DRAFT

Review of the Standard Modular High Temperature Gas Cooled Reactor Probabilistic Risk Assessment

J.W. Minarick
E.M. Dougherty
S.J. Hurrell

Science Applications International Corporation

October 16, 1987

DRAFT

Review of the Standard Modular High Temperature Gas Cooled Reactor Probabilistic Risk Assessment

J.W. Minarick
E.M. Dougherty
S.J. Hurrell

Science Applications International Corporation

October 16, 1987

Table of Contents

1.0 Introduction

A review was performed of the probabilistic risk assessment (PRA) of the modular high temperature gas-cooled reactor (MHTGR).[1] This review was intended to assess the overall adequacy of the PRA, the credibility of its results, and the uncertainty of these results with respect to contemporary LWR PRAs, as well as to identify those items which require further analysis prior to effective use of the PRA results in the NRC review of the MHTGR design. The overall adequacy of the PRA was assessed based on the review critieria described in Appendix A. A summary of the assessed adequacy of the PRA, based on this review, is presented in Table 1-1. As a result of the review, it is concluded that

- the absense of a detailed design to assess precludes the identification of some potential sequences which have been shown to be of major importance on LWRs,

- some sequences which are not important in LWRs because of their low relative frequency may be important contributors to MHTGR risk and may require modeling, if estimated sequence frequencies remain significantly lower than for LWRs, and

- the truncation method utilized in the PRA provides little confidence that dominant risk-related sequences have been identified.

The basis for the PRA assessment is the standard MHTGR design as presented in the Preliminary Safety Information Document (PSID)[2]. The MHTGR plant is comprised of four reactor modules and two turbine generator sets which combine to achieve a nominal plant rating of 558 MW(e). Each reactor module is housed in a vertical cylindrical concrete enclosure which is fully embedded in the earth. Each module contains separate reactor and steam generator vessels connected by a horizontal coaxial cross duct. The reactor core is composed of an annular array of fueled prismatic graphite blocks.

Section 2 of this report summarizes the intent in performing the PRA, the methodology and data utilized, plus the results of the analysis as described in Reference 1. Section 3 summarizes major issues considered unresolved based on this review of the PRA. Sections 4, 5, and 6 describe the selection of initiating events and the development of event trees and fault trees, respectively. Section 7 describes accident sequences identified in the PRA. Section 8 discusses insights gleaned from the PRA review.

Table 1-1. A Summary of Overall MHTGR PRA Adequacy.

Areas	Credibility	Completeness	Uncertainty
Plant representation	**moderate**	**moderate**	**high**
plant definition	moderate	low	high
system success criteria	moderate	moderate	high
system supports	moderate	moderate	moderate
dependencies	moderate	moderate	high
internal initiators	moderate	moderate	moderate
plant response events	high	high	moderate
system models	moderate	moderate	moderate
human interface models	low	low	high
Results	**low**	**low**	**high**
core damage cutsets	low	low	high
onsite events	moderate	moderate	moderate
offsite events/models	low	low	high
point estimates	high	high	low
uncertainty distributions	moderate	moderate	moderate
General PRA methods	**moderate**	**moderate**	**high**
scope of analysis	moderate	low	high
core damage event trees	high	high	moderate
containment event trees	n/a	n/a	n/a
system fault trees	high	high	moderate
data analysis	moderate	moderate	high
human reliability	low	low	high
Special methods	**low**	**low**	**high**
truncation of low frequency sequences	low	low	high

BLDG'

2.0 PRA Overview

Chapter 1 of Reference 1 describes four programmatic objectives for the MHTGR PRA:

1. Provide a means of characterizing the safety of the MHTGR such that the conceptual design can be evaluated in a logical fashion.

2. Provide the basis from which to select the MHTGR Licensing Basis Events (LBEs) evaluated in the PSID.

3. Evaluate a wide spectrum of events with offsite doses to show compliance with Protective Action Guidelines (PAGs) at the site boundary in support of the Emergency Planning Basis document.

4. Evaluate the MHTGR risk to the public to show compliance with the NRC safety goals.

Based on the results of the PRA, General Atomic (GA) concluded that the PRA confirms that the selection of LBEs included in the PSID is appropriate, that the MHTGR design is insensitive to failures in active and engineered systems, that the frequency of radioactive release is dictated by the failure of passive structures, and finally that releases with frequencies greater than 5E-7/yr are below the PAG sheltering limits of 1 Rem whole body and 5 Rem thyroid at the site exculusion area boundary (EAB).

The NRC was requested to respond to the following questions:

1. Does the NRC agree that for the MHTGR conceptual design the PRA provides a logical and structured method to evaluate the adequacy of the design?

2. Does the NRC agree that the level and extent of the PRA provides a sufficient basis from which to select the MHTGR LBEs?

3. Does the NRC agree that the PRA shows the MHTGR design to be capable of meeting the NRC Safety Risk Goals?

4. Does the NRC agree that the PRA shows that an accidental release from

the MHTGR resulting in a thyroid or whole body dose at the EAB in excess of the PAGs is extremely improbable?

Methodology Used

A combined event tree-fault tree approach was used to define risk-related sequences and their frequencies. Initiaing event groupings were established for primary coolant leaks, loss of heat transport system (HTS) cooling, earthquake, loss of offsite power, transient, control rod withdrawal and steam generator leak. Event trees describing sequences associated with the failure of functions provided to mitigate the effects of these initiators were then developed. Systems and functions included in the event trees then defined those systems for which fault tree models were developed or other reliability data provided. These models were of limited specificity because of the lack of detailed design information available at this stage of the plant design but addressed support system interactions based on an assumed set of high-level, functional intersystem dependancies. Following completion of the fault trees, sequence-level frequencies were developed. This development attempted to address support system interactions but apparently did not utilize linked fault tree or support state methodologies in the process.

Sequences were completely developed only in cases where the sequence frequency was greater than 1E-8/yr. For such sequencies, release categories were defined and used to describe plant risk.

Data Base Information

Since there is no plant-specific data for the MHTGR, a mix of data from light water reactors, non-nuclear facilities, and earlier gas-cooled reactor designs was utilized. Much of this data was developed prior to 1978 and was included in Reference 3. It is acknowledged in Reference 1 that substantial data does not exist concerning component reliability in helium environments, and that this substantially increases the uncertainty in the failure estimates.

For many components, there is general agreement between the failure values used in the MHTGR PRA and those used in other PRAs. While the potential effects of the helium environment on component reliability is not addressed, the component data analysis is considered adequate for a generic, conceptual analysis.

Human reliability is essentially unmodeled in the PRA. Some twenty-six human failure

events are identified but are too vaguely described in all but three cases to clarify or assess properly. Operator actions following an initiating event, particularly recovery actions, were not addressed.

Core Damage and Risk Results

As a result of the 1E-8/yr trunction method, potential offsite releases were identified for primary coolant leaks, loss of main loop cooling, earthquake, anticipated transients, and steam generator leaks. For loss of main loop cooling, earthquake, and anticipated transients, no more than two sequences were identified. No sequences were identified for loss of offsite power (including station blackout) and control rod withdrawal. No ATWS sequences were identified. Internal fire and flood and support system-induced initiators were not addressed. No sequences were identified which resulted in core damage; all releases were from activity in the primary coolant system, which is normally not even addressed in LWR PRAs.

Releases associated with all sequences identified in the PRA are estimated to be below ~0.3 rem whole body at the site boundary for frequencies greater than 1E-6/yr. Offsite dose is dominated by circulating and plateout activity, a result of the lack of consideration of any core damage sequences (which inherently limits the extent of the release) - a consequence of the conclusion that decay heat removal would always be available through either an engineered system, the passive reactor cavity cooling system (RCCS), or earth-conduction. It is important to note that no residual release is assumed for any truncated sequence, and hence it cannot be concluded from the PRA results that the sequences identified either categorize or bound the total risk.

3.0 Major Questions Requiring Resolution

A number of areas requiring additional elaboration and justification were identified during the MHTGR PRA review. These are addressed in applicable sections of this report. Major areas of concern are summarized below.

Initiating Event Selection

The initiators analyzed in the PRA appear appropriate but inadequate to describe the potential risk associated with the MHTGR. Additional initiators deserving review and analysis include system-level failures (for example, loss of a dc bus and loss of service water), internal fires, internal floods, and unexpected environmental conditions which may impact the RCCS.

System faults, fires and floods have been shown to be important risk contributors in LWR PRAs. While admittedly design-specific and difficult to address at this stage of the MHTGR design, the potential for dependencies is sufficiently high as to preclude any conclusion of completeness without consideration of these events. These events must be addressed before the very low risk claimed for the MHTGR design can be defended.

Unusual external events which could result in loss of RCCS effectiveness should be pursued in more detail. These initiating events have been excluded on the same basis as is typically done in LWR PRAs. However, since RCCS functionability is so important to the MHTGR design and currently identified risk-related sequences are of such low frequencies, a greater effort to identify and analyze initiators which impact the RCCS should be performed. Such an analysis may require additional efforts to define all potential RCCS failure modes. It must be noted that the PRA assumes earth-conduction will always prevent core damage in situations where RCCS failure occurs. This assumption appears crucial to several potentially important sequences (particularly if common-cause effects substantially increase sequence frequency) and must be carefully justified.

The above comments are more important in the MHTGR PRA than would be the case in a typical LWR PRA precisely because of the low sequence frequencies currently predicted for the MHTGR design. While an additional 1E-6/yr sequence would have little impact on the core damage frequency estimate for an LWR, it could have a substantial impact on the overall risk results predicted for the MHTGR.

Fault Tree Development

The limits in plant specification at this time posed constraints on reviewing the system models developed in the PRA. For example, the success criteria and normal configuration of the service water system and circulating water system are not defined. The ac power bus loads are not developed as yet. Also, specific valve types are not specified, e.g., the shutdown cooling water subsystem inlet and outlet valves, making failure modes and data analysis uncertain.

Some events are not defined explicitly enough to quantify properly. Common-mode/cause events are not present in the models explicitly. Human failure events are too vaguely described to determine whether they are assumed to occur before the initiator or after in many cases. The use of the phrase "inadvertently ..." for human failure events is not specific enough to allow quantification.

Most restrictive in tracing the results of the PRA is the fact that there is no list of basic events with the occurrence probability associated with each event.

Conditional RCCS reliability estimates must be developed for all applicable sequences. Because of the importance of the RCCS, defensible uncertainty estimates should also be provided.

Core Damage Sequences

The sequences that lead to core damage have all been truncated from detailed consideration. This is the major weakness in the PRA. These sequences, as well as those detailed, should be developed into cutset or equivalent representations so that the results can be understood and sensitivity and uncertainty analyses be performable.

If sequence truncation is utilized, then release categories should be assigned to such sequences. These release categories should carefully consider potential release given RCCS failure, if applicable. Sensitivity studies could then be performed to help understand the potential impact of the truncation process on the analysis results, identify the impact of potential dependencies between branches, and define the (probabilistic) importance of MHTGR systems.

It is not clear from a review of Reference 1 that the event trees were correctly utilized with the system fault trees in estimating sequence frequencies. Typically, one of two methods

are used in contemporary PRAs - linked fault trees or support-state methods. Based on the final sentence on page C-1, it does not appear that either method was used - certainly neither method is documented. Because of this, confidence that all system dependencies which exist in the logic models have been properly assessed is low. Without a clearly defined, integrated logic model, modification of the model to address changes as the design progresses will also be difficult to implement and defend.

Reference 1 defined four objectives for the PRA (see Section 2.0) and requested NRC response to four questions related to these objectives. While PRA can provide important information concerning these questions, the uncertainties associated with the current MHTGR PRA seriously hamper its usefulness in this regard. In particular, uncertainties in the modeling of dependancies and in the analysis of external events, and the failure to address all identified sequences (because of the method used to truncate sequences based on frequency) severely limit the usefulness of the PRA in evaluating the overall design, even at the conceptual stage. Because of this, confidence is low, based on the PRA, that all appropriate LBEs have been identified, that the current design meets the NRC Safety Goal, or that releases in excess of the PAGs are extremely improbable.

Additional efforts concerning specification of dependancies, more comprehensive analysis of external events, and a more thorough analysis of initiator/RCCS interaction could rectify this situation, unless unexpected, high frequency sequences were subsequently identified.

4.0 Initiating Event Selection

Initiating events were selected through the use of a top-down logic which addressed both systems and structures required to perform critical radionuclide control functions. Once these systems and structures were defined, applicable failure modes were defined. Based on these failure modes, front-line system, support system and external initiators which could challenge the top-level control functions were identified.

Exhibit 4-1 describes the process employed in the PRA to define initiators based on three functions which formed the basis of initiating event selection: control of heat generation, removal of decay heat and control of chemical attack. Items identified in diamonds in Exhibit 4-1 were addressed to a lesser extent or not at all in the analysis. For example, in the third tier, only radiation associated with the core and primary circuit were addressed - the potential for release of radiation from spent fuel was not considered.

Potential initiators were grouped based on their impact to reduce the number of event sequences requiring development, as is usually done in PRA. Initiators ultimately addressed in the PRA are shown in Exhibit 4-2, along with their impact on the three functions described above.

Initiators Considered

As can be seen from Exhibit 4-2, the initiators chosen for analysis are consistent with those typically addressed in LWR PRAs: loss of heat removal, ATWS, and primary and secondary-side breaks. Loss of offsite power (LOOP) is considered a support system fault. This event is usually addressed in a manner similar to loss of feedwater sequences; however, the lack of a substantial emergency power system appears to result in greater system-level impact than in LWR designs, justifying consideration of the initiator as a support system initiator.

A list of external initiating events consistent with that contained in Section 10, External Events, of the PRA Procedures Guide[4] was used as a basis for selection of external initiating events considered. Only one such event was eventually analyzed - earthquake. External events not addressed because of site/plant specificity include internal fires and floods, which have been significant contributors in some PRAs, as well as weather-related initiators not typically addressed in LWR PRAs.

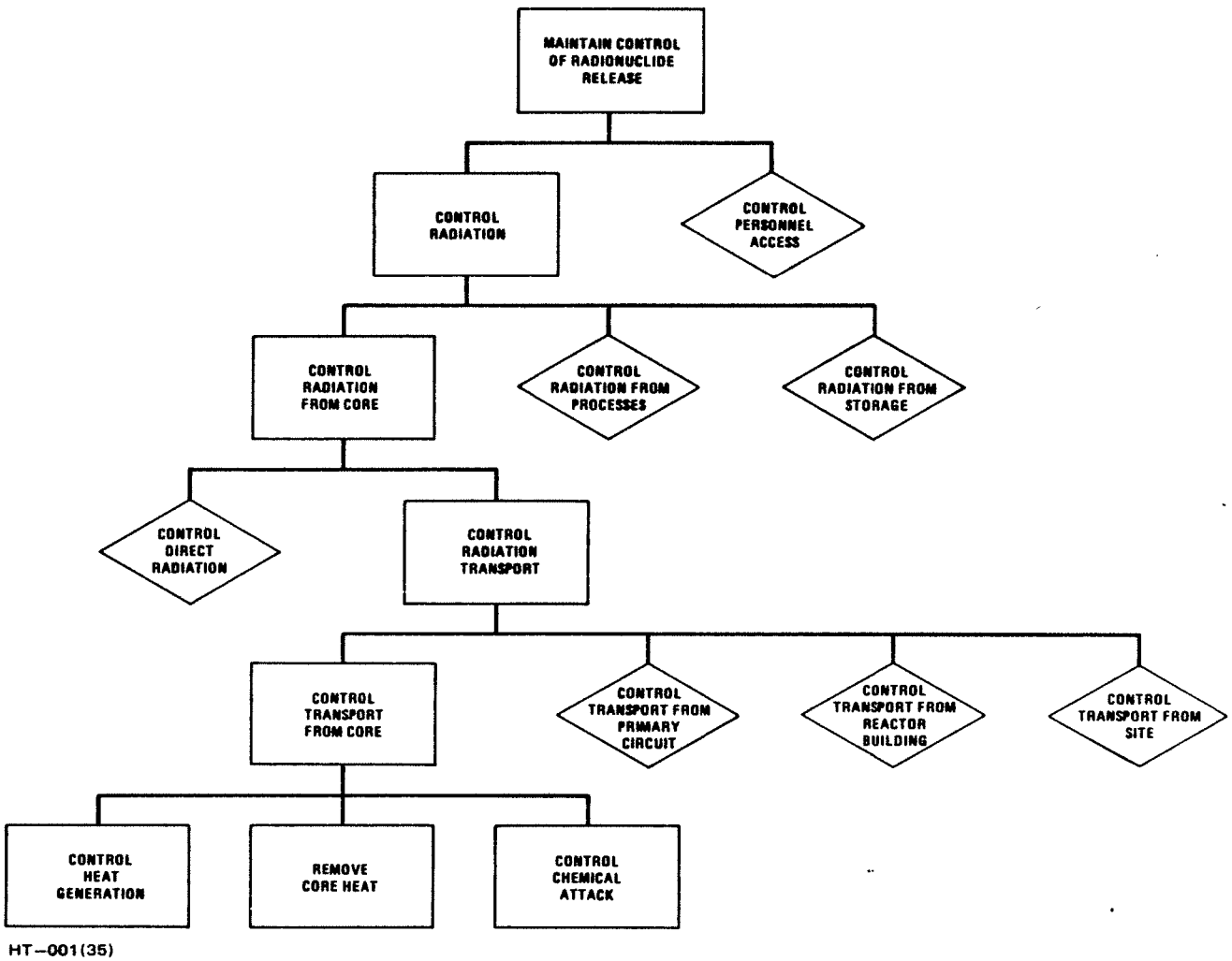

Exhibit 4-1. MHTGR PRA Initiator Definition Process.

SUMMARY OF ACCIDENT INITIATORS SELECTED FOR FURTHER ANALYSIS

Initiating Event	Function Challenged			Barriers Challenged		
	Heat Generation	Heat Removal	Chemical Attack	Fuel Particle	Primary Coolant	Reactor Building
Critical System Faults						
Anticipated transient without scram	X			X		
Control rod group withdrawal	X			X		
Loss of heat transport system		X		X		
Support System Faults						
Loss of offsite power	X	X		X		
Critical Structure Faults						
Primary coolant system leaks		X	X	X	X	X
Steam generator leaks	X		X	X	X	
External Faults						
Earthquakes	X	X	X	X	X	X

Exhibit 4-2. Initiators Addressed in the MHTGR PRA.

Completeness

The PRA studied a limited set of initiator classes. Fires and floods were considered too plant-specific to assess but earthquakes were not. Losses of certain front line systems were addressed as initiators but loss of support systems were not. Eliminating fires and floods for the stated reason was justified but could have large risk impact, since several LWR PRAs have found these sequences significant. Earthquakes are plant- and site-specific and cannot be assessed in a generic fashion, as was done, with any credibility. Also, several LWR PRAs have found dominant risk sources in the service water system, dc equipment and batteries, instrument air, HVAC, and other support systems.

Because of the low sequence frequencies calculated in the PRA, it is also possible that other initiators, such as weather-related events (which might impact the RCCS), initiators which impact spent-fuel cooling, and initiators at conditions other than power operation may contribute relatively significant sequences.

Contemporary PRAs typically use initiator listings (see, for example, Tables 2-3 and 2-4 of Reference 4) as a basis for initiating event selection in lieu of defining a set of events through a top-down approach, which may miss historically observed initiators or events which are of specific concern for other reasons. Such listings have been developed based on initiators addressed in numerous PRAs. In addition, system-based initiators, including those associated with support systems, are also identified during system analysis in a contemporary PRA. These initiators can be important because of their impact on multiple front-line systems. Examples of such events include failure of service water or instrument air.

Use of initiator listings such as those included in Reference 4 in developing MGTGR-related initiators would increase the confidence in the completeness of the initiator set addressed. Assumed system dependencies identified in Table 4-3 of Reference 1 were used in developing the fault trees used in the PRA. This information could also aid definition of a set of system-based initiators, again adding to the confidence in the overall initiator set.

As a whole, the list of sequences is moderately adequate with respect to a level 1 (core melt) PRA without external events but not a full level 1, much less a level 3 (public risk), PRA.

Table 5-1. Branches Addressed in the MHTGR Event Trees.

	Primary Coolant Leak	Loss of HTS Cooling	Earthquake	LOOP	Anticipated Transient	Control Rod With-drawal	S/G Leak
Reactor Trip (Control Rods)	x	x	x	x	x	x	
RSCE	x	x	x	x	x	x	
HTS Cooling	x		x		x	x	
SCS Cooling	x	x	x	x	x	x	x
RCCS Cooling	x	x	x	x	x	x	x
HPS Pump-down	x	x			x		
Cooling Restored Before Vessel Damage		x	x		x		
No of Modules Impacted		x		x			
S/G Leak-Related trip							x
S/G Isolation							x
S/G Dump							x
Primary Relief							x

RSCE - Reserve Shutdown Cooling System

HTS - Heat Transport System

SCS - Shutdown Cooling System

RCCS - Reactor Cavity Cooling System

HPS - Helium Purification System

S/G - Steam Generator

LOOP - Loss of Offsite Power

5.0 Event Tree Development

Event trees were constructed for each initiating event grouping. The event trees are system-based, and consider failures of those systems and functions capable of providing protection given each initiator. The development of each event tree is described in Appendix C of Reference 1. These descriptions are consistent with those found in other PRAs. Branches addressed for each initiator are shown in Table 5-1.

Response to differing initiator magnitudes was addressed when applicable on the single event tree associated with the initiator. The requirements for operator action and plant monitoring during each sequence were not identified or addressed in the fault tree models.

Release categories were assigned to all sequences with median frequencies greater than 1E-8/yr. Sequences with frequencies less than 1E-8/yr were truncated and assigned a frequency of ε with no specified release category.

Results

The resulting event tree for control rod group withdrawal is shown in Exhibit 5-1. This event tree demonstrates one result of the truncation process, the elimination from consideration of many release sequences because their estimated frequency was below 1E–8/yr. With the exception of primary coolant leaks (which inherently involves release because of the loss primary coolant) and steam generator leaks, very few release sequences are addressed in the PRA:

Initiator	Number of Sequences Identified
Primary Coolant Leak	30
Loss of HTS Cooling	1
Earthquake	2
LOOP	none
Anticipated Transient	1
Control Rod Withdrawal	none
S/G Leak	24

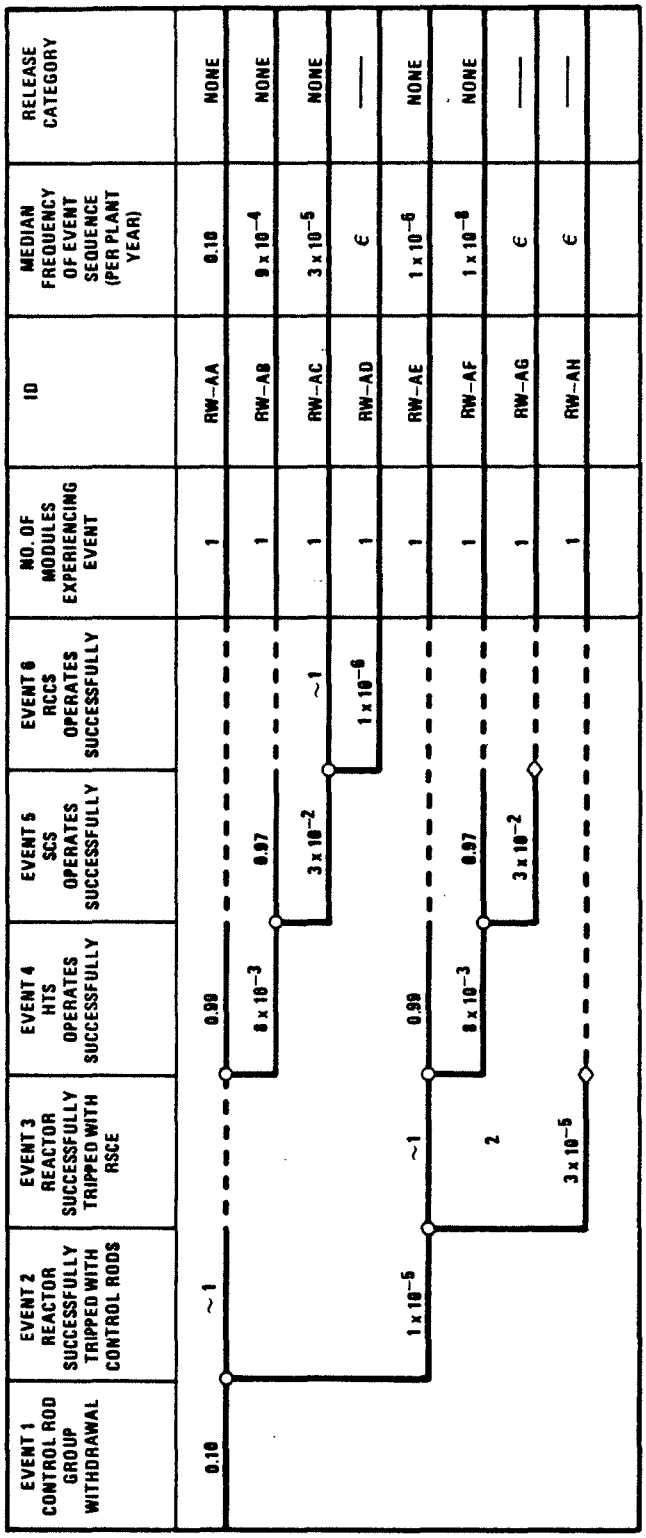

Exhibit 5-1. MHTGR PRA Event Tree for Control Rod Group Withdrawl

No core damage sequences are considered, only non-core damage releases, which are invariably ignored in contemporary LWR PRAs.

Completeness

The systemic event tree structures used in the PRA appear adequate to generate core damage cutsets. The functions (branches) seem to relate properly, logically, and chronologically. The release category binning scheme is consistent with current LWR PRA techniques. As structures the event trees appear credible and complete for the initiatior groupings analyzed and only moderately contribute to uncertainty in the risk results, comparable to LWR PRAs.

6.0 FAULT TREE CONSTRUCTION

System Selection

Reference 1 developed eight event trees to account for the initiators identified in section 4 of this report. The event headings included the following:

1. Reactor successfully tripped with control rods
2. Reactor successfully tripped with reserve shutdown cooling system (RSCE)
3. Operator successfully trips reactor (the ATWS event tree only)
4. HTS operates successfully
5. Shutdown cooling system (SCS) operates successfully
6. RCCS operates successfully
7. Helium purification system (HPS) pumpdown
8. Cooling restored prior to vessel damage
9. Various steam generator related events (steam generator leak event trees only)

Event tree headings 1, 2, 3, 6, 7, 8, 9 were not modeled using fault trees, but by using failure estimates from other sources.

Event tree heading 4 was modeled as the union of energy conversion system failure, service water failure, spurious PPIS trip, turbine building closed cooling water failure instrument and service air failure, reactor plant cooling water failure, non-class 1E electric power supply failure, HTS circulator failures, and loss of class 1E 120 vac uninterruptible power supply.

Event tree heading 5 was modeled as the startup or running failures of the SCS.

Support systems were introduced in the two models as needed in the logical progression of the faults in the trees. The support systems modeled included:

1. circulating water
2. service water
3. turbine plant closed cooling water
4. reactor plant cooling water
5. non-class 1E ac power

6. class 1E 120 (and higher) vac power
7. class 1E 125 vdc power
8. shutdown cooling water subsystem

A system interdependency chart was developed to describe postulated system interactions, and is presented as Exhibit 6-1.

Identification of System Interfaces

The plant is developed only to the major component connection schematic level, as indicated in the figures at the end of Section 4 of Reference 1. This allows fairly accurate representation of the interfaces among the water systems but no representation of the ac and dc power systems' interfaces (busses) with equipment. There are currently no convolutions of water systems that typically exist in a power plant which could lead to system interactions; this is likely to be a result of the immature status of the design, not some deliberate design philosophy (the plant, particulary the balance of plant, is simply not designed as yet).

Component Failure Data

There is no plant-specific data for the MHTGR. Generic data is mostly from LWRs and non-nuclear facilities and of specious comparability. The failure rate sheets show some component types and failure modes that are comparable to LWR generic sources. When compared, there is general agreement with some values higher and some lower. The MHTGR PRA did not document a sensitivity analysis and thus, the significance of the differences is not estimable. The helium environment effects on component reliability are not determinable from the PRA. Generally, the data analysis is adequate for generic analyses but the uncertainty is high without plant-specific data and substantial data applicable to helium environments.

Two systems are critical to the sequence development but unanalyzed in the PRA - the reserve shutdown control equipment (RSCE) and the reactor cavity cooling system (RCCS). The failure probability of the RSCE is given as 4E-5 and the failure probability of the RCCS is assigned 3E-6. These values are unusually low except for completely passive systems that are not susceptible to common-mode or common-cause failures. The RSCE would seem to have a common-cause potential from at least the PPIS and there may be common-mode/common-cause potential withing the two sets of RSCE. The absence of the potential for flow blockage in the RCCS is claimed but not demonstrated. There is also

MHTGR FUNCTIONAL INTERSYSTEM DEPENDENCIES

Systems	Support Systems																
	Non 1E ac	1E dc	Non 1E dc	1E UPS	Non 1E UPS	Instrument and Service Air	RPCW	Circ. Water	Service Water	TBCCW	PPIS	He S/T	Turbine/ Generator	PCDIs	Condensate Polishing	Heater Drains
Non 1E ac	--	X	X	X	X								X			
1E dc	X	--		X												
1E UPS	X	X		--												
Instrument and service air	X					--				X						
RPCW	X					X	--		X			X				
Circulating water	X							--								
Service water	X								--							
TBCCW	X					X			X	--						
PPIS				X	X		X		X		--			X		
Turbine/ generator	X							X		X			--	X	X	X
Feedwater and condensate	X	X				X		X		X	X			X	X	X
Main and bypass steam	X	X									X					
SG dump	X										X					
HPS	X				X		X				X	X				
Neutron control	X	X		X	X		X				X					
Pressure relief											X	X				
SCS	X					X			X		X	X				
HTS	X				X	X	X		X	X	X	X		X		
PCDIS																
Radiation monitoring	X				X									X		
Condensate polishing	X					X									--	
Heater drains	X					X										--

Exhibit 6-1. MHTGR PRA System Interdependancy Chart

Hey - It's in the PSID

no analysis in Reference 1 supporting the claim that the RCCS can fully replace the heat removal function if HTS and SCS both fail. Without appropriate analyses, the assigned failure probabilities are not conservative.

Another data related problem is that much of the equipment modeled in the PRA is non-safety grade. This makes the application of the generic database that is mostly based on safety-grade LWR equipment that more uncertain. If reliability values consistent with those estimated in LWR PRAs are to be assumed, the details of a reliability assurrance and performance monitoring program proposed to achieve such values must be provided.

Common-Cause Considerations (Including Shared Systems)

Common-cause failures of multiple components can arise from two main sources—functional connections or shocks. Plant equipment is complexly connected by equipment or environmental interfaces, e.g., an interconnection valve or the closeness of a heater to a flammable material, respectively. To the degree that the limited information on the plant design allows, the equipment interfaces were modeled explicitly in the two main fault tree models. For example, service water and ac power system interactions were modeled directly in the fault trees at the appropriate system interfaces. It must be recognized that additional interfaces will invariably be required as the design progresses, and these will most likely increase the frequency of analyzed sequences and add additional sequences.

The only shock modeled was that of an earthquake; fires, floods, winds, and other internal and external shocks were not be modeled. Further, given that the plant is not sited as yet nor are its basic structures or overall seismic characteristics specified, the earthquake analysis is of uncertain usefulness.

Common-Mode Failures

The term common-mode failure is usually taken to mean the multiple failure of redundant equipment by the same mode, e.g., fails to start. The causes of such failures include coincidental random failures and common-causes. Reference 1, as does many PRAs, uses a ß-factor approach to account for multiple failures of redundant, similar equipment. The ß-factor is a ratio of the common-mode failure rate to the total single component failure rate and is typically (or generically) on the order of 0.1. This factor is then used as the conditional probability that the second, third, and greater components of a like kind will fail. The ß-factors are derived from data and are notoriously uncertain. Their use also guarantees that failures due to common-mode is both significant to any system's overall

failure rate (which may not always be credible) and that the cause is completely unexplainable.

The use of this generic, unanalyzable source of system or multiple train failure probably is not detrimental in a generic PRA such as Reference 1 but should be avoided as plant information and data become available.

Human Actions

Plant operations, the operator and maintenance interfaces, procedures, the design of control boards, crew structure, and training are all requisite elements of a human reliability analysis and are not documented in Reference 1, and are presumed to be as yet undesigned. As a result, the study did not model so-called procedural failures, i.e., the failures in implementing procedures once a decision, a plan, and a procedure is made. The old NREP procedures guide cognitive model is used to model the response of operators to events, i.e., the decison making and planning. There are many better time-dependent human reliability models than the NREP correlation but given the lack of information on accident sequence timing and plant operations, no time-dependent model can be used effectively.

Since there is no record in Reference 1 of basic events with their occurrence probability estimates, there is no way to determine what values were used for the human failure events or why. Also, there is no accounting for the recovery mode of operator action during an ongoing offnormal event. The net result is that there is effectively no human reliability analysis in this study and the human contribution to risk - detriment or enhancement - is not assessed.

7.0 ACCIDENT SEQUENCES

A level 3 PRA has as its ultimate objective a quantitatively developed estimate of the health risks to the public. The standard approach in PRA is to develop hypothetical accident sequences that could lead to a release of radioactive material within the plant and then extend those sequences by postulating containment breach scenarios and weather and environmental phenomena that would allow for the transport of these materials to the surrounding population. Historically, the risk from a nuclear facility arises from low frequency, high consequence core damage sequences and routine, incidental releases have not contributed much to a facility's risk profile.

In the assessment of a new facility type, sequences involving both core damage and incidental releases must be considered to guarantee that risk is credibly assessed. Reference 1 used a frequency truncation scheme that resulted in not assessing any core damage sequences for consequences and thus, risk. The result is that the risk from the MHTGR is not completely assessed and cannot be claimed to be known.

Core Damage

The event tree stuctures in Reference 1 (discussed in Section 5) seem adequate for this level of plant detail to develop core damage and release sequences. There are no models of several of the event headings, e.g., RCCS, but the sequences at the event tree level seem to be valid.

However, a truncation scheme was used to stop further consideration of a sequence. If the estimated frequency of occurrence of a sequence fell below 1E-8/yr, then the sequence was arbitrarily removed from further analysis. As a result, any sequence in the event trees that was capable of producing significant core damage was assessed a frequency of less than the truncation value and dropped from the analysis. Further, those sequences that survived the truncation and were carried to risk measures were not developed into cutset descriptions and delineated so as to be able to trace the modeled systems to their sequence effects.

The LWR community has focused on several generic sequences, two of which are a loss of site ac power and an anticipated transient without scram. Examination of the analysis in Reference 1 of these particular sequences demonstrates the general pattern used to account for core damage.

Loss of AC Power. Protection against loss of offsite power is provided in the MHTGR

design by the use of non-class 1E gas turbines, uninterruptable power supplies, and a DC system. Battery life is specified to be one hour. The only non-ATWS version of the loss of ac power sequences that would lead to core damage is the sixth sequence in Figure C-5 of Reference 1. This sequence consists of a loss of power, a successful trip of the reactor, a failure of SCS, and a failure of the RCCS. The frequency of the loss of power is assessed at 5E-3/yr. This value is lower than the value used in LWR PRAs by a factor of 20. The SCS failure probability is assessed at 0.01, which is a credible system unavailability value. The RCCS failure probability is estimated to be 3E-6 (based on unrelated seismic response arguments). The net result is a sequence frequency of 1.5E-10/yr.

This net value is in itself incredible, estimating an occurrence frequency of once in about 7 billion years. Raising the loss of power frequency to 0.1/yr, a standard value, yields a sequence frequency of 3E-9/yr, which is still incredible.

The uncertainty in the frequency assessment of the loss of power sequence is substantial and warrants further support analysis and a full consequence analysis.

ATWS. The anticipated transient without scram sequence that could lead to significant core damage is the last sequence in Figure C-6 in Ref. 1. This sequence consists of a transient, followed by the failure of control rod trip, the failure of the RSCE, and the failure of the operator to manually trip the reactor. The transient frequency is 27/yr, which is reasonable for the first 1 or 2 years of plant operation. The control rod failure occurrence probability is assessed at 3E-5 and the RSCE failure probability is 4E-5. The operator failure probability is assigned 0.17. The net frequency of core damage from ATWS is 5.5E-9/yr.

Clearly, if both the control rods and the RSCE fail, there may be no credible sceanario for operator recovery. Thus, the human failure probability should be conservatively assumed to be 1.0. This raises the sequence frequency to 3.2E-8/yr, which is above the truncation value and means that the sequence should be analyzed for its consequences without further consideration. However, the multiplying of the two scram system failure probabilities, which yields a joint probability of 1.2E-9, is allowable only if there are no common-mode or common-cause failures among the systems or between them. In a conceptual design, this cannot be determined. Also, design experience does not support joint probabilities much lower than 1E-5 to 1E-6. The result is a conservative estimate on the ATWS sequence frequency more on the order of 2.5E-5/yr, or nearly 4 orders of magnitude higher than was assessed in Reference 1.

RCCS reliability. Fundamental to the low frequency of many MHTGR sequences is the assumption that the RCCS failure probabilty is on the order of 1E-6. This probability was developed using seismic analysis arguments which are inappropriate for non-seismic sequences. Because of the importance of the RCCS, it is vital that a defensible reliability analysis be performed. This analysis must be relevant to the initiators and sequences in which the RCCS functionality is addressed. Such an analysis must consider potential RCCS failure modes, potential RCCS status prior to each initiator, and the ability to monitor RCCS performance.

Because the RCCS reliability has been assumed to be so high, other systems have been designated non-safety related and often provided with no redundancy. This places an enormous burden on the RCCS design. No alternate protective features (systems, functions, etc.) which would provide a balanced defense-in-depth appear to exist for many sequences, and hence RCCS reliability must be demonstrated with confidence across the spectrum of initiators. (This also appears to be an economic risk concern, since poor RCCS "safety" performance could not be easily be compensated for with plant modifications in other areas.)

The quantification of any of the sequences that were assessed to have occurrence frequencies above the truncation level cannot be traced. There is no listing of basic events in the model with their assessed occurrence probability or frequency and no description of cutsets, their frequencies, or their sums. As a result, no estimate can be obtained of a total release frequency or a distribution over release types, nor any estimate of the expected core damage frequency for the MHTGR.

Since the results are not broken into cutsets, there is no easy mechanism to determine the sensitivity to risk of data, model assumptions, specific systems or equipment, etc. The numerical and qualitative contribution to uncertainty in any answer also cannot be assessed from the report itself.

The long durations expected for many MHTGR sequences appear to have been an important factor in assuming high recovery likelihoods from initial failures addressed in the PRA. Because a formal recovery analysis was not performed, the potential to have overestimated sequence recovery likelihoods is high. In addition, such long duration sequences raise the potential for political and legal interaction expected to a far lesser extent in short-duration sequences postulated for LWRs.

Risk-Related Sequences

The risk impact of sequences with frequencies greater than 1E-8/yr was defined by assigning release categories to similar sequences and then estimating a frequency for each type of release. Release types for the following four conditions were considered: forced convection cooldowns under dry and wet conditions and conduction cooldowns under dry and wet conditions. For each type, multiple categories were defined to describe differing release scenarios.

Conduction cooldowns involve loss of forced cooling and rely on conduction and radiation to remove heat from the core via the RCCS. Forced convection cooldowns under dry conditions are caused by primary coolant leaks and result in the release of fission products due to circulating and plateout activity. Conduction cooldowns under dry conditions are initiated by loss of main loop cooling and earthquake, as well as from primary coolant leaks and result in fission product release from heatup of fuel particles.

Forced convection cooldown under wet conditions are initiated by steam generator leaks. The fission product release is due to oxidation of graphite and hydrolysis of failed fuel in addition to the release of circulating and plateout activity. Conduction cooldowns under wet conditions are also initiated by steam generator leaks and involve the same release mechanisms as dry conduction cooldowns.

Frequencies and associated whole-body doses for all release category types are shown in Exhibit 7-1. The largest 30-day EAB doses in each of the four category types estimated in Reference 1 are also given in Table 7-1.

The magnitude of release for important nuclides is provided in Appendix D to Reference 1 for each accident category, although little additional information is provided to describe other assumed or calculated characteristics of the release, such as timing and particle size distribution. The largest evaluated release (category DC-1) includes 6E+4 curies of I-131, 3E+2 curies of Cs-137 and 3E+3 curies of Te-132. This is comparable in size to several of the release categories evaluated in WASH-1400, as indicated below.

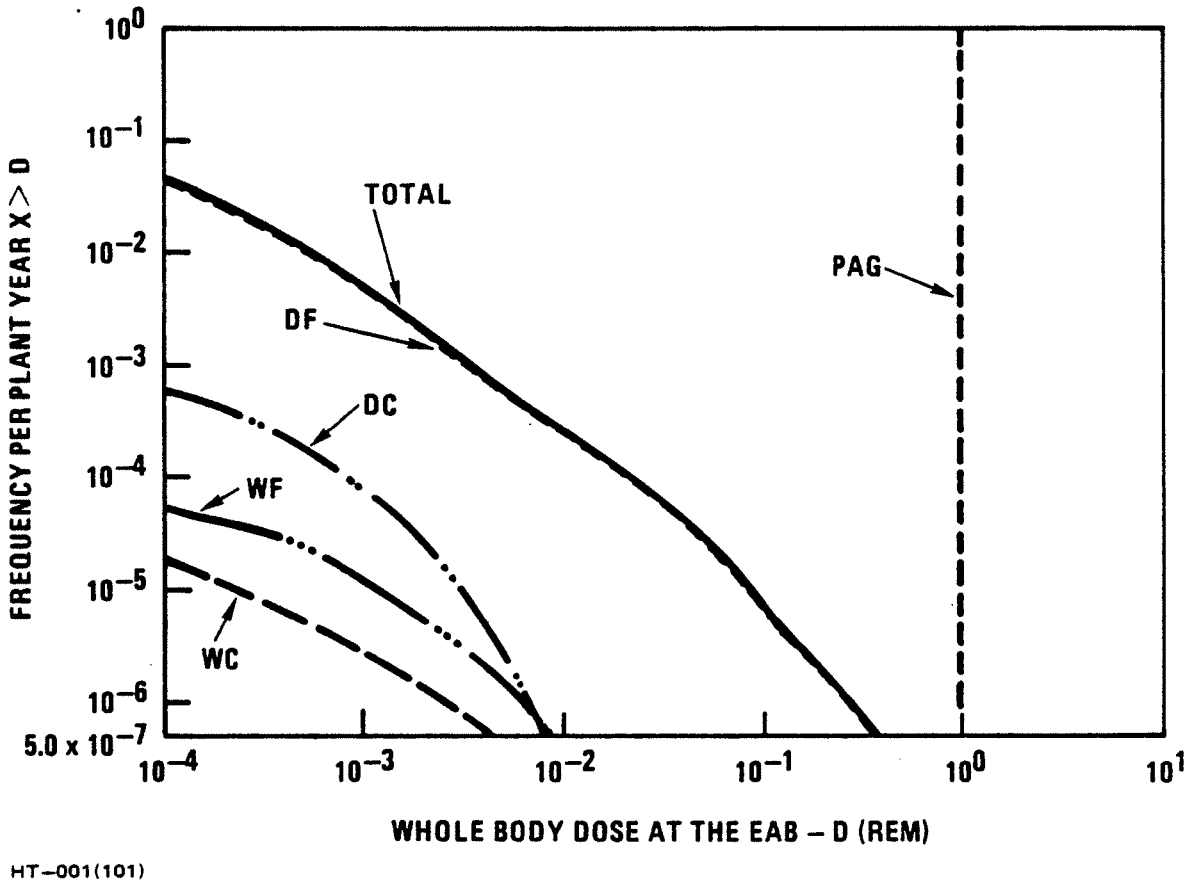

Exhibit 7-1. MHTGR Estimated Whole Body Dose-Frequency Curve at EAB.

Table 7-1. Doses Associated With Four Release Categories

Release Category	Sequence Description	Median Whole Body γ Dose, Rem.	Median Thyroid Dose, Rem.
DF-1	1" primary coolant leak, reactor trip, HTS or SCS maintains forced cooling, HPS pumpdown ineffective.	2.9E-4	1.4E-3
WF-1	Moderate S/G leak, reactor trip, S/G isolation and dump occurs within 20 minutes, SCS maintains forced cooling, primary relief opens and fails to close.	2.2E-3	3.4E-1
DC-1	Earthquake >0.8g results in instrument line failures in four modules, reactor trip, HTS, SCS, RCCS and HPS pumpdown fail, reactor vessel depressurization.	6.4E-2	5.0E+1
WC-1	Small S/G leak, reactor trip, and auto S/G isolation, S/G dump valves fail to open, SCS fails, RCCS cooling successful, primary relief valve opens and fails to reclose.	6.2E-3	2.4E+0

Release Category		Approximate Release (Ci)		
		I-131	Cs-137	Te-132
WASH-1400	PWR 9	9E+0	3E+0	1E-1
	PWR 8	9E+3	2E+3	1E+2
	PWR 7	2E+3	5E+1	2E+3
	PWR 6	7E+4	4E+3	1E+5
MHTGR	DC-1	6E+4	3E+2	3E+3

PWR and PWR 8 are "design basis accidents" and PWR 6 and PWR 7 are core melt accidents in which containment does not fail directly to the atmosphere. To compare with current LWRs on a per-MWe basis, estimated MHTGR consequences would need to be increased by nearly and order of magnitude.

Dominant Risk-Related Sequences

Dominant risk-related scenarios identified in Reference 1 are associated with three sequences involving primary coolant leaks where HTS or SCS maintains forced convection cooling. These sequences contribute a combined mean risk of 3E-5 rem/yr whole body at the EAB. This value is a factor of thirty higher than that contributed by any other release category. For thyroid dose, these three sequences are also the dominant contributors.

It is not possible to estimate the potential impact of more realistic dependancy and external events analyses on the dominant sequences predicted for the MHTGR since such sequences, if addressed at all, fall below the truncation limit and hence were not developed to the point of assigning release categories.

8.0 Insights Based on PRA Review

Many comments and conclusions developed during review of the PRA have been described in other sections of this report. This section presents selected insights concerning the use of the PRA in the design process, compliance with the Safety Goals, and the need for an external effects analysis for the RCCS.

Use of PRA in the Design Process

The assumed interaction between systems was summarized in Table 4-3 of Reference 1 (Exhibit 6-1). This information was then used as a basis for developing system fault trees, although in many cases it was not sufficiently specific to be used in detailed modeling. A more effective approach would have been to define a set of detailed functional relationships based on realistic support requirements, develop the PRA based on these assumed requirements, and then develop interface criteria which would limit actual support requirements to a set bounded by the analyzed configuration. Importance analyses could then be performed to define those functions and components which should be specified as important to safety. Sensitivity studies could also be used to understand the impact of alternate dependancy configurations.

To make effective use of the PRA in the design process, the logic model must be both scrutible and easy to modify. The current analysis lacks justification in many areas and is incomplete in others. It is also not clear that the model can be easily modified and re-solved, particularly if new support systems are defined.

Compliance with Safety Goals

Section 9 of Reference 1 presents a simplified analysis to demonstrate that expected releases from the MHTGR comply with the NRC safety risk goals of contributing no more than 0.1 percent to the overall prompt and cancer fatality risks. Because of the uncertainty in the present treatment of dependancies and external events, it cannot be concluded that these goals are currently met or will be met as the design proceeds without some plant modifications, although this is possible.

Meeting the MHTGR PAG goals is more problematic. The design is predicted to only marginally meet these limits at the conceptual stage, and the potential for a reduction in risk as the design proceeds and is analyzed in greater detail is low. If the PAG goals must be met, then consideration should be given to design changes, such as improved confinement,

to further reduce releases for dominant sequences.

RCCS External Effects Analysis

The need for a detailed external effects analysis of the RCCS has been addressed in Section 7 and will be reiterated here. The presently assumed RCCS failure rate is indefensible, considering the importance of the RCCS in many sequences. RCCS reliability must be estimated in a way which addresses the conditionalities inherent in each sequence.

At the present time, two situations are assumed - either the RCCS is operable and available to remove decay heat or the RCCS is "failed" but earth conduction is still effective in removing decay heat and limiting the amount of fission products released from the core. If this is not the case, then predicted releases could increase substantially for situations in which the RCCS is failed. All external initiators (including internal fire and flood and primary and secondary pipe breaks) which could impact RCCS functionality and potentially result in additional dominant sequences should be identified, binned if applicable, and analyzed. Such an effort is necessary if confidence is to exist in the overall low release frequences estimated for the design.

REFERENCES

1. GA Technologies, Inc., *Probabilistic Risk Assessment for the Standard Modular High Temperature Gas-Cooled Reactor*, DOE-HTGR-86-011, Rev 3, Volume 1 and 2, January 1987.

2. GA Technologies, Inc., *Preliminary Safety Information Document for the Standard MHTGR*, DOE-HTGR-86-024, September 1986.

3. G.W. Hannaman, *GCR Reliability Data Bank Status Report*, GA-A14839, July 1978.

4. *PRA Procedures Guide*, NUREG/CR-2300, January 1983.

5. S.A. Eide, et al., *An Approach to the Assurance of Technical Adequacy in Probabilistic Risk Assessments of Light Water Reactors*, NP-3298, Interim Report, Electric Power Research Institute, December 1983.

6. Brookhaven National Laboratory, *A Review of the Shoreham Nuclear Power Station Probabilistic Risk Assessment,* NUREG/CR-4050, for the US NRC, November 1985.

7. US General Accounting Office, *Probabilistic Risk Assessment: An Emerging Aid to Nuclear Power Plant Safety Regulation,* GAO/RCED-85-11, Report to the Committee on Energy and Commerce, House of Representatives, June 19, 1985.

APPENDIX A

REVIEW CRITERIA

A PRA is an extensive document that encompasses many disciplines and many results and is subject to potentially large uncertainties in the input information and the output interpretations. The nuclear utility industry has invested in PRAs for analysis of licensing and operational issues and has attempted to develop a QA procedure for assuring the accuracy of a PRA.[6] The NRC has reviewed PRAs to learn how they may be used in licensing[7] and the General Accounting Office has explored the usefulness of PRA relative to regulation of safety.[8]

This review of the HTGR PRA is not intended as a QA audit; however, QA of the technical work of a PRA is relevant. The major issues identified in the EPRI study relative to auditing the technical work (p. 3-2) are:

1. completeness related to the PRA scope
2. accuracy in the applications of methods and calculations
3. consistency between the study goals and scope and between the assumptions, methods, and study objectives.

The Brookhaven review, applied to internal events and core damage frequency risk only, included the following technical areas:

1. plant modeling—safety functions, system success criteria, support systems, and initiators
2. accident sequence definition—event trees and event dependencies
3. system fault trees
4. human performance analysis—cognitive errors and procedural errors
5. data assessment—initiator frequencies, component unavailabilities, and human error probabilities
6. quantification and the identification of dominant contributors.

The GAO report focused on the uncertainties of PRA and the usefulness of PRA in light of these uncertainties. "The uncertainties are not caused by and are not unique to PRA but reflect the incomplete knowledge about plant systems, human behavior, accident processes (the physical and chemical changes that take place during an accident), the off-site consequences of accidents, and how external events such as earthquakes, fires, and floods

can cause accidents." (p. ii) There were judged to be four ways that incomplete knowledge can contribute to the uncertainty in a PRA (p. ii):

1. PRA analysts may not identify all events that could start or direct the course of an accident.
2. Sufficient and reliable data may not be available to model and quantify the behavior of plant systems and accident processes.
3. Analysts may not make accurate assumptions where data is lacking.
4. Computer models may not realistically represent plant behavior and accident processes.

Specific areas that were assessed to need more development in PRA are, according to the GAO:

1. plant systems modeling
2. human reliability
3. accident phenomenology
4. off-site consequences
5. external events.

Abstracting from these documents and using the large experience base from LWR PRAs, three basic criteria relative to the adequacy of a PRA can be identified. These basic criteria are:

Credibility

1. Do the general results seem to encompass all elements of the risk criterion estimated?
2. Do the results match those that may be reasonably anticipated?
3. Are the results traceable to system failures and process phenomena that are credible?
4. Do the results adequately allow for the uncertainties that can be anticipated?
5. Are the assumptions used to bound the analysis adequately set?

Completeness

1. Do the sequences analyzed encompass the significant risk of the plant?
2. Is the plant represented adequately?
3. Do the methods accommodate all reasonable sources of risk?

Uncertainty

1. Are the anticipated sources of uncertainty identified?
2. Are the sources of uncertainty quantified as much as possible?
3. Do the results reflect these quantitative uncertainties?

There are four major areas of a PRA to which these general criteria should be applied:

Plant representation. PRAs of LWRs have shown that the risk profile of a plant is highly dependent on the specifics of the plant, its systems, operations, and processes. A "generic" risk assessment has proven to be of specious accuracy in measuring the level or sources of the plant's risk. For example, two generic PRAs of Crystal River-3 missed a key source of core damage frequency found in a third, plant-specific study. The degree to which the PRA adequately represents the plant is an area of review.

Results. The results of a PRA can be directed toward three risk criteria and be quantitative only, qualitative only, or both. These risk criteria are typically measured by core damage frequency, frequency of release, or frequency of loss of life or injury. The quantitative estimates should be expressed in terms of point estimates of some central tendancy and some measure of uncertainty. The qualitative contributions to risk should be identified and the sensitivity of their contribution obtained.

General PRA methods. PRAs of LWRs have matured over the decade since the WASH-1400 *Reactor Safety Study*. The basic tools of PRA include development of success criteria, system and system interaction modeling, accident modeling, data analysis, human reliability analysis, core phenomenology, off-site consequence modeling, and external events modeling. Today's methods are still evolving in several areas, e.g., external events, human reliability, core phenomena, and off-site consequences. Also plant data is being continually accrued and will contribute to risk-related knowledge. Any PRA of a nuclear facility must meet the, albeit implicit, standards of the PRA business.

Special methods. Most PRAs attempt to advance the state-of-the-art because of special objectives or concerns in the PRA. The special methods must be consistent with the general PRA methods and stand on their merits relative to credibility, completeness, and uncertainty.

These general criteria were used to group the Brookhaven factors as well as factors judged from SAIC experience to be important to be the adequacy of PRAs.