52-003

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

November 21, 1995

Mr. Nicholas J. Liparulo
Nuclear Safety and Regulatory Activities
Westinghouse Electric Corporation
P.O. Box 355
Pittsburgh, Pennsylvania 15230

SUBJECT: REQUEST FOR ADDITIONAL INFORMATION (RAI) RELATED TO THE AP600 PROBABILISTIC RISK ASSESSMENT (PRA) HUMAN RELIABILITY ANALYSIS

Dear Mr. Liparulo:

To support the Probabilistic Safety Assessment Branch (SPSB) review of the revised Westinghouse AP600 PRA and Westinghouse's responses to draft safety evaluation report (DSER) open items pertaining to the human reliability analysis, attached are RAIs related to level 1 PRA for internal events and include both power and shutdown operation. The response to these RAIs is needed to enable the SPSB staff to closed related DSER open items and complete the portion of the final safety evaluation report associated with these RAIs. You are requested to provide a response to these questions and comments within sixty days of receipt of this letter.

You have requested that portions of the information submitted in the June 1992 application for design certification be exempt from mandatory public disclosure. While the staff has not completed its review of your request in accordance with the requirements of 10 CFR 2.790, that portion of the submitted information is being withheld from public disclosure pending the staff's final determination. The staff concludes that these questions and comments do not contain those portions of the information for which exemption is sought. However, the staff will withhold this letter from public disclosure for 30 calendar days from the date of this letter to allow Westinghouse the opportunity to verify the staff's conclusions. If, after that time, you do not request that all or portions of the information in the enclosures be withheld from public disclosure in accordance with 20 CFR 2.790, this letter will be placed in the NRC Public Document Room.

These followon questions affect nine or fewer respondents, and therefore is not subjected to review by the Office of Management and Budget under P.L. 96-11.

9601040311 951121
PDR ADOCK 05200003
A PDR

DF03

NRC FILE CENTER COPY

040052

November 21, 1995

If you have any questions regarding this matter, you may contact me at (301) 415-8548.

Sincerely,

Original signed by
Diane T. Jackson, Project Manager
Standardization Project Directorate
Division of Reactor Program Management
Office of Nuclear Reactor Regulation

Docket No. 52-003

Enclosure: As stated

cc w/enclosure:
See next page

***30 DAYS HOLD**
DISTRIBUTION:
*Docket File
PUBLIC
TKenyon
JMoore, O-15 B18
MSiemien, OGC
NSaltos, O-10 E4
PDST R/F
TQuay
WHuffman
WDean, O-17 G21
ACRS (11)
TQuay
RArchitzel
DJackson
GSuh (2), O-12 E4
EJordan, T-4 D18

DOCUMENT NAME: A: PRAHUMAN.RAI

To receive a copy of this document, indicate in the box: "C" = Copy without attachment/enclosure "E" = Copy with attachment/enclosure "N" = No copy

OFFICE	PM:PDST:DRPM	SC:PDST:DRPM	
NAME	DJackson:sg	RArchitzel	
DATE	11/21/95	11/21/95	

cc: Mr. B. A. McIntyre
Advanced Plant Safety & Licensing
Westinghouse Electric Corporation
Energy Systems Business Unit
P.O. Box 355
Pittsburgh, PA 15230

Mr. M. D. Beaumont
Nuclear and Advanced Technology Division
Westinghouse Electric Corporation
One Montrose Metro
11921 Rockville Pike
Suite 350
Rockville, MD 20852

Mr. John C. Butler
Advanced Plant Safety & Licensing
Westinghouse Electric Corporation
Energy Systems Business Unit
Box 355
Pittsburgh, PA 15230

Mr. S. M. Modro
Nuclear Systems Analysis Technologies
Lockheed Idaho Technologies Company
Post Office Box 1625
Idaho Falls, ID 83415

Enclosure to be distributed to the following addressees after the result of the proprietary evaluation is received from Westinghouse:

Mr. Ronald Simard, Director
Advanced Reactor Programs
Nuclear Energy Institute
1776 Eye Street, N.W.
Suite 300
Washington, DC 20006-3706

Mr. James E. Quinn, Projects Manager
LMR and SBWR Programs
GE Nuclear Energy
175 Curtner Avenue, M/C 165
San Jose, CA 95125

Barton Z. Cowan, Esq.
Eckert Seamans Cherin & Mellott
600 Grant Street 42nd Floor
Pittsburgh, PA 15219

Mr. Frank A. Ross
U.S. Department of Energy, NE-42
Office of LWR Safety and Technology
19901 Germantown Road
Germantown, MD 20874

Mr. Ed Rodwell, Manager
PWR Design Certification
Electric Power Research Institute
3412 Hillview Avenue
Palo Alto, CA 94303

Mr. Charles Thompson, Nuclear Engineer
AP600 Certification
U.S. Department of Energy
NE-451
Washington, DC 20585

STS, Inc.
Attn: Lynn Connor
Suite 610
3 Metro Center
Bethesda, MD 20814

Mr. John E. Leatherman, Manager
SBWR Design Certification
GE Nuclear Energy, M/C 781
San Jose, CA 95125

Mr. Sterling Franks
U.S. Department of Energy
NE-42
Washington, DC 20585

REQUEST FOR ADDITIONAL INFORMATION

RAIs ON THE HUMAN RELIABILITY ANALYSIS FOR POWER OPERATION

RAIs Related to DSER Open Item 19.1.3.1-17

720.289 In page 30-2 of the revised HRA it is stated:

> "Because of some degree of uncertainty in the data, in terms of estimates for human error probabilities, it is often useful to perform a sensitivity analysis of the operator actions, during which the estimated human error probabilities, stress levels, dependency levels, or other human performance factors are systematically changed to determine the effect on the human reliability analysis results."

The staff agrees with this statement but could not find such sensitivity analysis in Westinghouse's submittals. Such sensitivity analysis, combined with insights from the importance and uncertainty analyses, would be very helpful to understand the plant's tolerance of human errors and to decide which (if any) human actions require more detailed analysis.

720.290 Several operator actions modeled in the ATWS event tree are required to be performed in a very short time. For example: (a) ATW-MAN03 (manually trip the reactor through the PMS in one minute), (b) ATW-MAN04 (manually trip the reactor through the DAS in one minute, given that an earlier attempt to trip the reactor through the PMS fails), (c) ATW-MAN01 (manually step-in control rods in one minute, using the plant control system, given that earlier attempts to trip the reactor through the PMS or DAS fail). These three actions have the same "time window" of one minute, defined in page 30-8 as the time from when cues are provided to the time when system failure is expected if no operator action is taken. Westinghouse estimated that approximately one minute is needed to perform both ATW-MAN03 and ATW-MAN04 (30 seconds each). Similarly, Westinghouse estimated that approximately one minute is needed to step-in the control rods (ATW-MAN01) to provide "sufficient" negative reactivity so that opening of the pressurizer safety valves can prevent RCS pressure from exceeding 3200 psig. Please provide the following information.

a. What is the "net" time window to manually trip the reactor through DAS (action ATW-MAN04), given that the attempt to manually trip the reactor through PMS (action ATW-MAN03) fails? What is the actual time needed to perform this action? What is the slack time for ATW-MAN04 assuming that this action follows an attempt by the operator to manually trip the reactor through PMS (action ATW-MAN03) and failed? How were dependencies evaluated? Please document your response by referring to specific subtasks and analyses and by stating clearly your assumptions.

b. What is the "net" time window to manually step-in the control rods (action ATW-MAN01), given that the attempts to manually trip the reactor through PMS (action ATW-MAN03) and through DAS (action ATW-MAN04) have failed? What is the actual time needed to perform this action? What is the slack time for ATW-MAN01 assuming that this action follows the attempts by the operator to manually trip the reactor through both the PMS (action ATW-MAN03) and the DAS (action ATW-MAN04) have failed? How were dependencies evaluated? Please document your response by referring to specific subtasks and analyses and by stating clearly your assumptions.

c. How were "mechanical faults," such as binding of rods within their channels and rod drive mechanisms failing to disengage, modeled in the AP600 PRA?

d. Westinghouse estimated that approximately one minute is needed to step-in the control rods (ATW-MAN01) to provide "sufficient" negative reactivity so that opening of both pressurizer safety valves can prevent RCS pressure from exceeding 3200 psig. Is this true even when an "adverse" moderator temperature coefficient (MTC) exists, such as at the beginning of fuel cycle? How is this modeled in the ATWS event tree? Please provide calculations of RCS pressure for the limiting transient (e.g., total loss of feedwater without turbine trip) assuming early core life MTCs. How was the failure of one safety valve to open modeled in the ATWS event tree?

720.291 Several assumptions about "time windows," used in the HRA, are not clear to the staff. For example, a "time window" of 30 minutes is assumed for events LPM-MAN01/LPM-MAN03/LPM-MAN07 (operator failure to recognize the need for RCS depressurization). A 30 minute "time window" is also assumed for event ADN-MAN01 (operator failure to perform RCS depressurization, given LPM-MAN01/LPM-MAN03/LPM-MAN07 success). Does this imply that the total "time window" for depressurizing the RCS (i.e., recognizing the need for depressurization and manually actuating the ADS) is one hour? Does the 30 minute "time window" for task LPM-MAN01 imply that task ADN-MAN01 (actuate ADS) will not be successful if it is initiated after 30 minutes, even if the estimated actual time to complete task ADN-MAN01 is 20 minutes? Is it true that the need to actuate ADS has been diagnosed when the 30 minute "time window" for task ADN-MAN01 begins? Westinghouse responses to same questions are also needed for the "time window" of 22 minutes for events LPM-MAN02/LPM-MAN04/LPM-MAN08 (operator failure to recognize the need for RCS depressurization during a medium or intermediate LOCA) in combination with the 30 minute "time window" for ADN-MAN01. Please explain.

720.292 The "time window" estimates used in the HRA, could be significantly affected by the various thermal-hydraulic (T-H) uncertainties associated with passive system T-H modeling. Do the "time windows" assumed in the HRA account for T-H uncertainties? Please explain how the issue of T-H uncertainties and their potential impact on "time windows" has been addressed, or will be addressed, in the HRA.

720.293 There seems to be a conflict between the operating philosophy as documented in the SSAR and the operating philosophy as modeled in the

PRA. The PRA states that the operator does not need to do any significant knowledge-based diagnosis and decision making (operators will only need to detect alarms, indications, etc., and then will be guided by the symptom-based procedures). On the contrary, in the SSAR (e.g., pages 18.8-14 and 18.6-7) it is stated that operators will be thinking ahead of the plant. This implies that the operators will not just be detecting information and then acting, but that they will be proactive. These two operating philosophies require a very different HRA model. Operating experience has shown that, even when "symptomatic" procedures are used, operators do still diagnose and, in fact, will circumvent procedures, skip ahead to solutions (which Westinghouse plants also allow) when operators know what the event is. This is modeled best by Table 20-3 of the HRA Handbook which includes perception, discrimination, interpretation, diagnosis and first level decision making. Please respond to these comments.

720.294 In the HRA quantification credit is often taken for separate recovery actions by the senior reactor operator (SRO) and the shift technical advisor (STA). The AP600 HRA is assuming a very low degree of dependence between recovery actions for a single subtask. One would argue that common operator training, communication and short time intervals provide strong sources of dependency between operators. For this reason, the THERP methodology does not allow to take credit for more than one recovery and only if there are formal checks. Given that the AP600 PRA credits recovery for every action by the control room crew, will there be formal checks in the procedures for each step for both the SRO and the STA? In addition, according to the HRA Handbook, the "one-of-a-kind checking with alert factors" recovery probability of 8.1E-2 is applicable to normal operating conditions, only. Please explain.

720.295 The passive nature of the safety systems in the AP600 design, combined with the reliance of the design on advanced instrumentation and control (I&C), has the potential to change the operator's interactions with the plant (as compared with operating plants) during accident conditions. In addition, operators may intentionally choose to circumvent procedures to avoid economic consequences (e.g., avoid containment steaming, avoid thermal shock due to overcooling or avoid water hammer). Please perform at least a qualitative evaluation of errors of commission that could impact the performance and reliability of the plant during accident conditions. This, also recommended by EPRI in its Utility Requirements Document (URD), is needed to identify potential errors of commission (and their consequences) and ensure that appropriate design certification and operational "requirements" will be used to prevent such errors.

720.296 Westinghouse needs to evaluate the uncertainty associated with human error probability (HEP) estimates (e.g., present the HRA results in terms of a mean value and an associated error factor).

720.297 Is event RNS-V024 (operator opens MOV 024 to replenish the IRWST inventory using the NRHR pumps) included in the revised PRA models? If yes, was its probability revised to address DSER concerns? Please explain.

720.298 The cues for LPM-MAN02 (failure to recognize the need for RCS depressurization) and CMN-MAN01 (failure to actuate the CMTs) are identical (see page 30-26). Could the operator fail to diagnose the need for CMT actuation believing that only depressurization is needed? What would the operator do first? How does this affect the estimated "actual time" and the diagnosis of either one of these events?

720.299 The "actual time" it will take the operator to actuate the CMTs (event CMN-MAN01) was estimated to be approximately 20 minutes during a small LOCA and only 8 minutes during a medium LOCA (see pages 30-26 to 30-28). Given that the operator will have to follow the same procedure and perform the same subtasks in both cases, what is the basis for the much shorter "actual time" during medium LOCAs?

720.300 Multiple alarms, close in time, could impact event diagnosis. By referring to the most risk important human actions, as determined by the importance analysis, please discuss how multiple alarms has been analyzed and accounted for in the HRA models.

RAIs ON THE HUMAN RELIABILITY ANALYSIS FOR SHUTDOWN OPERATION

720.301 The time window for operator action RCS-MANOD2S (detect failure of automatic closure of air-operated valves CVS-V045 and -V047 and manually close them) is very small (5 minutes). The shutdown PRA, as the PRA for power operation, states that the operator does not need to do any significant knowledge-based diagnosis and decision making (operators will only need to detect alarms, indications, etc., and then will be guided by the symptom-based procedures). Operating experience has shown that, even when "symptomatic" procedures are used, operators do still diagnose and, in fact, will circumvent procedures, skip ahead to solutions (which Westinghouse plants also allow) when operators know what the event is. This is modeled best by Table 20-3 of the HRA Handbook which includes perception, discrimination, interpretation, diagnosis and first level decision making. Please respond to these comments and re-quantify the probability of event RCS-MANOD2S as necessary.

720.302 Regarding DSER open Item 19.1.3.3-1, operator action, RHN-MANDIV, represents the likelihood that the operator would inadvertently drain reactor coolant into the IRWST through Normal RHR valve V-024. The probability of RHN-MANDIV was assigned a value of 1E-5 in Chapter 30 of the PRA. The corresponding task analysis for RHN-MANDIV evaluated the likelihood that the operator selects the wrong control to align Normal RHR and fails to close the diversion path. This probability was then used as a frequency (1E-5 per year) in the shutdown PRA to represent the frequency of overdraining the Normal RHR system through inadvertent opening of V-024. This frequency is very low and suggests that a pipe rupture of Normal RHR is more likely than an inadvertent draindown event.

a. Please search for other potential reactor coolant drain down paths that the operator could create, considering that the reactor coolant system may be pressurized (i.e. during hot shutdown) and document this search in the shutdown PRA.

b. The task analyses for RHN-MANDIV only evaluates the likelihood of the operator selecting the wrong control (V-024) to align Normal RHR. The staff believes that other conditions could create an opportunity to create this drain path (i.e. valve testing, etc.). Please use operating experience to obtain a frequency of inadvertent drain down events or justify in the shutdown PRA why operating experience is not applicable.

c. Please explain why the failure probability of RHN-MANDIV is used, also, as the frequency of overdraining the NRHR system.

d. Same time windows are used in the task analysis of event RHN-MANDIV for both pressurized (i.e., hot shutdown) and non-pressurized (i.e., cold shutdown) conditions. A draindown event when the RCS is pressurized would drain the RCS faster than an event with the RCS non-pressurized. This may require separate analysis of same scenario for hot and cold shutdown conditions, respectively. In addition, please provide the following details in the shutdown PRA for each potential drain path:

   (i) Define in the shutdown PRA what the term "time window" means for each scenario (time to core damage, time to core uncovery, etc.).

   (ii) Define in the shutdown PRA what the term "actual time" means for each scenario.

   (ii) Develop time windows considering both pressurized and non-pressurized conditions.