REQUEST FOR ADDITIONAL INFORMATION 100-1597 REVISION 1

11/12/2008

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

SRP Section: 19 - Probabilistic Risk Assessment and Severe Accident Evaluation
Application Section: 19.1

QUESTIONS for PRA Licensing, Operations Support and Maintenance Branch 1 (AP1000/EPR Projects) (SPLA)

19-194

The rupture of a main steam line due to water hammer is assumed (Section 6A.6.1) in the US-APWR PRA as a potential failure. This failure is assumed to occur when the emergency feedwater (EFW) flow to a ruptured steam generator (SG) is not stopped by the operator, thus resulting in the flooding of a main steam line. This failure can be prevented if the operator manually closes from the control room the motor-operated isolation valve on the EFW line to the affected SG. However, this “water hammer” failure is not treated as a human error (e.g., it is not included in Table 6A.6-9 where the human errors for the main steam pressure control system are listed) and was assigned a probability of 1E-2 per demand without providing any basis. Furthermore, instrumentation and control (I&C) failures may also contribute to the “water hammer” failure. It is important that all risk significant human actions be clearly identified as such in the PRA results and insights so they can be used accordingly in risk-informed applications. Please discuss.

19-195

It appears that several human errors and instrumentation and control (I&C) hardware and software failures associated with the main steam pressure control system have not been modeled. An example of a missing human error is the isolation of a ruptured steam generator (SG) by closing the motor-operated main steam relief valve (MSRV) block valve when the associated MSRV fails to reclose. This human error is not listed in Table 6A.6.9, where the human errors for main steam pressure control system are listed, and also it does not appear on fault tree MSP-OS (Ruptured SG isolation failure). An example of a missing I&C failure is the hardware and software failure to open the motor-operated safety MSRVs in order to perform depressurization by secondary side cooling (e.g., in fault tree MSP-SL). A systematic search is needed to identify any missing failures in the main steam pressure control system, as well as in other systems, and incorporate these missing failures in the revised fault trees or explain in the assumptions why they are not modeled.

19-196

It is stated in Section 6A.6.1.4 of the Revision 1 of the PRA report that the main steam relief valves (MSRVs) and the main steam isolation valves (MSIVs) are required to be

tested every 24 months. Nothing is mentioned for the main steam safety valves (MSSVs) and the turbine bypass valves (TBVs). Please list the assumptions made about test and maintenance for all components modeled in the PRA. Also, please verify the applicability of operating reactor demand failure rates to equipment used in the US-APWR which have much longer testing intervals (e.g., 24 months).

19-197

It is assumed that the two main steam safety valves (MSSVs) that are set to lower pressure will open to relieve secondary pressure following a steam generator tube rupture (SGTR) event if (1) the turbine bypass valves (TBVs) fail to operate as designed following a turbine trip (i.e. to open) or (2) the non-safety main steam relief valve (MSRV) in the line associated with the affected SG fails to operate (open). Therefore, the failure to close (re-close) of these two MSSVs is modeled in fault tree MSP-OS (failure to isolate the ruptured SG). The TBV failure to operate (open) is modeled by the fault tree node MSP-OS-02 (page 6A.6.B-31 in Revision 1 of the PRA report). It is not clear what constitutes a TBV failure to operate. Does the failure of even one of the 15 TBVs constitute a failure of the TBVs to operate (open)? What are the success criteria? Please provide a brief but clear description of the various failure modes of the TBVs to open (as modeled in the PRA in relation to fault tree node MSP-OS-02) and any related assumptions that were made. Specifically, explain basic events MSPIPFFLGUT (pressure indicator fails), MSPIPFFSLUT (pressure indicator fails), MSPWRBRDUMP (TBV wires open), MSPREXDDUMP (general relay fails to energize). Are these failures independent from other basic events used elsewhere in the PRA for the same components but with a different designator? Also, please explain the “operation by switch (interlock)” and “operation by control mode switch” human actions and state the reasons for not modeling the probability of human error for these actions as well as I&C failures in the PRA.

19-198

The ruptured steam generator (SG) is assumed to be always SG “A” for modeling simplicity. Similar assumptions are made for other initiating events, such as loss of coolant accidents (LOCAs). The PRA results and insights must be properly adjusted (e.g., to reflect the fact that a tube rupture is equally likely to all SGs) to prevent erroneous conclusions about the risk significance of systems, structures and components (SSCs) and, therefore, prevent incorrect decisions in risk-informed applications, such as those associated with the design reliability assurance program (D-RAP) and the risk managed technical specifications (RMTS). Please verify that the US-APWR PRA results and insights are properly modified to avoid mistakes stemming from simplifying modeling assumptions.

19-199

Table 6A.7-6 of Revision 1 of the PRA report lists common cause failure (CCF) events associated with the pressurizer pressure control system. Event PZRCF2MVCD58R is defined as the CCF of components MVRA, B to close (with basic event identifiers PZRMVCD58RA, B). However, this CCF to close event as well as the associated basic

event identifiers PZRMVCD58RA, B are not defined or even listed in Table 6A.7-5 where all the basic events for the system are listed. Also, Section 6A.7.1.1 states: "This chapter provides an evaluation of the reliability of the RCS depressurization by SDVs and the safety depressurization valve." How is the "safety depressurization valve" different than the "SDVs"? Please clarify.

19-200

The human error event PZROO02PORV (Table 6A.7-7 of Revision 1 of the US-APWR PRA report) is defined as the operator failure to depressurize the primary side by opening the safety depressurization valves (SDVs) from the main control room when steam generator tube rupture (SGTR) isolation fails. Through this action the equalization of the primary and secondary pressures can be achieved and allow control of the primary to secondary leakage, thus enabling the operation of the residual heat removal system (alternate core cooling). The frequency of the SGTR core damage sequence # 12, which involves the failure to isolate the faulted SG and the failure to depressurize the RCS using the SDVs, is estimated to be 1.8E-9 per year (Table 19.1-21 of the US-APWR DCD Ch. 19). The staff needs additional information about any design and operational features as well as any modeling assumptions that contribute to the low frequency of this sequence. In addition, the staff needs more detailed information to clarify the following:

(1) How the dependencies among the specific human errors appearing in the SGTR sequence #12 were determined (e.g., given that the operators fail to close the MSIV associated with the faulted SG, what is the probability that they will also fail to depressurize the primary using the SDVs?). Please explain all assumptions made with respect to the various dependency factors and address any uncertainties that may be introduced by these assumptions.

(2) The reasons why, following a turbine bypass valve (TBV) failure to reclose, the MSIV 533A hardware failure to close is not considered to be a failure to isolate the faulted SG while the operator failure to close MSIV 533A is considered to be a failure to isolate the faulted SG (see gate MSP-OS-05 of fault tree MSP-OS).

(3) The reasons why the potential rising of the water level in the faulted SG, which could cause the main steam safety valves (MSSVs) to pass water and fail open, has not been modeled.