ADVANCED GAS COOLED REACTORS - DESIGNING FOR SAFETY

by

Barry A Keen
Head of Engineering Development Unit
NNC Limited
Booths Hall
Chelford Road
Knutsford
Cheshire
UK

1 Introduction

The Advanced Gas-Cooled Reactor Power Stations recently completed at Heysham in Lancashire, England, and Torness in East Lothian, Scotland represent the current stage of development of the commercial AGR. Each power station has two reactor turbo-generator units designed for a total station output of 2 x 660 MW(e) gross although powers in excess of this have been achieved and it is currently intended to uprate this as far as possible.

The design of both stations has been based on the successful operating AGRs at Hinkley Point and Hunterston which have now been in-service for almost 15 years, although minor changes were made to meet new safety requirements and to make improvements suggested by operating experience. The construction of these new AGRs has been to programme and within budget. Full commercial load for the first reactor at Torness was achieved in August 1988 with the other three reactors following over the subsequent 15 months.

This paper summarises the safety principles and guidelines for the design of the reactors and discusses how some of the main features of the safety case meet these safety requirements. The paper also summarises the design problems which arose during the construction period and explains how these problems were solved with the minimum delay to programme.

2 Safety Principles and Guidelines

The overall probabilistic design safety guidelines applying in the UK require that the total frequency of all accidents that could lead to an uncontrolled release of radioactivity should be no greater than about 10^{-7}/year in order to avoid individual faults causing an excessive contribution to the overall station risk of 10^{-6}/year. Higher frequency faults are acceptable at commensurately lower releases.

The practical interpretation of these guidelines in terms of the design development has been to provide effective protective features and systems to ensure that the reactor pressure vessel, internal structures, and fuel are maintained within safe limits for all fault sequences more frequent than 10^{-7}/year. Thus, a design basis is determined within which the total envelope of initiating faults and fault sequences is considered. The aim is to show that even for the most limiting sequences, the possibility of any accidental release of a significant quantity of radioactivity can be discounted. The frequency of those sequences falling outside the design basis is calculated and shown to be acceptably low.

Good design, with the objective of reducing the probability of faults occurring, and the provision of reliable protection systems form the basis of the design approach. Reliability is achieved through the adoption of appropriate design standards and the use of redundancy. Following the more frequent faults for which very high reliabilities of protection are needed, it is not considered that redundancy alone within a single system is sufficient. The safety guidelines require that diverse means of protection are provided as a defence against common mode failure.

The guidelines require specific attention to be given to the potential consequences of internal hazards, i.e. those arising from failures within the power station, and external hazards, i.e. those which are a feature of the site in terms of both natural and man-made phenomena. These guidelines are responsible, in particular, for the layout, segregation and qualification of plant and systems as necessary for each of the possible hazards, which can themselves be considered as potential common cause failures.

Finally, an important principle having an influence on the design is the requirement that in the event of an initiating fault occurring, the benefit of operator actions to improve or ensure safety should not be claimed within at least 30 minutes post-fault. This has led to the provision of automatically initiated and controlled systems and the avoidance of dependence on operators to identify and control fault conditions in the short term with the risk of taking precipitate actions.

3 Development of the Safety Case

The following sub-sections discuss various aspects of providing the final safety submission to the UK licensing authorities.

3.1 The use of probabilistic safety assessment

The adoption of a probabilistic approach has had a major influence on design and safety assessment. Figure 1 shows the relationships which indicate that the PSA has not been a separate activity but that it has had an integrated role in ensuring that the design and safety case develop in sympathy. This integrated role has developed as the design proceeded from initial concept through Preliminary Safety Report, Pre-construction Safety Report and station safety report stages and will continue through operation.

The methodology comprises three major parts:

i) Fault schedule

The fault schedule is a comprehensive set of initiating events broken down into distinct categories. Within each category individual events are identified which lead to a similar reactor response and are significant in respect of both frequency and consequence.

ii) Fault sequence analysis

In satisfying the probabilistic guidelines the objective for each initiating event has been to provide and justify adequate redundancy and diversity of protection to trip, shutdown and cool the reactor.

The development of the safety case involves determining the family of possible fault sequences which could follow each initiating event depending upon the operation of the protection systems. Thus the role of PSA is twofold.

i) Firstly, all sequences where the frequency is sufficiently high must be identified and confirmed as having acceptable consequences.

ii) Secondly, the frequencies of all sequences outside this design basis are assessed and integrated for comparison with the probabilistic targets.

iii) Event and fault tree analysis

The execution of the PSA has used a combination of event tree and fault tree methodology. Event trees which consider the development of faults in time have been used in quantifying the frequency of fault sequences involved in the operation of the reactor trip and shutdown systems.

Fault trees have been used to quantify the integrated arrangement of gas circulators, main boilers, decay heat boilers and the associated auxiliary service systems including electrical supplies. Different fault trees are used to reflect the different cooling requirements and plant availability following each initiating event. This approach permits the functional dependencies arising from the division of the primary circuit into four quadrants and the associated arrangement of essential supplies to be correctly represented.

In carrying out the analysis, as far as possible the aim has been to adopt generic reliability data and thereby avoid the need for specific justification. This has been possible in most cases but for some specialised components alternative approaches have been followed. In some cases, reliability data has not been readily available and certain judgements have been made on the basis of engineering and operational experience. This is not inappropriate. The PSA has proved a ready means of establishing the importance of the individual component reliability data to prove acceptable while focusing on more critical items for which special attention can be given. A particular application of sensitivity analysis has been the numerical consideration given to common mode failure. Avoidance of such dependent failures has been achieved by careful attention to design specifications, quality assurance, construction, installation, commissioning and operating procedures.

The main objectives of the application of probabilistic safety guidelines in the design approach to safety for the UK AGR are:

i) To assist in the development of the design to achieve a very low probability of a radioactive release.

ii) To achieve the first objective primarily by the provision of a high standard of protection system design such that the probability of events leading to possible core damage is itself sufficiently low irrespective of the further probability of consequential events leading to a significant release.

iii) To provide a framework for a comprehensive and systematic assessment using both qualitative and quantitative measures to compare the importance of one aspect of the design with another.

iv) To ensure a balanced design is developed such that no single events or fault sequences make significant contributions to the overall risk.

In examining these objectives, it should be noted that none make any attempt to establish an acceptable level of safety of the reactor simply in terms of an absolute index of risk. The guidelines are specified and used as a powerful aid in ensuring an adequately safe design is achieved and as a means of providing a very detailed insight into the design and operation of the protection systems. However, the numerical results of the analysis does indicate a very low probability of a radioactive release. The total frequency of fault sequences which could lead to exceeding plant and fuel safety margins, i.e. potentially leading to a damaged core, is calculated to be close to 10^{-6} per reactor year. Notwithstanding this result, the very long timescale for response of the primary circuit following most faults means that many of the sequences considered to be unacceptable in the probability analysis will result in adequate heat removal achieved by operator action some time (hours) after the initial incident and before any radiological hazard occurs.

The more practical value of the analysis is the ability to systematically identify strengths and weaknesses in the design and implement protective measures in the most effective manner resulting in a balanced design.

The analysis also provides an effective basis for the practical translation of probabilistic safety guidelines into the operational stage. In the UK, operating instructions are applied to control the state of the reactor and associated systems during operation to ensure that the power station is always operated within safe limits determined by the outcome of the design safety analysis. In respect of requirements to take essential plant out of service for maintenance while the reactor remains at power, the probability analysis provides an appropriate means of identifying the importance of individual and combinations of plant outages. The design safety guidelines require specific protection system reliabilities to be met during maintenance and the analysis permits both an assessment to be made against such guidelines and the development of effective operating instructions allowing the greatest operational flexibility consistent with satisfying safety requirements.

While the role of PSA has developed rapidly over the last decade and has been a major influence on the design and safety assessment for Heysham 2 and Torness it must be remembered that it is only one part of the overall design and safety assessment. It is to be noted that the CEGB Design Safety Guidelines comprise 20 separate annexes which cover all aspects of design and safety, and define acceptable standards developed from the experience gained from previous generations of reactor design and operation. The effect of these and other measures is to complement the use of PSA in assuring overall adequacy. The use of PSA in design has assisted in making sure that design decisions have been arrived at systematically and justifiably and has avoided major design modifications as the project has proceeded.Despite the value of its contribution to the development of the design and safety assessment for Heysham 2 and Torness, there are important limitations to the use of PSA. In some respects, the methodology still awaits development. However, the introduction of explicit safety guidelines and the use of a probabilistic approach to safety from the earliest stages of design have meant that it has been possible to incorporate all the major safety features before construction started.

3.2 Design approach to hazards

Protection against hazards is a requirement of the safety guidelines and their possibility and consequences are specifically taken into account in the design approach. Internal hazards are those whose source is attributable to failures within the power station while external hazards are those whose source is outside of the station and include both natural and man-made phenomena. These are discussed in turn.

3.2.1 Internal hazards

The design approach followed is to recognise hazards by their consequence and systematically examine the plant and systems within the power station to identify potential causes. Internal hazards considered include fire, flooding, dropped loads, hot gas or steam release, pipe whip, missiles, failure of rotating machinery, release of toxic substances, and failure of pressurised systems (e.g. gas storage tanks).

Defences adopted in the protection against internal hazards depend on the nature and potential consequences but may include

i) Avoidance or minimisation of hazard potential, e.g. use of non-combustible materials

ii) Layout, e.g. remote location and careful orientation of high pressure storage tanks in respect of vital plant or systems

iii) Separation, e.g. provision of sufficient space between diverse systems or redundant parts of one system such that the consequences of a hazard are limited

iv) Segregation, e.g. provision of rated fire barriers between groups of components to limit the extent of a hazard

The recognition and treatment of hazards has a fundamental effect on the overall arrangement of systems. This is carried out through to the detailed segregation of electrical power and control cables which is arranged to satisfy principles which limit the impairment of redundancy within systems in the event of a hazard at any location on the station.

As an example of the application of these principles, a depressurisation fault arising from failure of a sidewall penetration leads to a hot gas release hazard which because of barriers within the reactor building can affect the operability of plant serving only one of the four quadrants. Similarly a major failure of the main feed and condensate system, e.g. catastrophic deaerator failure, can only affect the operation of the emergency feed system (which is in the same area) leaving the decay heat boiler feed system on the opposite side of the reactor building unaffected.

3.2.2 External hazards

The design approach is initially a site survey to quantify the frequency and severity of potential external hazards. Clearly, the subsequent treatment of external hazards is site-specific. A comprehensive range of possible hazards is studied and the possibility of adverse effects on the power station is examined. In addition to site location and defences, those requiring specific design solutions for plant and systems to satisfy the safety guidelines are considered further. For Heysham II and Torness these are earthquake and high wind for which suitable qualification of plant and systems to withstand the consequences of these hazards is necessary.

Although layout and separation or segregation of plant and systems may be important in terms of limiting the consequences of failures induced by the specific hazards, these are not the prime defence adopted. The approach followed is to specify for the site an appropriate intensity for each hazard and then to qualify sufficient plant to withstand the effects of the hazard, including possible consequential effects of the failure of non-qualified plant, to ensure safe reactor shutdown and decay heat removal with adequate reliability.

3.3 Seismic design

The rarity of destructive earthquakes in the UK means that seismic design needs to be incorporated only in equipment necessary to provide safe shutdown and cooling of reactors. Two main protection levels were chosen:

i) The "Safe Shutdown Earthquake" (SSE) is only likely to happen once in 10,000 years with a peak ground acceleration of 0.25g. The safety components designed against this include those associated with safely tripping and cooling the reactors.

ii) The "Operator Shutdown Earthquake" works at a much lower level of ground movement. Not all safety equipment is given a seismic designation, but some safety-related equipment is required for protection against other reactor faults that could occur at relatively frequent intervals. Because of this, the station operator will trip the reactors in case the non-seismic equipment has been damaged by an earthquake. An alarm operates at the chosen horizontal ground acceleration of 0.05g - 1/20th of the force of gravity.

Seismic classification of components is required because of the large number of them in a power station and their wide range of functions. The classification provides a systematic basis for the design of an individual component so that the final overall power station would possess a coherent level of seismic capability.

i) Class A equipment has to withstand an SSE and still function properly. This classification applies also to buildings and structures which house or support Class A components.

ii) Class B relates to equipment whose failure in an earthquake could affect safety-related seismic plant. Where necessary, appropriate strengthening or upgrading to aseismic standards was undertaken.

iii) Outside these categories, other components are allowed to fail as there were no safety implications for the plant.

In all, 72 basic components or systems have been designed to survive a safe shutdown earthquake.

Once the ground motions were chosen, it was necessary to translate these into loading conditions for incorporation into design specifications. The dynamic response of components and structures are not solely dependent on their mass, stiffness and damping characteristics but depend also upon the interaction between the different buildings and the ground itself.

The analysis carried out was broken down into two parts: soil-structure interaction studies and component studies, where the former provided the input to the latter. The soil-structure interaction studies investigated the behaviour of the overall system where the modelling of the structures and components was simplified but still retained the important features that govern their dynamic response.

Actual seismic qualification of equipment is done by:

-predicting the equipment's performance under analysis

-qualifying by combined testing and analysis

-shaker table testing under simulated seismic conditions

-comparison with similar equipment already qualified.

Most components could be qualified by analysis, using mathematical and computer techniques. A combination of analysis and testing was used where a basic dynamic characteristic was unknown. In addition to analysis of dynamic responses, the parameters of stress, strain and displacement had limits set on them.

The need to have aseismic components has an effect on the total design of a power station. In relation to aseismic components there is an increased likelihood of design changes because of aseismic requirements and those design changes have then to be checked for aseismicity. Another consideration is the need to avoid excessively conservative designs because of the particular characteristics of analytical and test methods used. The overall impact of seismic criteria was kept to an acceptable minimum by the four stages of careful selection of the SSE ground motion to represent UK seismic activity, component classification, phasing the overall station analysis with the concept of the Design Basis Earthquake being used for early work where design/layout changes were most likely. Selecting the most appropriate method to qualify equipment.

Owing to the non-linear response or low natural frequency, additional, more detailed, analysis had to be used on the boilers, fuel assembly, charge machine, charge hall crane, reactor core and pressure feed water tank.

3.4 The design of AGR thermal shield details for high temperature applications

The AGR pre-stressed concrete vessel (PCPV) liner, the gas baffle and the guide tubes are thermally shielded from the circulating coolant gas by a ceramic fibre insulant. The insulation is retained by a series of thin stainless steel plates and cylinders which are attached to the shielded structures by various means. In the plane areas of the PCPV liner and gas baffle the primary retention consists of a threaded stud welded to the shielded structure, and the cover plate is locked at the required position by means of a threaded clamping arrangement. The shield details around upstands and penetrations are frequently more complex and utilise cylindrical components.

A significant proportion of the thermal shield components are exposed to coolant gas temperatures of 425-650°C when the reactors operate at full power. At these temperatures creep effects become significant and the designer must utilise design rules which recognise these effects.

There are two basic routes for design by analysis contained within design codes. The elastic route requires the use of linear elastic analysis methods and contains a high degree of conservatism in many of the design rules. This is intended to cover the uncertainties which exist when dealing with components that are subject to plastic and creep deformation. The alternative inelastic route requires a better estimate of the plastic and creep strains that a component receives during service and provides less conservative design rules in recognition of this improvement.

Ideally, the designer needs to use simple methods of analysis with design rules which guarantee a minimum of conservatism. The present rules are particularly severe when designing thin components subjected to thermally induced loads, such as are seen in the AGR thermal shield. A need was identified therefore to develop simplified methods of design by analysis specific to the shield components.

It has been demonstrated that simplified methods of analysis can be applied which bound the inelastic stress-strain behaviour. These methods allow for an improved assessment against incremental behaviour and creep-fatigue damage criteria using the results of linear elastic analysis. If elastically calculated strain ranges are less than 0.1% then elastic shakedown will occur and creep-fatigue damage will be estimated with reasonable accuracy using the creep-fatigue design curves of the design code with elastically calculated quantities. For strain ranges in excess of 0.1% the use of design factors on best estimate cyclic frequencies gives an acceptable assessment of thermal shield components, since the additional damage due to elastic follow-up is effectively included in the creep-fatigue assessment. Utilising these guide-lines there is no requirement to compute additional creep damage separately since it is adequately catered for in the design creep-fatigue curves. A demonstration that components are not subjected to excessive incremental behaviour is dependent on the mechanical properties assumed and provides the major limiting design feature when utilising elastic analysis.

Particular attention has been given to the design of Alloy 800 cylindrical bellows units operating at temperatures up to 650°C. An extensive test programme has been carried out to consider the particular effect of cold work on the cyclic performance of a unit. From the mechanical properties it was found that significant incremental behaviour was not likely and that the resulting creep-fatigue endurance was a slight improvement over the anticipated annealed material behaviour. The creep-fatigue design line constructed from a consideration of material properties and inelastic behaviour at convolution crests is intended for use with simple elastic calculations and is an example of the application of simplified methods to the design of thermal shield components.

4 Resolving Design Problems During Construction

All Project Management Teams which are set up to drive complex projects like the design, construction and commissioning of a nuclear power station must realise from the beginning that unexpected problems will arise at various stages of the project. They must therefore have an organisation available which can swing into operation quickly to determine the cause of the problem and then to propose, agree and implement the preferred remedy. This section explains how two major problems which did arise were resolved with minimum project disruption.

4.1 Standpipe Cracking

The roof of the PCPV is penetrated by a series of carbon steel fuel standpipes which form a continuation of the PCPV liner. The standpipes are water cooled and thermally shielded by means of a stainless steel liner containing ceramic fibre insulant. The temperature at the top of the standpipe is monitored during operation to ensure that the closure arrangement is not at risk of losing effective sealing. Temperatures normally are of the order of 60°C, but during 1985 the temperature on one standpipe at Hunterston 'B' began to approach the operator action limit of 150°C.

4.2 Control Rod Vibration

Programmed dates were achieved throughout the first 6 years of the construction programme for each of the two reactors at Heysham 2 and Torness. Following the unfuelled engineering runs at both Heysham 2 and Torness, however, inspection of the control rod assemblies revealed wear marks on the control rods and immediate checks were then made on all the control rods and their channels. These revealed that there were spiral and circumferential wear marks on the outside of a number of rods and corresponding marks in the guide tubes and graphite core channels. Wear was also found in the joints between the control rod sections and on some of the chains which suspend them. The worst worn rod joints and worn chains were replaced but it was realised that serious wear problems could develop on the others if they were used for the reactors' thirty year life span. The control rods are the reactor's regulating and primary shutdown system and their vital safety role means that they must be of the highest possible integrity.

In order to review all possible causes of the problem, NNC constructed a full scale pressurised CO_2 rig and several water rigs and used a half length scale atmosphere air rig, followed by a full length full scale air rig. Other pressurised rigs in the UK were modified to assist in testing. In parallel with investigations on these rigs, tribological studies were carried out and it quickly became clear that the configuration of the cooling gas inlet ports to the control rod channels imparted a swirl to the gas (Fig. 5), which in turn generated a precessional movement of the control rods within the guide tubes and channels and so gave rise to the wear marks. These port arrangements differed from previous designs, because the control rod and fuel standpipe nozzles in the gas baffle were inverted at Heysham 2 and Torness relative to Hinkley and Hunterston in order to provide adequate dome cooling.

The solution adopted after much testing involved blanking off the inlet holes with collars clamped and welded around the original inlet ports, and drilling 32 new holes in each guide tube lower down. The size, number and location of the new holes was only decided after studying results from tests on numerous different hole arrays.

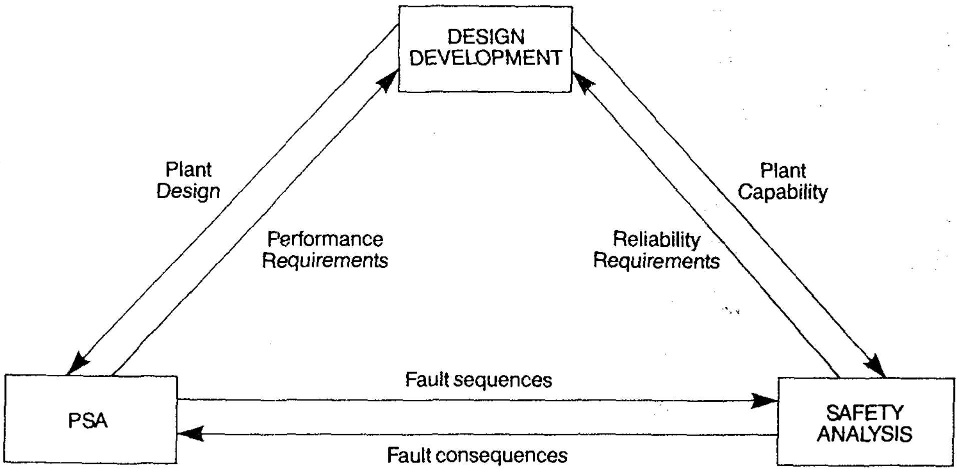
Putting these changes into effect required an unusual combination of thin men and remotely operated machinery. One contractor supplied the thin men who managed to squeeze between the guide tubes to position and weld the blanking collars and to drill some of the new holes while another produced machines, controlled by operators ten metres above on the pile cap, capable of accurately positioning and drilling new holes in the guide tubes from inside them, in a fraction of the time which was taken to do it manually from outside. Access conditions in the reactor were very difficult, and the remote machine helped to shorten considerably the time taken to drill the new holes.

The modifications have been successfully carried out on all four reactors and new tests on the control rods show that the activity has been reduced to a very low level, and that they should last the planned thirty year life of the stations.

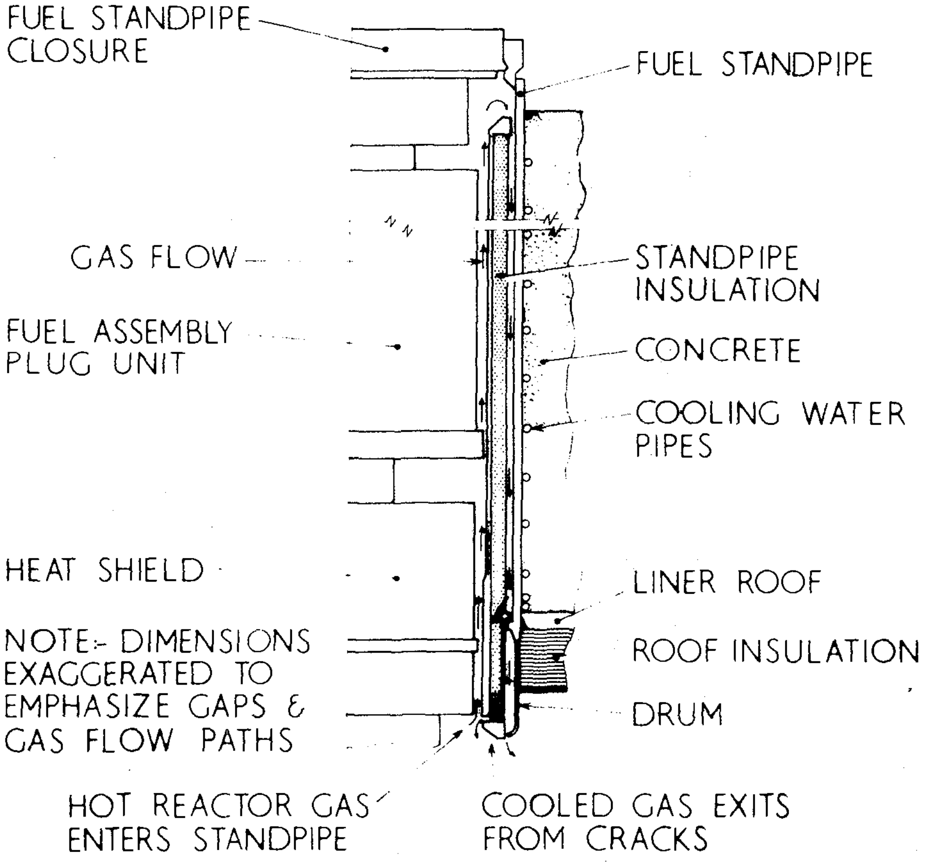
The examples illustrated above have led to an overall delay to the first reactors at Heysham 2 and Torness of about 9 months but the second two reactors were not significantly delayed.

5 Acknowledgements

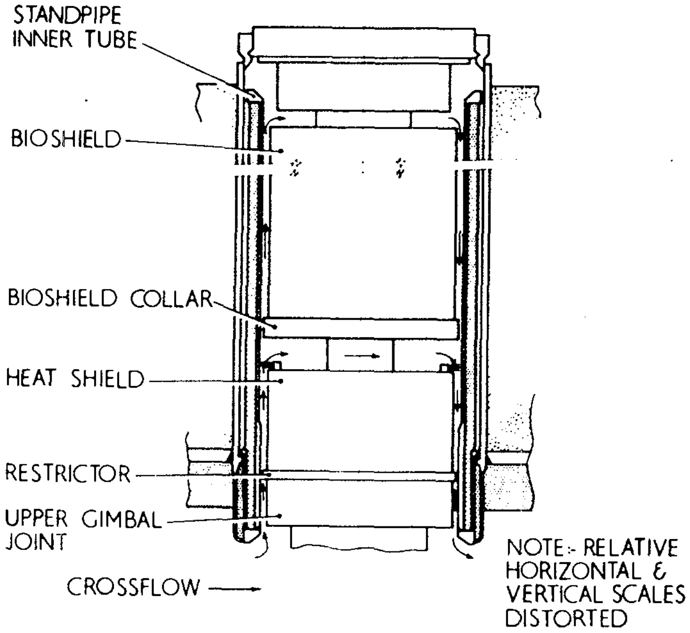
The author is indebted to his colleagues at NNC who provided the source material for this paper



ROLE OF PSA IN DESIGN DEVELOPMENT AND SAFETY ANALYSIS FIG 1

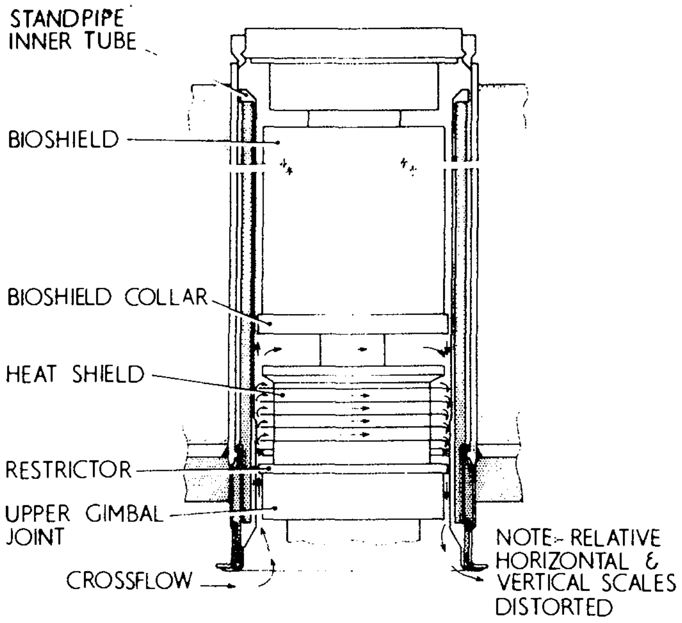


STANDPIPE THERMAL SYPHON FLOWS FIG 2



NOTE:- RELATIVE HORIZONTAL & VERTICAL SCALES DISTORTED

GAS FLOWS-OLD HEAT SHIELD FIG 3



NOTE:- RELATIVE HORIZONTAL & VERTICAL SCALES DISTORTED

GAS FLOWS-NEW HEAT SHIELD FIG 4

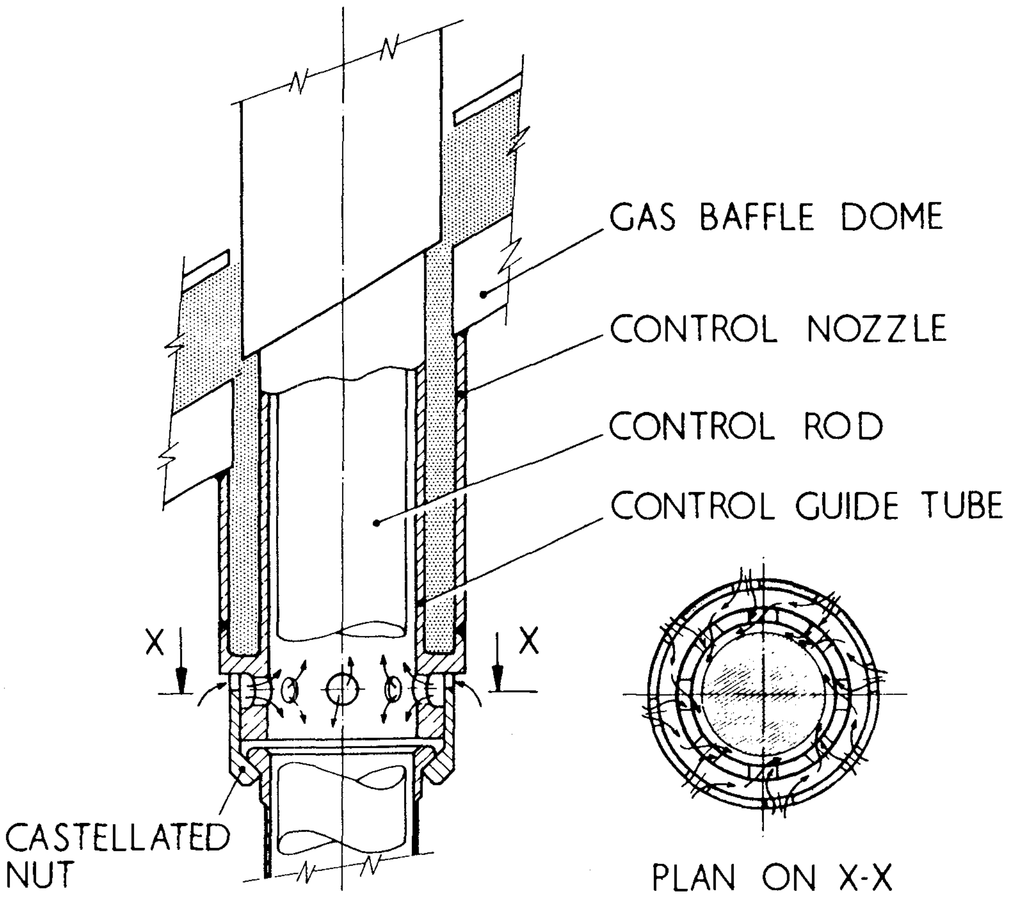


FIG 5 HEYSHAM 2 / TORNESS CONTROL ROD INLET PORT CONFIGURATION

The mechanism causing the temperature rise was considered to be associated with weld cracking at the bottom of the standpipe liner, which would lead to thermal syphon flows up the bore and down the outer of the standpipe liner. (Fig. 2)

The cracking was confirmed when, during a statutory shutdown of the reactor in 1985, the faulty liner was replaced by cutting through the bottom, removing the old and rewelding a new liner. During this outage a survey of all the peripheral standpipes accessible by man entry was carried out and revealed a significant proportion of the liner welds to be defective. A safety case was made on the basis of forwarning by temperature monitoring of any situation that could lead to a safety hazard and the reactor was returned to power.

Economically there were strong incentives to determine the cause of the cracking and to remedy it quickly. The technical investigation including the introduction of specially instrumented standpipe liners and fuel plug units to monitor operating conditions showed that the loading was thermally induced, with moderately high cycle fatigue associated with thermal syphon flows occurring around the plug unit heat shield.(Fig. 3)

These flow conditions led to large temperature asymmetries (200°C diametral difference) which were unstable and gave rise to the fatigue cracking of some welds in the standpipe liner. Since the new station design was very similar to the operating reactors it was to be expected that a similar phenomenon would occur, and it was shown that an unacceptable design life would result unless some late modification was introduced.

To solve the problem, thermal shielding is retained around the central structural component but a series of baffle plates are introduced to promote better mixing of the convective flows and hence reduce the diametral gas temperature differences imposed on the standpipe liner. (Fig. 4) The principle was demonstrated initially utilising half scale water rigs which gave reasonable representation of flow characteristics and a guide to changes in the temperature field. Thermal hydraulic material codes were also developed to explore sensitivity to such aspects as baffle size and position, and cross flow conditions. The final demonstrations were achieved by installing a number of heavily instrumented plug units with the proposed heat shield modification into the operating reactors. Data obtained from these units confirmed that the magnitude of thermal asymmetry was halved, that the level of thermal instability was reduced, and that the structural integrity of the plug unit and its modified components was adequately retained. This confirmation was obtained approximately 12 months after the problem was first revealed at which point manufacture of the modification was well advanced and backfitting on the new plug units at sites had begun. As a consequence the full station complement of heat shields was modified prior to power raising without influencing the overall programme to completion of Heysham 2 and Torness beyond that brought about by the control rod instability problem discussed in the next section.