SAFETY CLASSIFICATION AND DEFENCE IN DEPTH FOR HTRS

Albert Koster, David R Nicholls
PBMR (Pty) Ltd, Lake Buena Vista Building, Gordon Hood Avenue, Centurion 1267;
PO Box 9396, Centurion 0046, South Africa; albert.koster@PBMR.co.za

ABSTRACT: A suitable safety classification of systems, structures and components as well as a solid defence in depth in the design of nuclear power plants are considered to be amongst the most important fundamentals of safe nuclear reactor design and operation. The principles generally in use at present, as well as IAEA suggested principles, are heavily biased towards Light Water Reactor (LWR) design practices where active defence in depth is essential. Applying these principles to advanced reactors that are designed to preclude core or extensive fuel damage for all thinkable conditions, would result in considerable overdesign, and may even impact negatively on the overall safety of these designs. Over the past five years, the Pebble Bed Modular Reactor (PBMR) design team has reviewed existing legislation and guidance documents with a view to extracting the underlying safety philosophy, and has applied this to a consistent set of criteria to be used in the safety classification. Coupled to this, the defence-in-depth definitions for High Temperature Reactors (HTRs) of the design represented by PBMR have been developed to show compliance with existing principles, but with a different emphasis on the importance and execution of the various levels of defence in depth as suggested by the IAEA. A classification system that includes recognition of the long times available to take action before significant releases could occur is proposed and linked to the defence in depth requirements.

KEYWORDS:. HTR; Module; PBMR; Safety Classification; Defence in Depth

0. INTRODUCTION

The South African Pebble Bed Modular Reactor (PBMR), like other modular reactor concepts conceived earlier, aims to eliminate the possibility of severe core damage and consequent serious exposure of the public and plant personnel. Besides the use of TRISO fuel, the most important contribution to this goal comes from the requirement that there shall be no need for active measures to achieve this. Taking this objective and the resultant design, an investigation of international practice of safety classification was found to be too biased towards LWR technology to be directly applicable to the PBMR design. Initially, a methodology was sought that would allow the application of, for instance, ANSI 51.1 with certain adaptations. This was found to be both difficult to achieve and not acceptable to the regulator, who liked to see a simple list of main and defence-in-depth systems classified as in ANSI 51.1, and defined codes and standards for each of these. The fact that there is no need for active systems to ensure safety makes it very difficult to define such a system without burdening the design with unnecessary costs. As a result, it was decided to develop a safety classification system that places the emphasis on Structures, Systems and Components (SSC) that are indispensable for the stated safety goal, and allows a graded approach to classification of those SSC

that can be used to prevent or mitigate possible accidents. This approach is described in the following paragraphs.

1. PRINCIPLES

In defining the safety classification methodology to be adopted for PBMR, the following guidelines were included:

- The internationally accepted main or Fundamental Safety Functions (FSF) must be satisfied;
  1. Control of heat generation (reactivity control).
  2. Control of heat removal.
  3. Confinement of radioactivity.
- Credit must be allowed for the specific characteristics of the HTR design, in particular that any accident will develop very slowly, allowing time to muster on-site or off-site resources to stop progression of the event.
- When diverse systems are available to prevent or mitigate the accident, and there is sufficient time for operators to mobilize these, credit must be allowed to lower the safety classification of these systems.
-

2. APPLICATON

All SSC are subject to the classification process. Safety classification enables a grading of quality, design, operational and analysis requirements. The PBMR design is such that more than one SSC can fulfil each FSF. However, for each FSF, at least one SSC (nominated the Prime SSC) shall be identified that will be shown by analysis to be capable of ensuring the FSF under all Design Basis Accidents (DBA). These SSC are classified as Required for Safety (RS). Other SSC, which fulfil the FSF and provide defence in depth, are classified as Beneficial to Safety (BS). No credit is required, or taken, for these SSC in the safety analysis of any of the DBA.

The PBMR takes advantage of passive safety characteristics or attributes. The attributes necessary for an SSC to fulfil an FSF determine the Safety Class (SC) of the SSC. For example, graphite blocks are RS because of their heat removal attributes (conduction, heat capacity) required for core heat removal as well as preservation of geometry to enable insertion of neutron absorbers.

There are five safety classes:

- SSC that are Required for Safety are classified as SC-1 or SC-2. The first safety class (SC-1) is allocated to the SSC that are Prime SSC. SSC that also support an FSF are initially classed SC-1.
- SSC that are Beneficial to Safety are initially classed as SC-3.
- SSC necessary for long-term recovery are SC-4.
- The lowest safety class (SC-5) is allocated to the SSC that have Negligible Safety Impact.

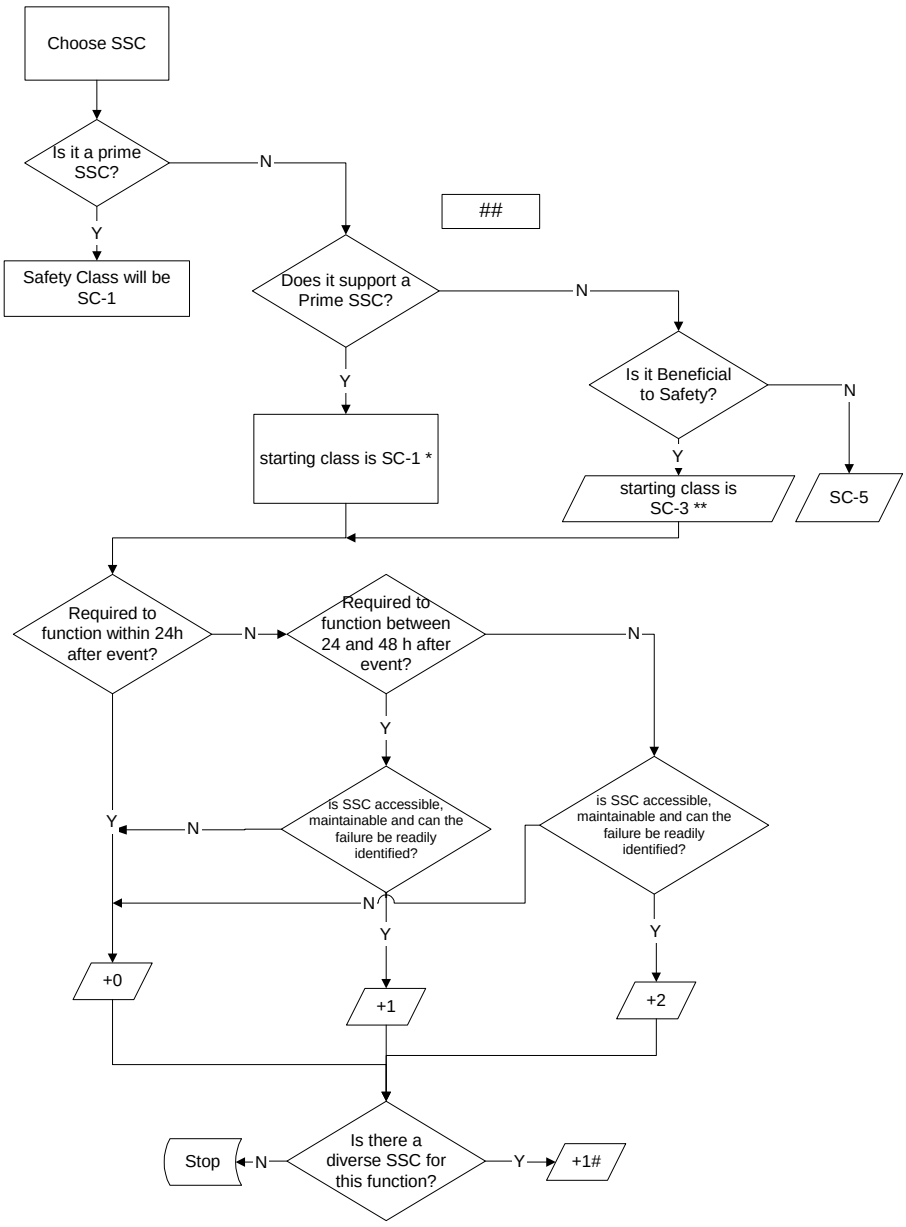
The described PBMR classification process is illustrated in FIGURE 1. The safety classification of SSC that are BS or that support an FSF may be relaxed (reduced in classification) based on:

- other systems fulfilling the same FSF (diversity);

- the time that the SSC is required after a DBA;
- whether the SSC is repairable/accessible in the time taken credit for.

A relaxation of one safety class is currently permitted for diversity for one of the diverse systems, and for all if conclusive proof can be provided that safety is not impaired by this action. A relaxation of one safety class is also permitted if the SSC is not needed until 24 hours after the DBA, and a relaxation of two classes is permitted for a 48-hour period. The time relaxation factors are based on the time to repair the SSC that is credible (accessibility, spares, trained staff), and that there is a reliable indication of the failure. The 24 hours is based on on-site staff being able to identify and rectify the defect, whereas the 48 hours is based on the on-site staff being able to identify and mobilize on-site or off-site resources. Application of relaxation can only be applied if it is demonstrated that the SSC in question is accessible for repair, and that its failure to operate is signaled to the operator.

Relaxation times are subject to constraints and also become design requirements to be met during the design process. This method derives a minimum safety class commensurate with the safety function of an SSC. This minimum level can be increased based on additional considerations over and above the technical requirement.



* Systems taken credit for in DBA analyses are either SC-1 or SC-2 (no further relaxation allowed)

** Maximum relaxation is to SC-5

\# Systems used for long term recovery may not be relaxed below SC-4

\#\# One SSC may support more than one fundamental safety function. Highest Safety Classification is used

FIGURE 1. Flow diagram for deciding safety class level of SSC.

3. DEFENCE-IN-DEPTH

The IAEA's five stages of defence in depth are adopted [1]; these are:

- Conservative design.
- Prevention of abnormal operation.
- Engineered safeguards to stop or mitigate accident progression.
- Mitigation of radioactivity release.
- Emergency procedures.

These five principles are applied by all existing commercial power plants. However, because even the conservative LWR designs do not preclude core damage, the last three stages carry a major part of the

burden of ensuring public safety. PBMR and other modular HTR designs concentrate in the first instance on having a design that is so conservative that core damage can be excluded. Thus the last three of the five principles should not have the same significance as they have in most operating nuclear power plants. The main emphasis of defence in depth in PBMR lies in prevention of abnormal operation, which includes efforts to stop an anticipated operational occurrence from developing into a DBA. The design efforts are concentrated on ensuring that the failure of active engineered safeguards will not cause a danger to the public and will not lead to the need for a level 4 action to prevent regulatory limits from being exceeded. Only passive SSC that are part of normal operation or are engineered safeguards are expected to be designated Prime SSC.

The connection between the safety classification and defence in depth is that SSC beneficial to safety, i.e. SC-3 and SC-4, are assumed to be operable for anticipated operational occurrences to prevent the escalation of an incident into a DBA. In the deterministic analysis of DBAs, these SSC are not credited with operation.

4. WORKED EXAMPLES

4.1General

The PBMR is a direct cycle power plant. Power level changes are effected by changing the helium inventory in the main power system. Adding coolant will temporarily lower the average fuel temperature, thereby increasing the power level until a new equilibrium is reached. Conversely, when gas is extracted, the fuel temperature temporarily increases to lower the power level. An essential requirement is a sufficiently large immediate negative temperature coefficient of reactivity.

Prior to a full classification of all SSC, the designers designated a number of SSC as being the Prime SSC as defined before. These are:

- For reactivity control, the core, in particular the reactivity temperature coefficient.
- For heat removal, all the core internals and the Reactor Pressure Vessel (RPV) that ensure that in the absence of active cooling, a temperature gradient develops and that heat can be conducted and radiated to a heat sink. Analysis shows that the reactor cavity walls provide sufficient heat capacity and conduction to ensure that the temperatures of the fuel and the RPV remain within a safe range. Thus the cavity walls are prime SSC class SC-1. However, it is deemed bad practice to solely rely on the concrete as the heat sink, as this would certainly prevent further operation of the plant after an event without active cooling. Thus the reactor cavity cooling system, which has a 72-hour passive cooling capacity, is also classified as a Prime SSC, abeit with safety class SC-2.
- As long as fuel temperatures do not reach excessive values (> 1 700), radioactivity confinement can be assigned to the coatings of the TRISO particles. Although the classification does not include the fuel, the reliance placed on fuel quality makes this the most important safety part of the plant, and fuel quality and testing are placed at the highest possible level.

Once the Prime SSC have been identified; all other SSC can be either Beneficial to Safety or have a Negligible Safety Impact.

4.2 Example 1

The Core Conditioning System (CCS) is used to cool the shutdown core in the absence of the main cooling function (frequency converter, generator as motor and compressors). It can keep the core at temperature or cool it down to maintenance conditions. As the Prime SSC for heat removal are the core structures, the RPV, the building and the Reactor Cavity Cooling System (RCCS), the CCS safety function is graded as Beneficial to Safety. Although a redundant system, there is no diversity, as the non-availability of the main system must be assumed (generator trip). Thus the CCS has a safety classification of SC-3.

4.3 Example 2

The Reactor Control and Shutdown System (RCSS). This system consists of two independent and diverse systems, the Reactivity Control System (RCS) and Reserve Shutdown System (RSS), both of which can make the reactor subcritical in a short time. Due to the fact that the core shuts itself down as soon as the temperature increases, and remains subcritical for about 70 hours, the RCSS is not a Prime SSC. This means that its initial classification is SC-3. The diversity provided by the RCS and RSS allows a relaxation of 1, and the fact that they are not needed within 24 hours provides a further relaxation. However, only the RSS is designed to provide assured shutdown under the most demanding DBA such as earthquake and very fast depressurization. This is because the structural integrity of the control rod sleeves cannot be guaranteed for extreme conditions. Consequently only one relaxation factor is applied, and the classification for both is SC-4. Despite this, there is a conscious decision not to try and argue such a low classification for a first of a kind reactor, and the safety classification for the RCSS is by choice fixed at SC-2.

5. CONCLUSION

The safety classification methodology described in paragraph 4 distinguishes between design features, including SSC that are required to satisfy the fundamental safety functions and those that can also satisfy them, but are used in a defence-in-depth capacity. Thus of the five safety classes, two are of high safety significance, two are of low safety significance and one has negligible safety impact. There is thus a close resemblance to the NRC rulemaking of 50.69, with the difference that the safety significance in 50.69 is mainly determined on a risk-based assessment. It is expected that over time and when reliable and accepted, probabilistic risk assessment results for HTR plants such as PBMR become available, that the two systems will tend to merge. As the ultimate goal of safety classification is to procure and maintain SSC to the required quality level, the relationship between the safety class and the mandated codes and standards and quality levels is of great importance. In determining these on a case-by-case basis using the methodology described, it was found generally that the quality assurance level for availability is more demanding than that for safety. It is expected that for PBMR there will be only a few SSC where the quality assurance level is prescribed by safety and not by availability demands.

ACKNOWLEDGEMENT

The contributions to the debate and definition of the proposed methodology by PBMR and Eskom specialists are gratefully acknowledged.

REFERENCES

[1] Safety of Nuclear power Plants: Design – IAEA NS-R-1.

AUTHOR INTRODUCTION

Albert Koster is a senior nuclear safety specialist with PBMR (Pty) Ltd and has been involved in various aspects of HTR technology since 1988. He has worked in the fields of reactor physics and nuclear safety since 1963, mainly at the South African Atomic Energy Corporation.

David Nicholls started his nuclear career in the UK Royal Navy as a nuclear engineer officer. He joined Eskom in the nuclear engineering division in 1984 and has since held a range of functions in the nuclear field, principally in the nuclear safety area, ending as the utility's head of Nuclear Safety. He has been involved in the PBMR since its inception in Eskom in 1993.