ABB
ASEA BROWN BOVERI

June 3, 1992
LD-92-073

Docket No. 52-002

Mr. Dennis M. Crutchfield
Office of Nuclear Reactor Regulation
Attn: Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Subject: System 80+™ Diversity for Digital Instrumentation Systems

Reference: ABB-CE Letter LD-92-068, May 18, 1992

Dear Mr. Crutchfield:

On June 1, 1992, ABB-CE met with NRC staff to discuss our approach to diversity (referenced letter) and the forthcoming proposed policy "Defense Against Common Mode Failures in Digital Instrumentation and Control Systems". A draft version of the policy was distributed and detailed discussions resulted in a much more clear understanding of the technical issues involved. A proposed revision and the corresponding rationale are attached to this letter. They are intended to clarify the proposed policy based upon our understanding of the staff's intentions.

If you have any questions, please call me or Mr. Stan Ritterbusch at (203) 285-5206.

Very truly yours,

COMBUSTION ENGINEERING, INC.

S. E. Ritterbusch for

C. B. Brinkman
Acting Director
Nuclear Systems Licensing

CBB/ser
cc: J. Trotter (EPRI)
T. Wambach (NRC)

110058

D032 1/1

Combustion Engineering, Inc
1000 Prospect Hill Road
Post Office Box 500
Windsor, Connecticut 06095-0500
Telephone (203) 688-1911
Fax (203) 285-9512
Telex 99297 COMBEN WSOR

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:

- o 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 functions performed by the digital instrumentation and control (I&C) systems.

- o 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.

- o 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,

- o assessment of diversity

- o requirements for engineering activities

- o requirements for design implementation

- o 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

simple, proven

easily

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~~. Insert 6

Recommendation:

The staff recommends simple, proven 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; critical safety functions

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. Insert 1 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. Insert 2

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. adequate 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. Insert 3

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 manual 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. Insert 4 Insert 5

Insert A

Insert A

more complex

simple, proven

The ~~hardwired~~ system-level controls and displays provide the plant operators with unambiguous information and control capabilities. These ~~hardwired~~ simple, proven 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 systems. 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 ~~adequate segments of~~ the emergency response organization are in place, to take such actions.

and fully briefed

Insert 1

for all computer-dependent functions.

Insert 2

Concurrent independent failures and events such as losses of offsite power or earthquakes need not be considered in conjunction with design basis events.

Insert 3

Adequate protection may be demonstrated by qualitative, best-estimate analysis to show compliance with 10 CFR 100 radiological release limits.

Insert 4

It shall be demonstrated that these displays and controls are of adequate simplicity and are proven (e.g., time in-service in similar applications) to have reasonably minimized the potential for common mode failure. Such simple designs could include hard-wired analog components. Alternately, simplicity could be accomplished via digital instrumentation and controls where reliance is minimized on applications level software, inter-computer data communication links, and computer sub-elements that are also relied upon for automatic actuation.

Insert 5

but shall be sufficient to monitor and actuate systems intended to control the following critical functions: reactivity control, core heat removal, reactor coolant system inventory control, containment isolation, and containment integrity.

Insert 6

specific components and design features of the instrumentation and control systems being considered.

Rationale for Proposed Revisions

Rationale for the Revision to the Section on "Defense-in-Depth":

"Non-software" was deleted as an adjective for the I&C backup systems to avoid an impractical or impossible requirement on the design of backup systems. "Simple, proven" were inserted as more appropriate characteristics for the backup systems. "Insert 6" is provided as a modification to the same paragraph to clarify that the specific design features of the system being backed up must be considered in evaluating the design of the backup system.

Rationale for the Revision to the Introductory Paragraph in the Recommendations Section:

The proposed wording change from "non-computer based" to "simple, proven" provides a functional requirement for the backup system without specifying what hardware is or is not acceptable. This paragraph and the following recommendations should provide functional requirements for protection against common mode failures, not dictate the type of hardware.

Rationale for Revision of Recommendation 1:

The proposed wording change (Insert 1) is provided to clarify that electro-mechanical and analog components need not be considered in the common mode failure analysis. The probability of common mode failure of these devices is considered to be sufficiently low as to not require consideration. This is based on their simplicity, time in service, and the time between actual independent failures that would be propagated by a potential common mode failure.

Rationale for Revision of Recommendation 2:

The proposed wording (Insert 2) is provided because the probability of a design basis event (i.e., Chapter 15 event) concurrent with another event is so low as to not require consideration in conjunction with a common mode failure (the common mode failure is also a very low probability event).

Rationale for Revision of Recommendation 3:

The proposed wording change from "equivalent" to "adequate" and the added sentence (Insert 3) provides a more specific definition of the protection to be provided.

Rationale for Revision of Recommendation 4:

The word deletions and additions (Inserts 4 and 5) are proposed to establish criteria for displays and controls of maximum reliability, rather than limiting the designs by dictating the acceptable hardware type. The proposed wording would allow the designer to achieve the necessary reliability goals while not precluding the benefits of digital technology.