

---

---

## PROBABILISTIC RISK ASSESSMENT OF HTGRs

K.N. FLEMING, W.J. HOUGHTON, G.W. HANNAMAN, V. JOKSIMOVIC

General Atomic Company  
San Diego, California  
United States of America

### ABSTRACT

Probabilistic Risk Assessment methods have been applied to gas-cooled reactors for more than a decade and to HTGRs for more than six years in the programs sponsored by the U.S. Department of Energy. Significant advancements to the development of PRA methodology in these programs are summarized as are the specific applications of the methods to HTGRs. Emphasis here is on PRA as a tool for evaluating HTGR design options. Current work and future directions are also discussed.

### INTRODUCTION

Much has been written about probabilistic risk assessment (PRA) since the release of the Reactor Safety Study report, WASH-1400, (Ref. 1). It is well known that this study was the first comprehensive application of PRA methodology and represented a significant advance in the state-of-the-art in light-water reactor (LWR) safety assessment. The roots of PRA in the nuclear reactor field actually date back about a decade earlier to the pioneering contributions of Farmer (Ref. 2). Subsequently, important contributions to methodology development were made, for example, those by Mulvihill (Ref. 3), Joksimovic (Ref. 4), and Garrick (Ref. 5).

Because of WASH-1400 and its acknowledged breakthrough in obtaining the first set of comprehensive results, PRA in the U.S. has been closely associated with light-water reactor safety assessment in recent years. However, the first applications of PRA concepts in the nuclear reactor safety field have been to gas-cooled reactors in the United Kingdom as exemplified by papers presented at an IAEA Conference in 1967, and at a British Nuclear Energy Society Symposium in 1969. These papers included, among others, Farmer's pioneering work as well as an application to *Advances Gas-Cooled Reactors* by Cave and Holmes (Ref. 6).

The application of PRA to gas-cooled reactors continues in the U.S. as a major part of the HTGR program. In view of the timing, scale, and maturity of this effort which began in 1974, it is safe to say that the

HTGR design and development has benefited more from PRA than any other nuclear reactor system. A number of technical reports have been published including GA-A15000 (Ref. 7), which is the most comprehensive report available on PRA applications of HTGR safety. The purpose of this paper is to summarize some more recent advances in PRA in its application to the HTGR. An earlier perspective on this subject can be found in Reference 8.

PRA is a systematic, disciplined method for quantifying the losses or gains from events which can occur at random points in time. It evaluates and ranks various outcomes of an event or alternative decision choices. Practitioners regard PRA as the science of quantifying uncertainty. Further perspective as to what PRA is and is not is provided in a recent paper by Joksimovic and Vesely (Ref. 9).

In its application to nuclear reactor safety, PRA provides a comprehensive framework for estimating and understanding the risks of reactor accidents by providing answers or describing the state of knowledge associated with three basic questions:

1. What can go wrong?
2. How frequently is it expected to happen?
3. What would be its consequences?

One of the objectives of the HTGR risk assessment effort has been to develop and refine the methodology in order to provide better answers to these questions. Specific advancements in this area are discussed in the next section.

The potential applications of the knowledge obtained with PRA are limited only by the number of different types of decisions which are encountered. Applications of PRA in the HTGR program, in addition to public risk assessment, have included design options evaluation, safety research and development prioritization (Ref. 10), reactor siting (Ref. 11) and licensing (Ref. 12), plant productivity improvement and investment risk assessment. In support of these activities, the reliability data base was expanded on gas-cooled reactor components (Ref. 13). The main application to be discussed in this paper is the evaluation of design options.

### METHODOLOGY ADVANCEMENTS

Although PRA has not yet matured to the extent that the methodology has become standardized, there are certain general aspects of the approach utilized in WASH-1400 which have reappeared in other risk assessment applications including that of the HTGR. With regard to Question 1 above, the topology of accident sequences is generally identified with a collection of initiating events and event trees. The latter are used to enumerate a wide spectrum of accident scenarios that can be hypothesized to stem from the initiating event. Answers to Question 2 are provided by a number of different types of probability models including fault trees and their equivalents which are derived from elementary probability theory and borrowed from the field of systems reliability. The ability to predict accident consequences in answer to Question 3 essentially depends on that to model fission product transport

and associated physical processes. Though these processes are highly dependent on the type of reactor for that part of the transport path inside the reactor building, comparisons indicate that several of the available atmospheric dispersion models tend to produce consistent results (Ref. 7).

Beyond the general elements described above, a number of significant advancements have been made in some of the detailed aspects of the methodology since WASH-1400 was published. Advancements attributed to HTGR programs are summarized in Table 1. Of these, the most important in terms of their potential for changing previously computed risk assessment profiles are the treatment of common cause failures (Ref. 14) including major fires (Ref. 15) and the quantification of consequence uncertainties (Ref. 16). The latter includes those associated with modeling the physical processes of radioactivity transport. The other advancements of note include the use of fault trees to structure the process of selecting initiating events, the integration of accident simulation and system analysis tasks in constructing the event trees and the use of a time-dependent operator response model (Ref. 17).

One of the earliest contributions to PRA methodology in the HTGR risk study was the development of the Beta Factor method of common cause failure analysis (Ref. 18). This method is now widely used to estimate the reliability characteristics of redundant systems subject to multiple, dependent or common cause failures as well as the independent failures which are usually modeled. In addition to requiring the usual input data such as component failure rates, the degree of failure coupling associated with common cause failures is measured directly in terms of a parameter, Beta, defined as the ratio of the common cause failure rate to the total component failure rate.

A sample of the types of common cause failures which have occurred and which have been accounted for using the Beta Factor method in the HTGR risk study is presented in Table 2. The existence of a significant amount of data such as these runs contrary to a popular misconception that there are inadequate data available to quantify common cause failure probabilities. In order to obtain common cause failure information from the data base, however, it is necessary to invest a significant fraction of the available resources for application of PRA to the collection and interpretation of available data as exemplified by Reference 13. With the use of data such as those in Table 2 in conjunction with independent failure data, common mode coupling factors, or Beta factors, have been estimated for generic component types. Estimates of the pooled value of Beta averaged over the available experience base have ranged from less than .01 to more than .5 depending on the type of component and failure mode.

Another significant contribution in the area of common cause failure analysis was the development of a comprehensive approach for the treatment of major fires (Ref. 15). Several aspects of the PRA methodology were specialized to take into account some of the unique characteristics of fires important to determining their risk. Two methods were developed to screen the plant layout to identify the most important fire locations in terms of the likelihood of a major fire and the location's inventory of safety related equipment, cables and piping. Data on fires in nuclear

plants was compiled and analyzed in terms of initiation frequency, propagation distances and burn time. This information was incorporated into a fire propagation model which was used in conjunction with detailed fault trees to estimate the location-dependent common cause failure probabilities. The fire methodology was applied to the same HTGR steam cycle design which has been extensively analyzed throughout the HTGR risk study. 69

One of the most important facets of the PRA methodology developed in the Reactor Safety Study was the analysis of uncertainties in the prediction of accident occurrence frequencies. In the HTGR programs the Monte Carlo method of error propagation utilized in the RSS was adopted, significant improvements to the computer program developed to implement it were made (Ref. 19) and, most importantly, the application of this technique was extended to the analysis of uncertainties in the prediction of accident consequences.

The method begins with a series of point estimate consequence calculations using detailed deterministic computer models. Simplified consequence models are then derived which describe the key underlying physical processes in terms of relatively small set of important variables. In view of the large uncertainties in the input data, much of the fine detail and complexity in the existing computer models can be eliminated from these sample models without introducing significant errors. The Monte Carlo method of error propagation is then applied in which the simplified models are executed tens of thousands of trials. In each trial, a random value is selected from an uncertainty distribution for each of the key model variables. Some of the key variables whose uncertainty has been analyzed in this way for the HTGR are described in Ref. 16. One of the key results of this analysis is the increased importance of uncertainties in predicting the magnitude of releases during accidents in comparison with meteorological variabilities which heretofore have been the focus of consequence uncertainty analysis in PRA.

#### Salient Applications to HTGRs

A major portion of the HTGR risk assessment study has been devoted to application of the PRA methodology to a particular design of a steam cycle plant for electricity generation designed in 1975. A number of reports were published on the results at key stages in the study including GA-A15000 (Ref. 7), which provides the most complete description of the analyses of potential HTGR accidents involving core overheating. Subsequently, the study discussed earlier on major fires was carried out which enhanced the completeness of accident scenarios assessed for the 1975 steam cycle plant. The overall risk curves for this plant are presented in Figure 1 in which the accidents involving major fires are plotted separately. The dominance of fires in the low frequency part of the accident spectrum underlines their importance as a common cause failure of multiple systems. It was determined that enhanced physical separation of electrical cables which is provided in more recent HTGR designs would have diminished the relative significance of fires. The risk curve derived from the remaining set of initiating events analyzed in GA-A15000 (Ref. 7) is used as a basis for comparison in the analysis of various design systems and variations such as those described below.

The design of the steam cycle HTGR has evolved somewhat since 1975. In 1979, a description of a 900 MW(e) plant was published. The risk profile for this plant was calculated by transforming the work in GA-A15000 (Ref. 7) in accord with the changes to the design features. One noteworthy change was that the new design did not specify reheat of main loop steam by means of primary helium coolant. Therefore, the reheater leak events on the risk plot were removed. There were several changes which affected core heat-up risks slightly, but these only raised consequences of dominant accident sequences by about a factor of 1.5 and frequencies by about a factor of 2.

A smaller steam cycle/cogeneration plant of 1170 MW(t) has also been designed, and a brief risk analysis was performed for it. The analysis was based on GA-A15000 (Ref. 7) and on the above mentioned assessment of the 900 MW(e) which was very similar except for power level.

As safety became more important in the aftermath of the accident at Three Mile Island, interest arose as to how the HTGR-SC could be made safer even though many assessments showed it to be a very safe concept already. The investigation was conducted using probabilistic risk assessment techniques. A number of combinations of design options were analyzed to determine which options could satisfy the quantitative safety criteria that had been chosen. Since the criteria were very stringent, one of the options selected by the process was the addition of natural circulation core cooling in order to reduce the projected frequency of core heatup to even lower values than had been calculated previously. The designs studied for the natural circulation loops were conceptual. Therefore, more design effort to clarify their feasibility and cost is needed and will be applied next year. But the probabilistic study assisted greatly in clarifying the reliability problems and requirements for decay heat removal systems under accident conditions. This study demonstrated that it is necessary to apply the PRA approach at the early conceptual stage of design to achieve a significant increase in safety.

Probabilistic safety techniques have been applied to the Gas Turbine concept on a more limited basis. This version of the HTGR has a helium closed cycle loop with the turbo-compressor inside the prestressed concrete reactor vessel. The probabilistic analysis was applied to the question of turbomachine failure. The missiles from the rotor cannot penetrate enough concrete to damage the reactor core and cooling systems, but the pressure transients associated with shaft failures are important to consider. Some design changes in safety valve systems were identified and made on the basis of PRA assessments to reduce frequencies of turbomachine overspeed. Event trees constructed for major failures of the turbomachine were found to be helpful in clarifying design problems with design and project people. Misunderstandings were uncovered and resolved, and a list of design improvements was generated to provide a balanced design against these types of accidents.

Another example where PRA has provided a more rational basis for decision making at the early stages of conceptual design has occurred in the development of a VHTR process heat/cogeneration plant. One of these decisions

was the selection of a configuration of core cooling loops for decay heat removal. It was concluded, in this evaluation, that the design alternative with the lowest cost among those evaluated had the greatest potential for achieving high reliability. In addition, it was found that the use of pony motors as a backup to the main drives on the helium circulators in conjunction with specific system configurations had little reliability improvement impact. Current PRA applications to the VHTR involve the investigation of potential accident scenarios involving the chemical processes, e.g., hydrogen production, which utilize the process heat.

PRA has also served as a vehicle for feedback of operational experience data from the Fort St. Vrain HTGR Demonstration Plant to the design of the next generation of HTGR plants. The basic tools of PRA such as event trees and fault trees have been employed to provide a systematic review of this experience and to identify precursors of potential accident scenarios. The probability of occurrence of these scenarios should be significantly reduced in the future as PRA information is incorporated into operator retraining programs.

#### CURRENT WORK AND FUTURE DIRECTIONS

The currently perceived trajectory of future applications of PRA in the HTGR programs calls for further refinement of the methodology, enhanced completeness in the coverage of potential accident scenarios for each of the HTGR designs under consideration and application of the PRA methodology to new areas. One of the most important new areas in which work has already been started is the assessment of the financial risks to the utilities, lenders and insurance industry associated with potential accidents resulting in costly plant damage and extended outages. Early indications from this effort are that the PRA methods developed previously for public health and safety assessment are generally applicable to assessment of investment risk. An equally important new area is the refinement of proposed Quantitative Safety Goals (Ref. 20) which include numerical targets to meet for the reliability characteristics of reactor systems. Work is in progress on the use of PRA to establish siting requirements for HTGRs in the light of those proposed for LWRs in NUREG-0625 (Ref. 11).

Although the PRA methodology has already benefited from a substantial amount of development effort, continued refinements are needed in support of the extension to wider applications and because of the desire for enhanced completeness. Although specific tasks in next year's HTGR programs have not been developed as of yet, it is thought worthwhile to mention some of the candidate areas for further methodology advancement. A partial list includes treatment of intersystem dependencies in event tree quantification, effects of acts of sabotage and terrorism, human factors, external actions to mitigate long term accident consequences, and improved methods for treatment of uncertainties. The ultimate benefits of continuing the development of PRA and applying it to the HTGR will be realized in terms of continued advancement in the state-of-the-art of designing and operating safe nuclear reactors.

#### ACKNOWLEDGEMENT

This work was sponsored by the U.S. Department of Energy under Contract DE-AT03-76ET35300 with the San Francisco Operations Office.

#### REFERENCES

1. Reactor Safety Study - WASH-1400 (NUREG-75/014) October (1975).
2. F. R. Farmer, "Siting Criteria - A New Approach", Proceedings IAEA Symposium on Containment and Siting (1967)
3. R. J. Mulvihill, et al, "A Probabilistic Methodology for the Safety Analysis of Nuclear Power Reactors", USAEC Report No. SAN-570-2, (1966).
4. V. Joksimovic, "Fault Analysis of Nuclear Reactors" PhD Thesis. Univ. of London, (1970).
5. B. J. Garrick, "Principles of Unified Systems Safety Analysis", Nuclear Engineering and Design 13(1970) North Holland Publishing Co.
6. L. Cave and R. E. Holmes, "Suitability of AGRs for Urban Siting", Proceedings IAEA Symposium on Containment and Siting (1967).
7. "HTGR Accident Initiation and Progression Analysis- Phase II Risk Assessment", General Atomic Report for U.S. Dept. of Energy, No. GA-A1500, April, 1978.
8. V. Joksimovic and K. N. Fleming, "Applications of Probabilistic Risk Assessment in the Development of HTGR Technology", Proceedings of the ANS Thermal Reactor Safety Meeting, Sun Valley, 1978.
9. V. Joksimovic and W. E. Vesely, "Use of PRA in Evaluating Safety of Nuclear Power", Proceedings IEEE Region 6 Conf., San Diego, (1980).
10. A. W. Barsell, et al, "HTGR Safety Research Program," paper presented at this meeting.
11. Report to be published by General Atomic on NUREG-0625 and its Implications on HTGR Siting.
12. W. J. Houghton, "Licensing Topical Report: Application of PRA in the Selection of Design Basis Accidents," General Atomic Report for U.S. Dept. of Energy, No. GA-A15314, June 1980.
13. G. W. Hannaman, "GCR Reliability Data Bank Status Report", General Atomic Report GA-A14839, July 1978.
14. K. N. Fleming and P. H. Raabe, "A Comparison of Three Methods for the Quantitative Analysis of Common Cause Failures", Proceedings of the ANS Meeting on Probabilistic Safety Analysis, Los Angeles, 1978.
15. K. N. Fleming, W. J. Houghton and F. P. Scaletta, "A Methodology for Risk Assessment of Major Fires and its Application to an HTGR Plant", General Atomic Report for U.S. Dept. of Energy No. GA-A15402, (1979).
16. D. J. Wakefield and A. W. Barsell, "Monte Carlo Method for Uncertainty Analysis of HTGR Accident Consequences," Proceedings ANS Thermal Reactor Safety Meeting, Knoxville (1980).
17. K. N. Fleming, G. W. Hannaman and F. A. Silady, "Treatment of Operator Actions in HTGR Risk Assessment Study," Trans. ANS, San Francisco, (1979).
18. K. N. Fleming, "A Reliability Model for Common Mode Failures in Redundant Safety Systems," Proceedings of the Sixth Annual Pittsburgh Conference in Modeling and Simulation: (1975).
19. J. J. Cairns and K. N. Fleming, "STADIC - A Computer Code for Combining Probability Distributions," General Atomic Report for U.S. Dept. of Energy, No. GA-A14055 (1977).
20. V. Joksimovic, "Statement on Quantitative Safety Goals Before the ACRS Subcommittee on Reliability and Probabilistic Assessment," Los Angeles, CA., July 1, 1980.

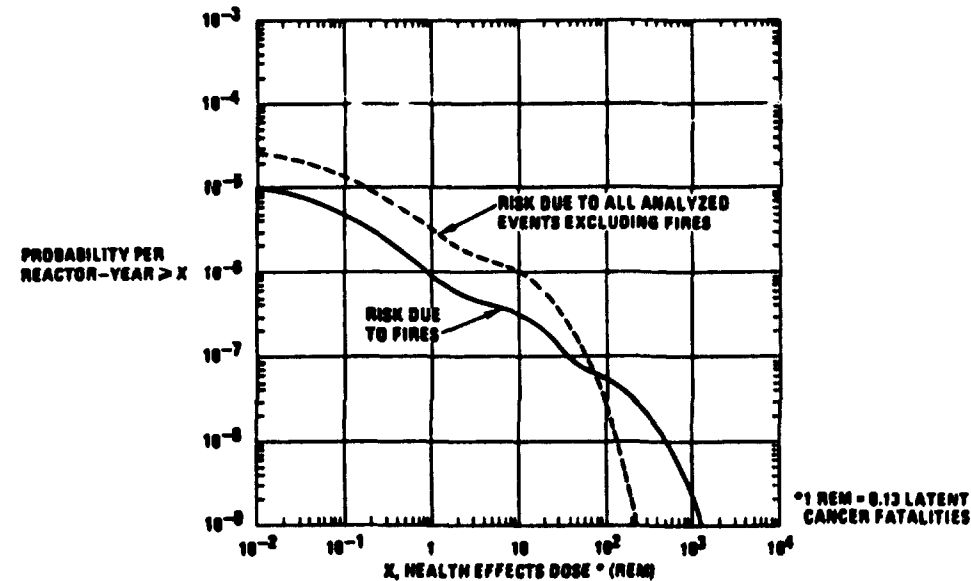


Figure 1 Overall HTGR Risk Assessment<sup>(7)</sup> for 1975 Steam Cycle Plant with Fire Contribution<sup>(15)</sup> shown separately.

Table 1. Contributions to PRA Methodology in HTGR Risk Assessment Study.

Fundamental Safety Question	Applicable Element of PRA Methodology	Methodology Advancements
o What can go wrong?	o Initiating event selection. o Event tree construction.	o Fault tree analysis of barriers. o Treatment of major fires o Integration of physical processes.
o How frequently is it expected to happen?	o Event frequency estimation.	o Beta Factor Common Cause Failure Method (10). o Fire propagation model o Time-dependent operator response model
o What would be its consequences?	o Accident consequence assessment.	o Monte Carlo uncertainty analysis o Analysis of radioactivity transport.

Table 2. Some instances of common cause failure used in estimating component beta-factors.

Station	Date	Description of Common Cause Failure Incident
Three Mile Island-2	3/28/78	Redundant auxiliary feedwater system inadvertently valved out, ECCS turned off by operator, containment isolation design error.
Kewaunee	11/5/75	All 3 auxiliary feedwater pumps fail due to clogging of strainers.
Oyster Creek	1/5/77	Both diesel fuel transfer pumps failed to start due to dirty switch contacts.
Quad Cities	6/17/72	17 pumps in 4 systems, including the RHR and DG cooling water system, failed as the result of a flooded room.
Millstone 2	5/15/77	Both diesel-generators failed to run after start, fuel supply lines inadvertently left valved out.
Haddam Neck	4/27/68	All three diesel-generator units tripped off-line following start subsequent to loss of offsite power, action of voltage regulator and overload protection.