19N Analysis of Common-Cause Failure of ~~*Multiplex*~~ Essential Communications Equipment

The information in this appendix of the reference ABWR DCD, including the above title, subsections, tables, and figures, is incorporated by reference with the following departures.

STD DEP T1 3.4-1

19N.1 Introduction

STD DEP T1 3.4-1

The effect of common-cause failures of the ABWR Essential Communications Function (ECF) *equipment ~~(EMUX)~~ on each safety function is included in the PRA analysis of each of the transient and LOCA initiating events (Appendix 19D). The fault tree designators for ~~EMUX~~* ECF *CCF are CCFMUX, CCFTLU, and ILCCFH. The probability values used in the PRA analysis are based on random probabilities of failure and common-cause beta-factor. The effect on total core damage frequency (CDF), as evaluated, is found to be significant.*

Because of the importance of the ~~multiplexing~~ ECF *equipment to ABWR instrumentation and control, a supplemental study of ~~EMUX~~* ECF *CCF has been performed to further investigate the effects of the use of common instruments, ~~multiplexers~~* ECF equipment*, and transmission networks for reactivity control (scram), ECCS (core cooling and decay heat removal), and LDIS (isolation).*

The safety system logic and control (SSLC) has four independent divisions of instrumentation having separate sensors, actuators and ~~EMUX~~ ECF *equipment. ~~Within a given division, the only restriction regarding assignments of sensors and actuators to RMUs is that wide-range and narrow-range reactor water level sensors cannot be input to and processed by the same RMU.~~*

The primary effect considered in this analysis is that due to common-cause failure of automatic initiation of the ECCS and RPS functions. The study also examines the effects of ~~EMUX~~ ECF *common-cause failure on containment isolation.*

19N.2 Results and Conclusions

STD DEP T1 3.4-1

The effects of ~~EMUX~~ ECF *CCF on total core damage frequency are found to be significant for transient and LOCA initiating events as analyzed in the PRA (Subsections 19N.5.1 - 19N.5.3). Additional "special" initiating events have been analyzed and found to not be affected by ~~EMUX~~* ECF *CCF (Subsection 19N.5.4) Common-cause failure of the ~~EMUX~~* ECF *equipment during normal plant operation at power has also been examined as a potential accident initiator, and found to be a negligible CDF contributor (Subsection 19N.5.5).*

The PRA analysis contains several conservatisms in regard to the evaluation of the effect of ~~EMUX~~ ECF *CCFs on CDF.*

The potential causes of common failure of multiple divisions of ~~EMUX~~ ECF *have been identified as the following:*

- *~~RMUs~~* Remote Digital Logic Controller (RDLC) *Miscalibration*

These eleven potential common causes have been examined (Subsection 19N.4) and only three of them appear to be credible:

(1) *~~RMU~~* RDLC *miscalibration*

All three of these potential causes could exist across division boundaries in spite of physical separation and electrical independence. Because of the existence of these three potential causes of common-cause ~~EMUX~~ ECF *failure, several precautions are being taken regarding defense against them:*

(1) *To eliminate the ~~RMU~~* RDLC *miscalibration as a credible source of* ECF *commoncause failure, administrative procedures will be established to perform crosschannel checking of ~~RMU~~* RDLC *outputs at the main control room SSLC instrumentation, as a final checkpoint of ~~RMU~~* RDLC *calibration work.*

(2) *To eliminate maintenance/test error as a credible source of ~~EMUX~~* ECF *commoncause failure, a thorough post-maintenance test (Subsection 7.1.2.1.6 (4), (5), (6), Protection System Inservice Testability) will be conducted ~~using the surveillance test controller (STC) that is provided in each instrumentation division as part of the EMUX and SSLC designs. The STC contains preprogrammed test sequences for each sensor type and each safety-related system supported by EMUX and SSLC. The tests cannot be changed by the maintenance technician; the technician only selects which system is to be simulated. The STC then injects appropriate simulated sensor signals (traceable to and automatically checked against known standards) into the RMUs of the EMUX. Failure of the calibration standards is alarmed. Testing is dynamic; i.e., the STC injects ramp-type analog signals over the full range (including abnormal upscale and downscale) of the simulated transmitters and also injects pulse, contact closure or frequency-modulated signals as required by the system under test~~. In this way, the full transmission capability of ~~EMUX~~* the ECF *and the functional control and interlock logic in SSLC are tested. Test results are monitored either at the ~~EMUX~~* ECF *outputs in the control room or local area, or at the SSLC outputs, depending upon where test or maintenance was performed. ~~The STC logs the test results, which can also be sent to the process computer or printed out. The STCs are normally off, have continuous self-test, and are operated one at a time, so they are not subject to CCFs of their own. Since the logged test results can verified independently by control room personnel, a single technician can safely maintain multiple divisions of EMUX.~~*

The test features described above check the electronic circuitry from the signal conditioning and A/D converter inputs through the digital processing electronics. Transmitter calibration and other sensor calibration activities will *require two technicians for the four safety divisions. Each will calibrate his division to the inputs of the ~~RMUs~~* RDLCs *and then check the other's work. This will then be repeated for the remaining two divisions.*

(3) To prevent any unidentified ~~EMUX~~ ECF *faults/failure modes (e.g., an undetected software fault) from propagating to other ~~EMUX~~* ECF *divisions, so that such unidentified faults are effectively eliminated as a credible source of ~~EMUX~~* ECF *common-cause failure:*

(a) Chapter 16, Plant Operating Technical Specifications will incorporate requirements on the "Limiting Conditions of Operation" and "Required Action" that must be followed in the event of a failure of a single division of ~~EMUX~~ ECF *and in the event of a failure of multiple divisions of ~~EMUX~~* ECF.

(b) The plant operating procedures will include the appropriate detailed procedures necessary to assure that the ABWR plant operations are maintained within compliance with the governing "Plant Operating Technical Specifications" during the periods of divisional ~~EMUX~~ ECF *failure. These will also include the appropriate symptom-based procedures to assure that adequate core cooling is maintained in the hypothetical event of an entire ~~EMUX~~* ECF *failure.*

The following site-specific supplement addresses COL License Information item 19.8 This COL license information item is addressed in subsection 19.9.8.

19N.3 Basis for the Analysis

The information in this appendix section of the reference ABWR DCD and all subsections is incorporated by reference with the standard departure numbered STD DEP T1 3.4-1.

STD DEP T1 3.4-1

The design features of the ~~EMUX~~ ECF *that are of most importance to and form the basis for this analysis are the following:*

(1) There is complete separation of ~~RMUs, DTMs~~ RDLCs, *Digital* Trip Units Function (DTF) components, DLCs (performing the Safety Logic Function (SLF)), *Trip Logic ~~Units (TLU)~~* Function (TLF) components, *sensors and ECCS actuators, etc., between the four safety divisions of control and instrumentation.*

~~*(2) Within a given division, the only restriction regarding assignments of sensors and actuators to RMUs is that wide-range and narrow-range reactor water level sensors cannot be input to and processed by the same RMU.*~~

(3) There is separation of ~~DTM~~ DTF *and ~~TLU modules~~* TLF components *within a division along the lines of "~~de-energize~~* deenergize *to operate" and "energize to operate" functions, i.e., RPS, and MSIV signals are processed by different*

~~DTM~~ DTF and ~~TLU~~ TLF modules than the ~~DTM and SLU~~ DTF and DLC modules used for ECCS control and PCV isolation (PCV isolation is also ~~deenergize~~ deenergize-to-operate). The RPS/MSIV process channel is "de-energize to operate", while the ESF process channel is predominantly "energize to operate".

(4) *The ~~RMUs~~ RDLCs are connected by ~~a~~ separate ECF ~~network~~ redundant point-to-point serial data links (~~EMUX~~) in each division~~, which is a redundant or reconfigurable control data network of high reliability~~.*

(5) *All data communications to and from other divisions of control and instrumentation, and all data communications to nondivisional systems are electrically isolated.*

(6) *Comparison of a sensed input to a setpoint for generating a trip is done by a~~DTM~~ DTF. Coincident 2/4 trip logic processing for generating a divisional output trip is done by a ~~TLU~~ TLF or DLC performing the SLF.*

(7) *Loss of data communications in any division to the RPS (and deenergize-to operate isolation functions) will result in a trip (and isolation, respectively) in the failed division due to the fail-safe design.*

(8) *Manual scram is implemented by hard wire to the scram pilot valve solenoids and does not depend on the correct operation of the ~~DTM~~ DTF or ~~TLU~~ TLF.*

(9) *A bypass of the RPS output logic unit is a manual, division out-of-service bypass, which allows repair of the ~~DTM~~ DTF or ~~TLU~~ TLF of that division without a half scram condition or half MSIV isolation condition. Only one division can be bypassed at a time.*

(10) *To reduce the probability of spurious initiation of ECCS, two ~~SLUs~~SLFs are used in parallel within a division, with 2/2 voting ~~at~~ of the ~~final channel~~ output to initiate ~~equipment actuation~~ the function. The final vote of the system initiation signals is accomplished with non-microprocessor based equipment in the logic or with a separate actuation of system valves and pumps, where both are required to initiate coolant injection. ~~If one ECCS SLU is in a failed condition, it is automatically bypassed, the control room is alerted, and the remaining SLU operates with 1/1 logic until the failed SLU is restored.~~*

(11) *~~RMUs and EMUXs are self-tested every 15 minutes and repaired/replaced~~ ECF module transmission or reception utilizes self diagnostics for each message. ECF modules can typically be replaced in an average time of 4 8 hours.*

(12) *Control room indicators, annunciators, and alarms associated with ~~EMUX~~ECF-transmitted control signals are dependent on correct operations of ~~EMUXs~~ECFs.*

(13) ~~(12)~~Vital plant parameters are hard-wired to the remote shutdown panel independent of ~~EMUX~~ the ECF.

In addition to the design features listed above, the following assumptions and ground rules also supply the basis for this analysis:

(1) Common-cause failure of all ~~RMUs~~ RDLCs *or all ~~EMUX~~* ECF *point-to-point serial datalinks cannot be ruled-out as impossible or incredible. The reason for this is that several potential common causes can be postulated. (Subsection 19N.2)*

(2) The probability of common-cause failure of ~~inter-divisional~~ all ~~RMUs~~ RDLCs *or ~~EMUX~~* the ECF *is extremely low. The reasons for this are the common-cause defenses built into the design-physical separation, electrical separation, asynchronous operation, optical isolation, ~~natural-convection~~ cooling ability, and the self~~-testing~~* diagnostic *feature-in addition to the special defenses discussed in Subsection 19N.2.*

(3) ~~RMUs~~ The SSLC channels *may be postulated to have common-cause failures of* channels configured either in *the energize-to-trip mode or the deenergize-to-trip mode, but not of both modes simultaneously.*

(4) ~~EMUX~~ ECF *transmission may be postulated to have common-cause failures of the energize-to-trip mode only. Failure of the deenergize-to-trip mode is considered to be not possible.*

(5) Simultaneous failure of all ~~RMUs~~ RDLCs *or ~~EMUXs~~* ECF networks *in the energize-to-trip mode would result in an automatic scram and MSIV and PCV isolation valve closure, and loss of automatic ECCS initiation capability. Some ECCS could be initiated manually from the remote shutdown panel.*

(6) In addition of complete failure of energize-to-trip or deenergize-to-trip functions, the ~~RMUs~~ RDLCs *may have common-cause calibration errors.*

19N.4 Potential Causes of and Defenses Against EMUXECF CCF

STD DEP T1 3.4-1

The information in this appendix section of the reference ABWR DCD, including the above title and all subsections, is incorporated by reference with the standard departure numbered STD DEP T1 3.4-1.

19N.4.1 Earthquake

STD DEP T1 3.4-1

The ~~multiplex~~ ECF equipment consists of solid-state electro-optical modules, which are vibration and shock resistant by nature. In addition, the equipment is designed and tested to very high acceleration levels (7-10g). Earthquakes of magnitudes above 2g have never been experienced, are not expected to occur, and if they did occur would *have much more serious consequences than loss of ~~EMUX~~* ECF *equipment. Even allowing for magnification above ground level, earthquake does not appear to be a credible cause of concern.*

19N.4.2 Loss of D.C. Power

STD DEP T1 3.4-1

Common-cause loss of DC power has been examined intensively in an EPRI analysis (Reference 19N-1). Most of the identified potential common causes were found to either result in gradual degradation and/or be self-announcing. The consequences of actual loss of all DC power would be far more serious than the loss of ~~EMUX~~ ECF *equipment since most control instrumentation in the plant's safety equipment depends on DC power. (Loss of DC power is evaluated as part of the station blackout analysis of Appendix 19D.) Loss of DC power does not constitute a significant cause of common-cause ~~EMUX~~* ECF *failure.*

19N.4.3 Loss of Cooling

STD DEP T1 3.4-1

It is a design requirement that the ABWR ~~EMUX~~ ECF *equipment must be capable of continuous operation at 323.15 K (50°C), and must be capable of continuous operation in its installed condition without fans. This is not a problem for present-day low-power solid-state electronic equipment, and the maximum anticipated ambient temperature is 313.15 K (40°C). Loss of cooling is not a credible common cause.*

19N.4.4 Sensor Miscalibration

STD DEP T1 3.4-1

Sensor miscalibration does not represent a common-cause failure of ~~EMUX~~ ECF *equipment per se, but is identified here because of the fact that there is a reduction in the number of sensors in the ABWR ~~multiplexed~~* ECF *instrumentation configuration relative to earlier designs, and the sensors are shared between safety functions.*

19N.4.5 ~~*RMU*~~ Remote DLC Miscalibration

STD DEP T1 3.4-1

*Only the analog-to-digital converters of the ~~EMUX~~*RDLCs *require calibration. The calibration is automatic and computer-controlled. Calibration is accomplished by comparison to voltage, resistance and time references that are verified against external laboratory standards. The ~~EMUX~~* ECF *transmission equipment is self-calibrating. The ~~technician only initiates calibration by pushing a button~~* equipment calibration is monitored continuously and automatically adjusted if needed to maintain calibration to on-board verified standards*. In addition, ~~the self-test feature of~~* self-diagnostics in *the equipment detects certain types of calibration faults.*

19N.4.7 Maintenance/Test Error

STD DEP T1 3.4-1

The ~~EMUX~~ ECF equipment has a built-in provision to prevent bypassing multiple divisions simultaneously. This feature would not prevent common maintenance or test errors that were done consecutively and were latent by nature, such as set points being erroneously set. Periodic surveillance, as required by the technical specifications, includes verification of setpoints. The self-test feature of the equipment will also identify some types of maintenances/test errors.

19N.4.9 Electromagnetic Interference (EMI)

STD DEP T1 3.4-1

EMI is a potential cause of failure of solid-state electronic equipment. EMI can enter a circuit through any of several paths-power supplies, adjacent equipment, adjacent cabling, or input signals. In the case of the ~~EMUX~~ ECF equipment, none of these paths would affect multiple divisions since the divisions are widely separated physically and are electrically independent. In addition, the nature of electro-optics reduces the susceptibility to EMI. Fiber-optic transmission lines are not subject to EMI and will not propagate transients between lines. EMI is not a credible common cause.

19N.4.10 Fire

STD DEP T1 3.4-1

The four divisions of remote ~~EMUX~~ ECF equipment are located in separate rooms of the reactor building and are separated by barriers. The fiber optic transmission cables have fire-resistant protective covering. A localized fire would affect only one division. A more wide-spread fire might affect two divisions, but a fire large enough to affect three or four divisions would have more far-reaching effects than the loss of ~~EMUX~~ ECF transmission. Because of the physical separation, common-cause failure of remote ~~EMUX~~ ECF equipment due to fire does not appear to be a credible concern.

19N.4.11 Software

STD DEP T1 3.4-1

The ~~EMUX~~ ECF equipment is programmed to perform the essential communications function, self-test, and calibration. The software that provides the programming is subject to extensive "debugging" procedures and strict quality control and test requirements (verification and validation). Nevertheless, it is not impossible that an undetected "bug" could remain. If such were the case, it would most likely affect all divisions. It would not necessarily cause all divisions to fail simultaneously. Common-cause software fault is a credible, although unlikely, possibility. To provide additional defense against software CCF, technical specification requirements and administrative procedures will be established, as discussed in Subsection 19N.2, to assure taking of appropriate action in the event of failure of individual ~~multiplex~~ divisions.

19N.4.12 Summary

STD DEP T1 3.4-1

Of the eleven potential common causes examined, only three appear to be credible:

(1) ~~RMU~~ RDLC *miscalibration*

The failure that would result in a significant contribution to core damage frequency would be complete failure during plant operation of three or four divisions of ~~EMUX~~ ECF *that transmit signals from wide-range water level sensors. This condition could result in failure to automatically initiate ECCS. Since failure of ~~EMUX~~* ECF *equipment is annunciated, the operator would be aware of the need for manual initiation of ECCS. Appropriate instrumentation and control is available at the remote shutdown panel, if needed.*

19N.5 Discussion of the Effect on Core Damage Frequency

The information in this appendix section of the reference ABWR DCD, and all subsections, is incorporated by reference with the following standard departure numbered STD DEP T1 3.4-1.

STD DEP T1 3.4-1

The three primary safety functions that are necessary to prevent core damage are reactivity control, core cooling, and decay heat removal. The effects of ~~EMUX~~ ECF CCF *are included in the quantification of core damage frequency in the internal events analysis of Appendix 19D. Additional discussion is given herein to provide further information and insight into the nature of ~~EMUX~~* ECF CCF *contribution to core damage frequency. The isolation function does not contribute directly to core damage frequency and is evaluated separately in Subsection 19N.6.*

19N.5.1 General Plant Transient Events

STD DEP T1 3.4-1

In the ABWR, automatic response of the safety functions to a plant transient producing decreasing water level is initiated by signals transmitted through the ~~EMUX~~ ECF*. Initiation of ECCS and closure of some isolation valves is by the presence of an energizing signal. Initiation of RPS (scram) and MSIV and PCV closure is by a deenergizing signal or absence/loss of energization.*

There are four independent divisions of sensors and ~~EMUX~~ ECF *equipment. Simultaneous loss of transmission capability on any two of the four divisions would result in a scram on loss of energization. Loss of transmission capability on any three divisions simultaneously would result in loss of automatic initiation of ECCS and loss of low pressure permissive signals for reactor shutdown cooling. When a single division is lost, the control room is alerted and that division is bypassed by the operator. Bypassing of a division results in that division becoming inoperative; i.e., that division cannot contribute to scram, isolation, or ECCS initiation. Technical specification requirements govern actions to be taken under those conditions.*

Because of the high degree of independence between divisions in the ABWR design, the probability of simultaneous failures in multiple divisions is very low. If there were no common failure cause, the random probability of failure of n divisions would be the nth power of the probability of failure of a single division. In the presence of potential *common failure causes, the probability of multiple failures could increase. Potential multiple failure causes are listed in Subsection 19N.2. Defenses against these common-cause failures are discussed in Subsections 19N.2 and 19N.4. These defenses provide a high degree of independence between instrumentation channels and divisions in the ~~EMUX~~* ECF *control data network.*

The relationship of the safety function initiation and the ~~EMUX~~ ECF *is depicted in a simplified event tree, shown on Figure 19N-3. This event tree is for a plant transient initiating event and loss of transmission capability from three or four divisions of ~~EMUX~~* ECF *transmission of wide-range RPV water level signals. Loss of transmission of narrow-range water level sensor ~~RMUs~~* RDLCs *due to common-cause failure would not affect the results since scram would be automatically initiated by loss of energization. The purpose of this event tree is to provide a means for examining the effect of common-cause failures of safety function initiating signals. Random failures of instrumentation and failures of mechanical execution of the safety function are evaluated in Appendix 19D.*

The first safety response to a plant transient is a reactor trip and scram. Because of the deenergize-to-trip feature, a scram would be initiated, even with a common-cause failure of all ~~EMUX~~ ECF *transmission. (A loss of transmission through the ~~EMUX~~* ECF *would result in a plant scram at any time, even without a plant transient. That event is evaluated in a later subsection-Subsection 19N.5.5.) Common-cause failure of transmission would also result in closure of the MSIVs.*

Given a successful scram, the next essential safety function is to maintain water level in the reactor pressure vessel. The limiting case for common-cause failure of the ~~EMUX~~ ECF *is common-cause failure of three or four of the individual ~~remote multiplexing units~~* RDLCs *processing wide-range RPV water level signals. Since ABWR has motor-driven feedwater pumps, closure of the MSIVs would not cause loss of feedwater unless the feedwater pumps tripped because of the transient. If the feedwater pumps did not trip, RPV waterlevel could be maintained as long as there was water in the condenser hotwell. In ABWR, the condenser hotwell inventory is automatically replenished from the condensate storage tank. If the feedwater pumps were tripped, they could be started manually from the control room, since the feedwater control system is independent of the ~~EMUX~~* ECF*. If necessary, sufficient ECCS pumps could be started manually from the remote shutdown panel to provide water to the RPV. Automatic initiation of ECCS would not occur because of the common-cause failure of ~~EMUX~~* ECF *to transmit wide-range RPV water level signals.*

To manually start some ECCS pumps, the operator may have to use the remote shutdown panel, since manual start signals from the control room are normally transmitted through the ~~EMUX~~ ECF *and may not be operable. The operator would have correct indication of RPV water level in the control room since water level is hard wired in addition to being transmitted through the ~~EMUX~~* ECF*. He also would be aware of the reactor scram. If control is not possible from the control room, the EOPs will tell the operator to proceed to or send someone to the remote shutdown panel where true indications and means of control are supplied through independent channels. In this* *simplified bounding analysis, failure of the operator to manually start ECCS pumps would result in uncovering of the reactor core and eventual core damage.*

The effect of common-cause ~~EMUX~~ ECF *failure on CDF is included in the quantification of the event trees in Appendix 19D for transient-initiated and LOCA events. The random unavailability of the ~~RMUs~~* RDLCs *and ~~TLUs~~* TLFs *is derived from an expected mean time between failures and a mean time to detect and repair a failure (MTTR). The random unavailability of the ECF is derived from an expected MTBF and an MTTR. The MTBF values are estimated, based on information from the supplier. The MTTR value is based on the use of a self-test feature which detects a failure within* one minute*, and the existence of spare replacement units on hand at the plant. The self-test feature detects most of the failures. The remaining failures are detected by surveillance testing conducted quarterly.*

If there were sufficient experience data for multiple failures of solid-state ~~multiplexing~~ digital communications *equipment, the experience data would be used directly and there would be no need for use of the beta-factor model. However, there is a dearth of multiple-failure data pertaining to ~~solid-state multiplexer~~* such *equipment, particularly equipment with a self-test feature. The alternative is to evaluate or estimate the relative susceptibility of the ~~EMUX~~* ECF *to multi-divisional failures through use of the beta-factor.*

A recent report by the Electric Power Research Institute (EPRI) (Reference 19N-1) discusses the beta-factor model and lists representative values for beta. The values listed generally range from 0.1 down to about 0.01, but there is no value given specifically for solid-state ~~multiplexing~~ digital communications *equipment. Considering the defenses in the ABWR design, particularly the self-test feature, a lower value for beta is justified and may even be conservative. The self-test feature of the ~~EMUX~~* ECF *equipment provides detection of failures* within one minute*, and on-hand spare modules provides restoration of operability within* an average time of 8 hours*. This feature limits the available time for propagation of multiple failures to* an average time interval of approximately 8 *hours, and essentially eliminates several of the more likely causes of multiple failures.*

The ABWR PRA indicates that the total core damage frequency for the ABWR design will be very low. The PRA analysis also indicates that potential ~~EMUX~~ ECF *CCFs during plant transient events are significant contributors to the low total CDF. ~~EMUX~~* ECF *CCFs appear in many of the top cutsets. An importance analysis indicates that all three ~~EMUX~~* ECF *CCFs have relatively high "risk achievement worth", i.e., increases in the CCF probabilities would result in significant increases in total CDF. The defenses against ~~EMUX~~* ECF *CCFs in the plant design (Subsection 19N.4) and the administrative procedures prescribed in Subsection 19N.2 should prevent increases in ~~EMUX~~* ECF *CCF probabilities above the values used in the PRA analysis. Conservatisms in this part of the PRA tend to somewhat overestimate the importance of ~~EMUX~~* ECF *CCFs.*

19N.5.2 Loss of Feedwater Event

STD DEP T1 3.4-1

The previous analysis considered the effect of loss of transmission capability of the ~~*EMUX*~~ ECF*, that is, an instance where the* ~~*EMUX*~~ ECF *failed to transmit an energization signal. The reverse failure mode would be failure to lose the energization signal for RPS due to common-cause failure of the narrow-range water level sensor* ~~*RMUs*~~ DTFs *to properly sense a Level 3 condition. For many plant transients, automatic scram would occur due to increased neutron flux or other direct-input signals to the RPS logic. For purposes of this analysis, an initiating event is used that would require response of the narrow-range* ~~*RMUs*~~ DTFs *that sense a Level 3 water-level condition. A feedwater pump trip can be used to represent such an event.*

The probability of common-cause failure in this mode is much lower than for the loss-of-transmission mode since most of the identifiable common causes would not cause a failure in this mode. The ~~*EMUX*~~ ECF *failure in this mode could result in failures of automatic scram. There is a very high probability that the operator would provide manual scram based on independent indications of the feedwater pump trip. Since the MSIVs would not close, the power conversion system would remain in operation. Based on past operating experience, there is a high probability that the operator would recover feedwater in addition to initiating manual scram. If feedwater were not recovered before low water level (Level 2) was reached, ECCS would be initiated automatically by means of transmission through the wide-range water-level sensor* ~~*RMUs*~~ RDLCs.

Initiation of decay heat removal would not be affected by the ~~*EMUX*~~ ECF *failure in the deenergize-to-trip mode.*

19N.5.3 Loss of Coolant Accidents

STD DEP T1 3.4-1

Because of the low frequency of occurrence, LOCA events are very small contributors to ABWR core damage frequency. The probability of a coincidental common-cause ~~*EMUX*~~ ECF *failure together with a LOCA is an extremely low probability event. The possibility of a common-cause* ~~*EMUX*~~ ECF *failure occurring as a result of a LOCA, where the LOCA would provide the common cause, is highly unlikely because of the locations and physical separation of the* ~~*EMUX*~~ ECF *divisions.*

19N.5.4 Other Initiating Events

STD DEP T1 3.4-1

19N.5.4.1 Loss of Offsite Power

STD DEP T1 3.4-1

Loss of all offsite power would have no direct effect on ~~*EMUX*~~ ECF *operability since* ~~*EMUX*~~ ECF *equipment operates completely on divisional DC power. A loss of offsite power would cause a small increase in the conditional probability of loss of DC power since DC power is supplied by batteries or an AC converter-charger. The probability of loss of DC power is very low as discussed below in Subsection 19N.5.4.2.*

19N.5.4.2 19N.5.4.2 Loss of DC Power

STD DEP T1 3.4-1

Each division of the ~~EMUX~~ ECF is powered by a division of DC power. Loss of all divisions of DC power would result in loss of ~~EMUX~~ ECF transmission capability. The annual probability of loss of DC power on one essential bus is estimated to be approximately 1.0E-3. The complete loss of DC power to all four divisions of essential power is considered to be essentially zero since the four divisions are independent, loss of DC power on any one division is alarmed, and the station batteries are routinely tested. Very few credible causes of common-cause failure of multiple DC buses have been identified (Reference 19N-1.)

19N.5.4.3 Inadvertent Open Relief Valve7

STD DEP T1 3.4-1

An inadvertent open relief valve (IORV) as an initiating event is treated in this analysis as just another plant transient. Although the plant response is somewhat different for an IORV, there is no peculiar impact on ~~EMUX~~ ECF operation or response, and common-cause failure of ~~EMUX~~ ECF would have the same effect on plant response as it would in any other plant transient event.

19N.5.4.4 Loss of Service Water

STD DEP T1 3.4-1

Loss of essential service water has been hypothesized and studied as an initiating event since loss of service water could disable some ECCS equipment. Service water is not used directly by any ~~EMUX~~ ECF equipment and is not used for room cooling. The effects of loss of service water on essential safety equipment is evaluated in the system fault trees of Appendix 19D.

19N.5.4.5 19N.5.4.5 Loss of Instrument Air

STD DEP T1 3.4-1

Instrument air is not used by ~~EMUX~~ ECF equipment. As with essential service water, loss of instrument air would not affect ~~EMUX~~ ECF equipment or this analysis.

19N.5.5 CCF of ~~EMUX~~ ECF During Normal Plant Operation

STD DEP T1 3.4-1

Results of the above analyses indicate that common-cause failure of ~~EMUX~~ ECF equipment in response to a demand from a plant transient or other off-normal event is a very small contributor to core damage frequency. This subsection examines the effect of a common-cause ~~EMUX~~ ECF failure at a random time during normal plant operation (~~EMUX~~ ECF failure as an initiating event).

The limiting failure in this case would be common-cause failure of the three or four divisions of ~~remote multiplexing units~~ RDLCs *transmitting the signals from the narrow-range and wide-range water level sensors. If only the narrow-range transmission channels failed, the plant would scram on loss of energization, and ECCS would be initiated automatically through the wide-range ~~RMUs remote DLCs~~ RDLCs. If only the wide-range water level sensor ~~RMUs~~* RDLCs *failed, the plant would not scram from that failure alone and there would be no demand on ECCS unless a plant transient occurred. Thus, both wide-range and narrowrange ~~RMUs~~* RDLCs *must fail in multiple divisions to cause a condition of concern and a potential accident initiator. In that event, the plant would scram and ECCS would not be automatically initiated.*

Using the beta-factor method of CCF evaluation, the expected frequency of common-cause failure of all ~~RMUs~~ RDLCs *in three or four divisions would be equal to the product of the expected frequency of random failure of a single ~~RMU~~* RDLC *and a beta-factor. In this case, the beta-factor should be lower than for the transient-initiated event since twice as many ~~RMUs~~* RDLCs *must fail; however, the assignment of a specific value to beta in this case is extremely uncertain.*

Because of the great degree of uncertainty in any quantitative analysis that could be performed at this level, it appears preferable (and sufficient) to make a qualitative judgement. Since two or three ~~EMUX~~ ECF divisions must fail in two distinct modes involving separate equipment, and they must fail in a nearly simultaneous manner, i.e., in a sufficiently short interval to not allow mitigating action to be taken, the expected frequency of occurrence must be extremely low.

19N.6 Discussion of the Effect on Isolation Capability

STD DEP T1 3.4-1

Failure of the Leak Detection and Isolation System (LDIS) does not have a direct effect on core damage frequency. The primary purpose of the LDIS function is to isolate the reactor and associated primary equipment and certain fission products in the event of a loss-of-coolant accident. A simplified event tree for a LOCA with common-cause loss of transmission capability of all ~~RMUs~~ RDLCs *is shown on Figure 19N-4. For this condition, MSIVs and PCV isolation valves would close on loss-of-signal.*

The largest expected initiation frequency for a LOCA is for a small LOCA. The conditional probability of common-cause unavailability of ~~RMUs~~ RDLCs *is extremely small. There is no identifiable mechanism by which the LOCA could increase the probability of common-cause ~~RMU~~* RDLC *failure.*

One additional isolation failure event should be considered-the effect of failing to isolate in a severe accident situation with a severely damaged core. In accident sequences resulting in core damage because the operator failed to maintain water inventory to the reactor (given an ~~EMUX~~ ECF CCF), it is possible that he would also fail to close isolation valves.

19N.7 Summary

STD DEP T1 3.4-1

This analysis has focused on the use of common ~~multiplexing~~ essential communications *equipment in the ~~EMUX~~ ECF. Because it is possible to identify feasible causes of multiple failures, the possibility of common-cause failure of identical ~~multiplexing~~* ECF *units has been studied. In view of the number and types of defenses built in to the ~~EMUX~~ ECF design, the probability of common-cause failure should be very low. Because of the lack of multiple-failure experience data on equipment of this type, it has been necessary to predict the common-cause failure probability by use of an analytical model. The model used is a simple model-the betafactor model-that hypothesizes that common-cause failure probability is proportional to the random failure probability of a single unit. The proportionality factor is beta. The hypothesis may not be true in all cases, and there is a great deal of uncertainty in assigning a value to beta.*

Beta represents the fraction of total failures that would involve multiple identical units. The expected value of beta is dependent on the nature of the possible causes, how and how fast failures would propagate between units, and what defenses exist to the causes. There is no established method for quantifying these factors. In the absence of good and sufficient data, assignment of a value to beta is a matter of judgement. Values that have been used for beta range from 0.1 down to 0.001 and lower. Values of beta between 0.1 and 0.01 are common for mechanical equipment. Values below 0.01 are more common for instrumentation. The value used in the analysis of Appendix 19D may be conservative, considering the defenses in the ABWR ~~EMUX~~ ECF design.

Using a conservative value for ~~EMUX~~ ECF beta, the results of the Appendix 19D analysis show that use of the ABWR ECF shared-sensor configuration results in very little contribution to core damage frequency in response to demands from plant transients or off-normal events. This is because of the high availability on demand of the limiting equipment, the ~~RMU~~ RDLCs*. The high availability of the ~~RMU~~* RDLCs *is due to the self~~-test~~ diagnostic capability and the resulting short mean time to detect and recover from a failure. This same ~~selftest~~ self-diagnostic feature is the best protection against common-cause failures, since multiple failures must all occur within an average time interval of* approximately 8 *~~4.25~~ hours. This study tends to confirm the conclusions of the Appendix 19D analysis in regard to the effect on CDF of ~~EMUX~~ ECF CCF in response to transient and LOCA initiated events.*

Also of potential concern is common-cause failure of ~~EMUX~~ ECF as an initiating event. The ~~EMUX~~ ECF must be available at all times when the plant is operating because of the "failsafe" (deenergize-to-trip) design for scram and MSIV closure. A simultaneous common-causefailure of two ~~EMUX~~ ECF divisions at any time during plant operation would result in a plant trip, even though all plant parameters were normal. In a sense, this is a "false alarm" that results in a scram, which is a potential accident initiating event. If the third and/or fourth division of ~~EMUX~~ ECF equipment also failed simultaneously, there could be a loss of automatic initiation of ECCS.

The expected frequency of occurrence of common-cause ~~EMUX~~ ECF failure during normal operation is a function of the ~~EMUX~~ ECF reliability, including D.C. power reliability. Fast recovery time due to the ~~EMUX~~ ECF self~~-test~~ diagnostic feature does not help if two divisions fail simultaneously, since a plant trip is immediate. (The self-

~~test~~ diagnostic feature is a major defense if the CCFs do not occur simultaneously.) The probability and expected frequency of occurrence of such an event is extremely low. Administrative controls will be imposed to minimize the probability of progressive common-cause failures. With the present design, the frequency of occurrence can be further reduced only by increasing the reliability of the ~~remote multiplexing unit~~ RDLC.

One type of administrative action that will effectively eliminate several common causes including software faults is establishment of required action to be taken in the event of functional failure of a single ~~EMUX~~ ECF channel during plant operation. The action to be taken in the event of functional failure of ~~an EMUX~~ an ECF *channel during plant operation is to re-establish operability and determine the cause of the failure as soon as possible. During the period of repair/replacement and diagnosis, the remaining channels are monitored closely. In the event of a second channel failing before the first channel is restored, the safest available action is immediately taken as prescribed by technical specifications and/or emergency operating procedures.*

The sensitivity of core damage frequency to ~~EMUX~~ ECF MTBF and beta can be seen from the event tree of Figure 19N-3. The ~~RMU~~ RDLC *CCF probability or frequency is a direct function of both of these reliability elements. In turn, the core damage frequency is directly proportional to the ~~RMU~~* RDLC *CCF probability and the initiating event frequency. If the ~~RMU~~* RDLC *MTBF was twice as high, the core damage frequency would be reduced by half. In like manner, uncertainty in the initiating frequency propagates directly into uncertainty in CDF.*

Figure 19N-3 Event Tree for Analysis of Common-Cause Failure of ~~*EMUX*~~ECF

STD DEP T1 3.4-1

There is no logic change to this Event Tree. The changes are limited to nomenclature as listed below:

- ~~*EMUX*~~ ECF TRANSMISSION
- CCF of ~~*EMUX*~~ ECF *
- * COMMON-CAUSE FAILURE OF ~~*REMOTE MULTIPLEXING UNITS,*~~ ESSENTIAL COMMUNICATIONS FUNCTION~~*, OR TRIP LOGIC UNITS*~~ (ECF, RDLC, DTF, DLC performing SLF, TLF)

Figure 19N-4 Event Tree for Failure to Isolate Due to ~~*EMUX*~~ECF CCF

STD DEP T1 3.4-1

There is no logic change to this Event Tree. The changes are limited to nomenclature as listed below:

- AUTOMATIC INITIATION THROUGH~~*EMUX*~~ ECF
- CCF of ~~*EMUX*~~ ECF *
- * COMMON-CAUSE FAILURE OF ~~*REMOTE MULTIPLEXING UNITS,*~~ ESSENTIAL COMMUNICATIONS FUNCTION~~*, OR TRIP LOGIC UNITS*~~ (ECF, RDLC, DTF, DLC performing SLF, TLF)