GENERAL ATOMIC

GA-A14119

RELIABILITY EVALUATIONS OF GCFR RESIDUAL HEAT REMOVAL SYSTEMS

by

A. P. Kelley, Jr. and P. DeLaquil, III

This is a preprint of a paper to be presented at the International Meeting on Fast Reactor Safety and Related Physics, October 1976, Chicago, Illinois, and to be printed in the Proceedings.

NOTICE

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Energy Research and Development Administration, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights.

Work supported by the U.S. Energy Research and Development Administration, Contract E(04-3)-167, Project Agreement 23.

General Atomic Project 3228

October 1, 1976

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

RELIABILITY EVALUATIONS OF GCFR RESIDUAL HEAT REMOVAL SYSTEMS

A. P. Kelley, Jr.
General Atomic Company
San Diego, California

P. DeLaquil, III
Sandia Laboratories
Livermore, California

ABSTRACT

Using the component reliability data base and accident analysis methodology similar to that employed in the Reactor Safety Study, the authors have separately evaluated the likelihood of failure of core residual heat removal (RHR) for the conceptual design of a 300 MW(e) gas-cooled fast breeder (GCFR) demonstration plant.

Although employing somewhat different methods, these two evaluations have arrived at similar conclusions with regard to the total probability of RHR failure, as well as the relative contributions of particular accident sequences to this total. Both studies have considered a spectrum of initiating events leading to RHR requirements and have quantified potential common cause failures within the RHR systems by use of an empirical factor relating the fraction of component common-cause failures to the total component failure rate. By these methods, the total probability of residual heat removal failure has been estimated as less than 10^{-5} per year, dominated by sequences involving loss of electrical power.

INTRODUCTION

A probabilistic approach to the evaluation of accidents in nuclear power reactors has been considered by a number of investigators over a period of years. Major steps in the use of these approaches have taken place recently with the release of the Reactor Safety Study for light water reactors [1] and recently with the issue of a status report on similar studies for the high temperature gas-cooled reactor [2]. The techniques and data developed by these studies have been separately employed by the authors to evaluate the likelihood of failure of the residual heat removal systems for a 300 MW(e) gas-cooled fast breeder reactor design [3,4]. This paper summarizes the major results of these two studies.

SYSTEM DESCRIPTION

The reliability required of forced-convection shutdown core cooling in the Gas-Cooled Fast Breeder Reactor (GCFR) is achieved through the use of two separate residual-heat-removal (RHR) systems. The normal operational RHR system employs the redundancy of the three main cooling loops and associated steam-driven helium circulators, with heat rejection through the normal power conversion system components or, if necessary, to the atmosphere. The initial shutdown phase of main loop cooling (Fig. 1) lasts for the first half-hour to an hour after shutdown, during which decay heat provides the heat source for generating circulator drive steam. Following this, long-term decay heat removal is initiated with oil-fired auxiliary boilers providing circulator drive steam and the steam generators serving as heat dumps.

A diverse backup safety RHR system, called the Core Auxiliary Cooling System (CACS) (Fig. 2), is provided in case the normal operational RHR system fails. The CACS consists of three independent auxiliary loops with electric-motor-driven circulators and pressurized water loops for heat rejection to the atmosphere.

The operational RHR system is designed so that no single failure of an active component will prevent safe shutdown operation, with components providing the initial shutdown cooling designed as seismic Category 1. The CACS is designed as a seismic Category 1 system with the capability to remove residual core heat following all anticipated transients and postulated accidents. Both systems are designed to remove residual heat under pressurized and depressurized conditions, including accomodation of the design basis depressurization accident (DBDA).

METHODOLOGY

Using the component reliability data base of the Reactor Safety Study [1], the likelihood of failure of the RHR systems was evaluated with two distinct accident modeling approaches. The first utilized event tree accident sequence representations, with the event tree branch points defined by conventional fault tree and reliability diagram methods [4]. The second approach [3] employed an expansion of the event tree method, labeled an event sequence diagram (ESD). Fig. 3 illustrates a portion of an event sequence diagram and shows its similarities and differences to an event tree. The ESD utilizes two major symbols - descriptive blocks (rectangles) and branch points (hexagons). The descriptive blocks represent the possible operating states of the subsystems in the RHR systems. The branch points create distinct accident sequence paths according to the availability states of the redundant RHR subsystems. In the ESD, the main loop RHR system is expanded into its major subsystems, with their success or failure described explicitly. This differs from the event tree approach in which detailed fault trees are used to describe the success or failure of the RHR systems. The ESD describes a large number of accident sequences (of which only a few are shown in Fig. 3) with essentially the same outcome as those of the event tree. The probability of the ESD accident sequence can then be combined to give results analogous to those for the conventional event tree. Because of the complexity of the ESDs developed for the RHR systems, a computerized method was developed and employed for the quantification of the various accident sequence outcomes.

Common Cause Failures

A key item in these studies was the treatment of potential common cause failures within redundant systems which cannot be otherwise identified through analysis of system schematics. Multiple failures resulting from common design or manufacturing defects, operator and maintenance errors, and environmental effects have occurred with too significant a frequency in current nuclear plants to be ignored in any realistic assessment of system failure rates.

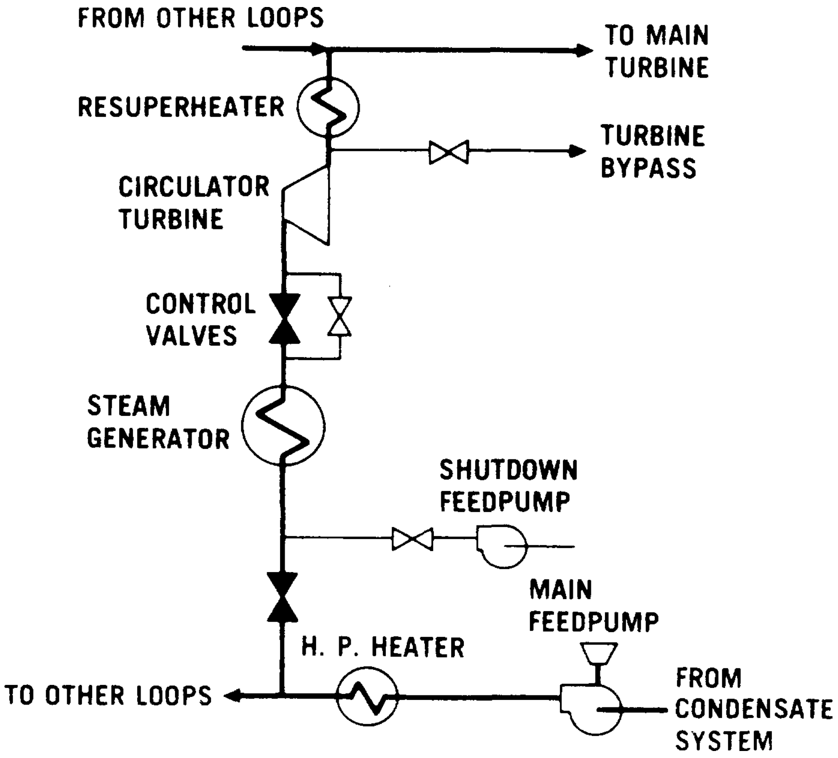


Fig. 1. Shutdown operation of main-loop cooling system

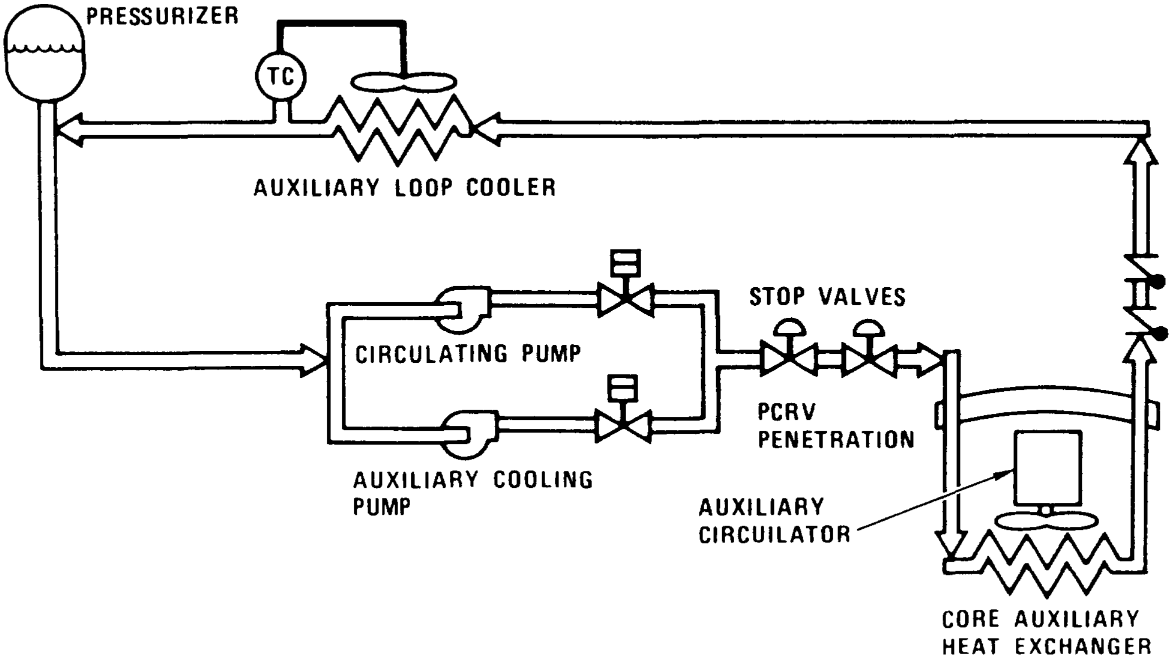
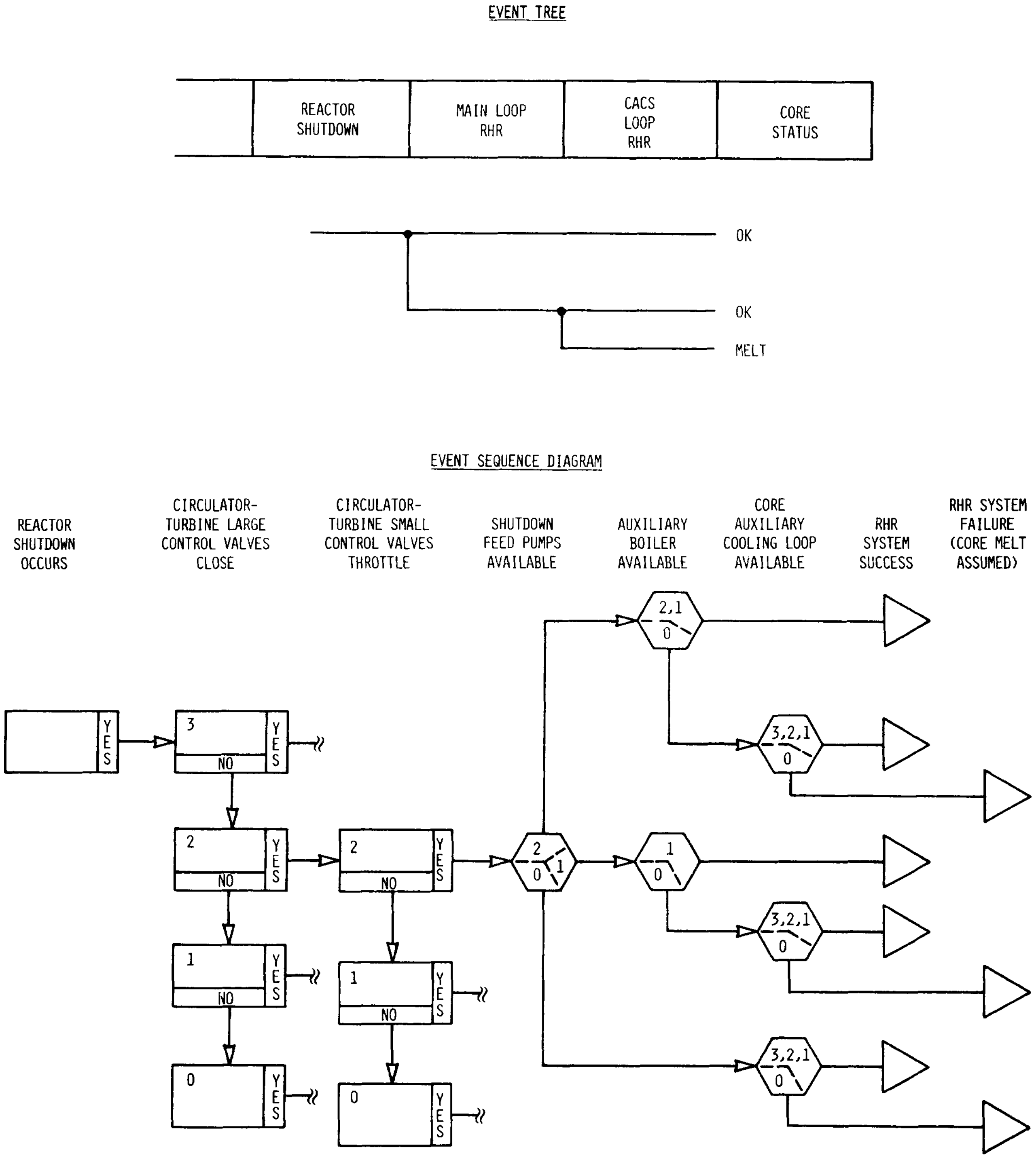


Fig. 2. Auxiliary cooling operation



EVENT TREE

REACTOR SHUTDOWN
MAIN LOOP RHR
CACS LOOP RHR
CORE STATUS
OK
OK
MELT

EVENT SEQUENCE DIAGRAM

REACTOR SHUTDOWN OCCURS
CIRCULATOR-TURBINE LARGE CONTROL VALVES CLOSE
CIRCULATOR-TURBINE SMALL CONTROL VALVES THROTTLE
SHUTDOWN FEED PUMPS AVAILABLE
AUXILIARY BOILER AVAILABLE
CORE AUXILIARY COOLING LOOP AVAILABLE
RHR SYSTEM SUCCESS
RHR SYSTEM FAILURE (CORE MELT ASSUMED)
YES
3
2
1
0
NO
2,1
0
3,2,1

Fig. 3. Event tree and event sequence diagram comparison

This common cause failure potential has been included by use of an empirical factor relating the fraction of common cause failures in a given component to the total component failure rate [5]. Current nuclear experience indicates this factor to be significant, in the range of one-to-ten percent. The inclusion of this common cause factor has proved to have a very major impact on the reliability calculated for the GCFR's redundant cooling systems. Fig. 4 illustrates the use of the common cause factor and some typical values for generic equipment types.

Initiating Events

Another key item in these studies was the identification of key initiating events. Attention was directed at those less likely initiators which might degrade the reliability of one or both RHR systems, as well as more frequent events for which the full diversity of the systems is available. Fig. 5 illustrates the approach taken to identify initiating events within three groups: 1) the more frequent initiating events for which both RHR systems (main cooling loops and CACS) are expected to be available, 2) lower frequency events involving multiple failures of main loop support systems or large external events which cause a loss of the main loop cooling system and require CACS operation, and 3) extremely low frequency events which commonly degrade the reliability of both RHR systems. External forces due to natural or man-made hazards, particularly seismic events, have been considered to determine whether such events could significantly impact the results obtained for intrinsic plant equipment failures.

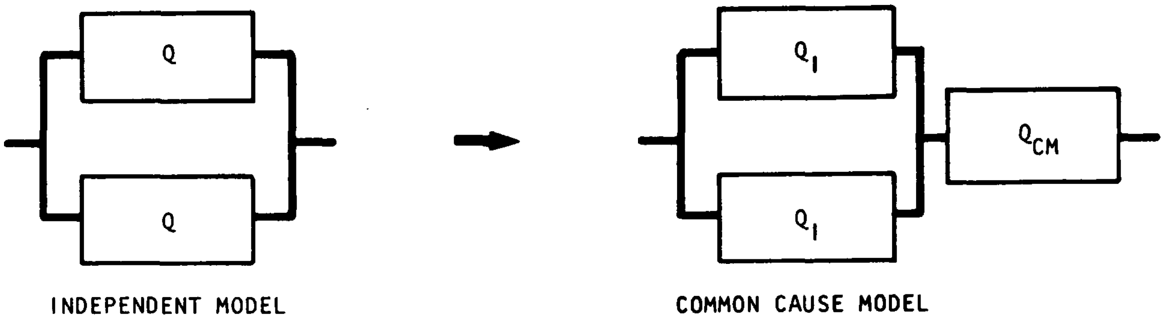
RESULTS

In both of the above described approaches, the probability of residual heat removal failure was evaluated for a spectrum of initiating events. Fig. 6 summarizes, in event tree format, the more significant accident sequences considered within each of the three initiating event groups identified by Fig. 5. To display the results of the two studies, the accident sequence probabilities shown in the right hand column of Fig. 6 have been rounded to the nearest half-order of magnitude. These probability evaluations include contributions from random equipment failures, test and maintenance unavailabilities, and common cause failures. The total probability of RHR failure for all the initiating events and accident sequences analyzed is shown to be less than 10^{-5} per year.

Innocuous Trips

Sequences initiated by an innocuous reactor trip event have been found to dominate the first group of initiators for which two RHR systems are available. Such a reactor trip event may be caused by protection system malfunctions, operator errors, or other such innocuous mechanisms. The event is significant for its relatively high frequency of unscheduled demands for residual heat removal.

On the basis of an average of three innocuous trip events per year, a total probability of approximately $1x10^{-6}$ per year has been assessed for RHR failure. Detailed reliability model and event sequence diagram predictions give the unavailability of the main and CACS RHR functions as approximately 10^{-3} and $3x10^{-4}$, respectively.



DEFINE $Q = Q_I + Q_{CM}$

WHERE $Q_{CM} = \beta \cdot Q$

$Q_I = (1 - \beta) \cdot Q$

AND β = FRACTION OF UNIT FAILURES WHICH ARE COMMON CAUSE

THEN SYSTEM FAILURE PROBABILITY $= Q_I^2 + Q_{CM}$

$$\approx \beta \cdot Q(Q_{CM} >> Q_I^2)$$

TYPICAL Q AND β VALUES

UNIT	Q	β
DIESELS	3×10^{-2}	0.08
VALVES	1×10^{-3}	0.06
PUMPS	1×10^{-3}	0.01
RX TRIP CHANNELS	1×10^{-2}	0.09
PRESSURE SWITCHES	1×10^{-4}	0.28
ALL EQUIPMENT	--	0.08

Fig. 4. Common cause factor approach illustration

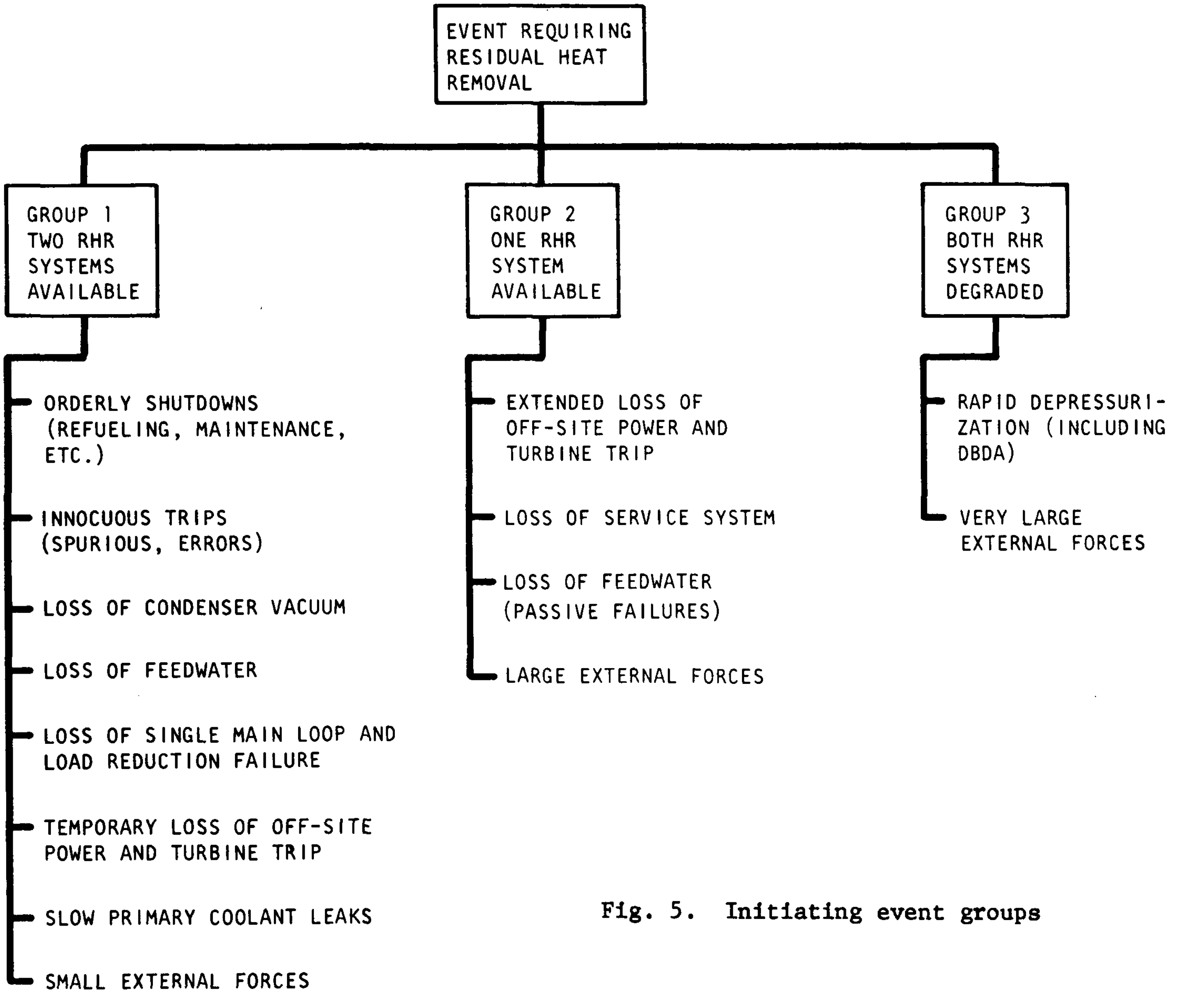

EVENT REQUIRING RESIDUAL HEAT REMOVAL
GROUP 1 TWO RHR SYSTEMS AVAILABLE
GROUP 2 ONE RHR SYSTEM AVAILABLE
GROUP 3 BOTH RHR SYSTEMS DEGRADED
ORDERLY SHUTDOWNS (REFUELING, MAINTENANCE, ETC.)
INNOCUOUS TRIPS (SPURIOUS, ERRORS)
LOSS OF CONDENSER VACUUM
LOSS OF FEEDWATER
LOSS OF SINGLE MAIN LOOP AND LOAD REDUCTION FAILURE
TEMPORARY LOSS OF OFF-SITE POWER AND TURBINE TRIP
SLOW PRIMARY COOLANT LEAKS
SMALL EXTERNAL FORCES
EXTENDED LOSS OF OFF-SITE POWER AND TURBINE TRIP
LOSS OF SERVICE SYSTEM
LOSS OF FEEDWATER (PASSIVE FAILURES)
LARGE EXTERNAL FORCES
RAPID DEPRESSURIZATION (INCLUDING DBDA)
VERY LARGE EXTERNAL FORCES

Fig. 5. Initiating event groups

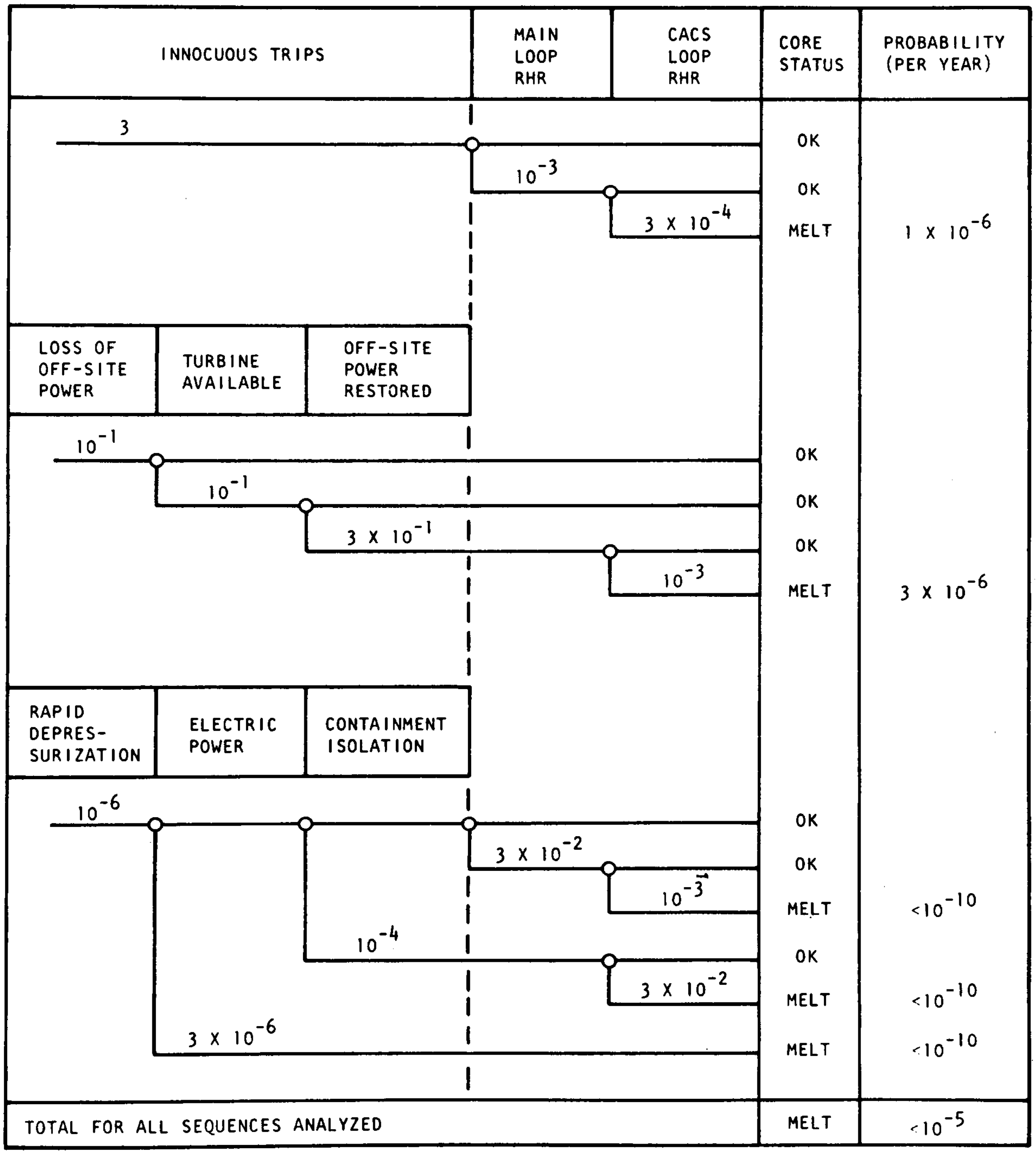


Fig. 6. Significant accident event sequences ending in RHR system failure

Loss of Preferred Electrical Power

Sequences initiated by a loss of preferred electrical power have been found to dominate the second group of initiators which cause a loss of the main loop RHR function. Since the main turbine generator is capable of remaining on line supplying the plant electrical requirements following loss of offsite power and load rejection, a loss of preferred power for the GCFR requires failure of both the offsite power source and onsite turbine generator power. The probability of a loss of preferred power is therefore the product of the probability of offsite power loss (10^{-1}/yr based on U.S. nuclear plant experience) and turbine trip (10^{-1} based on British gas-cooled reactor experience) for a total of 10^{-2} per year.

Following the reactor shutdown which accompanies a loss of preferred power event, heat removal can be provided by the main loop cooling system using the steam generator water inventory for approximately one-half hour without an AC electrical supply. Failure to restore offsite power within one-half hour (a .3 probability based on U.S. nuclear plant experience) would cause a loss of the main loop RHR function, placing a demand on the CACS. The availability of the CACS, given this demand is dependent on the availability of at least one of the three emergency diesel generators. The common mode failure of the emergency diesels is assessed as 10^{-3}. The total probability of RHR failure is the product of the above events or $3\text{x}10^{-6}$ per year.

Depressurization Accident

The last event tree in Fig. 6 summarizes the event sequences leading to RHR failure following a rapid depressurization event, the design basis accident for the GCFR cooling systems. Because of the total containment of the cooling systems, except for small diameter instrument and process lines, within the prestressed concrete reactor vessel (PCRV), the likelihood of such an event is expected to be extremely low (assessed as 10^{-6} per year). Further, the capability of either of the two diverse RHR systems to respond to this event causes the probability of cooling failure, given the rapid depressurization, to be extremely small.

Although many paths have been analyzed which lead to RHR failure following a depressurization accident, such sequences have proved to contribute insignificantly to the total cooling failure probability. Severe external forces, particularly earthquakes, may more likely lead to RHR failure within the third initiating event group, although not with a frequency comparable to the dominant sequences in the other event groups.

Other Accident Initiators

The total probability of RHR system failure for all accident sequences identified has been determined as less than 10^{-5} per year, which compares favorably with the $6\text{x}10^{-5}$ value calculated by the Reactor Safety Study group for light water reactor systems. The error range of both values has been assessed as less than a factor of ten.

Sensitivity studies have been done to determine the effect of potential shutdown cooling system design changes to reduce the likelihood of failure, if deemed necessary. In particular, decreasing the RHR system's reliance on AC electrical power supplies has been shown to be useful. By capitalizing on light water reactor experience in the U.S. and gas cooled reactor experience in Europe to improve equipment reliability and to reduce the potential for common mode failures, and by incorporating design improvements identified as a result of system reliability studies during the design's evolution, the ultimate RHR system failure probability for the GCFR demonstration plant might be significantly reduced.

ACKNOWLEDGMENTS

The work at General Atomic was performed under Contract E(04-3)-167, Project Agreement 23, of the U.S. Energy Research and Development Administration (ERDA). Work performed by P. DeLaquil was under the direction of Professors N. C. Rasmussen and D. D. Lanning, Dept. of Nuclear Engineering, M.I.T.

REFERENCES

1. "Reactor Safety Study - An Assessment of Accident Risks in U.S. Commerical Nuclear Power Plants," USNRC Report WASH-1400 (NUREG-75/014) (1975).

2. "HTGR Accident Initiation and Progression Analysis Status Report," Report GA-A13617, General Atomic Company (1975).

3. P. DELAQUIL III et al, "An Accident Probability Analysis and Design Evaluation of the Gas-Cooled Fast Breeder Reactor Demonstration Plant," Report MITNE-184, Massachusetts Institute of Technology (1976).

4. "GCFR Reactor Safety Progress Report for the Period July 1, 1974 through June 30, 1975," Report GA-A13703, General Atomic Company (1975).

5. K. N. FLEMING, "A Reliability Model for Common Mode Failures in Redundant Safety Systems," Proceedings of the Sixth Annual Pittsburgh Conference on Modeling and Simulation, April 1975 (General Atomic Report GA-A13284).