

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].

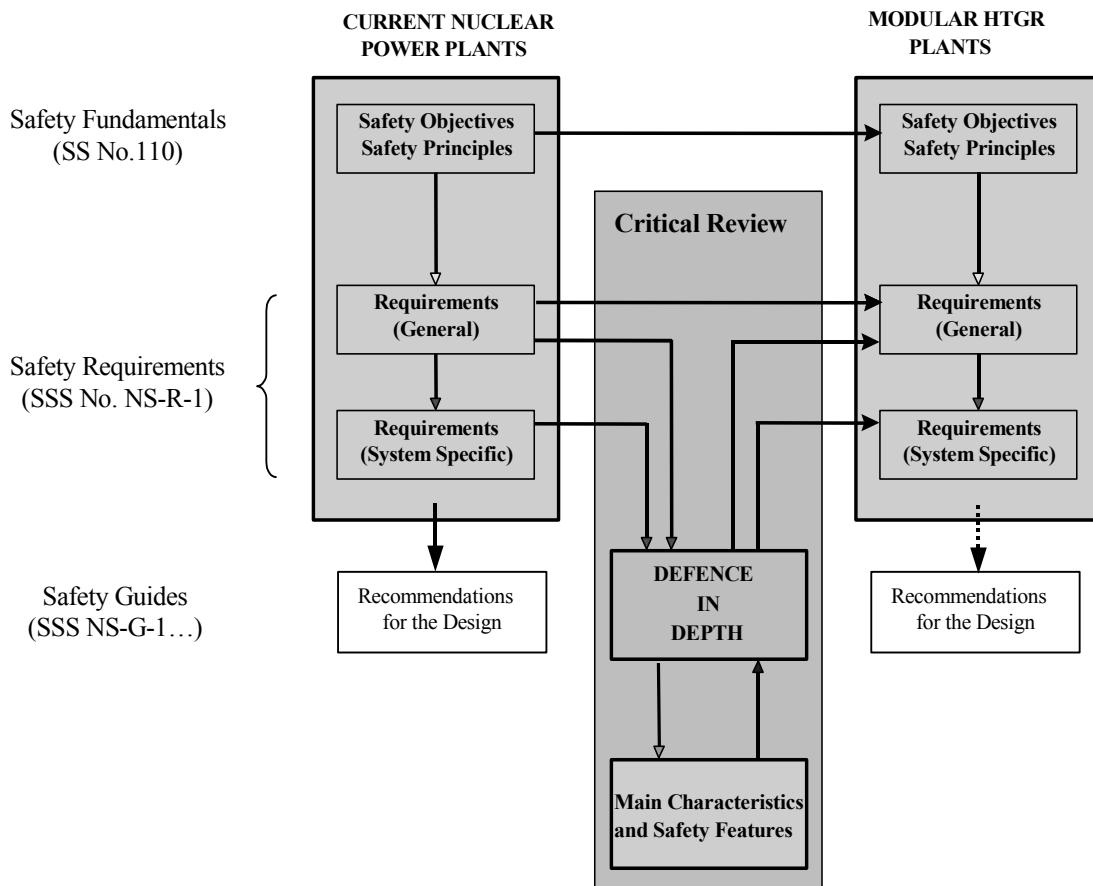


Fig. 6. Generation of Requirements for an MHTGR.

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.

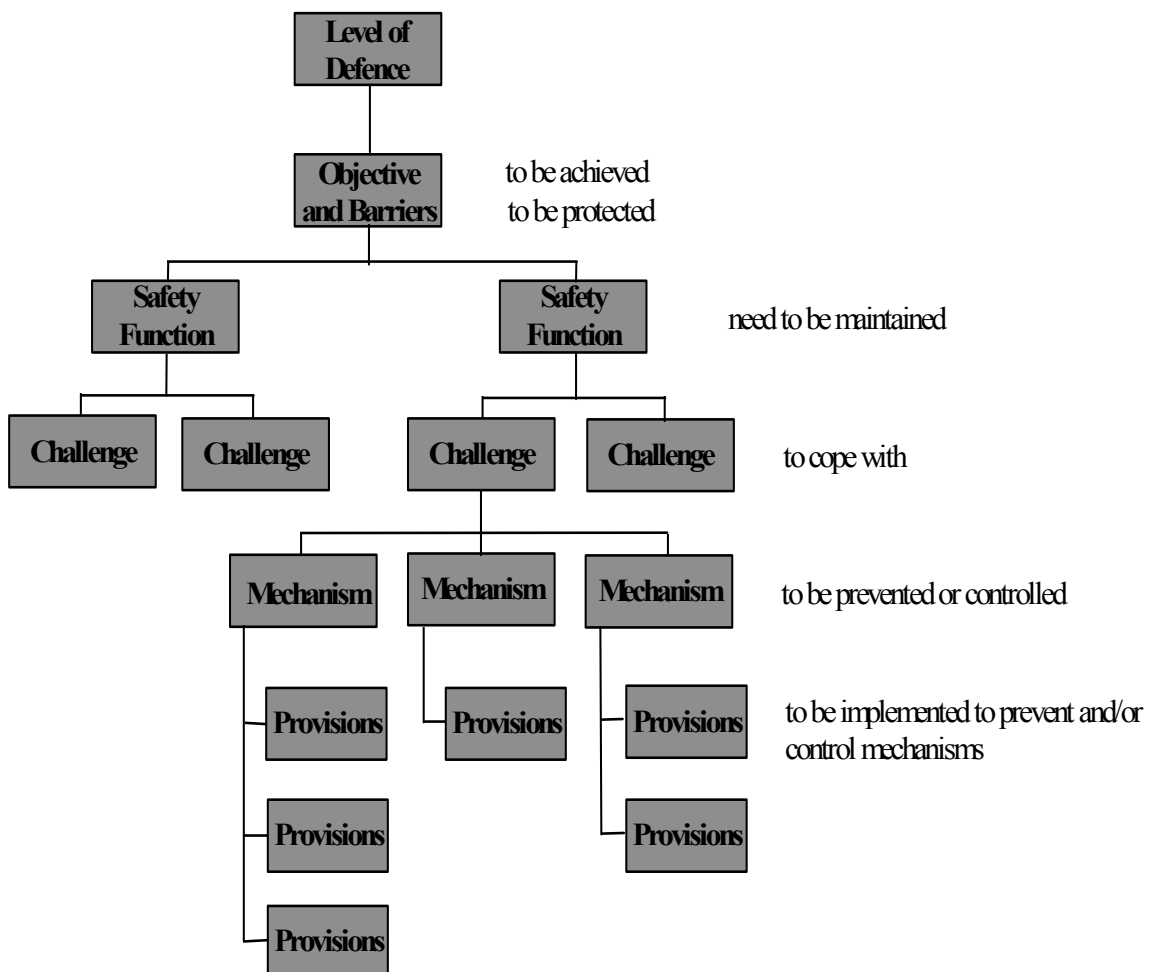


FIG. 7. Defence in depth objective-provisions tree.

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.