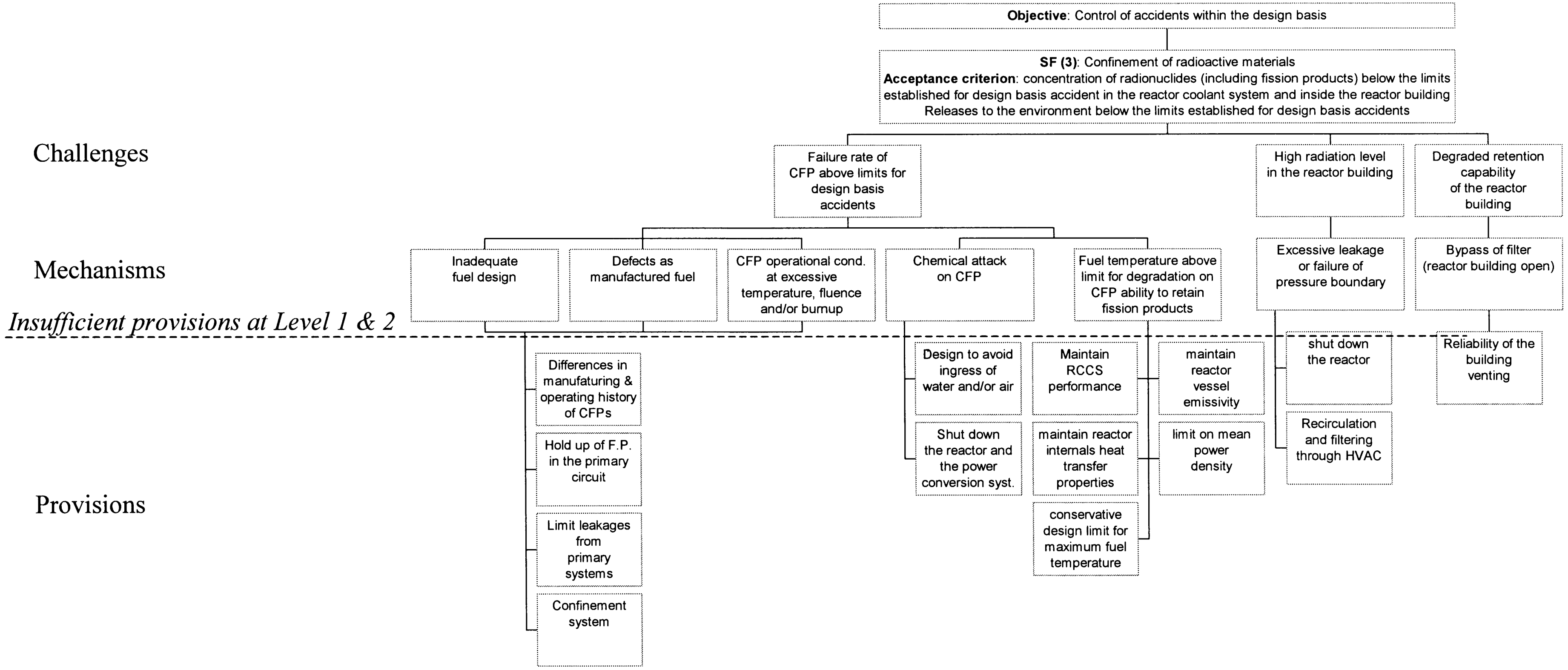

Objective: Control of accidents within the design basis
SF (3): Confinement of radioactive materials
Acceptance criterion: concentration of radionuclides (including fission products) below the limits established for design basis accident in the reactor coolant system and inside the reactor building
Releases to the environment below the limits established for design basis accidents
Challenges
Failure rate of CFP above limits for design basis accidents
High radiation level in the reactor building
Degraded retention capability of the reactor building
Mechanisms
Inadequate fuel design
Defects as manufactured fuel
CFP operational cond. at excessive temperature, fluence and/or burnup
Chemical attack on CFP
Fuel temperature above limit for degradation on CFP ability to retain fission products
Excessive leakage or failure of pressure boundary
Bypass of filter (reactor building open)
Insufficient provisions at Level 1 & 2
Provisions
Differences in manufaturing & operating history of CFPs
Hold up of F.P. in the primary circuit
Limit leakages from primary systems
Confinement system
Design to avoid ingress of water and/or air
Shut down the reactor and the power conversion syst.
Maintain RCCS performance
maintain reactor internals heat transfer properties
conservative design limit for maximum fuel temperature
maintain reactor vessel emissivity
limit on mean power density
shut down the reactor
Recirculation and filtering through HVAC
Reliability of the building venting

Fig. 16. MHTGR Level 3 of defence in depth: Objective provisions tree for safety function (3) — confinement of radioactive materials.

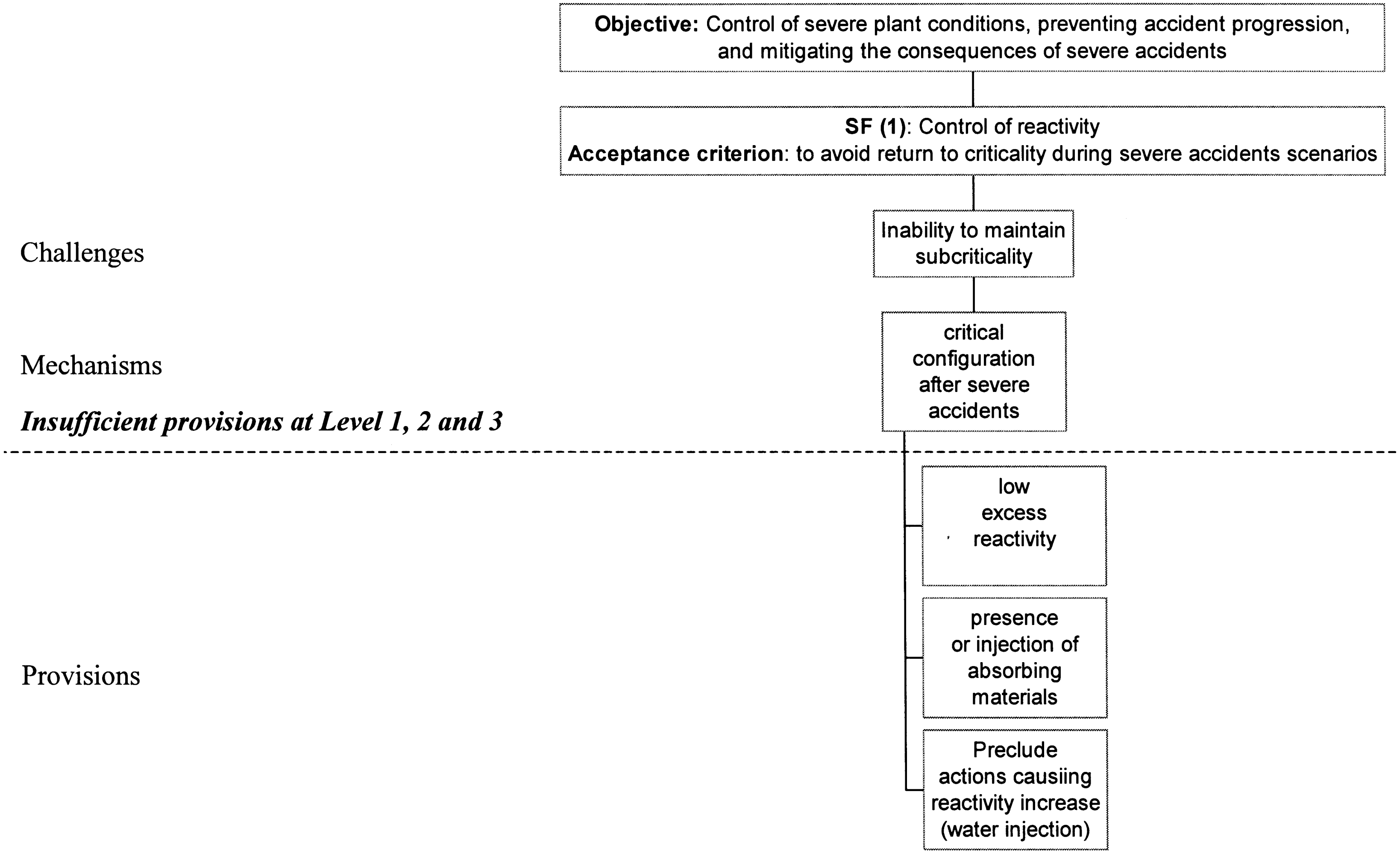

Objective: Control of severe plant conditions, preventing accident progression, and mitigating the consequences of severe accidents
SF (1): Control of reactivity
Acceptance criterion: to avoid return to criticality during severe accidents scenarios
Challenges
Inability to maintain subcriticality
Mechanisms
critical configuration after severe accidents
Insufficient provisions at Level 1, 2 and 3
Provisions
low excess reactivity
presence or injection of absorbing materials
Preclude actions causiing reactivity increase (water injection)

Fig. 17. MHTGR Level 4 of defence in depth: Objective provisions tree for safety function (1) — control of reactivity.

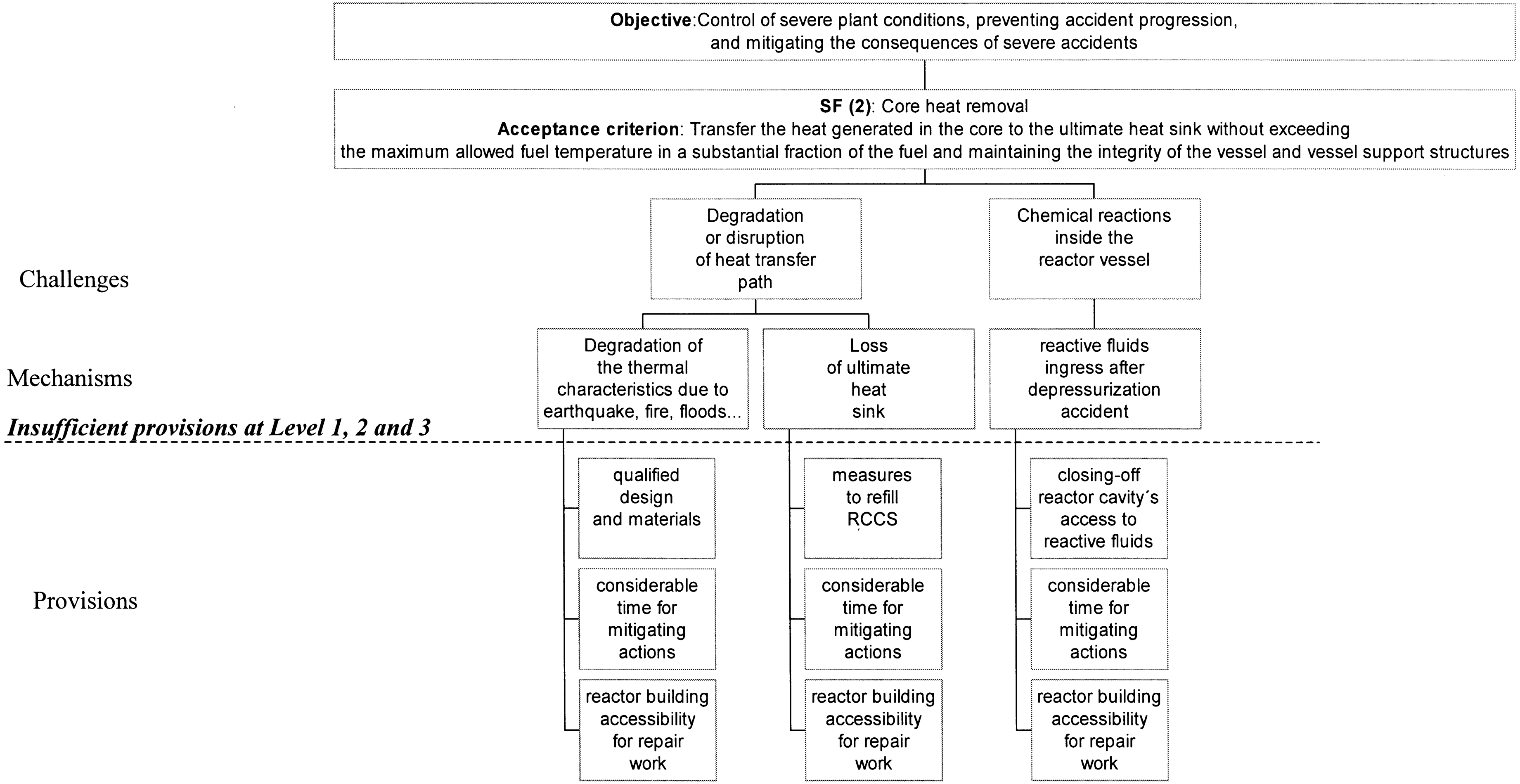

Objective:Control of severe plant conditions, preventing accident progression, and mitigating the consequences of severe accidents
SF (2): Core heat removal
Acceptance criterion: Transfer the heat generated in the core to the ultimate heat sink without exceeding the maximum allowed fuel temperature in a substantial fraction of the fuel and maintaining the integrity of the vessel and vessel support structures
Challenges
Degradation or disruption of heat transfer path
Chemical reactions inside the reactor vessel
Mechanisms
Degradation of the thermal characteristics due to earthquake, fire, floods...
Loss of ultimate heat sink
reactive fluids ingress after depressurization accident
Insufficient provisions at Level 1, 2 and 3
Provisions
qualified design and materials
considerable time for mitigating actions
reactor building accessibility for repair work
measures to refill RCCS
considerable time for mitigating actions
reactor building accessibility for repair work
closing-off reactor cavity´s access to reactive fluids
considerable time for mitigating actions
reactor building accessibility for repair work

Fig. 18. MHTGR Level 4 of defence in depth: Objective provisions tree for safety function (2) — core heat removal.

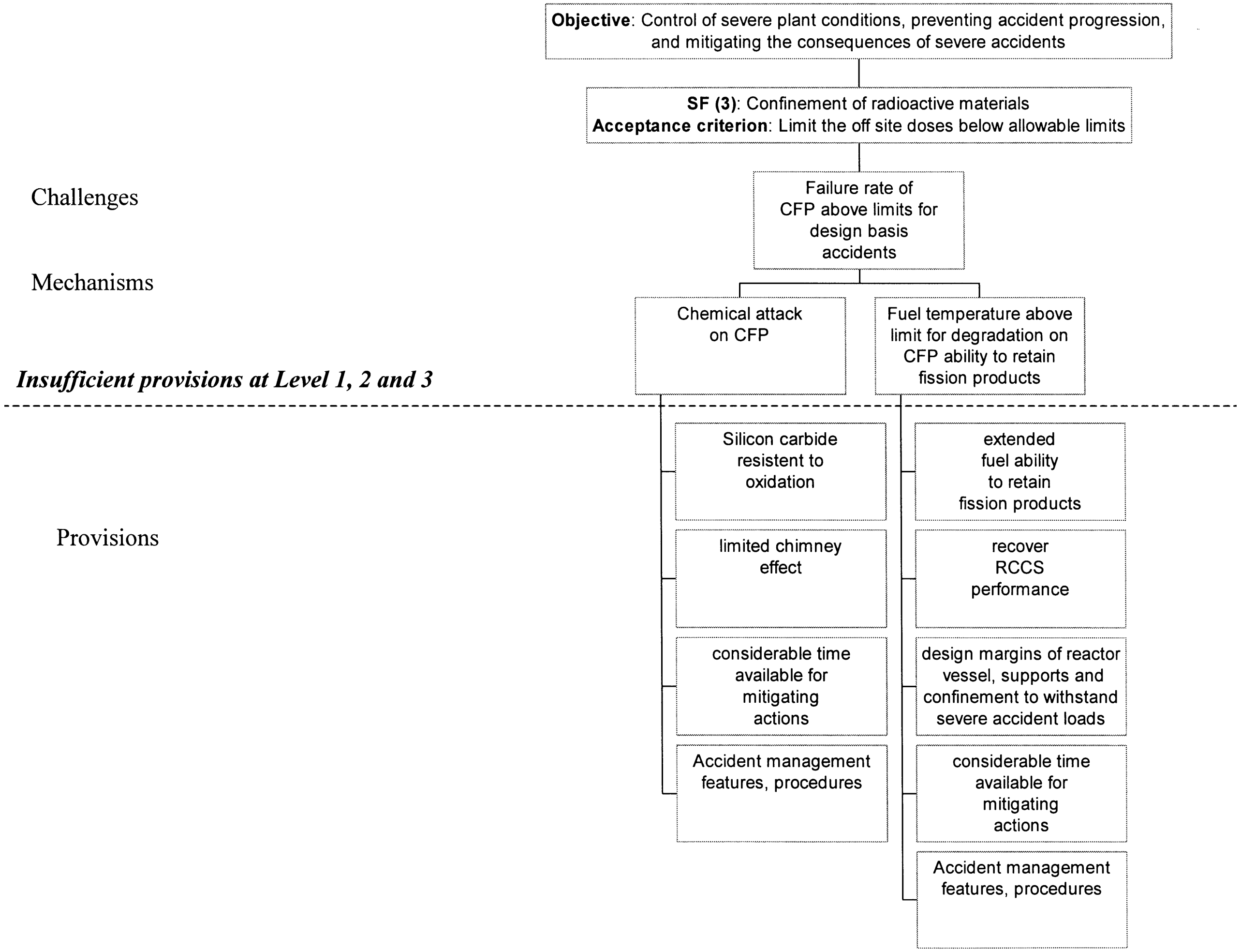

Objective: Control of severe plant conditions, preventing accident progression, and mitigating the consequences of severe accidents
SF (3): Confinement of radioactive materials
Acceptance criterion: Limit the off site doses below allowable limits
Challenges
Failure rate of CFP above limits for design basis accidents
Mechanisms
Chemical attack on CFP
Fuel temperature above limit for degradation on CFP ability to retain fission products
Insufficient provisions at Level 1, 2 and 3
Provisions
Silicon carbide resistent to oxidation
limited chimney effect
considerable time available for mitigating actions
Accident management features, procedures
extended fuel ability to retain fission products
recover RCCS performance
design margins of reactor vessel, supports and confinement to withstand severe accident loads
considerable time available for mitigating actions
Accident management features, procedures

Fig. 19. MHTGR Level 4 of defence in depth: Objective provisions tree for safety function (3) — confinement of radioactive materials.

6. FINAL REMARKS

The top-down approach discussed in this report is intended to be a general method for assessing the safety and developing safety requirements for the design of nuclear reactors taking into consideration the implementation of the principles of defence in depth. The method is applicable to any kind of reactor, however, how defence in depth is implemented and the implications on safety requirements are concept specific.

The application to MHTGRs, although very preliminary, proved that the method is viable and useful. The specific features of the MHTGR concept are significantly different from those of LWRs and they have great influence on the implementation of defence in depth.

Stronger provisions at Level 1 could reduce the requirements on monitoring and controlling at Level 2. Passive safety features at Level 3 reduce the requirements on active engineered safety features at the same level and enhance the overall safety performance. Design basis accidents are mostly dealt with by inherent features and passive systems. The large thermal inertia of the MHTGR enhances the effectiveness of Levels 2 and 3 of defence by providing very long times for systems and operator response and implementation of any mitigating measures. Needs for functional redundancies must be checked carefully through a deep and comprehensive analysis of the safety related architecture performance and reliability (PSA, for instance).

Quantitative comparisons between the safety performance of MHTGRs and LWRs could show that similar postulated initiating events could lead to accident sequences with lower consequences or probabilities of occurrence in MHTGRs than in LWRs. Of comparable importance is the potential that monitoring and surveillance requirements in Level 2 could be simplified or reduced in scope while providing an equivalent level of safety. The exercise also showed that areas such as the definition of success criteria for each Level of defence in depth and the integration of deterministic and probabilistic approaches need more investigation.

The MHTGR fuel characteristics indicate that for internal initiating events, severe accident scenarios involving core melt can be practically excluded although severe scenarios involving extensive oxidation of the fuel could be envisaged. Design provisions and accident management measures must be considered carefully for very unlikely external challenges, like severe earthquakes, floods or airplane crashes in the context of retaining the structural integrity of the core.

The methodology discussed here and illustrated by application to a general MHTGR concept will be used as basis for developing international safety requirements for advanced reactors comparable to those that have been developed for existing and evolutionary water reactors. Establishing these requirements will involve extended participation and review by Member States interested in the future deployment of advanced reactors and in particular MHTGRs.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Gas Cooled Reactor Design and Safety, Technical Reports Series No. 312, IAEA, Vienna (1990).

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

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

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

[5] GASPARINI, M., "The IAEA Safety Standards for Design. Application to Small and Medium Size Reactors", C&S Papers Series No. 14, IAEA, Vienna (2002).

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

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Fuel Performance and Fission Product Behaviour in Gas-Cooled Reactors, IAEA-TECDOC-978, Vienna (1997).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Heat Transport and Afterheat Removal for Gas-Cooled Reactors Under Accident Conditions, IAEA-TECDOC-1163, Vienna (2001).

[9] WILLIAMS, P.M., "Bases for the modular HTGR source term and containment concepts", Decay heat removal and heat transfer under normal and accident conditions in gas cooled reactors", IAEA-TECDOC-757, IAEA, Vienna (1994) 41-46.

Appendix

COMPARISON BETWEEN THE SAFETY CHARACTERISTICS AND FEATURES OF WATER REACTORS AND THOSE OF MODULAR HIGH TEMPERATURE GAS COOLED REACTORS

As stated earlier, in the recommended process the requirements for a specific type of reactor (e.g. MHTGR) are to be generated through a critical interpretation of the ‘objectives’ and ‘essential means’ associated with each level of defence in depth (see Table 3.1) for the reactors upon which the existing requirements are based. This requires a full understanding of the safety characteristics and features of the specific type of reactor under consideration as well as those of the water reactors on which the existing requirements were based. The applicability of an existing requirement must then be determined by a comparative evaluation of the two types of reactors. The purpose of this appendix is to provide a summary comparison of MHTGR safety characteristics and features with those of water reactors. Nothing presented here should be interpreted as criticism of the safety case for existing water reactors. Their performance speaks for itself as they have demonstrated a very high level of safety over many thousands of reactors years of operation. The water reactor safety case has been based upon highly reliable active systems to maintain the system parameters within the required envelope at all times and to respond rapidly as warranted for specific event conditions. The MHTGR safety case utilizes the characteristics of HTGR fuel and core materials in conjunction with a passive design approach to avoid reliance on active systems, and thus takes a very different approach. Some of the key differences are summarized below, with representative characteristics from existing reactors upon which the current requirements are based referred to as the base case.

A.1. ALLOWED CONDITIONS WITHIN THE DESIGN BASIS

In the base case, fuel failure in the form of limited melting and/or cladding failure is allowed within the design basis, as long as a core geometry that is capable of being cooled is maintained. A comparison of allowed conditions within the design basis between the base case and MHTGR is shown in Fig. A.1. As shown in the figure, the combined effect of the initiating event and system response is allowed to fail two radionuclide containment boundaries in several events for the base case. MHTGR design practice has been to preclude failure of any barrier except that associated with the initiating event. This difference, in conjunction with the ineffectiveness of a typical LWR containment design for MHTGR conditions requires a different approach to radionuclide containment than has been used in the base case.

	Fuel Radionuclide Containment Failed	RCS Pressure Boundary Failed	Containment Building Boundary Failed
Base Case Design Basis Events			
Loss of Coolant	🟥	🟥	
Control Rod Ejection	🟥	🟥	
Main Steam Line Break	🟥		
Locked Rotor	🟥		
SG Tube Rupture		🟥	🟥
MHTGR Design Basis Events			
Loss of Coolant		🟥	
Max. Reactivity Insertion			
Loss of Cooling			
Water Ingress		🟥	

FIG. A.1. Table which compares the allowed conditions within the design basis for a water reactor and for an MHTGR.

A.2. FUEL FAILURE MECHANISMS

A comparison of fuel failure mechanisms for the base case and MHTGR is shown in Figure A.2. While there are a comparable number of mechanisms for fuel failure, there is a major difference with regard to the implications for safety, particularly with regard to the need for protection systems. As indicated in the figure, many of the mechanisms in the base case can cause fuel failure in the short term (seconds to minutes after the allowed envelope is exceeded). This leads to safety requirements for maintaining the allowed operating envelope on a moment-to-moment basis, and requirements for immediate response of mitigation systems. The last two mechanisms (clad ballooning/bursting and zirconium/water reaction) relate to loss of coolant accident conditions, where the residual fission and short term decay heat distribution is important and thus power level and power distribution just prior to the event are the primary operational state variables of interest. In the case of the MHTGR, the failure mechanisms are for the most part related to long term operational conditions of the fuel. In the case of a loss of coolant, the slow response results in reaching a peak temperature days after the initiation of the event, thus operational state variables in the short term prior to the event are of little importance from a safety standpoint. This is discussed further below.

Fuel Failure Mechanisms - Base Case

Controlled State Variables (Short Term)	Flow Induced Vibration	Stress Corrosion Cracking	Pellet/Clad Mechanical Interaction	Fuel Centerline Melt	DNB/CHF	Clad Ballooning/Bursting	Zirc/Water Interaction
Power Level				🟥	🟥	🟥	🟥
Power Distribution			🟥	🟥	🟥	🟥	🟥
Power Change Rate			🟥				
Flow Rate	🟥				🟥		
Flow Distribution	🟥				🟥		
Coolant Temperature		🟧			🟥		
Coolant Pressure		🟧			🟥		
Coolant Chemistry		🟧					

Fuel Failure Mechanisms - Modular HTGR

Controlled State Variables (Long Term)	Coating Dimensional Change	Corrosion	Internal Pressurization	Fission Product Diffusion	FP Chemical Attack	SiC Decomposition
Power	🟧		🟧	🟧	🟧	🟧
Power Distribution	🟧		🟧	🟧	🟧	🟧
Temperature	🟧		🟧	🟧	🟧	
Temperature Dist.	🟧		🟧	🟧	🟧	
Coolant Chemistry		🟧				

Short Term - seconds/minutes
Long Term - weeks/months

FIG. A.2. Table which compares fuel failure mechanisms for a water reactor and for an MHTGR.

A.3. CORE TEMPERATURE MARGINS AND THERMAL RESPONSE

The combined effects of large temperature margins and slow thermal response are a central safety aspect of MHTGR, allowing major simplification of the operational safety requirements. Figure A.3 illustrates typical margins to fuel structural limits for the base case in comparison to an MHTGR. In the base case, the structural limit is taken as the onset of rapid oxidation of the zircaloy cladding at approximately 1200ºC. The onset of cladding ballooning and bursting in the base case typically occurs at a lower temperature, but is a function of design specific internal pressurisation and cladding mechanical properties. The chemical decomposition of silicon carbide, which becomes important around 2200ºC was taken as the structural limit for the MHTGR fuel. As with the base case, other mechanisms such as diffusion of some fission products through the coatings begins at lower temperatures, affected by coating properties and fuel operating history. Note that the average fuel temperature in the reference case is higher than for the MHTGR even though the coolant temperature is considerably lower. This is due to the much higher power densities in the base case, which cause a large temperature rise across the cladding/fuel pellet gap and within the fuel pellet.

Typical margins to fuel melt limits are illustrated in Fig. A.4. The fuel melting temperature includes an allowance for a reduction of the melting point with fuel burnup. In the base case the design peak fuel temperature at full power is seen to be relatively close to the centreline melting limit. As with the fuel average temperature, the fuel maximum temperature is much higher for the base case due to the much higher power density. Protecting against this limit for the base case requires monitoring of power level and power distribution on a momentary basis. The large margins for the MHTGR are a primary reason that fuel melting is not a credible condition.

The full power core adiabatic heatup rate is a hypothetical figure of merit for comparing thermal response. It is the rate of increase in temperature that would occur if the reactor core were operated at full power with no heat removal. The values for the base case and a typical MHTGR, both with and without coolant present, are shown in Fig. A.5. The heatup rates for the base case are higher by between one and two orders of magnitude, depending on whether the coolant is present or not. The absence of the coolant has no significant effect on the response of the MHTGR. This difference, which is the combined result of the low power density and high heat capacity of the MHTGR, translates into a very slow response to conditions involving a mismatch between heat generation and removal. This characteristic, in conjunction with the large thermal margins and a limitation on rated thermal power, constitutes the essence of the passive safety characteristics of MHTGR.

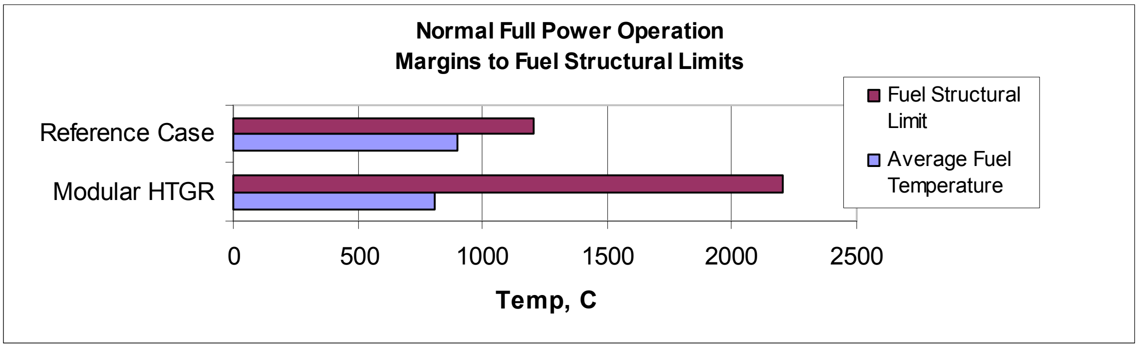


FIG. A.3. Comparison of margins to the structural limits for fuel for a water reactor and for an MHTGR.

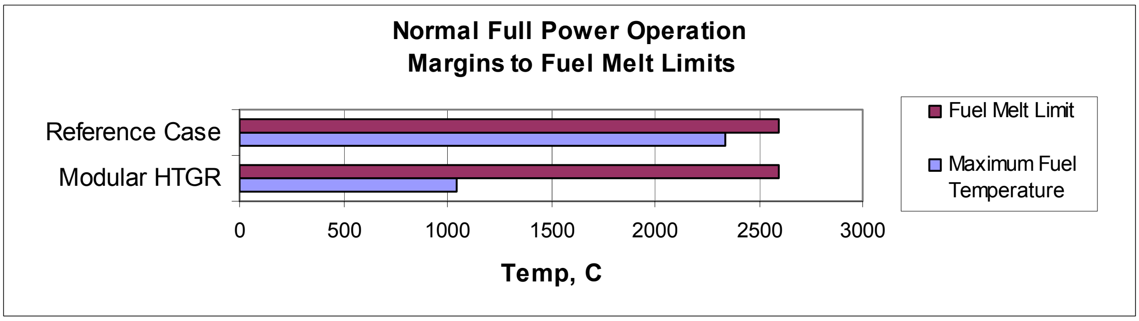


FIG. A.4. Comparison between the margins to the melt limits for fuel for a water reactor and for an MHTGR.

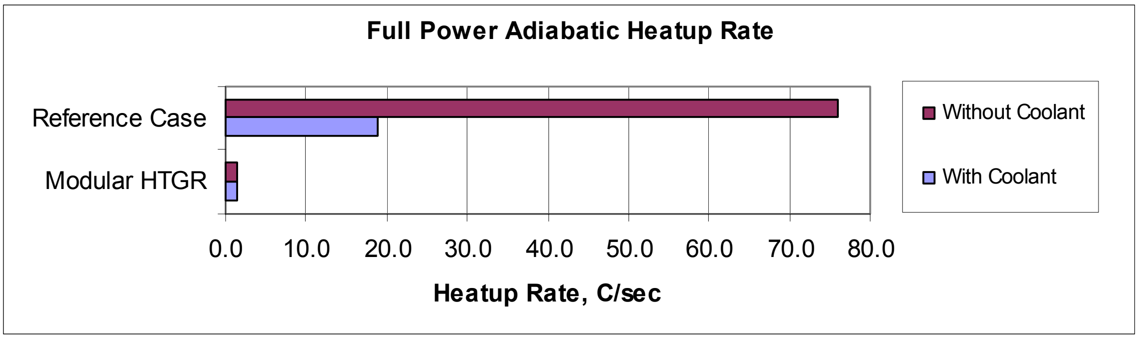


FIG. A.5. Comparison showing the full power, adiabatic heatup rates for a water reactor and for an MHTGR.

A.4. OPERATIONAL IMPLICATIONS OF SLOW THERMAL RESPONSE

The long slow thermal response and large thermal margins of MHTGR opens the possibility of major simplifications of operational safety requirements. For example, the peak temperature on a loss of coolant with sustained loss of active cooling systems is reached days after the initiation of the event. The temperature distributions of interest with regard to fuel performance during the event are determined by the heat transfer characteristics for heat removal through the walls of the reactor vessel, and thus are effectively decoupled from the temperature distribution in the core prior to the event.

In addition, the power distribution affecting the event temperature distribution is the distribution of the longterm decay heat. This is determined by the longterm core power distribution, and not significantly affected by the shortterm core power distribution prior to the event. This effect is illustrated in Figure A-6, which shows decay heat levels, as a function of duration of full power operation prior to shutdown, for several times after shutdown. The shortterm decay heat levels, of importance to the safety case for existing water reactors, are shown as the top set of curves. In this case levels approach equilibrium within minutes to hours of operation prior to shutdown, thus the decay power distribution is strongly influenced by the shortterm power distribution prior to shutdown. For the longterm decay heat of importance to the MHTGR safety case, days to weeks of operation are required to approach equilibrium, and the shortterm power distribution prior to shutdown has no significant effect.

The factors discussed above, in conjunction with the importance of controlling the integrated temperature, fluence and burnup history of the fuel, point to potential for a major simplification of operational safety requirements relative to existing water reactor plants. It is important to maintain the longterm core power and temperature distributions within an allowed envelope, but shortterm operational variations may be shown to be of no safety significance. Thus time compensated control and protection systems with restrictive requirements on accuracy and response times and resulting surveillance requirements typical of existing water reactors may be eliminated.

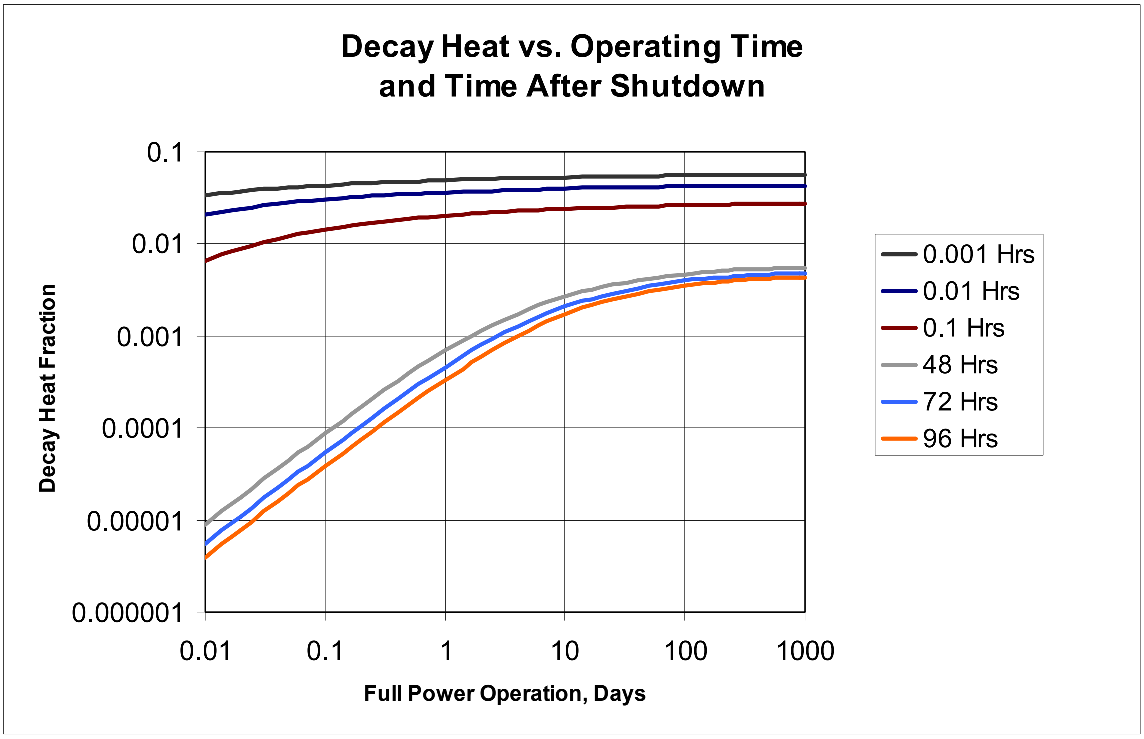


FIG. A.6. Comparison between the decay heat characteristic of importance to safety for water reactors (top set of curves) and for an MHTGCR (bottom set of curves).

CONTRIBUTORS TO DRAFTING AND REVIEW

Ball, S.	ORNL, United States of America
Camargo, C.	Commissão Nacional de Energia Nuclear, Brazil
Fiorini, G.	Commissariat à l’énergie atomique, France
Gasparini, M.	International Atomic Energy Agency
Kadak, A.C.	Massachusetts Institute of Technology, United States of America
Kendall, J.M.	United States of America
Mysen, A.	National Nuclear Regulator, South Africa
Sun, Y.	Institute of Nuclear Energy Technology, Beijing, China

Consultants Meetings

Aix en Provence, France: 3–7 July 2000
Beijing, China: 22–23 March 2001
Centurion, South Africa: 14–18 May 2001
Boston, Massachusetts, United States of America: 20–25 June 2002