Docket File

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

June 10, 1992

Docket No. 52-002

APPLICANT: Combustion Engineering, Inc. (ABB-CE)

PROJECT: CE System 80+

SUBJECT: INSTRUMENTATION AND CONTROL SYSTEMS DIVERSITY

The Nuclear Regulatory Commission (NRC) and ABB-CE representatives held a public meeting on June 1, 1992, regarding a draft staff position on diversity of instrumentation and controls for the CE System 80+ nuclear plant. The list of attendees is provided in Enclosure 1. The NRC staff presented material at the meeting which is provided in Enclosure 2 to this summary.

ABB-CE stated that it is performing a common mode failure analysis for the digital computer systems of System 80+ which is not yet complete and will report the results when they are available. This analysis includes the assumption of no common mode failures for analog and electro-mechanical devices. ABB-CE also stated that forcing common mode failures in the analysis would render results that will not necessarily meet the Standard Review Plan (SRP) acceptance criteria for Chapter 15 accidents and transients. However, 10 CFR Part 100 criteria will be met.

NRC staff indicated that the parameters required for diverse monitoring were the Category I parameters of Regulatory Guide 1.97. Back-up controls would be required for reactivity control, core cooling, reactor coolant inventory control, containment isolation and containment integrity.

NRC staff requested reliability data for the Programmable Logic Controllers (PLC's) employed as a basic element of the System 80+. ABB-CE indicated that they would provide this information based on the many years of operating experience for these devices. ABB-CE agreed to investigate incorporating the non-safety-grade components of the control system into the reliability assurance program (RAP) to gain credit for reliance as a back-up to the safety-grade computer system.

DF03
1/1

ABB-CE intended to submit within a few days, proposed revisions to the staff's draft position that was presented at this meeting. ABB-CE provided an overview description of the computer systems used for System 80+ and their independence and diversity. NRC staff stated that this information would be considered in the final position to be recommended to the Commission.

Since there was insufficient time at this meeting, discussions regarding the additional items, including the sixteen on the last three pages of Enclosure 2, were deferred for later telephone calls.

(Original signed by)

Thomas V. Wambach, Project Manager
Standardization Project Directorate
Associate Directorate for Advanced Reactors
and License Renewal
Office of Nuclear Reactor Regulation

Enclosures:
1. Attendees List
2. Presentations

cc w/enclosures:
See next page

DISTRIBUTION:

Docket Files	PDST R/F	TMurley/FMiraglia	THiltz
NRC PDR	DCrutchfield	WTravers	RPierson
JNWilson	TWambach	PShea	SFlanders
JMoore, 15B18	GGrant, EDO	EJordan, MNBB3701	JJoyce, 8H7
MWaterman, 8H7	SNewberry, 8H7	MChiramal, 8H3	JStewart, 8H3
ACRS (10)	CMcCracken, 8D1	JGallagher, 8H7	

OFC:	LA:PDST:ADAR	PM:PDST:ADAR	SC:PDST:ADAR
NAME:	PShea PWS	TWambach:sl	JNWilson
DATE:	06/9/92	06/9/92	06/10/92

OFFICIAL RECORD COPY:
DOCUMENT NAME: MTGSUM61.TVW

cc: Mr. C. B. Brinkman, Acting Director
Nuclear Systems Licensing
Combustion Engineering, Inc.
1000 Prospect Hill Road
Windsor, Connecticut 06095-0500

Mr. C. B. Brinkman, Manager
Washington Nuclear Operations
Combustion Engineering, Inc.
12300 Twinbrook Parkway, Suite 330
Rockville, Maryland 20852

Mr. Stan Ritterbusch
Nuclear Systems Licensing
Combustion Engineering, Inc.
1000 Prospect Hill Road
Post Office Box 500
Windsor, Connecticut 06095-0500

Mr. Daniel F. Giessing
U. S. Department of Energy
NE-42
Washington, D.C. 20585

Mr. Steve Goldberg
Budget Examiner
725 17th Street, N.W.
Washington, D.C. 20503

Mr. Raymond Ng
1776 Eye Street, N.W.
Suite 300
Washington, D.C. 20006

Mr. Mark McCabe
U.S. Department of Justice/EAG
555 4th Street, N.W.
Room 11-809
Washington, D.C. 20001

Enclosure 1

List of Attendees

June 1, 1992

NAME	ORGANIZATION
Thomas Wambach	NRR/ADAR/PDST
Stan Ritterbusch	ABB-CE
John Gallagher	NRR/DST/SICB
Charles Brinkman	ABB-CE
Scott Flanders	NRR/ADAR/PDST
Joseph Joyce	NRR/DST
Robert Pierson	NRR/ADAR/PDST
Scott Newberry	NRR/SICB
Robert Harvey	ABB-CE
Thomas Starr	ABB-CE
Ken Scarola	ABB-CE
Matt Chiramal	NRR/DST/SICB
James Stewart	NRR/DST/SICB
William Travers	NRR/ADAR
J. Regan	MPR
Mike Waterman	NRR/DST

1. Defense Against Common Mode Failures in Digital Instrumentation and Control Systems

Background:

The use of digital computer technology in protection and control systems raises a concern that the software and hardware for these computer systems could be vulnerable to programming errors that could lead to safety-significant common mode failures. Reasons for this concern and defenses against common mode failures were discussed in SECY-91-292 and can be summarized as follows:

- common mode failures could defeat not only the redundancy achieved by the hardware architectural structure but also could result in the loss of more than one echelon of defense in depth provided by the monitoring, control, reactor protection and engineered safety actions performed by the digital instrumentation and control (I&C) systems.

- the two principal factors for defense against common mode failures are quality and diversity. High quality will increase the reliability of both individual components and complete systems. Diversity in assigned functions, for both equipment and human activities, and diversity in equipment, hardware and/or software, can reduce the probability of propagation of common mode failures.

- In SECY-91-292, the staff stated that some level of diversity, such as a reliable analog backup, would be required.

Discussion:

The goal for digital computer-based I&C systems must be to contribute towards the safe and reliable operation of nuclear plants. While there is general agreement among designers, operators and regulators of nuclear power plants with respect to the general importance of quality and diversity as defense against common mode failures there are no consensus standards for certification of the design of digital I&C systems. Enclosure 2 of SECY-91-292 reviews considerations by the staff for regulatory requirements regarding several key subjects relevant to defense against common mode failures including,

- assessment of diversity

- requirements for engineering activities

- requirements for design implementation

- safety classification of I&C systems.

The first of these four subjects, assessment of diversity, has progressed farthest with respect to establishing regulatory requirements. The staff, with Lawrence Livermore National Laboratory (LLNL), has performed a study of the General Electric Advanced Boiling Water Reactor (ABWR) design to assess defense-in-depth and diversity. This assessment was performed using the method described in NUREG-0493, A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System for each transient and accident evaluated in Chapter 15 of the Safety Analysis Report. The results of this assessment are used to determine if additional diversity is necessary to defend against postulated common mode software and hardware failures.

The second and third subjects above have been discussed at length in the EPRI Advanced Light Water Reactor Utility Requirements Document (URD), Chapter 10, for both the evolutionary and the passive plants (VOL'S II and III). Both of these subjects were reviewed in SECY-91-292. The EPRI URD provides a frame of reference for the development by the NRC of acceptance criteria for the digital control systems. The issue of diversity in digital control systems has been raised with EPRI, but is not yet included to the degree the staff believes necessary.

The fourth subject, safety classification, is under review by the staff, as presented in SECY-91-292; in the international community for ballot on the draft International Electrotechnical Commission (IEC) standard, "The Classification of Instrumentation and Control Systems Important to Safety for Nuclear Power Plants"; and with EPRI on the "ALWR Position Paper for Passive System Classification and Requirements". The subject of safety classification is relevant to the subject of diversity through the question of determining safety credit for traditionally non-safety systems, in accord with the principle of defense-in-depth.

Defense-in-Depth of Digital I&C Systems

The staff review on the matter of diversity and defense-in-depth has progressed significantly since issuance of SECY-91-292.
With the completion of the LLNL assessment of the ABWR and the staff's assessment of the state-of-the-art on this issue, summarized in the following, the staff has established a recommendation.

In recent years, there has been a significant increase in the in-depth assessments of the integrity of software applied to safety-critical functions. These assessments have covered the range from computer based medical treatment facilities to computer-based fly-by-wire aircraft control systems and nuclear power plant protection systems. While there are many different opinions amongst the computer science or software engineer experts who have been involved in assessing the design processes and tools used to produce highly dependable software, the staff believes that there is a consensus that a quantitative estimate for the reliability of high integrity software based I&C systems cannot be developed and as a result, there is a need for some type of non-software based backup in safety-critical

applications. The type and functional extent of this backup is dependent on the degree of confidence one is willing to assign to the computer based systems.

Recommendation:

The staff recommends the assessment of diversity and the requirement for a non-computer based backup for manual systems level actuation and displays. This approach and requirements for the backup are defined as follows;

1. The applicant shall perform a "Defense-in-Depth and Diversity Assessment" of the proposed instrumentation and control system to demonstrate that vulnerabilities to common mode failures have been adequately addressed. The staff considers software design errors to be a credible common mode failure which must be specifically included in the evaluation. An acceptable method of performing analyses is described in NUREG-0493, "A Defense-In-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System", March 1979. Other methods proposed by an applicant will require case-by-case NRC approval.

2. In the above analysis sufficient diversity within the design should be demonstrated for each event evaluated in Chapter 15 of the Safety Analysis Report on Accident Analyses, occurring in conjunction with each postulated common mode failure.

3. If a postulated common mode failure is capable of disabling a safety function, then a diverse means, with a documented bases that the diverse means is unlikely to be subject to the same common mode failure, shall be required to perform either the same function or a different safety function that provides equivalent protection. The diverse or different safety function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the appropriate conditions. Diverse digital or non-digital systems are acceptable means. Manual actions from the control room are acceptable if time and information are available to the operators. The amount and types of diversity may vary from design to design and will be evaluated on a case-by-case basis.

4. A set of safety grade displays and controls, independent of the computer system(s) and located in the main control room, shall be provided for system-level actuation and monitoring of critical safety functions and parameters. The displays and controls shall be conventionally hardwired to as low a level in the system architecture as possible. The specific set of equipment required will be evaluated on a case-by-case basis.

The hardwired system-level controls and displays provide the plant operators with unambiguous information and control capabilities. These hardwired controls and displays are required to be in the main control room to enable the operators to expeditiously mitigate the effects of the postulated common mode failure of the digital I&C system. The control room would be the center of activities to safely cope with the event which would also involve the initiation and implemention of the plant emergency plan. The design of the plant should not require operators to leave the control room for such an event. For the longer term recovery operations, credit may be taken for actions from outside the main control room when the emergency response organization are in place and fully briefed to take such actions.

Enclosure

POTENTIAL OPEN ITEMS

Of the following issues, (2), (6), (7), (11), (13), (14), and (16) will likely be open issues in the DSER. We should be able to close out the other issues through discussions with ABB-CE.

Issue 1 - Section 7.2.1.2(K) states that system components with known susceptibility to electromagnetic interference (EMI) are subjected to EMI qualification in accordance with applicable requirements of MIL-STD-461C, 1986, "Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference." The complementary MIL-STD 462 should also be referenced. The frequency range for the EMI tests should also be specified. Additionally, on-site testing for EMC must be included in the ITAAC.

There have been instances when an Electromagnetic Compatability (EMC) standard has been referenced, but the range of frequencies over which the tests have been conducted has been inadequate. For example, a range of 20MHz to 1 GHz is a typical range of frequencies used in testing for EMC. MIL-STD-461C covers the lower frequencies (down to 30 HZ), but only if the vendor selects that frequency range.

Issue 2 - Section 7.2.2.3.2, "Equipment Design Criteria," (G)(4), Multiple Failures Resulting from a Credible Single Event. The DC states that this cannot occur because failures within the protective system cannot propagate to the control systems due to the isolation devices. This issue should be addressed in the CMF analyses.

ABB-CE is in the process of performing CMF analyses. They will not be using the 0493 methodology. Instead, they will fail the entire PPS and look at which systems are available for recovering the plant. This will be done for each Chapter 15 transient. LLNL (Bob Wyman) is looking at the CMF analyses.

Issue 3 - Section 7.3.1.1(A), "ESF-CCS Configuration," states that primary and secondary processors function such that the primary unit actively performs the control functions while the standby unit passively follows (tracks) the actions of the primary unit. Primary and standby processor performance is continuously monitored by a redundancy controller. Control tasks are automatically transferred to the standby unit upon detection of a primary unit failure and confirmation of standby unit operability. What happens when the standby unit is not available? What happens if the redundancy controller fails?

Issue 4 - The discussion of Local Control Switches in Section 7.3.1.1(C) did not indicate whether the operator at the local switches could monitor the results of actuating equipment. In

the event of a common mode failure of the remote field multiplexers or the data highways, the operators in the control room may not have adequate information to assess the plant status. Consequently, the operators at the local control switches may need local indications of plant status. Is there addtional design information regarding LCS configuration?

The discussion of the LCS also stated that the controls are hardwired to MCCs, etc. Does this wiring bypass the PLCs such that the LCS satisfy the intent of Diversity Position 4?

Issue 5 - The MFWCS wide range level reference leg is the same reference leg as the EFAS level and pressure leg. Additionally, Figure 10.1-2 shows 2 channels of EFAS pressure and level measurement use the same reference leg. Will rupture of a reference leg cause a MFWP trip on high indicated level, and a coincident trip of EFW on 2/4 indicated high levels/low pressure?

Issue 6 - The ITAAC have not been completed for the I&C systems. These will be an open item in the DSER.

Issue 7 - A Software Capabilities Evaluation (SCE) should be perfomed to determine ABB-CE's ability to design, produce, and maintain high-integrity software. Note that ABB-CE has extensive experience with the CPCs and COLSS. What is not known is whether this expertise is held by the organizational unit or by selected experts within that unit. If the expertise depends on selected personnel, continued success depends soley upon the continued employment of these key personnel. This should be addressed in the ITAAC.

Issue 8 - Bypassing SCS Heat Exchanger 1 results in a loss of flow indictation in the Shutdown Cooling System. Midloop operations need that indication to prevent SCS pump cavitation. The MCBD for the SCS (Figure 7.3-22) indicates valve SD-312 in the heat exchanger bypass line and valve SD-310 in the normal line are both normally open. Consequently, the flow trnasmitter (FT-302) will not indicate the correct flow.

Issue 9 - ABB-CE implies that the SCS trains are redundant and diverse. The trains are redundant, but not diverse.

Issue 10 - Table 7.4-1 lists the instrumentation and controls available at the RSP. There are no MFW or Startup Feedwater (SUFW) indications or controls. During operations at the RSP when MFW/SUFW is still available, there is no means available to monitor or control MFW/SUFW. It could be argued that there are indications of steam generator level and pressure; but levels do not provide the operator with a direct indication of MFW conditions or MFW system performance, and the means of responding

to level perturbations still do not exist.

Issue 11 - Has ABB-CE reviewed the CE 80+ design against the EPRI Utility Requirements Document for Evolutionary Plant designs?

Issue 12 - Once a sensor is selected by the operator for sensor validation use, that sensor is used by the validation algorithm to automatically return "bad" sensors to "good". A "good" sensor is declared when its deviation check against the selected signal is acceptable. This appears to conflict with IEEE 338-1987, which states that when a test fails, an additional test cannot be used to cancel out the unsuccessful test. Some other action must be taken first. Retesting alone is not acceptable.

Issue 13 - The DIAS-PA and DIAS-PB CPUs have a failover link that allows "bumpless" transfer in the event DIAS-PA fails. If DIAS-PA has an execution error, will that error propagate the DIAS-PB? Can DIAS-PB be failed by actions in DIAS-PA? The failover link appears to defeat the requirements for independence and redundancy.

The same question arises regarding the Interprocessor Link between the Primary Host Processor and the Backup Host processor in the DPS.

Issue 14 - ABB-CE assumes credit for a two-out-of-four system, with one channel in bypass. The limits on the time the channel may remain in bypass have not been stated (indefinite limit). Indefinite bypass implies that there are only three channels in the Protection System. Is this configuration assumed in the FMEA, the PRA, and the Chapter 15 analyses? See Item (5) as an example of a single failure that can defeat the 2/3 system configuration.

Issue 15 - The annunciators are non-Class 1E, although the power supplies for the annunciators are from Class 1E buses. Address how the design meets the EPRI URD requirements for ALWR annunciators. The alarms provided for manually controlled actions for which no automatic control is provided and which are required for the safety systems to accomplish their safety functions should be fully Class 1E.

Issue 16 - The staff positions on diversity assessment and backup systems (Positions 1- 4) must be addressed.