# SAFETY DESIGN FEATURES FOR CURRENT UK ADVANCED GAS-COOLED REACTORS

**J.M. YELLOWLEES, E.C. COBB**
**Nuclear Power Company Ltd.**
**Risley, Warrington, Cheshire**
**United Kingdom**

## 1. Introduction

The nuclear power stations planned for Heysham II and Torness will each have twin 660 MW(e) Advanced Gas-cooled Reactors (AGR) based on the design of those which have been operating at Hinkley Point 'B' and Hunterston 'B' since 1976. Following submission of the Pre-Construction Safety Report in the autumn of 1979, construction on site is programmed to start in the autumn of 1980. Some design changes have been introduced where necessary to meet enhanced safety requirements which have arisen over the decade since the Hinkley and Hunterston reactors were ordered, and also to improve features in which deficiencies were identified during the construction and operation of these stations. The experience gained in the design and construction of the Hartlepool and Heysham I AGRs has also been taken into account.

This paper describes current safety requirements for thermal reactors in the UK and explains how particular requirements are met in the design of the Heysham II and Torness reactors.

## 2. Current Safety Requirements in the UK

Construction and operation of a commercial nuclear power station in the UK requires the granting of a license by the Health and Safety Executive under the Nuclear Installations Act of 1965. The HSE is advised by the Nuclear Installation Inspectorate (NII) and the licence is granted to either the Central Electricity Generating Board (CEGB) or the South of Scotland Electricity Board (SSEB). A major activity in licensing is the assessment by NII of the Pre-Construction Safety Report, prepared by the single UK Design and Construction company, Nuclear Power Company Limited, under the terms of its contracts with the Generating Boards. Preparation of the Pre-Construction Safety Report is seen as important not only to confirm that safety requirements have been met but also to ensure that any design changes required during construction are kept to a minimum.

While detailed guidance is provided by the principles by which the NII (Ref 1) will assess the safety of the design of a nuclear power station and by the safety requirements of the Utilities (as the licensees), all parties in the UK recognise clearly that the adoption of a formal legalistic approach could, in practice, prove counter-productive to the achievement of real safety. It is important to note that while the requirements are not mandatory, this does not mean that any variations which are agreed are only relaxations; if considered feasible and appropriate, more stringent provisions may also be demanded.

The aim of the safety design approach is to meet the recommendations of the International Commission on Radiological Protection and the EEC Directive of 1 June 1976 in respect of exposures of the general public and workers to ionising radiation; this requires a sound design concept, well-engineered and proven design and high quality construction. The current UK methodology embodies an evolution from the earlier 'credible/incredible' approach to one combined with a comprehensive Quantitative Risk Assessment (QRA). For the former, certain events may be classified as being so low in risk of occurrence that general further provisions or particular distortions of the design to deal with them are not justified. For the latter, sets of numerical targets are set and reliability values are specified which relate to the performance of the kinds and numbers of components in the systems used in safety roles. While QRA is not to be employed as the sole basis for safety assessment, it is seen to have particular value in ensuring that a systematic approach is followed and that a balanced design is achieved in terms of safety performance.

Some major examples of the requirements of the safety systems and their performance are:

(i) For any single accident which could give rise to a large uncontrolled release of radioactivity to the environment, resulting from some or all of the protective systems and barriers being breached or failed, then the overall design should ensure that the accident frequency is less than $10^{-7}$ per reactor year.

(ii) For major safety functions (e.g. reactor shutdown, shutdown cooling) the reliability target is not to exceed 1 failure in $10^{7}$ demands.

(iii) The reliability of a single system cannot be claimed as better than 1 failure in $10^{5}$ demands (to allow for Common Mode Failure considerations).

(iv) Each system must perform adequately assuming a single failure of any plant item.

(v) Operator actions should not be claimed or required within 30 mins of reactor trip.

## 3. Principal features of the Heysham II and Torness AGRs

The nuclear island, Fig 1, at each of the sites at Heysham and Torness comprises two reactors (Ref 2), each of 660 MW(e)(gross), surrounded by the building structure which also accommodates a central block for the fuelling facilities. A refuelling machine in the charge hall services

both reactors. The graphite core structures, the boilers and the carbon dioxide gas circulators are housed in the two single-cavity concrete pressure vessels prestressed with helical multi-layer tendons in the vertical walls. The fuel elements, of which there are 8 in each of the 332 fuel channels, incorporate 36 pins containing uranium dioxide fuel pellets clad in stainless steel. The average fuel channel gas outlet temperature is 645°C, and the coolant pressure is 43.5 bar a (circulator outlet).

Four boiler groups, located in the annulus surrounding the reactor core, allow heat rejection in independent quadrants. Separate tube banks, sited below the economiser section in the main boiler casings, form decay heat boilers which may be used for shutdown cooling. Associated with each boiler quadrant are two induction-motor-driven constant speed gas circulators located in horizontal penetrations below the boilers. The coolant flow is controlled in normal operation by variable inlet guide vanes. Post reactor shutdown the gas circulators are energised via variable frequency converters at 7.5Hz (15% full speed) and up to 100% speed in loss of coolant pressure accidents.

The primary control and shutdown system consists of 89 absorber rods and drives housed in standpipes in the top cap of the pressure vessel. A back-up secondary shutdown system, mounted through the bottom slab of the pressure vessel, injects nitrogen into the core channels, and, if necessary in the long term, boron beads.

## 4. Definition of fault categories

The target data for risk and system reliability quoted in Section 2 has required an overall risk assessment using event and fault trees and data on component reliabilities taking into account plant testing and maintenance. The aim has been to demonstrate that an adequate balance of safeguards plant has been provided.

A first step in risk assessment is the identification of all credible initiating faults. To rationalise fault transient analyses and the proof that reactor plant constraints relevant to safety are not violated during fault conditions, the various faults are grouped into eight categories in each of which the fault characteristics, the reactor system response and the final consequences are roughly similar. Faults are further divided into two classes, 'Frequent' and 'Infrequent', according to whether the predicted frequency of occurrence is greater or less than about $10^{-3}$/yr. The objective is to relate the diversity of safeguards to the two fault frequency classes. In order that individual 'frequent' faults do not exceed the radioactive release limitations, diverse safeguards are necessary, such as the secondary nitrogen shutdown system and natural convection cooling as back-ups, respectively, to the rod primary shutdown system and forced gas circulation. This diversity provides high reliability and protects against some unforeseen common-mode faults inhibiting a primary safeguard. 'Infrequent' faults do not require the same diversity since adequate redundancy of a single type of safeguard satisfies the acceptable risk levels.



The eight categories of faults are as follows:

1. Spurious reactor trip

   This category includes all automatic and manual reactor trips which are not due to a failure which causes the reactor to depart from its permitted operating regime. At the high frequency assumed for design purposes (10/y) this category makes the most onerous demand on the diverse heat removal system.

2. Pressurised reactor faults - These include:

   - Main boiler feed and condensate system failures. These define the duty of the decay heat boiler feed system which, with forced gas circulation, provides the means of heat rejection in these events.
   - Fracture of a steam main. The steam released by a failure within the reactor building can be allowed to fail the gas circulators in up to two quadrants. Barriers prevent further failures.
   - Water ingress into the vault from main boiler leakages. Protection is given by reactor trip on two lines of vault overpressure in addition to the reactor overpressure relief valves.
   - Partial loss of primary coolant flow. The failure of the two circulators within one quadrant does not necessitate a reactor trip.
   - Reactivity faults, i.e. symmetric and asymmetric withdrawal of control rods.
   - Quadrant faults; examples are mis-match of gas flow and boiler feed in a quadrant necessitating trip of one quadrant but not of the reactor.

3. Loss of grid connection

   This category of electrical faults causes rundown of all gas circulators together or sequentially. This moderately frequent event demands diverse shutdown and cooling systems and power supplies from diesel generators.

4. Depressurisation faults

   The design maximum breach occurs outside the quadrant space and is limited by design to $0.03m^2$.
   To meet reliability requirements it is shown that safe shutdown heat rejection is possible with only two of the four quadrants in operation, emergency boiler feed supplied to the main boilers and gas circulator speed programmed to increase as reactor pressure reduces.

It is assumed for design purposes that the hot gas issuing into the quadrant space from a failed vessel side-wall penetration could put the circulators in that quadrant out of action. To meet the more onerous requirements in this event it is therefore shown that one other quadrant of the three remaining will be adequate for heat removal. This is possible by providing engineered restraints at the side wall penetrations to restrict the breach area to $0.006m^2$ and $CO_2$ injection to hold the circuit pressure at about 2 bar for a period.

5. Faults arising in essential mechanical/hydraulic systems

Because of the redundancy in these systems, this fault category does not lead to an automatic reactor trip but requires the consideration of failures such as pipe failures which could demand action to trip the reactor eventually, albeit by the operator.

6. Refuelling route faults

This category covers faults in fuelling plant and refuelling operations and is extended to include reactor faults occurring whilst refuelling which will normally be carried out with the reactor at power.

7. Internal hazards

This fault category comprises:

- fires
- floods from on-site sources
- loads dropped from lifting equipment
- disruption of rotating machinery
- disruption of on-site pressure vessels
- hot gas release following breach of the primary coolant circuit
- steam release following steam pipe failure
- release of toxic substances on site

The reactor and safeguards plant is protected by limiting the effects of each hazard by means of selected plant layout, by segregation barriers and by physical restraints.

8. External hazards

This fault category comprises:

- earthquakes
- extreme winds

Particular plant and structures are designed to survive specified conditions to ensure reactor shutdown capability and reliable post-trip cooling.

The preliminary risk assessment showed that the contributions of the individual fault categories to the summated risk were approximately similar and that there were no fundamental design deficiencies in the provision of plant for tripping the reactor and cooling it subsequently. These plant provisions are described in the sections following.

5. Layout and segregation of plant

For protection against hazards, the reactor building surrounding the pressure vessel is divided into 4 segregated quadrants, A, B, C, & D, Fig 2, each quadrant being associated with a pair of gas circulators and a boiler unit housing main and decay heat boilers; also with an independent electrical system, Fig 3.

The inter-quadrant barriers are designated 'primary' and 'secondary'. Primary barriers are designed to contain minor fires and hot gas releases within a single quadrant, leaving three others available post-shutdown. The more substantial secondary barriers will contain the lower-frequency major fires and the effects of steam pipe breaches within two quadrants, leaving the other two quadrants available post-shutdown.

The secondary barrier principle is extended to the independent electrical systems, pairs of which are therefore isolated from each other by the building structure, Fig 2. There is a primary barrier within each electrical system pair.

An electrical system (Fig 3) includes an 'X' diesel-backed train to energise its quadrant pair of gas circulators and certain essential auxiliaries, and a 'Y' diesel-backed train to energise diverse cooling services. There are therefore 8 diesel-generators and trains per reactor but the diesel-generators are connected also to similar plant on the second reactor.

The 'X' and 'Y' trains of a particular quadrant do not require to be segregated because there is available sufficient redundant and diverse plant associated with the other quadrants.

Auto-sequencing equipment controls plant operation. Sequence initiation uses 'de-energise to operate' signals and all parameter sensing and plant state checks are done in a way that maintains 'X' and 'Y' train electrical independence. This restriction on cross-checking simplifies auto-sequencing but entails the starting up of all parallel plant for each post-shutdown cooling function.

For hazards segregation and operational convenience, certain motor-pump units for feed and cooling services are grouped with appropriate segregation in the mechanical annexe and in the reactor services annexe, Fig 2, and not in the building quadrants.

## 6. Reactor shutdown systems

For those faults for which failure of the shutdown system would risk a radioactive release, the shutdown systems must perform with a reliability better than $10^{-7}$ failures per demand. This cannot be achieved by a single system of similar components irrespective of the degree of redundancy employed due to the possibility of a common-mode failure invalidating all equipment of a similar nature. Consequently, each fault in this category will be detected by sensing two independent diverse parameters with each diverse system designed to a reliability of about $10^{-4}$ f/d.

The two diverse guardline systems comprise a main electro-magnetic pulsed (Laddic) guardline which initiates the primary shutdown system (rods) and a diverse, relay, guardline which initiates the secondary shutdown system (nitrogen injection) at, for example, a higher temperature trip level in event of failure of the main guardlines or primary shutdown system. The diverse guardline also provides a back-up route for tripping the main guardline.

A further guardline protects boilers and circulators against faults in individual quadrants. As some such faults have safety implications, there is not complete separation between this primarily economic guardline and the reactor safety guardlines.

## 7. Post-trip cooling systems

### (a) Post-trip cooling at normal gas pressures

Frequent faults, such as category 1 faults, require exceptional redundancy and diversity in the shudown cooling provisions in order to meet the reliability target. For those faults the cooling safeguards are therefore divided between the 'X' and 'Y' trains in such a way that either train system acting on its own will cool the reactor safely. This arrangement provides redundancy and, by virtue of the diversity, gives protection against common-mode failure of cooling. The two means of gas circulation, i.e. forced and natural convection, determine the allocation of functions to the 'X' and 'Y' trains. These functions are listed in Table 1 and the various post-trip cooling systems in Fig 4.

#### Mode 1 - 'X' trains alone - forced gas circulation at pressure

Primary fuel cooling when shutdown is by forced convection using the gas circulators, the decay heat boilers rejecting the heat. The circulators, their auxiliaries and those of the decay heat boilers are allocated to the 'X' trains. Seconds after a reactor trip the circulator 11kV circuit breakers are opened, Fig 3, and the frequency converters are energised. The IGVs are opened. Following a delay with checks that the circulator speeds are below a predetermined setting, the frequency converter circuit breakers close to maintain 15% speed which, with two quadrants of decay heat boilers, is sufficient for safe fuel cooling but all quadrants are normally initiated.

The safety requirements call for one aseismic cooling route and the 'X' trains provide this. Owing to the difficulty of making the seawater system aseismic, the decay heat boilers reject heat to air coolers.

Fig 4 is extended to show as an example the 4 decay heat boilers supplied by 4 feed pumps. To improve availability all pumps are headered and any pattern of 2 energised out of the 4 connected to the trains provide sufficient flow. Headering is acceptable because the frequency of header failure is not greater than the frequency of failure of all 4 trains in a common-mode equipment fault. Pairs of pumps are segregated by fire/missile barriers and the system as a whole is segregated from the main boiler feed system to avoid common failures arising from the range of internal hazards (category 7 faults).

Because the decay heat and main boilers are mounted in the same casings, there is no need for any gas flow diversion valves which would otherwise contribute to overall unreliability. It is also acceptable to use the normal duty gas circulators with the decay heat boilers because by design and segregation the gas circulator common-mode failure frequency is as low as the acceptable overall failure frequency of the decay heat boiler feed system.

#### Mode 2 - 'X' and 'Y' trains together - Forced gas circulators at pressure

The main boiler auxiliaries are allocated to the 'Y' trains. Thus the 'X' and 'Y' trains with the gas circulators, their auxiliaries and the main boiler auxiliaries together provide a second shutdown cooling mode. The auto-sequence system would introduce this mode following total failure of the decay heat boiler heat rejection system.

#### Mode 3 - 'Y' trains alone - Natural convection gas circulation at pressure

Natural gas convection provides the diverse means of gas circulation when the reactor is pressurised and requires that the main boilers be in use; this is why the main boiler emergency feed system is assigned to the diverse 'Y' trains

### (b) Post-trip cooling in depressurising faults

The characteristics of the principal depressurisation faults are summarised under fault category 4 of Section 4. Owing to the reduced gas density the main boilers have to be employed for shutdown cooling. A major breach of the pressure boundary is an 'Infrequent' event, the frequency being such that the reliability requirements do not call for two independent cooling means. The 'X' and 'Y' circuits are therefore used together to power the gas circulators, their auxiliaries and the main boiler auxiliaries, the four independent circulator/boiler quadrant systems providing sufficient redundancy of cooling.

## 8. Conclusion

This paper has described the way in which the shutdown and cooling systems for the Heysham II and Torness AGRs have been selected in order to meet current UK safety requirements. Fault tree analyses have been used to identify the credible fault sequences, the probabilities of which have been calculated. By this means the relative importance of the various protective systems has been established and redundancy and reliability requirements identified. This systematic approach has led to a balanced design giving protection over the complete spectrum of fault sequences.

ACKNOWLEDGMENT

The principles and designs summarised in this paper were developed by numerous engineers within NPC Ltd in discussion with the UK Generating Boards.

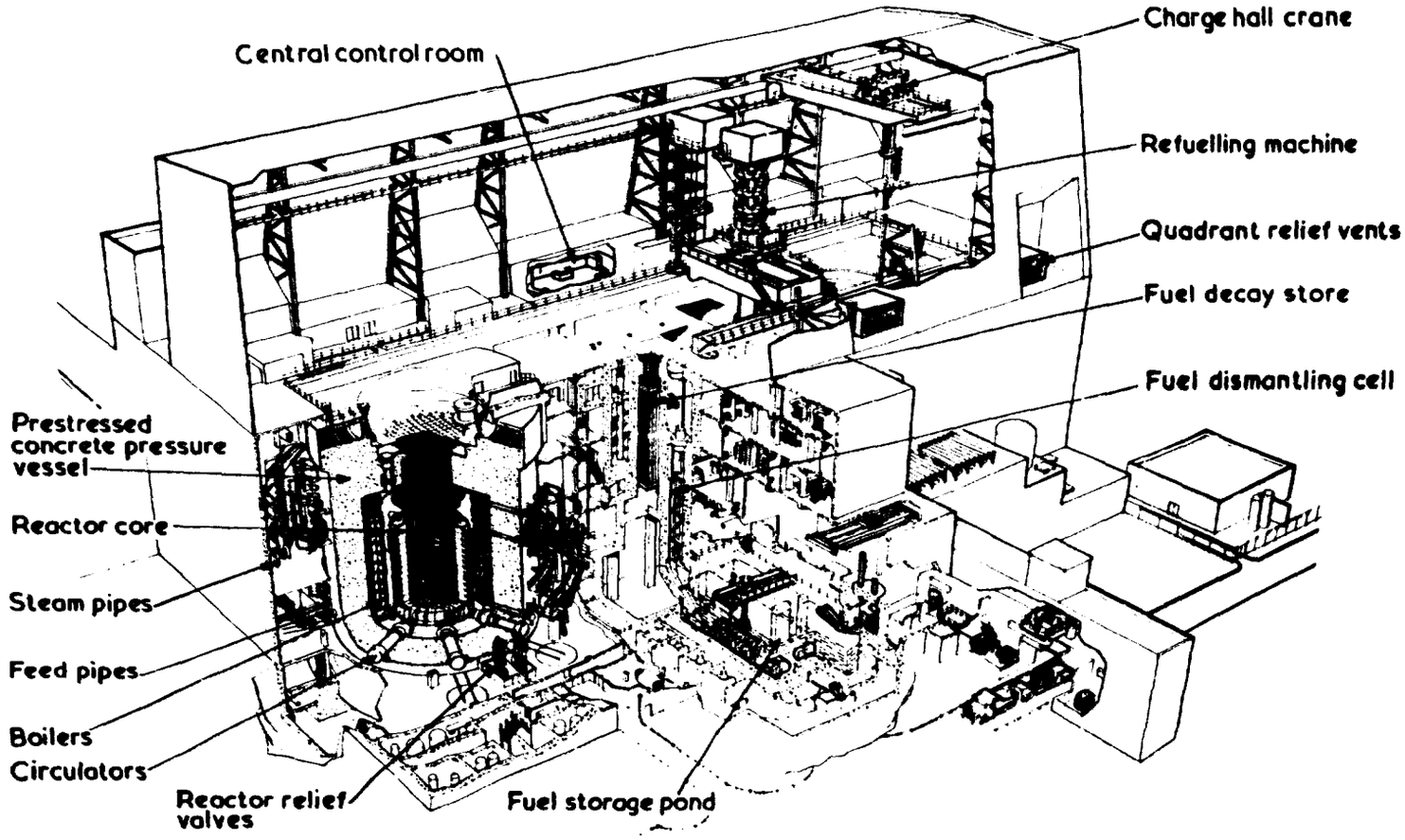
REFERENCES

1. Safety Assessment Principles for Nuclear Power Reactors; Health and Safety Executive, London, April 1979.

2. D R Smith - AGR Design for Heysham II and Torness; Nuclear Energy, Aug 1979, Vol 18, No 4, pp 251-259

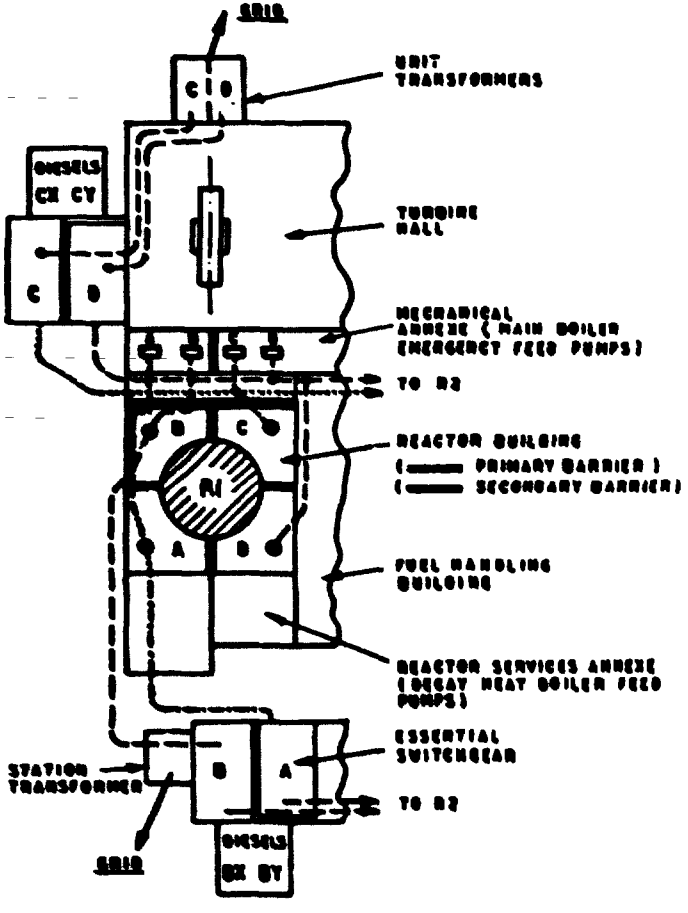
TABLE 1 - SHUTDOWN COOLING PROVISIONS

| Reactor condition | Mode | Train usage | Circulation | Boiler plant | Heat rejection | Minimum allowable number of quadrants |
|---|---|---|---|---|---|---|
| Normal pressure post-trip | 1 | 'X' | Forced 15% speed | Decay heat boilers | Air coolers | 2 ex 4 |
| | 2 | 'X' & 'Y' | Forced 15% speed | Main boilers (diverse) | Steam to atmosphere | 1 ex 4 |
| | 3 | 'Y' | Natural convection (diverse) | Main boilers | Steam to atmosphere | 3 ex 4 |
| Depressurisation faults | - | 'X' & 'Y' | Forced 100% speed | Main boilers | Steam to atmosphere | (a) $\frac{.03m^2 \text{ Breach}}{2 \text{ ex } 4}$ (b) $\frac{.006m^2 \text{ Breach in quadrant}}{1 \text{ ex } 3 \text{ with } CO^2 \text{ pressure support}}$ |

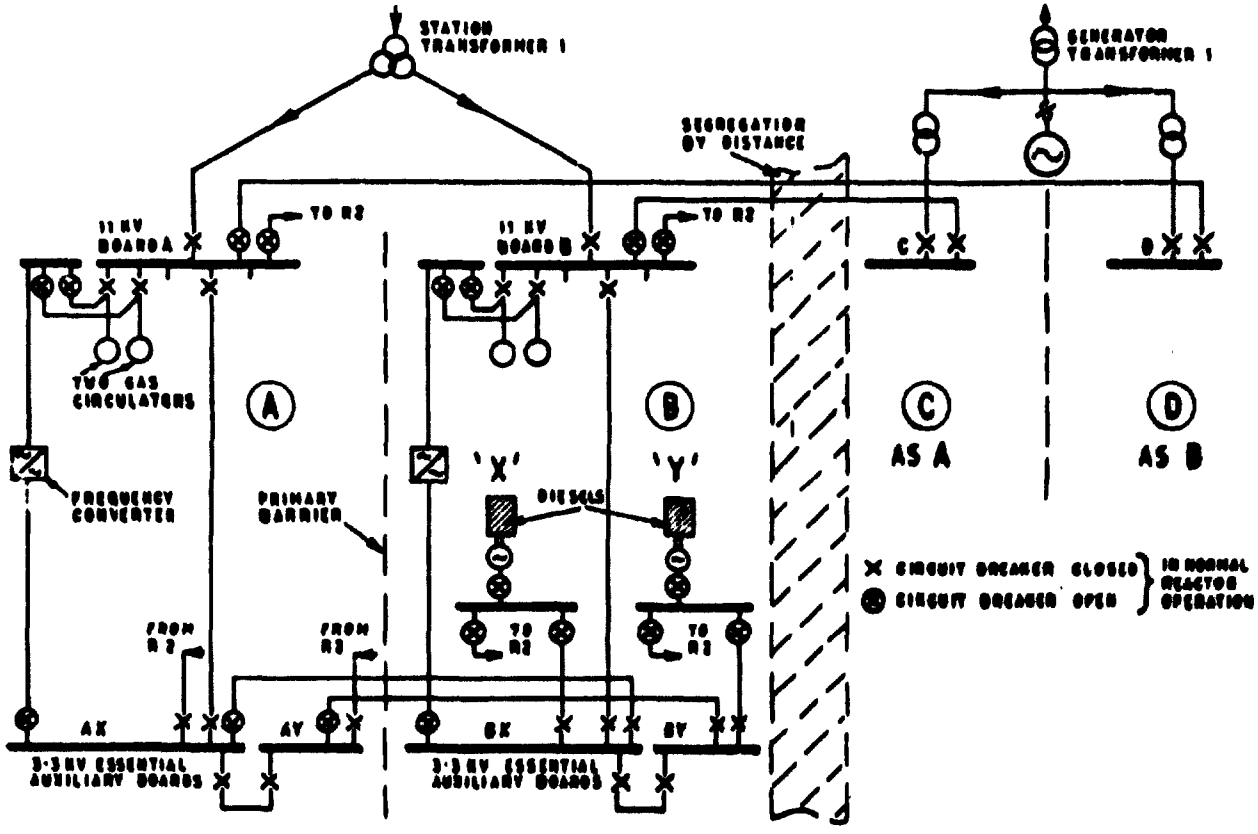



HEYSHAM II / TORNESS A.G.R. NUCLEAR ISLAND

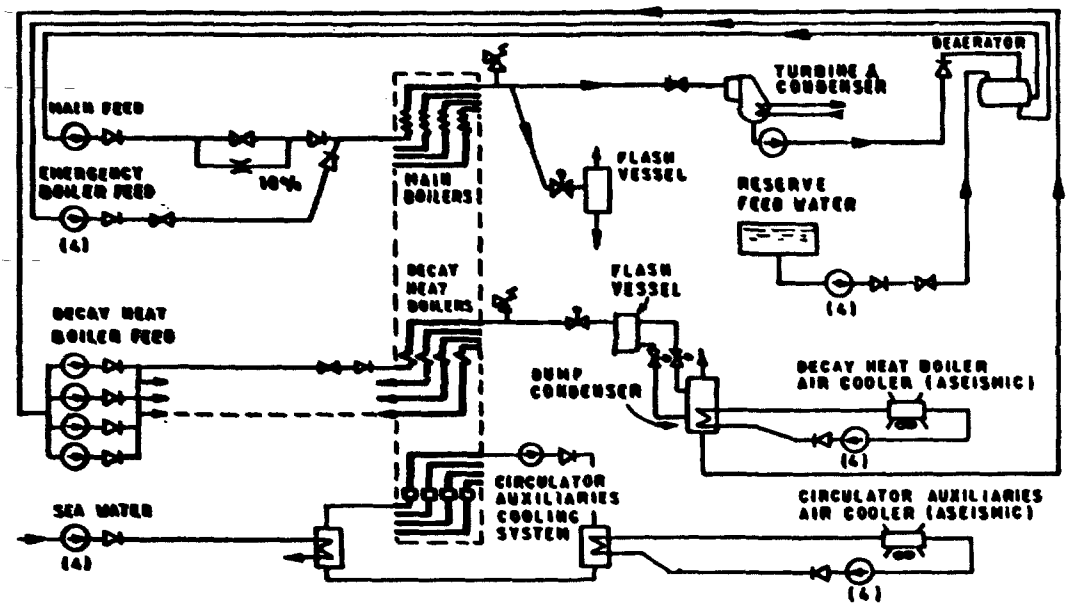
FIG. 1.




SEGREGATION PRINCIPLES (SCHEMATIC) FIG 2




ELECTRICAL SYSTEM REACTOR 1 (SCHEMATIC) FIG 3




COOLING SYSTEMS (SCHEMATIC) FIG 4
(DECAY HEAT BOILER SYSTEM EXTENDED IN DETAIL.
NUMBERS INDICATE PUMP REDUNDANCY)

# THE REACTOR SAFETY STUDY OF EXPERIMENTAL MULTI-PURPOSE VHTR DESIGN

T. YASUNO, S. MITAKE, M. EZAKI, K. SUZUKI
Japan Atomic Energy Research Institute
Tokai Research Establishment
Tokai-Mura
Naka-Gun
Ibaraki-Ken
Japan

## 1. Introduction

Over the past years, the design works of the Experimental Very High Temperature Reactor (VHTR) plant have been conducted at Japan Atomic Energy Research Institute. The conceptual design has been completed and the more detailed design works and the safety analysis of the experimental VHTR plant are continued.

The purposes of design studies are to show the feasibility of the experimental VHTR program, to specify the characteristics and functions of the plant components, to point out the R & D items necessary for the experimental VHTR plant construction, and to analyze the feature of the plant safety.

The experimental VHTR must be provided with the function as follows.

- Demonstration test for future nuclear process heat applications.
- Irradiation test for development of fuels and materials for high-temperature use.
- Confirmation test for large VHTR plant safety.

The design conditions of experimental VHTR were determined due to considerations of the three functions mentioned above. These conditions are summarized in Table 1. Thermal power of 50 MWT is considered combinient for doing the demonstration test, and the coolant temperature 1000°C at the outlet of the reactor is required from a nuclear heat utilization system such as a direct steel making.