AECL
TECHNOLOGIES INC.

April 15, 2004

Our File: 108US-01321-021-001
Your File: Project No. 722

U.S. Nuclear Regulatory Commission,
Document Control Desk,
Washington, D.C. 20555

Attention: Ms. B. Sosa
Project Manager, ACR

Reference:

1. E-mail J. Kim to V. Langman, "ACR-700 RAI #5 PRA Analysis Basis", January 20, 2004.

Re: **Response to NRC's Requests for Additional Information (RAIs) #4 on PRA Analysis Basis**

In response to NRC's request (Reference 1) and in support of the NRC's pre-application review of the ACR (i.e., specifically focus topic # 11 – ACR PRA Methodology), attachment 1 provides AECL's responses to NRC staff requests for additional information on PRA Analysis Basis.

If you have any questions on this letter and/or the enclosed material please contact the undersigned at (905) 823-9060 extension 6543.

Yours sincerely,

for: Vince J. Langman
ACR Licensing Manager

/Attachment:

1. Response to NRC's Requests for Additional Information (RAIs) #4 on PRA Analysis Basis

D070

Attachment 1
(Letter V. Langman to B. Sosa, "Response to NRC's Requests for Additional Information (RAIs) #4 on PRA Analysis Basis", April 15, 2004)

Response to NRC's Requests for Additional Information (RAIs) #4 on PRA Analysis Basis

AECL's responses to NRC's requests for additional information on PRA Analysis Basis are provided in italic fonts following each of the NRC's questions as follows:

The following questions and comments were generated from an initial review of "Analysis Basis: Probabilistic Safety Assessment Methodology," AECL Report 108-03660-AB-001, Revision 1, July 2003. The following additional information is required to complete the review.

37. Section 1.1, Page 1-2: This section states that the PSA will satisfy ASME Capability Category I. Based on Table 1.3-1 in ASME RA-S-2002 (which provides the bases for PSA capability categories), Section 2.2.3 of Regulatory Guide 1.174, Section III.2.2.4 in Chapter 19 of the Standard Review Plan (SRP), and Section 1.3 of Regulatory Guide 1.200, the NRC staff believes that most elements of the ACR-700 PSA should meet or exceed Capability Category II. The ACR-700 PSA should identify the relative importance of dominant contributors at the component level, using design-specific data and models to the extent practicable. Any departures from realism should have a small impact on the conclusions and risk insights. The NRC staff notes that ASME RA-S-2002 does not provide a means to determine the overall capability of a PSA; rather, different capability categories are used for various PSA elements. Please provide a self-assessment of the ACR-700 PSA that indicates the expected ASME capability category for each supporting requirement, and provide justification for acceptance of PSA elements that not meet ASME Capability Category II.

AECL Response:
As stated in the response to RAI #34 (sent with cover letter dated February 12, 2004), AECL is preparing the self assessment table and will provide it to the NRC by June 01, 2004.
For each item in the ASME standard, the category level achieved by the ACR PSA will be identified. An explanation will be given for the basis of assigning the Category Level for each supporting requirement.

38. Section 1.3, Page 1-7: The methodology document states that a Level 1 and Level 2 PSA addressing internal events, internal floods, internal fires, and shutdown states will be performed. However, no technical details have been provided about how specific plant operating states (POS) and off-normal, but periodic changes in plant configurations will be reflected in the PSA. Please explain how POSs and off-normal, but periodic changes in plant configuration will be defined, including those related to shutdown operations and on-power refueling. Describe how the PSA logic model will reflect each unique POS and off-normal, but periodic change in plant configuration.

AECL Response:
PSA logic model for different POSs for the selection of initiating events in the PSA is described in report 108-03660-ASD-001 Rev. 1.

The scope of the PSA will have the following plant operating states:

1. *Nominal full power*
2. *Shutdown state*
    a. *Reactor coolant system[1] (RCS) cold, depressurized, and full (including, channel freeze plugging)*
    b. *RCS cold, depressurized and drained to the headers*
    c. *RCS warmup and cooldown*

Separate event trees will be prepared for states 1, 2a and 2b. The RCS warmup and cooldown states will be described outlining for such short time period, approximately an hour, that initiating events are screened out based on frequency (< E-07/yr), or that the event is bounded by full power operation, or by 2a.
Potential on-power refueling accidents are considered under state 1.

For each Plant Operating State, plant configuration will be identified. A reactor shutdown fault tree will be developed which can toggle various trains and equipment that may be out for maintenance during shutdown. For each set of analyses, the flags will be recorded and documented.

1 *In CANDU terminology, Heat Transport System (HTS) is used for the Reactor Coolant System (RCS).*

39. Section 1.3, Page 1-8: Describe the process used to feedback PSA insights to the designers. Is this feedback ongoing, time delayed, or a future activity? In addition, describe how design changes are incorporated into the PSA to ensure that it reflects the actual to-date design. What freeze date is associated with the PSA to be provided as part of the standard design certification application (e.g., three months before the application date)?

AECL Response:
Feedback is ongoing as the PSA team is part of the design organization. This process is iterative between the PSA team and designers.

PSA analysts contact designers to get the latest design information (see also response to RAI #36, submitted with cover letter dated February 12, 2004). The PSA analyst will document the design and assumptions in the fault tree analysis of the system. The design freeze date is several weeks prior to the time of accident sequence quantification (ASQ).

40. Section 2.1, Page 2-1 and Section 11.1, Page 11-1: The stated objectives of the PSA imply that the main purpose for developing the PSA is to demonstrate compliance with various numerical risk acceptance guidelines. The NRC staff notes that compliance with numerical risk acceptance guidelines does not mean that the design is acceptable, and that noncompliance does not mean that the design is unacceptable. Therefore, while numerical risk acceptance guidelines are useful tools, the NRC staff believes that the main purpose of performing the PSA is to obtain insights on severe accident vulnerabilities. For example, the PSA should provide information to designers, plant owners and operators, regulators, and the public about the types of risk-significant accidents and their causes (e.g., human error, common-cause failure, etc.). It is suggested that this section be revised to reflect these uses of the PSA.

AECL Response:
The section will be revised to include other benefits/objectives of PSA. AECL intends to provide risk informed information. Risk insights will be described, such as importance measures, what dominates the risk, vulnerabilities due to human error, and common cause failures, etc.

41. Section 2.1, Page 2-1: AECL's risk acceptance guidelines do not match those contained in SECY-90-16 (see ADAMS Accession Numbers ML003707849 and ML003707885). AECL has proposed a severe core-damage frequency (SCDF) target of < 1E-5/year, which is an order of magnitude less than the NRC's target for the total core-damage frequency (CDF) of < 1E-4/year. However, AECL has not proposed a target for the limited core-damage frequency (LCDF), although the PSA appears to be capable of estimating the LCDF. In addition, the NRC target for the conditional containment failure probability (CCFP < 0.1) is not discussed in the AECL PSA methodology document.

AECL Response:
AECL has adopted Advanced Light Water Reactor (ALWR) targets for SCDF and LRF. The conditional containment failure probability (CCFP) is derived as CCFP=LERF/SCDF, and will be quantified for ACR-700.
Dose limits, rather than frequency targets, are set for limited core damage accidents (LCDA) to ensure that their consequences do not pose an undue risk to the health and safety of the public. Conditional containment failure probability following SCD is a maximum of 0.1 and is established as a cumulative frequency of 10(-6) per year for large release (see ACR Safety Basis 108-03600-AB-003 Rev. 0 and PSA Methodology 108-03660-AB-001 Rev. 1)

42. Section 4.2.4, Page 4-2 and Section 4.3.2.1, Page 4-5: Please explain how success criteria are developed from the definitions of limited core damage (LCD) and severe core damage (SCD). Describe the extent of the thermal-hydraulic calculations used to determine success criteria. For example, will all success criteria be based on calculations? If not, what decision process is used to determine that certain calculations are not necessary? Since the NRC has limited experience with CANDU plants, success criteria should have objective bases rather than relying upon engineering judgement that cannot readily be confirmed by the NRC staff.

AECL Response:
Success criteria are based on engineering calculation for successful operation. Calculations will not be performed for all success criteria. The decision on which case needs success criteria calculation will depend on statements that the consequences are bounded with respect to another success criteria calculation. Safety analysis defines the success criteria for mitigating systems for accidents. For events that are not documented, PSA support analyses will be performed to confirm the PSA assumptions.
The PSA support analysis confirmation process was applied to previous CANDU 6 PSAs. PSA revision is performed where the analyses do not confirm the assumptions.

43. Section 4.2.5, Pages 4-2 to 4-3 and Section 4.4.1, Page 4-9: The methodology document lists three methods for estimating IE frequencies, all of which are statistical in nature. Will fault trees be used to estimate some IE frequencies (e.g., for support systems failures that would initiate a transient)? If so, which ones?

AECL Response:
AECL plans to use CANDU plant operating experience, to derive initiating event frequency for the majority of events. In a limited amount of cases IE fault trees may be prepared because of differences between the ACR and current CANDU operating plants. The differences are due to improvements in the ACR design. At this time AECL has not identified which IE frequency will be derived by fault tree.

44. Section 4.2.5.4, Page 4-3 and Appendix A, Section A.1: The chi-squared approximation using 2n+1 degrees of freedom is an estimator for the median of the failure rate uncertainty distribution. The PSA should be quantified using the means of the uncertainty distribution.

AECL Response:
Mean values will be used in the ACR PSA.

45. Section 4.3.2.4, Page 4-6 and Section 9.3, Page 9-2:: How does the PSA methodology account for the dynamic effects of high-energy line breaks (pipe whip, jet blast impingement, steam flooding)?

AECL Response:
The ACR is designed for pipe whip effects, leak before break and jet impingement effects, from high energy piping. The safety design guide on environmental qualification (108-03650-SDG-003) caters for environmental effects due to steam flooding.
The screening analysis, assuming that all equipment in the area and in the flooding propagated area is not available, would cover the impacts of high energy line breaks (HELB). For the area not screened out, the detailed analysis will identify HELB source and develop detailed flooding scenarios. The flooding scenario would include the effects of jet impingement and steam flooding. The effects would consider the directional factor and the distance from the jet impingement and the potential impacts of hot temperature, humidity, and condensation from the steam flooding.

46. Section 4.3.4, Page 4-7: The methodology document states that sequence development is terminated on low frequency. Since sequence development occurs before PSA quantification, how can this approach be practically applied? The NRC staff notes that this approach may work for a baseline risk estimation, but produces a PSA that is inadequate to support future changes to the licensing basis (where some previously terminated sequences may need further development) or real-time risk monitoring. It seems better to completely model all sequences, then let the computer software truncate low frequency sequences.

AECL Response:
Based on previous CANDU PSAs, sequence frequencies for event trees is known. Based on preliminary ACR reliability targets, analysts can assess whether "not developed further" (NDF) sequence can be applied to the ACR ETs. When ASQ is performed, AECL will quantify all plant damage state (PDS) sequences including those identified as "not developed further" (NDF) sequences.
After ASQ, if individual sequences occur >1.0 E-9 /yr and are terminated prematurely in the event trees (ET), then the ET logic will be extended and the accident sequence re-evaluated. For design stage PSA this approach is considered adequate.

47. Section 4.3.4, Page 4-7: This section proposes to use a truncation limit of 1E-10/year for accident sequences. However, external events will be screened at 1E-07/year. Please reconcile this difference. Also, will the truncation limit be varied to demonstrate convergence of the accident sequence frequencies?

AECL Response:
The screening criteria of external events analyses is not compatible with the truncation limits. The screening will be done on an area basis and only be done after SCDF quantification for the worst case scenarios due to the external events for each area/zone. NUREG-1407 recommends using 1.0E-06/yr as the screening criteria for the external events. AECL will use a lower screening criteria of 1E-07/yr for the ACR-700 external events PSA.

AECL will show the convergence of the frequencies for internal events. The ASQ will be performed using truncation limits of 1E-08 first and then lowering the limit to 1E-09 and 1.0E-10. If it shows the convergence, then the ASQ will stop at the 1.0E-10 truncation limits. If it does not show the convergence, the ASQ will be continued until the convergence is shown.

48. Section 4.3.4, Page 4-7: This section implies that sequences resulting in limited core damage(LCD) will not be addressed in the Level 2 PSA. However, AECL Report 108-126810-LS-001, Chapter 3, Page 3-1 states that LCD accidents will, in fact, be addressed in the Level 2 PSA. The NRC staff believes that the Level 2 PSA should address all core-damage sequences (both SCD and LCD). Please reconcile this difference.

AECL Response:
Level 2 PSA will cover severe core damage (SCD) sequences (with and without containment functional), as well as limited core damage (LCD) sequences (with impaired containment function). The LCD event with containment functions maintained will be covered in a subsection of Chapter 19 of the design control document.

49. Section 4.4.5, Page 4-11: The use of a basic event naming scheme alone will not completely defend against mislabeling errors. The entire set of fault trees must be reviewed, paying particular attention to the system boundaries to ensure that the same basic events in different system models have the same labels.

AECL Response:
Fault trees will be reviewed to identify mislabeling errors, and system boundaries to confirm the scope of the analyses. The review will identify any system boundary overlap by different analysts.

50. Section 4.4.6.3, Page 4-12: Does this section contain a typographical error ("2 months" is used in the second paragraph whereas "4 months" is used in the third paragraph)?

AECL Response:
AECL will correct the typographical error to 2 months.

51. Section 4.4.8, Page 4-14: The systems analysis documentation should contain or reference the basis behind system success criteria.

AECL Response:
The success criteria will be based on design documentation and the Design Control Document, or PSA support analysis.

52. Section 4.5, Page 4-14: This section appears to contain an editorial error since it is entitled "Labelling [sic] of Fault Tree Events," but partially discusses the dependent failure analysis.

AECL Response:
The subsection title will be corrected to dependent failure analysis.

53. Section 4.7.2.1.1, Page 4-15: Data will be based "as much as possible" on operating experience at Pickering NGS A and Bruce NPS A. Why only these plants? Why not use data from all CANDU plants?

AECL Response:
Presently component data for the PSA is based on generic operating experience CANDU data from Pickering A &B (8 units), and Bruce A & B (8 units) and Point Lepreau (1 unit) power plants.

54. Section 4.7.2.1.2, Page 4-16: This section states that generic data will be obtained from IEEE Standard 500-1984 and NPRDS 1983 Annual Report. Since these data sources are more than 20 years old, how do they apply to an advanced reactor such as ACR-700?

AECL Response:
The Darlington "A" Risk Assessment (DARA) component reliability database has some input from NPRDS and IEEE. ACR-700 is an evolutionary design. Some components of the ACR-700 have not changed radically in design /operation from operating CANDU plants. It is felt that the DARA database can still apply for ACR-700 for a design stage PSA. It is expected that the utility will later collect the operating experience data of the ACR and update the PSA with site specific reliability data.

55. Section 4.7.3, Page 4-16: Describe how the "total component operating time" will be obtained. This information should depend on the specific failure mode ("failure to start," "failure to run," etc.).

AECL Response:
AECL agrees that to obtain the best estimate of a failure rate, the total operating time should depend on the failure mode. For example, for a standby generator, the "total operating time" for calculating the running failure rate should be its running hours, which is usually a very small fraction of its in-service hours; the "total operating time" for calculating the (time-based) start failure rate could be its in-service hours.
The component reliability data used for the ACR PSA does this to the extent practical.

56. Section 4.7.3, Page 4-17: How will uncertainty in MTTR be estimated and propagated in the logic model?

AECL Response:
AECL will apply error factors to the MTTR. This will be an input into the basic event fault tree modeling.

57. Section 4.8.2.1, Page 4-20: Describe how logic flags (house events) will be defined, incorporated in the logic model, set during accident sequence quantification, and documented.

AECL Response:
Plant response information identifies which part of fault tree models is relevant. An example of a flag is shutdown system trip parameters. Based on the plant response, the appropriate trip parameter is credited in the event tree, whereas the inappropriate trip parameters are not credited. Flags are placed strategically in the fault trees so that relevant parts of the system are modeled.
AECL will discuss the use of logic flags as part of the chapter on accident sequence quantification (ASQ). The flag settings (whether true or false) for each event tree is recorded during the ASQ process and then documented in this chapter.

58. Section 4.8.2.1, Page 4-20: Describe how top logic (fault tree logic used to combine systems for a particular event tree heading) is reviewed and documented.

AECL Response:
In most cases, there is a one to one correspondence between the ET heading and the fault tree top event such as ECI (emergency coolant injection) and SGCC (steam generator crashcool). For a specific event tree heading, there could be a need for " bridging fault tree logic" between the event tree heading, and the system reliability models. The "bridging fault tree logic" will be reviewed by the PSA team leader. These models will be prepared, and documented in the accident sequence quantification chapter.

59. Section 4.8.2.6, Page 4-22: Will fault tree modularization be performed by each system analyst, or done during the PSA quantification effort?

AECL Response:
Modularization will be done during the system analysis stage by each system analyst.

60. Section 4.8.2.8, Page 4-22: Please describe how the intended recovery analysis scheme (applying recoveries only to sequences with frequency > 1E-9/year) avoids skewing the risk profile.

AECL Response:
The recovery analysis will be performed in the following manner:

1. *For each individual plant damage state sequence, the cutsets will be reviewed to gain engineering and operation insights on what action the plant staff can perform.*
2. *The cutsets will be reviewed to identify running failures of components. Component running failures allow time for operator action.*
3. *Depending on the accident sequence, what component has failed, the available operator action time to prevent an undesirable event (e.g., empty steam generator), and equipment accessability, the recovery action can be credited for that cutset listing contributor to plant damage.*
4. *The rules for recovery are documented and automatically implemented on the cutset listing via the software.*

For a design stage PSA, the event tree end states that are estimated to occur <1.0 E-09/yr, recovery analyses will not be applied. The subsequent PSA for COL stage will extend the ET logic with no frequency truncation, and recovery analyses will be performed on all core damage sequences.

61. Section 4.8.2.8, Page 4-22: Could multiple recoveries be applied to the same cut set? If so, how are potential dependencies among the recoveries addressed? If not, what scheme will be used to prioritize the application of recoveries?

AECL Response:
Potentially multiple recovery actions could be applied to a specific cutset listing. However, this depends on the number of staff complement in the main control room (MCR) and the field. Based on past experience AECL has not applied multiple recovery actions. Normally, there is one recovery action in each cutset where certain conditions apply. However multiple recovery actions could be applied. If multiple recovery actions are credited, AECL will develop a process to consider the recovery action dependency.

62. Section 4.9.1, Page 4-23: Please clarify the first paragraph of this section. Are all cut sets in a given sequence assigned to the same PDS?

AECL Response:
Section 4.9.1 will be revised to clarify that for a given sequence all the cutsets are assigned to the same PDS.

63. Section 4.9.2.7, Page 4-27: AECL should already have adequate information ("The Technology of On-Power Refueling," 108-35000-LS-001, Rev. 0, September 2003, which has 238 pages of information) to analyze PDS10 (fueling machine failures). The NRC staff expects that the PSA will contain adequate modeling to support the quantification of PDS10.

AECL Response:
As per the systematic plant review report (108-03660-ASD-001 Rev. 1) fuel machine (F/M) failure events for both cases of fueling machine "on' reactor, and fueling machine" off" reactor are considered. PDS 10 applies to F/M failure events when the machine is "off" reactor.

64. Section 5.1, Page 5-2: The most recent NRC guidance on common-cause failure (CCF) methods is contained in NUREG/CR-5485, and the most recent CCF data is NUREG/CR-5497. The cited references should be updated.

AECL Response:
The references will be updated.

65. Section 5.5.1, Page 5-8: The Unified Partial Method (UPM) is a methodology for determining CCF beta factors. It is not capable of modeling partial CCF groups (e.g., two-out-of-three components in a CCF group fail). Ignoring partial CCF groups is not acceptable. Please describe how partial CCF groups will be addressed.

AECL Response:
AECL recognizes the limitation in applying the UPM for CCF analysis. AECL believes the UPM approach for modeling CCF is conservative. The CCF modeling approach is the following:

1. *AECL will apply a CCF value of 0.1 for screening purposes;*
2. *If the reliability targets are not met, AECL will apply the UPM for CCF;*
3. *If the UPM results are not acceptable, an alternate method, such as "alpha" will be used.*

66. Section 5.5.3.2, Pages 5-11 and 5-12: How is uncertainty in CCF event probabilities estimated?

AECL Response:
Component failure rates have error factors of 3. AECL proposes to assign the same error factor for CCF as the component failure rates.

67. Section 5.5.3.1, Page 5-11: Will AECL employ the screening approach to CCF modeling? If so, NUREG/CR-5485, Table 3-1 contains the latest recommendations for beta factors to be used in the screening analysis.

AECL Response:
AECL plan to use the CCF screening approach, by assigning a 0.1 factor.

68. Section 5.5.3.2, Table 5-1, Page 5-12: Since human factors are presumed to be addressed in the HRA, they have been removed from the CCF analysis. Has the denominator used to develop the beta factor (the value of 50000) been adjusted/renormalized to remove the human factor contributions? (Otherwise, the beta factor estimates would consistently be too low.)

AECL Response:
AECL will review this topic and will respond to the NRC by April 30, 2004.

69. Section 5.5.4, Table 5-2, Page 5-13: Please justify that the list of component types for CCF analysis is adequate. In particular, justify omitting circuit breakers, heat exchangers, strainers, check valves, and relief valves (PORVs, etc.). NUREG/CR-5485 provides CCF data for these components.

AECL Response:
These items above were not omitted, as Table 5-2 is a list of typical components, not an all inclusive one. For ECCS sump strainer plugging, a sensitivity analyses will be performed. Relief valves such as liquid relief valves for reactor coolant system overpressure protection (OPP), and main steam safety valves for main steam line OPP, CCF will be included.

70. Section 5.5.5.6, Page 5-17: How will AECL ensure consistency if the subfactor categories in UPM are reassigned? The work is likely to be done by different analysts.

AECL Response:
To date AECL is using specific categories in the UPM manual. No subfactors are being considered. If in the future subfactors are to be used, AECL will document guidelines for consistent application. The subfactors would be reviewed by the PSA supervisor for consistency between separate analysts.

71. General: The NRC staff presumes that the ACR-700 design will utilize state-of-the-art digital control and instrumentation systems. How will software reliability and CCF potential in digital systems be addressed in the PSA?

AECL Response:
Software reliability is not addressed in the PSA. Software reliability is addressed in the software QA program, in terms of design, implementation and exhaustive testing.
For the time being, modeling of the digital control will be treated as a " black box". AECL will review what CCF factor should be assigned for digital control equipment (PDC,CPU, PLC) and will respond by April 30, 2004.

72. Section 6.3, Page 6-4: What style of emergency operating instructions (EOIs) will be developed for the ACR-700: symptom-based EOIs or event-based EOIs?

AECL Response:
There will be both types of procedures; symptom and event based. ACR-700 will have symptom based emergency operating procedures (EOPs) for generic actions on power reduction, heat sinks and containment integrity. Event based EOPs will be prepared for events where the entrance conditions are clear. The shift supervisor is responsible for implementation of the generic EOP and the reactor operator is responsible for implementation of the event based procedure. The human reliability assessment (HRA) description will recognize the use of these EOPs.

73. Section 6.5.5, Page 6-18: For the post-initiator execution errors, what does "maximum time available" mean? Is this the maximum available execution time, or the maximum available time from the compelling signal (including diagnosis time and execution time)?

AECL Response:
The maximum available time is the time from the compelling signal to some undesirable event. For loss of main and auxiliary feed water event, and no automatic makeup to the steam generators, the compelling signal is low steam generator level. The steam generator level will drop via the secondary side inventory boiling, and the steam being discharged to atmosphere via the main steam safety valves. The maximum time available for operator action is between the compelling signal and the steam generator becoming empty.

74. Section 6.5.6, Page 6-19: This section states that completely dependent post-accident human actions will not generally be modeled in the event trees. While this approach may produce acceptable numerical results, it is essential to provide adequate explanation and documentation. It may be better to include completely dependent post accident human actions in the PSA logic model.

AECL Response:
AECL will explain why a specific subsequent operator action is not credited after a previous human error in the event trees due to dependencies. Subsequent operator actions may be credited as part of recovery analyses at the cutset level. AECL will address additional human actions, and their probabilities during recovery analysis.

75. Section 6.8, Page 6-21: How is the recovery of offsite power addressed in the PSA?

AECL Response:
AECL has used in the past probability of the recovery of offsite power based on NUREG-4550 Vol 3 Part 1 Rev 1, and added the recovery of offsite power to the relevant cutsets. AECL will look at more up to date information. As agreed at the February 5 and 6, 2004 meeting, the NRC will advise AECL if there is more recent data on recovery of offsite power probabilities.

76. Section 6.8.9, Page 6-23: This section states that recoveries will be modeled using the post-accident diagnosis and execution models. Justify using this approach. The NRC staff expects that some recoveries will have higher failure probabilities that estimated using the post-accident HRA models (e.g., recoveries that rely upon knowledge-based behavior).

AECL Response:
For recovery actions, that have no EOP, the human error will be based on cognitive thinking. The human error probability for recovery action is based on diagnostic and execution errors. The recovery action needs to have a diagnostic input. Diagnostic model in Table 6-3 will be revised recognizing that no EOP exists for the recovery action.

77. Section 7.1, Page 7-1: SECY-93-087 (see ADAMS Accession Nos. ML003708021 and ML003708056) specifies that bounding analyses be provided for site-specific external events likely to be a challenge to the plant (e.g., river flooding, storm surge, tsunami, volcanism, high winds, and hurricanes). However, the ACR-700 PSA methodology focuses only on seismic events, internal fires, and internal floods. What are AECL's plans for addressing the other types of external events?

AECL Response:
The other types of external events will be analyzed during the site specific PSA phase. ACR will perform progressive screening analysis for other external events as follows. The analysis step is consisted of following:

1. *Identify all potential external events to be considered.*
2. *Group events with similar plant effects and consequences.*
3. *Establish screening criteria to determine which events are risk insignificant and can therefore be excluded from detailed quantitative evaluation.*
4. *Evaluate the events against the screening criteria to determine if the event was risk-significant.*
5. *Perform bounding analysis for the external events, which are not screened out from above process, to show that the external events are non-risk significant.*
6. *Determine external events requiring detailed analyses.*
7. *Perform detailed analyses.*

The screening criteria presented below will be used:

- *Criterion 1: The event is of equal or lesser damage potential than the events for which the plant has been designed.*
- *Criterion 2: The event has a significantly lower mean frequency of occurrence than another event, taking into account the uncertainties in the estimates of both frequencies, and the event could not result in worse consequences than the consequences from the other event.*
- *Criterion 3: The event cannot occur close enough to the plant to affect it.*
- *Criterion 4: The event is included in the definition of another event implicitly or explicitly.*
- *Criterion 5: The event is slow in developing and it can be demonstrated that there is sufficient time to eliminate the source of the threat or to provide an adequate response.*
- *Criterion 6: The current design-basis-hazard event cannot cause a severe core-damage accident.*
- *Criterion 7: The current design basis hazard event has a mean frequency less than 10^{-5} per year, and the mean value of the conditional severe core damage probability (CCDP) is assessed to be less than 10^{-1}.*
- *Criterion 8: The severe core-damage frequency (CDF), calculated using a bounding analysis, has a mean frequency less than 10^{-6} per year.*

78. Section 7.5.1, Page 7-9: How will the high confidence of low probability of failure (HCLPF) values be determined for ACR-specific structures and components (e.g., the calandria)? Since these components are unique to the ACR design, the use of generic fragilities, expert opinion, or screening values needs justification.

AECL Response:
It is expected that the information about the seismic design for those SSCs is not available during the design certification stage. Therefore in principle, 0.5g HCLPF capacity is assumed for the SSCs. The seismic fragility calculations for those SSCs will be listed as one of COL action items. To provide some input to the designers, limited assessment using the demand data of ACR (0.3g with enveloped Design Ground Response Spectra) and the capacity data of existing CANDU-6 (0.2g, rock site) will be performed. Any findings and vulnerabilities will be transferred to the designers for input to the seismic design for those SSCs if needed.

79. General: For the seismic, internal fire, and internal flood analyses, AECL should calculate the frequencies of all PDSs, not just those that comprise SCD.

AECL Response:
AECL will quantify the frequencies of all PDSs from external events, except for seismic events. AECL is planning to perform PSA based seismic margin analysis in deriving the plant HCLPF.

80. Section 8.3, Page 8-3: During the fire analysis, why may it be necessary to use judgement and assumptions to determine cable locations? The NRC staff expects that the actual cable routing has already been designed and will be used in the PSA.

AECL Response:
The cable routing design is performed in the final stage of detailed design. It is not considered practicable that the design certification stage of ACR design produces detailed cable routing information. However, it is expected that the layout plan for the major cable raceways, which shows how the cable trays are located on division/train basis, is available when the plant layout is fixed. The fire analysis will be performed using the layout plan and supplemental assumptions about the some cable routing. The assumptions incorporated in the fire analysis will be documented and transferred to the designers for further use in the design.

81. Section 8.4.2, Page 8-6: The section states that if a fire could cause several initiating events, AECL will pick the worst one for further analysis. Define "worst," and justify why multiple initiators caused by a single fire event will not be addressed.

AECL Response:
The "worst" means the highest conditional core damage probability given the external events induced situation. When the fire causes multiple failures of systems or equipment, the worst initiating event is selected for developing the accident sequences. Other failures will be considered as boundary conditions for the initiating events. For example, when small LOCA and loss of offsite power occurs due to the fire, small LOCA will be selected as the initiating event and loss of offsite will be considered as the boundary conditions for the small LOCA event.

82. Section 9.6.1, Page 9-8: How will maintenance-induced floods be addressed in the PSA? The current AECL approach only considers floods originating from piping failures.

AECL Response:
During the screening analysis, the flooding frequency due to the maintenance error is considered to be 1.0E-3 for each flooding area considered and the flooding frequency is added to the flooding frequency from other causes. For the flooding area not screened out, the flooding due to the maintenance error will be considered as follows:

1. *The maintenance activity that can cause the flooding will be identified. The concern would be the maintenance activity that needs isolation of flow.*
2. *For those maintenance activities, the flooding frequency will be estimated, considering 1) maintenance frequency, 2) operator error to secure the isolation, and 3) the probability that the erroneous signal to open the valve occurs.*
3. *If there is a specific procedure for securing the isolation, the operator probability of 0.01 will be used. If not, that of 0.1 will be used.*
4. *0.01 will be in general used for the probability of occurring erroneous signal during maintenance activity, if there is not specific design or administrative provisions to prevent that.*

The flooding due to maintenance will be added in the flooding frequency for the area and the flooding scenarios due to maintenance will be developed considering the specific condition of the flooding.

83. Section 10.1, Page 10-1: AECL should perform uncertainty calculations for each plant damage state (PDS), the limited core-damage frequency (LCDF), the severe core damage frequency (SCDF), the large release frequency (LRF), and the conditional containment failure probability (CCFP).

AECL Response:
AECL agrees to assess the scope of the uncertainty analysis and inform NRC by May 17, 2004.

84. Section 10.1.3.4, Page 10-2: The approach to uncertainty analysis only addresses parametric uncertainties. What analyses (e.g., sensitivity analyses) will be performed to address modeling uncertainties?

AECL Response:
AECL plans to perform selective sensitivity analyses for addressing modeling uncertainties.

85. Section 10.2, Page 10-4: AECL should provide importance measures (Fussell-Vesely and risk achievement worth) in the PSA documentation.

AECL Response:
AECL will provide importance measures (Fussell-Vesely and risk achievement worth) in the PSA report.

86. Section 11.2, Page 11-1: Please define the term "large release" that will be used in the ACR-700 PSA. Note that the NRC has not formally issued such a definition (see the Staff Requirements Memorandum for SECY-93-138, ADAMS Accession No. ML003761015). However, Appendix A to NUREG/CR-6595, Revision 1 (issued August 2003 as a Draft for Comment) provides three working definitions of large early release frequency that could be adapted.

AECL Response:
AECL will review Appendix A of NUREG/CR 6595 Revision 1, to see which working definition applies to the ACR definition of a large release. The large release for ACR, will be defined by May 30, 2004.

87. Section 11.4, Page 11-3 and Figure 11-1, Page 11-6: The methodology presumes that anticipated transients without scram (ATWS) sequences (PDS0) will have low frequency, so it is not necessary to address them in the Level 2 PSA. The NRC staff disagrees; it is essential to obtain risk insights (both Level 1 and Level 2 PSA) about ATWS sequences.

AECL Response:
The ACR has 3 automatic means to shutdown the reactor. The individual ATWS sequence frequency is much less than 1E-07/year, considering that each shutdown system has unavailability less than E-03 and the stepback has an unavailability of the order of E-02. The preliminary design assist ACR PSA work done to date, derived the summed failure to shutdown frequency ~ 5E-08/yr. Because the ACR has 3 independent means to shutdown the reactor, there are no plans to analyze the ATWS event in the Level 2 PSA.

88. Section 11.6, Pages 11-4 and 11-5: Please clarify what is meant in this section concerning the development of ACR-relevant failure criteria. The text implies that some design details needed to develop the failure criteria (and hence, the source terms) are not readily available. Why not?

AECL Response:
Before the start of the level 2 PSA, the failure criteria will be defined. Failure criteria will be defined for channel disassembly, calandria vessel, and calandria vault breach. This section will be revised by deleting the above sentence in Section 11.6.

89. Section 11.8, Page 11-5: This section states that "The large release frequency will be derived by screening the source terms bins against criteria of Section 11.2." However, Section 11.2 does not provide any screening criteria.

AECL Response:
Section 11.2 will be revised to describe the screening criteria by May 30, 2004.

90. Section 11.8, Page 11-5: This section states that "The large release frequency will be derived by ... identifying the accident with the highest frequency of relevant bins." Please clarify this statement.

AECL Response:
This section will be expanded, to describe the derivation of the large release frequency. AECL will respond to NRC by May 30, 2003 with the expanded section.