REACTOR PROTECTION AND CONTROL
PROCESS INSTRUMENTATION REPLACEMENT PROJECT AT
DONALD C. COOK NUCLEAR PLANT UNITS 1 AND 2

REACTOR PROTECTION SYSTEM FUNCTIONAL DIVERSITY ASSESSMENT

REPORT NO. 2985-VDV-01, REV 0

Prepared by: _____ Date 12-7-92

Concurred by: _____ Date 10 Dec 92

Approved by: _____ Date 12/14/92

QUALITATIVE FUNCTIONAL DIVERSITY ASSESSMENT

EXECUTIVE SUMMARY

On April 21, 1992, AEPSC representatives had a meeting with the NRC on the replacement of existing analog reactor protection process instrumentation with digital Foxboro Spec 200/Spec 200 Micro Electronics instrumentation. During this meeting, AEPSC was asked to assume a common mode failure (CMF) of the software of the new digital equipment during a postulated accident and then provide details as to whether operators could mitigate the consequences of the accident.

In response to this request, a functional diversity assessment of each updated FSAR (UFSAR) event assuming a common mode failure of the software has been performed. In this assessment, all the events for both Units 1 and 2 of the Cook Nuclear Plant given in the UFSAR were considered. A review was performed to divide events into potentially affected and not affected. Table-1 lists these events and indicates whether they would be potentially affected or not affected if a CMF were to occur. The potentially affected transients were then individually evaluated qualitatively in light of the FSAR analysis.

Each event evaluation was recorded on a form of the type shown in Appendix A. This form outlines the thought process employed. The first column in Appendix A contains the UFSAR transient number listed in Table-1. The second column includes the name of the transient. The third column depicts the trip/safeguard function for reactor trip. This information was obtained from the UFSAR. The fourth column includes the information on the impact of common mode failure on the reactor trip function. If the trip function is processed outside of the new digital reactor protection system, then the trip is available, e.g., trip on nuclear instrumentation system high flux. If the trip is processed by a function that is a part of the new digital equipment, then the trip/ESF function is assumed to be lost. However, for some functions, alternate indications and/or diverse alarms are available. The alarm/alternate indications that are available to the operator to mitigate the transient are given in the next column. The sixth column lists pertinent diagram numbers. The seventh column summarizes the consequences of the unavailability of diverse alarm. The last column provides the evaluation of the event. In this column, we have discussed the consequences of the operator's response on reactor safety.

Based on this evaluation, we have concluded that the CMF of the new digital equipment has no significant adverse impact on the public safety. Some reactor trips are not affected by the installation of the new digital equipment. Among these trips are neutron high flux and high rate trips, undervoltage and underfrequency trips and reactor trip on turbine trip. However, for events protected by trip actuations affected by the CMF, the operator will be alerted to the event by an alarm. He will then provide the appropriate actuations manually and enter the emergency operating procedures. For some accidents, such as locked rotor, the consequences could be more severe than currently analyzed due to the longer response time for the required actuation. However, our evaluation indicates that the affected unit can be brought to a safe condition and the current LOCA offsite dose evaluation will remain bounding. From these results, it is believed that a CMF of the new digital system would have no adverse effect on the health and safety of the public.

Table-1

UFSAR TRANSIENT #	TRANSIENT	POTENTIALLY AFFECTED (A)/ NOT AFFECTED(NA)
14.1.1	Uncontrolled RCCA Withdrawal from a Subcritical Condition	A
14.1.2	Uncontrolled RCCA Withdrawal at Power	A
14.1.3	Rod Cluster Control Assembly Misalignment	A
14.1.4	RCCA Drop	A
14.1.5	Chemical Volume and Control System Malfunction	A
14.1.6	Loss of Reactor Coolant Flow	A
14.1.7	Startup of an Inactive Reactor Coolant Loop	A
14.1.8	Loss of External Electrical Load	A
14.1.9	Loss of Normal Feedwater Flow	A
14.1.10	Excessive Heat Removal due to Feedwater System Malfunction	A
14.1.11	Excessive Load Increase Incident	A
14.1.12	Loss of All A.C. Power to the Plant Auxiliaries	A
14.1.13	Turbine-Generator Safety Analysis	A
14.2.1	Fuel Handling Accident	A
14.2.2	Accidental Release of Radioactive Liquids	A
14.2.3	Accidental Waste Gases Release	A
14.2.4	Steam Generator Tube Rupture	A
14.2.5	Rupture of a Steam Pipe	A
14.2.6	Rupture of a Control Rod Drive Mechanism Housing (RCCA Ejection)	A
14.2.7	Secondary System Accidents Dose Consequences	A
14.2.8	Major Rupture of a Main Feedwater Pipe	A
14.3.1	Large Break LOCA Analysis	A
14.3.2	Loss of Reactor Coolant from Small Ruptured Pipes or from Cracks in Large Pipes which Actuates the Emergency Core Cooling System	A
14.3.3	Core and Internals Integrity Analysis	NA
14.3.4	Containment Integrity Analysis	A
14.3.5	Environmental Consequences of a Loss of Coolant Accident	A
14.3.6	Hydrogen in the Containment After a Loss of Coolant Accident	A
14.3.7	Long Term Cooling	NA
14.3.8	Nitrogen Blanketing	NA
14.4.2	Postulated Pipe Failure Analysis Outside Containment	NA
14.4.3	Analysis of Emergency Conditions	NA
14.4.4	Stress Calculations	NA
14.4.5	Description of Pipe Whip Analysis	NA
14.4.6	Compartment Pressures and Temperatures	NA
14.4.7	Description of Jet Impingement Load Analysis	NA
14.4.8	Containment Integrity	NA
14.4.9	Plant Modifications	NA
14.4.10	Environment	NA
14.4.11	Electrical Equipment Environmental Qualification	A

APPENDIX A

FSAR TRANSIENT #	TRANSIENT	TRIP/SAFEGUARD FUNCTION FOR RX TRIP FSAR	IMPACT OF COMMON MODE FAILURE (CMF) ON TRIP FUNCTION	ALARM/ALTERNATE INDICATION SYSTEM AVAILABLE	DIAGRAM #	CONSEQUENCES OF UNAVAILABILITY OF DIVERSE ALARM	EVALUATION OF EVENT

UNIT 1 and UNIT 2

FSAR TRANSIENT #	TRANSIENT	TRIP/SAFEGUARD FUNCTION FOR RX TRIP (FSAR 14.1.6.1)	IMPACT OF COMMON MODE FAILURE (CMF) ON TRIP FUNCTION	ALARM/ALTERNATE INDICATION SYSTEM AVAILABLE	DIAGRAM #	CONSEQUENCES OF UNAVAILABILITY OF DIVERSE ALARM	EVALUATION OF EVENT
14.1.6.1	Loss of Forced Reactor Coolant Flow	1. Rx trip on reactor coolant pump power supply undervoltage or underfrequency	Not Affected	Reactor Coolant Pump underfrequency and undervoltage alarm (Procedure 1, 2-OHP, 4024, 107, 207)		None	The Rx trip on reactor coolant pump power supply undervoltage and underfrequency remains unaffected by a common mode failure (CMF) of the new digital instrumentation. The reactor trip on loss of flow in a coolant loop is lost on CMF for each loop. There are no Diverse Alarms available; however, panel indication and computer indication are available for the low coolant loop flow.
		2. Rx trip on low reactor coolant loop flow.	Low flow Rx trip lost (for all four loops)	Indication Available Panel indication computer indication Diverse Alarm Available None Other Indications Pressurizer pressure panel indication Pressurizer pressure recorder Pressurizer pressure computer indication Pressurizer level panel indication Pressurizer level recorder Pressurizer level computer indication Wide range temperature records Other Alarms Pressurizer high pressure deviation via control system Four high pressure alarms via control system Pressurizer high level deviation via control system High level via control system Acoustic monitor flow detected	FD-2101 Sheet 3 and 4	If the Rx is at power at the time of the accident, the immediate effect of a loss of coolant flow is a rapid increase in the coolant temperature which is magnified by a positive MTC. This increase could result in DNB with subsequent adverse effects to the fuel, if the Rx is not tripped promptly. (FSAR, page 14.1.6-1)	Two cases of loss of flow are discussed in FSAR (14.1.6). The simultaneous loss of power to all 4 RCPs can occur due to either underfrequency or undervoltage, which is not impacted by CMF. This situation is highly unlikely, since each pump is connected to a separate bus, which is supplied by one of two transformers. The consequences of the loss of flow include an increase in Tavg, pressurizer pressure, and pressurizer water level. Wide range RCS temperature recorders (memo dated 9/2/92 from W. G. Sotos to V. D. VanderBurg) are available to the operator to indicate an increase in Tavg. There is no Rx trip on high Tavg. The pressurizer pressure will continue to rise until the operator gets a high pressure deviation alarm at 2325 psia (2-OHP 4024.208 Drop 7) for Unit 2 and 2175 psia for Unit 1. The Rx trip on high pressure (setpoint $\leq$ 2400 psia) is lost due to CMF. However, diverse alarms (memo dated 9/2/92 from W. G. Sotos to V. D. VanderBurg) are available. It is evident that the high pressure deviation alarm will draw the operator's attention, and he will trip the Rx manually. The operator will also be likely to see the high level deviation alarm at 5% above program. The consequences of this manual Rx trip are discussed below. Crude extrapolations of DNBR for these events suggest that MDNBR could be reached within ~16 to ~18 seconds for loss of flow in one loop. Similar extrapolations suggest that the high pressure deviation alarm would first be received ~6 seconds into the transient although the operation of pressurizer sprays will increase this estimate. Allowing ~60 seconds for operation response it is clear that DNB could

UNIT 1 and UNIT 2

FSAR TRANSIENT #	TRANSIENT	TRIP/SAFEGUARD FUNCTION FOR RX TRIP (FSAR 14.1.6.1)	IMPACT OF COMMON MODE FAILURE (CMF) ON TRIP FUNCTION	ALARM/ALTERNATE INDICATION SYSTEM AVAILABLE	DIAGRAM #	CONSEQUENCES OF UNAVAILABILITY OF DIVERSE ALARM	EVALUATION OF EVENT
14.1.6.1 (cont'd)							occur resulting in clad damage. Since a massive multiple failure is assumed for this event, this is believed to be acceptable. With a loss of flow in one loop total core flow should remain ~80% removing the bulk of the heat from the core, limiting the deterioration of the core prior to manual reactor trip. The portion of the core that experiences DNB is expected to heat up until the Doppler coefficient shuts it down. Fuel is not expected to melt but clad burst and oxidation are anticipated. It should also be noted that this event was analyzed with a positive moderation coefficient (MTC) of +5 pcm/°F. This value is more limiting than the Technical Specification limit at 100% RTP. It is conservative and provides substantial margin throughout most of the life. This causes power to increase as the coolant temperature increases. A more realistic assumption for beginning of cycle is ~-4pcm/oF. A negative MTC will tend to shutdown the core as temperature increases mitigating the event. The MTC becomes substantially more negative as burnup progresses. The Cook Units are base loaded and operate with control rods in the all out position at full power. Therefore, the possibility that automatic rod control might withdraw rods will have no impact because rods are essentially fully withdrawn. After reactor trip, the emergency operating procedures provide for mitigation activities to bring the machine to a safe condition. In the evaluation of the previous paragraph, an operator response time of ~60 seconds was assumed. Without a reactor trip, pressurizer pressure and level are expected to continue to increase after the first alarms are received. When pressure reaches 2250 psia, the PORV's will open resulting in an acoustic monitor flow detected alarm. Extrapolating the analysis curves, which do not model pressurizer spray, this could occur before MDNBR is reached. Therefore, it is likely that an accumulation of alarms will occur before 60 seconds have elapsed. Therefore, the operators response time may be less than 60 seconds for this event.

UNIT 1 and UNIT 2

FSAR TRANSIENT #	TRANSIENT	TRIP/SAFEGUARD FUNCTION FOR RX TRIP (FSAR 14.1.6.1)	IMPACT OF COMMON MODE FAILURE (CMF) ON TRIP FUNCTION	ALARM/ALTERNATE INDICATION SYSTEM AVAILABLE	DIAGRAM #	CONSEQUENCES OF UNAVAILABILITY OF DIVERSE ALARM	EVALUATION OF EVENT
14.1.6.1 (cont'd)							The most likely cause of an event of this type, is a failure of the reactor coolant pump (RCP) or its motor. The operator is provided with a significant number of alarms to give him information regarding the RCP's and motors. These alarms include RCP motor differential trip, RCP motor overload trip, and RCP motor overheated. Therefore, it is likely that the operator will have information available which will allow him to anticipate and, therefore, substantially mitigate the event.

UNIT 1 and UNIT 2

FSAR TRANSIENT #	TRANSIENT	TRIP/SAFEGUARD FUNCTION FOR RX TRIP (FSAR 14.1.6.2)	IMPACT OF COMMON MODE FAILURE (CMF) ON TRIP FUNCTION	ALARM/ALTERNATE INDICATION SYSTEM AVAILABLE	DIAGRAM #	CONSEQUENCES OF UNAVAILABILITY OF DIVERSE ALARM	EVALUATION OF EVENT
14.1.6.2	Locked Rotor/Shaft Break Accident	Reactor trip on low flow signal	Low flow reactor trip lost (memo 9/2/92 memo from W. G. Sotos to V. D. VanderBurg)	Indications Available Panel indication Computer indication Diverse Alarm Available None Other Indications Pressurizer pressure panel indication Pressurizer pressure recorder Pressurizer pressure computer indication Pressurizer level panel indication Pressurizer level recorder Pressurizer level computer indication Wide range temperature records Sound of pressurizer safety valves Other Alarms Pressurizer high pressure deviation via control system Four high pressure alarms via control system Pressurizer high level deviation via control system High level via control system Acoustic monitor flow detected	FD-2101 Sheet 3 and 4	If the Rx is at power at the time of accident, the immediate effect of a loss of flow (seizure of a RCP rotor) is an increase in the coolant temperature. This increase could result in DNB with subsequent adverse effects to fuel, if the Rx is not tripped promptly (FSAR, Page 14.1.6-1)	The FSAR analysis for this event assumes an instantaneous seizure of a reactor coolant pump rotor. For this event, the reactor trips on low flow signal. The common mode failure (CMF) of the new digital instrumentation would result in a loss of low flow Rx trip signal. The loss of flow will increase the coolant temperature and an increase in pressurizer pressure due to a reduction in heat removal. The wide range RCS temperature recorders (memo dated 9/2/92 from W. G. Sotos to V. D. VanderBurg) are available to the operator. The pressurizer pressure will continue to rise, and the operator will get a high pressurizer deviation alarm at 2325 psia (Procedure 2-OHP 4024.208 Drop 7) for Unit 2 and 2175 psia for Unit 1. The reactor trip on high pressure (≤2400 psia) is lost due to CMF. However, high pressure diverse alarms are available (memo dated 9/2/92 from W. G. Sotos to V. D. VanderBurg). Therefore, the high pressure deviation alarm will draw the operator's attention to trip the reactor manually. This event is very much like the loss of forced reactor coolant flow in one loop. However, it is more severe in that total core flow is reduced more rapidly to a lower value. The total core flow is reduced to ≈70% within ≈2 seconds. As the coolant heats up, a significant increase in pressure occurs. The peak analyzed pressure for both units is ≈2590 psia. This peak occurred at ≈2 seconds after the reactor trip at 1 second. This pressure is less than 110% of the design pressure, i.e. 2750 psia. However, if reactor trip is delayed ≈60 seconds, it cannot be stated with certainty that this pressure would not be exceeded. However, the analysis takes no credit for pressurizer spray or the pressurizer PORV's. It is also the case as with the loss of forced reactor coolant flow that the analysis was performed with a positive moderator temperature coefficient (MTC) of +5 pcm/°F. This value is more limiting than the Technical Specification limit at 100% RTP. It is conservative and provides substantial margin throughout the core life.

UNIT 1 and UNIT 2

FSAR TRANSIENT #	TRANSIENT	TRIP/SAFEGUARD FUNCTION FOR RX TRIP (FSAR 14.1.6.2)	IMPACT OF COMMON MODE FAILURE (CMF) ON TRIP FUNCTION	ALARM/ALTERNATE INDICATION SYSTEM AVAILABLE	DIAGRAM #	CONSEQUENCES OF UNAVAILABILITY OF DIVERSE ALARM	EVALUATION OF EVENT
14.1.6.2 (con't)							Therefore, as Tavg is increased, power increases in the analysis. As indicated in the loss of forced reactor coolant flow, a more realistic beginning of cycle MTC, would be ≈-4pcm/°F. Throughout core life the MTC would decrease to the ≈-20pcm/°F. The feedback from the MTC would therefore tend to shut the reactor down rather than increase power in an actual event. The Cook units are base loaded and operate with control rods in the all out position at full power. The possibility that automatic rod control might withdraw rods will have no impact because rods are essentially fully withdrawn. These considerations lead us to conclude that it is unlikely that pressurizer pressure would exceed 2750 psia and virtually impossible to exceed 3200 psig, the ASME Boiler and Pressure Vessel Code Level C criterion, which was used for AMSAC design. In the analysis, DNB is expected to occur. In the event of a delay of reactor trip by ≈60 seconds, this situation can only be exacerbated. The operation of pressurizer sprays and PORV's which were not modeled in the analysis will also result in an increase in fuel rods in DNB. However, it is believed that the available flow will prevent the core from degrading to condition where it cannot be cooled after trip. The portion of the core that experiences DNB is expected to heat up until the Doppler coefficient shuts it down. Fuel is not expected to melt but clad burst and oxidation are anticipated. Substantial core damage is acceptable for this event which is an ANS condition IV event with massive multiple failures. In the evaluation of the previous two paragraphs, an operator response time of ≈60 seconds was assumed. However, this event is expected to be very dramatic. Several pressurizer alarms can be expected within seconds of the start of the event including the acoustic monitor flow detected alarm. The pressurizer safety valves can be expected to lift which creates an impressive sound in the control room. Therefore, the operators response may be less than 60 seconds for this event.

UNIT 1 and UNIT 2

FSAR TRANSIENT #	TRANSIENT	TRIP/SAFEGUARD FUNCTION FOR RX TRIP (FSAR 14.1.6.2)	IMPACT OF COMMON MODE FAILURE (CMF) ON TRIP FUNCTION	ALARM/ALTERNATE INDICATION SYSTEM AVAILABLE	DIAGRAM #	CONSEQUENCES OF UNAVAILABILITY OF DIVERSE ALARM	EVALUATION OF EVENT
14.1.6.2 (con't)							As in the case of loss of forced reactor coolant flow, the most likely cause of event of this type, is the failure of the reactor coolant pump (RCP) or motor. The operator is provided with a significant number of alarms to give him information regarding the RCP's and motors. These alarms include bearing temp high, lower bearing seal water temperature high, lower bearing cooling water flow low, upper oil pot level high or low, and lower oil pot level high or low. Therefore, it is likely that the operator will have information available which will allow him to anticipate and therefore, substantially mitigate the event. For Unit 2 an offsite dose calculation was performed as a part of the transition to Westinghouse Vantage 5 fuel. The site boundary doses were 3 rem, thyroid and 0.3 rem whole body. These are very small fractions of the 10CFR100 criteria. However, with a delay in reactor trip of ~60 seconds, it is anticipated that core damage will be increased significantly. Nevertheless, the 10CFR100 criteria are expected to be satisfied for this condition IV event. In section 14.3.5, an offsite dose analysis for LOCA which is identified as the maximum hypothetical accident is described. For this analysis, it is assumed that 50% of the core inventory of halogens and 100% of the core inventory of nobel gases are released to containment atmosphere. Table 14.3.5-10 of the Unit 2 UFSAR and Table 14.3.5-7 of the Unit 1 UFSAR display the doses for this analysis. They satisfy the criteria of 10CFR100. Since the RCS is anticipated to be intact after a locked rotor event, it is expected that the doses for the maximum hypothetical accident will substantially bound the locked rotor event doses.

RESPONSE TO RAI ITEM 2

This item requested information pertaining to a) the need to perform a pre-operational end-to-end check of the new equipment, and b) information related to the effect of resistor tolerance on equipment calibration.

Regarding item a, as discussed with your staff during the December 20, 1993 meeting, a pre-operational end-to-end loop check is not necessary, based on the pre-operational test methodology that will be employed. Pre-operational testing is comprised of the following elements:

1. Electrical wiring and basic functional checks of the racks, using standard plant installation procedures.

2. Electrical wiring and basic functional checks, from the rack bistable output to driven devices external to the racks, using project-specific installation procedures.

3. Calibration from the transmitter to the first rack test point, using standard plant calibration procedures.

4. Calibration from the rack test jack/first test point to the end panel or control device, using standard plant calibration procedures.

It is important to note that the first rack test point is the key overlap point, and that loop current is monitored at each calibration test segment (via test point resistors). This test program results in a total end-to-end loop check through overlapping. This methodology is the current practice at the Donald C. Cook Nuclear Plant and is common for the industry. The test methodology adequately complies with IEEE Standard 338-1977.

Regarding Item b, as discussed during the December 20, 1993 meeting, the calibration methodology adequately compensates for test resistor tolerance effects. Test point resistor tolerances do not impact loop accuracy or performance. There are no effects caused by test point resistor tolerances because these effects are calibrated out per the system design and the calibration methods. This is accomplished by calibration of the field device and the rack components using a common reference test point as the key overlap point. Use of this common test point allows the technician to adjust the calibration of the rack components so that test point resistance tolerance effects are eliminated.