

MAR 12 1987

Mr. Francis X. Gavigan, Director  
Office of Advanced Reactor Programs  
Office of Nuclear Energy  
U.S. Department of Energy  
Washington, D.C. 20545

Dear Mr. Gavigan:

On February 18, 1987, members of the NRC staff and its contractors from ORNL and BNL met with representatives of DOE and its contractors to review Chapters 7 and 8 (Plant Protection, Instrumentation and Control, and Electrical Systems) of the Modular HTGR (Project 672) Preliminary Safety Information Document (PSID). The agenda and list of attendees are given in Enclosures 1 and 2, respectively. The meeting consisted of presentations by DOE and its contractors on the multi-module control systems and on the control room design bases, followed by discussions of NRC comments on Chapters 7 and 8. Action Items and Clarifications resulting from the meeting are given in Enclosure 3 for your action. Your response to these items is required by April 3, 1987 in order for us to maintain our review schedule.

I want to take this opportunity to emphasize two of our comments contained in Enclosure 3. First, from our review to date of the MHTGR PSID, and as discussed at the subject meeting, it appears you are proposing that only those portions of the design which are necessary to maintain off-site releases less than the 10CFR100 dose guidelines be given a safety classification. No other plant systems, structures or components are proposed as having any safety classification or as being items over which NRC should have regulatory jurisdiction. It does not appear that this approach is consistent with NRC's mission to protect public health and safety or consistent with past regulatory practice. The NRC regulations contain many other requirements besides 10CFR100 dose guidelines considered necessary for the protection of public health and safety (for example the dose requirements of 10CFR20 and many portions of 10CFR50) which are independent of reactor type. Features of the design necessary to comply with these other requirements or otherwise judged to be necessary for the protection of public health and safety are items over which NRC has traditionally had regulatory jurisdiction via approval of the design and design requirements, inclusion in Technical Specifications and inspection and oversight. A similar approach in the review and licensing of the MHTGR would seem appropriate, unless justification can be provided for proceeding otherwise.

To illustrate the above concern consider your proposal to classify the primary system moisture monitor and steam generator dump portions of your Plant Protection and Instrumentation System (PPIS) as non-safety grade. The rationale given was that moisture ingress events do not lead to releases of radioactive material which exceed 10CFR100 guidelines; therefore, automatic dump of the steam generator water/steam inventory following a moisture ingress event is not considered a safety function. Accordingly, that portion of the PPIS related to primary system moisture monitoring and steam generator dump is classified as non-safety. However, without automatic plant shutdown and steam generator dump, it appears off-site doses from the plant could exceed 10CFR20 limits and 10CFR50

Project #672

8703190038 870312  
PDR PROJ  
672

PDR

Appendix I guidelines for anticipated operational occurrences involving water ingress. Therefore, to adequately protect public health and safety we believe that the primary system moisture monitoring and steam generator dump should be governed by the provisions of Appendix I to 10CFR50 and 10CFR20.

In consideration of the above, it is requested that you reconsider your recommendation with respect to the safety classification of systems, structures and components. Specifically, please discuss the basis by which you classify each MHTGR system, structure and component, including how it is ensured each applicable NRC regulation is complied with. It should be noted that this same fundamental issue was discussed in my February 9, 1987 letter to you as it related to the development of Principal Design Criteria for the MHTGR.

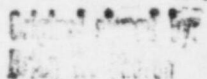
Related to the above is the issue of utilizing, where practical, applicable guidance in the LWR Standard Review Plan, Regulatory Guides, NUREG Reports and other NRC documents in defining the MHTGR design and design requirements. Such an approach is consistent with the Commission's Policy Statement on Advanced Reactors (51 FR 24643, dated July 8, 1986) and will ensure that existing applicable guidance developed and matured through years of application and experience are utilized in the MHTGR. Again this was discussed in my February 9, 1987 letter to you as it related to the development of Principal Design Criteria; however, I want to emphasize the importance of building upon what has already been developed, applied and understood. In particular, for MHTGR systems and components that have a counterpart in LWRs (in function and in importance to safety), and for which the counterpart LWR systems are governed by existing regulatory requirements, the governing regulatory requirements should either be adopted or justification provided as to why they have not been adopted. The staff's review plans for the MHTGR were developed assuming that those features of the MHTGR common to LWRs would make use of applicable LWR criteria and standards. If this turns out not to be the case then additional review time may be necessary.

The second comment that I wish to emphasize it that, the proposed MHTGR design requirements appear to be based on the premise that the presence of an operator is not required to protect public health and safety. The safety analyses for the proposed design do not assume an operator taking any action during the course of an accident and, as stated at the subject meeting, the presence of an operator as a line of defense to monitor and provide confirmation of plant response, to communicate plant conditions following an accident or to initiate recovery action is not considered a safety function. Although we fully support your effort to design a reactor which eliminates the need for operator action during the course of an accident, we cannot concur at this time that the role of the operator to monitor safety systems, act as a communication link and initiate recovery action is not a necessary line of defense and a safety function. To accept such a position would require your demonstrating that all MHTGR failure modes, initial conditions and failure scenarios are known and that the operator's role, including communication with offsite personnel, under each of these situations is not required to assure public health and safety. Our view is that only after extensive experience has been obtained from plant operations, including the demonstration of plant safety characteristics, could such a case possibly be made. Accordingly, the MHTGR design should make provision for

an accessible and habitable safety grade shutdown area (main control room or remote shutdown area) until such time as the above can be demonstrated.

If you have any questions please do not hesitate to contact Dr. Peter Williams, Project Manager for this review.

Sincerely,



Themis P. Speis, Director  
Division of Safety Review and Oversight  
Office of Nuclear Reactor Regulation

Enclosures: As stated

cc: D. Mears, GCRA

DISTRIBUTION:

Central File  
SPEB R/F  
DSRO C/F  
TSpeis  
BSheron  
KKniel  
TKing  
PWilliams  
DJones/AR-5209  
MEI-Zeftawy, ACRS/H-1016  
RColmar  
RJohnson/Rm. 212  
GPlumlee/EWS263  
LSoffer/Rm. 266  
DThatcher/Rm. 212  
PWood, RES/NL-007

WMorris/NL-007  
SSHaukat/Rm. 212  
CAllen  
CMcKinley, ACRS/H-1016  
EChelliah/Rm. 244  
FEltawila/Rm. 266  
JRead/Rm. 266  
JSwift/Rm. 244  
RFoulds, RES/NL-007  
RIreland, Region IV  
CPTan/P-1132  
KHeitner/P-234  
WKennedy/AR-5209  
BSenseney/EWS403  
Project File 672  
PDR

*Rm. 016*

\*See previous concurrences

\*\*Phone concurrence

|      |                               |               |               |            |           |                       |
|------|-------------------------------|---------------|---------------|------------|-----------|-----------------------|
| OFC  | : DSRO: SPEB*                 | : DSRO: SPEB* | : DSRO: SPEB* | : DSRO: DD | : DSRO: B | : HFIB**              |
| NAME | : PWilliams: sd: <i>TKing</i> | : KKniel      | : BSheron     | : TSpeis   | : DJones  | : <i>By Telephone</i> |
| DATE | : 3/1/87                      | : 3/10/87     | : 3/16/87     | : 3/12/87  | : 3/12/87 | : 3/3/87              |



function. To accept such a position would require your demonstrating that all MHTGR failure modes, initial conditions and failure scenarios are known and that the operator's role, including communication with offsite personnel, under each of these situations is not required to protect public health and safety. Our view is that only after extensive experience has been obtained from plant operations, including the demonstration of plant safety characteristics, can such a case be made. Accordingly, the MHTGR design should make provision for an accessible and habitable safety grade shutdown area (main control room or remote shutdown area) until such time as the above can be demonstrated.

If you have any questions please do not hesitate to contact Dr. Peter Williams, Project Manager for this review.

Sincerely,

Themis P. Speis, Director  
Division of Safety Review and Oversight  
Office of Nuclear Reactor Regulation

Enclosures: As stated

DISTRIBUTION:

Central File  
SPEB R/F  
DSRO C/F  
TSpeis  
BSheron  
KKniel  
TKing  
PWilliams  
MEI-Zeftawy, ACRS/ H-1016  
RColmar  
RJohnson/ Rm. 212  
GPlumlee/ EWS 263  
LSoffer/ Rm. 266  
DThatcher/ Rm. 212  
PWood, RES/ NL-007  
WMorris/ NL-007  
SShaukat/ Rm. 212  
CAllen  
CMcKinley, ACRS/ H-1016  
EChelliah/ Rm. 244

Feltawila/ Rm. 266  
JRead/ Rm. 266  
JSwift/ Rm. 244  
RFoulds, RES/ NL-007  
RIreland, Region IV  
CPTan/ P-1132  
KHeitner/ P-234  
WKennedy/ AR-5209  
Project File 672  
PDR  
Daniel Jones/ AR-5209  
Bob Senseney/ EWS403

|      |              |              |              |            |           |             |   |
|------|--------------|--------------|--------------|------------|-----------|-------------|---|
| OFC  | : DSRO: SPEB | : DSRO: SPEB | : DSRO: SPEB | : DSRO: DD | : DSRO: D | : 4FIB      | : |
| NAME | : PWilliams  | : sd: King   | : KKniel     | : BSheron  | : TSpeis  | : Dan Jones | : |
| DATE | : 3/ 3/87    | : 3/3 /87    | : 3/3 /87    | : 3/ /87   | : 3/ /87  | : 3/3 /87   | : |

Attendance List  
NRC/DOE Meeting on MHTGR-PSID - Chapter 7 & 8

| <u>Name</u>        | <u>Organization</u>  |
|--------------------|----------------------|
| Tom King           | NRC/NRR/DSRO/SPEB    |
| Karl Kniel         | NRC/NRR/DSRO/SPEB    |
| Peter M. Williams  | NRC/NRR/DSRO/SPEB    |
| Jim Zgliczynski    | GA                   |
| William C. Craig   | Stone & Webster      |
| Lloyd P. Walker    | Stone & Webster      |
| William G. Kennedy | NRC/NRR/DHFT         |
| Dale F. Thatcher   | NRC/NRR/DSRO/EIB     |
| Peter G. Kroeger   | BNL                  |
| Syd Ball           | ORNL                 |
| Jim Quinn          | General Electric     |
| Carmelo Rodriguez  | GA Technologies      |
| Tony Neylan        | GA                   |
| A. Millunzi        | DOE                  |
| Donald Graf        | MHTGR-PDCO           |
| Phil Wood          | NRC/RES              |
| E. Chelliah        | NRR/DSRO             |
| George Sherwood    | DOE                  |
| Yogi Dayal         | General Electric Co. |
| David M. Zizzo     | GE                   |

# AGENDA

February 18, 1987 Meeting on MHTGR  
PSID Chapters 7 and 8  
(Phillips Building - Rm. P-422)

- 9:00-10:30 a.m. - Presentation by DOE of Multi-Modular Control Systems, including:
- Description of Protection System
  - Description of Control System
  - Interfaces between Control and Protection System
  - Operator's Function
  - Extent of Computer Control
- 10:30-12:00 p.m. - Presentation by DOE on Control Room Design Bases, including
- Description of Control Room
  - Alternate Shutdown Provisions
  - Role of Operator in normal operation, AOOs, DBAs and EP events
  - Philosophy on Protection of Operators
  - Provisions for Post Accident Monitoring and Communication
  - Design Basis for Control Room considering: SSE/OBE, Tornado, Habitability, Shielding, 1E Power and Instrumentation, Security, Fire Protection
- 12:00-1:00 p.m. - Lunch
- 1:00-4:00 p.m. - Discussion of NRC Comments on Chapters 7 and 8.
- This period will provide for additional discussions of items not fully completed during the morning's presentations and the development of a list of agreements and action items.
- Discussions will include items such as the following:
- (1) How are failures in the automatic control systems to be modeled in accident analysis?
  - (2) How are limitations in software to be considered?
  - (3) Are there provisions for unplanned, creative, remedial actions?



- (4) How does the Data Management Subsystem (DMS) interface and affect "safety-related" control and instrumentation systems (pg. 7.1-2)?
- (5) What criteria will systems not designated "safety related" meet? (e.g., seismic monitoring)?
- (6) Can DOE site examples in quality, reliability, diversity, etc. of control systems that are improvements over current NRC criteria?
- (7) Discuss non-safety related reactor trips, especially the omission of the steam generator dump. (pg. 7.2-6).
- (8) Why isn't manual actuation of the reserve shutdown system available in the control room (pg. 7.2-7)?
- (9) How are the fusible links in the reserve shutdown system to be tested and qualified?
- (10) Discuss what is meant by "appropriate reliability" with respect to the Special Nuclear Area Instrumentation Subsystem (pg. 7.2-2).
- (11) What are the consequences of a Class 1E failure?
- (12) Can failures in non-class 1E systems cause a failure in Class 1E systems?
- (13) Will the Class 1E system meet the appropriate SRP for this system?
- (14) What SRPs, Regulatory Guides, or industry standards are considered relevant to Communications and Service Systems?

4:00-5:00 p.m. - Status of Submittals/Plans for next meeting

Action Items and Clarifications from NRC/DOE  
Meeting, 2/18/87 on MHTGR-PSID Chapters 7 and 8

(Numbering system continued from 1/20-21/87 Meeting Letter)

General Comments

G-4 Identification of Systems, Structures, Components Important to  
Safety:

From our review to date of the MHTGR PSID, and as discussed at the subject meeting, it appears you are proposing that only those portions of the design which are necessary to maintain off-site releases less than the 10CFR100 dose guidelines be given a safety classification. No other plant systems, structures or components are proposed as having any safety classification or as being items over which NRC should have regulatory jurisdiction. It does not appear that this approach is consistent with NRC's mission to protect public health and safety. The NRC regulations contain many other requirements besides 10CFR100 dose guidelines considered necessary for the protection of public health and safety (for example the dose requirements of 10CFR20 and many portions of 10CFR50) which are independent of reactor type. Features of the design necessary to comply with these other requirements are items over which NRC has traditionally had regulatory jurisdiction via approval of the design and design requirements, inclusion in Technical Specifications and inspection and oversight. A similar approach in the review and licensing of the MHTGR would seem appropriate, unless justification can be provided for proceeding otherwise.

To illustrate the above concern consider your proposal to classify the primary system moisture monitor and steam generator dump portions of your Plant Protection and Instrumentation System (PPIS) as non-safety grade. The rationale given was that moisture ingress events do not lead to releases of radioactive material which exceed 10CFR100 guidelines; therefore, automatic dump of the steam generator water/steam inventory following a moisture ingress event is not considered a safety function. Accordingly, that portion of the PPIS related to primary system moisture monitoring and steam generator dump is classified as non-safety. However, without automatic plant shutdown and steam generator dump, it appears off-site doses from the plant could exceed 10CFR20 limits and 10CFR50 Appendix I guidelines for anticipated operational occurrences involving water ingress. Therefore, to adequately protect public health and safety we believe that the primary system moisture monitoring and steam generator dump should be governed by the provisions of Appendix I to 10CFR50 and 10CFR20.

In consideration of the above, it is requested that you reconsider your recommendation with respect to the safety classification of systems, structures and components. Specifically, please discuss the



basis by which you classify each MHTGR system, structure and component, including how it is ensured each applicable NRC regulation is complied with. It should be noted that this same fundamental issue was discussed in my February 9, 1987 letter to you as it related to the development of Principal Design Criteria for the MHTGR.

Related to the above is the issue of utilizing, where practical, applicable guidance in the LWR Standard Review Plan, Reg Guides, NUREG Reports and other NRC documents in defining the MHTGR design and design requirements. Such an approach is consistent with the Commission's Policy Statement on Advanced Reactors (51 FR 24643, dated 7/8/86) and will ensure that existing applicable guidance developed and matured through years of application and experience are utilized in the MHTGR. Again this was discussed in my February 9, 1987 letter to you as it related to the development of Principal Design Criteria; however, I want to emphasize the importance of building upon what has already been developed, applied and understood. In particular, for MHTGR systems and components that have a counterpart in LWRs (in function and in importance to safety), and for which the counterpart LWR systems are governed by existing regulatory requirements, the governing regulatory requirements should either be adopted or justification provided as to why they have not been adopted. The staff's review plans for the MHTGR were developed assuming that those features of the MHTGR common to LWRs would make use of applicable LWR criteria and standards. If this turns out not to be the case then additional review time may be necessary.

G-5 Operator Functions:

It is DOE's position that the human operator functions are not a safety function. Accordingly, it must be demonstrated that it is not necessary that the operator be available to serve as a line of defense against single or other type of equipment failures, to confirm plant response, to communicate plant status to offsite personnel and to initiate recovery action. It is our view that such a demonstration would require demonstrating that all MHTGR failure modes, scenarios and initial conditions are known and that the plant safety characteristics will perform as designed. Without plant operating experience to support such a demonstration it is not clear that such a case can be made.

Therefore, it is our view that the MHTGR design should make provision for an accessible and habitable safety grade shutdown area (main control room or remote shutdown area) until such time as the above can be demonstrated. Accordingly, the proposed elimination of the manual scram as a safety function, the role of operators following an earthquake, the need for operator capability for response to unplanned situations and remedial actions, and the safety classification of equipment available to the operator to assure that safe shutdown is achieved and maintained should be discussed and justified in light of the above.

G-6

Documentation of Presentation Material:

Additional material pertaining to Chapters 7 and 8, together with material pertaining to other sections of the PSID, were presented in the form of view-graphs and in oral response to questions. The following specific items are to be documented.

1. DOE stated that it believes that the protection and control systems are completely separate and independent in the MHTGR design and that no sensory equipment, including neutron detectors, are shared between protection and control systems. DOE will confirm this statement and justify any exceptions.
2. The times available before safety related trip actions were needed were given in a table for several postulated, low probability accidents. The table will be revised to present these postulated accidents in terms of the accident descriptions and assumptions given in Chapter 15 or in the PRA and the times will be reestimated for protective action guideline limits. The much shorter automatic protection initiation times should also be documented in the revised table.
3. Locations and descriptions of Plant Protection and Instrumentation System (PPIS) equipment, as presented in view-graphs, will be documented.
4. Information on view-graphs that identified LWR and IEEE criteria that the safety protection subsystem will "meet the intent of" will be documented. The exceptions taken to IEEE 603 will be documented with justifications (e.g., non-safety manual scram).
5. Information presented pertaining to automatic plant control, including operating crew shift size, control room location, development of software, and the development and use of a simulator for operator task analysis will be documented. We suggest that DOE consider development of a Chapter 18 that would address SRP 18, "Human Factors Engineering." The information to be documented should discuss the role of the operator and automatic systems for normal operation and off-normal situations, the basis for the shift size, how the validity of software will be assured (consider R.G. 1.152), the available background that justifies the use of automatic control systems in nuclear power plants (including experience potentially available from the aerospace industry), and justification for not including automatic control as a topic in the Technology Development Plan.
6. The design, locations, and design requirements of the main control room and the remote shutdown area as augmented in view-graphs and discussions beyond that already contained in the PSID will be documented. For the remote shutdown area the access provisions, staffing, safety classification, instrumentation and communications should also be described.



7. DOE will describe and discuss that withdrawal of all control rods followed by failure of the reserve shutdown system to actuate will not result in an unacceptable transient or release an unacceptable amount of radiation. Similarly, DOE will document that the full contents of the steam generator could be introduced in the primary system and not result in an unacceptable level of reactivity addition, even under failure to scram conditions. This documentation should address the effects of delay time in isolating the steam generator.

#### Specific Comments

- 7.2-1 In 7.2.1.4 it should be clarified that the word "microprocessor" in the PPIS is taken to mean programmed software.
- 7.2-2 It appears that the trip signal for "Primary Coolant Pressure Low" (7.2.1.4.1) must either be bypassed (via a safety grade bypass on the PPIS) or have its set point lowered at reactor startup in order to startup the plant. The PSID should be revised accordingly.
- 7.2-3 The staff reserves its opinion until after its review of Chapter 15 and the PRA on whether trips d, e, f, and g given in Section 7.2.1.4.1 can be considered non-safety. However, for any non-safety scrams agreed upon, IEEE 603 criteria will be required to be met on those portions of the system common to the safety related portions.
- 7.2-4 DOE will clarify whether the operating bypass (top, page 7.2-8) is manual or automatic.
- 7.2-5 DOE will clarify whether or not the setting of the high coolant pressure scram prevents lifting of primary system relief valves. Also, it should be clarified whether or not it is a design requirement of this scram signal to preclude lifting of the primary system relief valves.
- 7.2-6 In order to accept portions of the PPIS as non-safety related it must be demonstrated that the safety protection system fails into a safe condition as a result of failures in non-safety portions of the PPIS. An acceptable approach would be to perform a failure modes and effects analysis at the FSAR stage. DOE will document that it recognizes this need for demonstration at the final design stage. DOE should clarify the meaning of "fails as is" on the top of page 7.2-15.
- 7.2-7 DOE will provide a table that identifies actuation logic (2 out of 4 or 1 out of 2) for safety protection systems and demonstrate that IEEE 603 is met, particularly that all operating bypasses of the PPIS are automatically removed.
- 7.2-8 Emergency battery power is needed to burn through "fusible" links which activate the reserve shutdown system. One of two fusible links is need for activation. The fusible links are to be tested from



manufacturers samples, on-line continuity, and when an entire control rod unit is removed for periodic inspection. The above should be documented.

- 7.2-9 DOE will identify the location of the HVAC system and clarify how loss of HVAC itself causes a reactor trip (Section 7.2.2). It is to be determined how long instrument and electrical cabinets can be reliably operated without restoration of HVAC.
- 7.2-10 DOE will reassess and document its position with respect to the non-safety related status of the interlock system for the vessel system pressure relief valves.
- 7.2-11 The safety status of the post accident monitoring system and seismic monitoring system will be reassessed on the basis of material to be presented under G-5 above and considerations of PRA and Chapter 15 material.
- 7.2-12 DOE will provide and clarify the discussion in Chapter 4 on the operational role of the non-safety related inner control rods, including whether or not they are needed for cold shutdown, that the operating bypass is automatic, and that the rods can be driven in from the control room if the trip signal does not function.
- 7.2-13 It will be necessary for NRC to review in detail postulated accident SRCD-6 before it can agree that the steam generator isolation and dump system is non-safety related. A related concern, no provision for dump of the Shutdown Cooling System (SCS), will also be studied.
- 7.3-1 DOE will provide a table to illustrate the plant parameters that are inputs to the control system and verify that the sensors are independent of the PPIS.
- 7.3-2 DOE will improve Figures 7.3-8, 7.3-10, 7.3-11 to clarify units and interpretations.
- 7.4-1 Clarifications will be provided on: (1) The meaning of the last sentence of the first paragraph in Section 7.4.1.5.1, (2) Whether the RMS provides a signal for automatic isolation of the helium sample line (Section 7.4.1.5.2) and if so shouldn't it be considered important to safety and designed for the SSE, and (3) Whether software is involved for the microprocessor described on page 7.4-9.
- 7.4-2 DOE will review and consider whether the seismic monitoring system will be in accord with Regulatory Guide 1.12, "Instrumentation for Earthquakes."
- 8.2-1 Four Class 1E buses are located in a single location of the reactor service building and each of the four can serve each of the four reactor modules. This sharing is in opposition to Regulatory Guide 1.6, "Independence Between Redundant Standby (Onsite) Power Sources

and Between Their Distribution Systems" which prohibits such sharing. DOE needs to justify its Class 1E design and also illustrate how the 1E electrical systems are to be isolated from non-1E electrical systems.

- 8.2-2 We understand that the Class 1E electrical system capacity is based upon being able to activate the Reserve Shutdown System. Are there any other safety functions of this system? Based upon your response to Item G-5 above is the one hour battery capacity still adequate?
- 8.2-3 DOE will describe the seismic design requirements of the electrical system.
- 8.2-4 DOE will clarify the fourth paragraph on page 8.2-4 regarding fault clearing.
- 8.2-5 DOE will give additional definition to the use of "as required" in its description of the fire detection and protection system used to preserve the integrity of Class 1E circuitry. (Page 8.2-5)