COMBUSTION ENGINEERING

September 14, 1988
LD-88-091

Docket No. STN 50-470F
(Project No. 675)

Mr. Guy S. Vissing, Project Manager
Standardization and Non-Power Reactor
Project Directorate
Office of Nuclear Reactor Regulation
Attn: Document Control Desk
U. S. Nuclear Regulatory Commission
Washington, D.C. 20555

Subject: CESSAR-DC, Program for Addressing Sabotage Protection

References: (A) Letter, G. S. Vissing (NRC) to A. E. Scherer (C-E), dated December 8, 1987

(B) Letter, LD-88-020, A. E. Scherer (C-E) to G. S. Vissing (NRC), dated March 18, 1988

Dear Mr. Vissing:

The purpose of this letter is to respond to Reference (A) concerning sabotage protection. To give some insight to your review on this subject, you summarized some specific areas of interest. For convenience, those specific items are provided in Attachment (1) to this letter. Our approach to Physical Security, including sabotage protection, was described in our response to NRC Question 500.2 [Reference (B)]. Your phone call of March 31, 1988, expressed the concern that our response was based on current NRC criteria and would not include a search for new criteria.

Combustion Engineering is establishing a sabotage protection program to address your concerns. Our program will be based on the general criteria and guidance from EPRI's ALWR Requirements Document. The basic elements of our program are:

1. Development of design bases for System 80+™ relative to sabotage which conform to the EPRI Requirements Document. Attachment (2) provides the current draft of this guidance.

2. Development of a ranking of systems and components important to sabotage, using an approach consistent with the Department of Energy's report "Ranking of Light Water Reactor Systems for Sabotage Protection" (SAND82-7053, July 1982).

Power Systems
Combustion Engineering, Inc.
1000 Prospect Hill Road
Post Office Box 500
Windsor, Connecticut 06095-0500
(203) 688-1911
Telex 99297

E007
1/1

3. Development of a plant layout with the system and component ranking as an input, in a manner which supports implementation of area-type physical protection measures as identified in the NRC's report "A Review of Selected Methods for Protecting Against Sabotage by an Insider" (NUREG/CR-2643, August 1982).

4. Evaluation of the fluid, electrical, and nuclear systems from the standpoint of damage control to mitigate sabotage, consistent with the approach outlined in the NRC's report "Acceptance Criteria for the Evaluation of Nuclear Power Reactor Security Plans" (NUREG/CR-0908, August 1982).

5. Implementation of additional design improvements, as necessary, to ensure appropriate ability to achieve safe shutdown for attempted sabotage events.

We expect to complete our program in 1989, however, this is contingent on timely development of the corresponding chapters of the EPRI ALWR Requirements Document. The EPRI ALWR Requirements Document should be very useful in addressing Items 1, 2, 3, 5, and 6 in the attached list of NRC sabotage protection considerations [Attachment (1)]. Also, we expect that in the fourth quarter of 1988, we will propose to meet with you to describe our program (and progress) and obtain your feedback. In the meantime, we would be pleased to receive any additional input that you might have on criteria for sabotage protection so that it can be considered in the System 80+ design or the EPRI Requirements Document as appropriate.

If you have any questions or comments, please feel free to call either me or Mr. S. E. Ritterbusch of my staff at (203) 285-5206.

Very truly yours,

COMBUSTION ENGINEERING, INC.

A. E. Scherer
Director
Nuclear Licensing

AES:dmb
Attachments: As Stated

cc: E. B. Abrams (Duke Power Company)
Frank Ross (DOE-Germantown)
J. Devine (EPRI)

Summary of Sabotage Protection Considerations Identified by NRC December 8, 1987

1. Resolution of USI A-29.

2. Identification of design criteria to reduce the dependence on security systems for protection against radiological sabotage.

3. Description of the design features that implement the criteria of item 2 without impeding emergency access to safety-related equipment.

4. Analysis of sabotage to demonstrate the effectiveness of design features in item 3 above.

5. Implementation of the Regulatory Guide 5.65 position on physical barriers, which could affect the design of ducts and ventilation openings.

6. Discussion of how many decay heat removal systems would have to be defected to prevent mitigation of a loss of off-site power event.

7. Identification of the equipment within Combustion Engineering's scope, but outside the containment, that would have to be protected as vital in the context of 10 CFR 73.2(i).

8. Identification of systems not within Combustion Engineering's scope that applicants would have to list as vital.

9. Protection of listings of vital equipment (items 7 and 8) from public disclosure in accordance with either 10 CFR 50.34(e) or 10 CFR 2.790.

DRAFT REQUIREMENTS FOR SABOTAGE DESIGN FROM THE EPRI ALWR REQUIREMENTS DOCUMENT

1. Insider threat is based on one knowledgeable individual working alone without armament or explosives to create an offsite release in excess of 10CFR100 limits.

2. The security detection systems cannot be disabled without detection by the security force.

3. Insider sabotage can result in either/both an event initiation or a latent functional impediment (also called tampering).

4. Outsider sabotage by force can be effectively deterred by the onsite and/or offsite security assets. The size and means of outsider threats must be assumed in the design of security systems and assets.

5. The security system shall perform its functions during all modes of plant operation.

6. Sabotage events are not taken in conjunction with some other independent single failure (such as diesel engine failure or redundant system failure) or independently initiated events such as external events (e.g., seismic, tornado) or internal events (e.g., LOCA, SGTR).

7. Design for protection against sabotage shall prevent a release in excess of the guidelines of 10CFR100 from irradiated fuel.

8. The security restrictions for access to equipment and plant regions must be compatible with loss of site power access requirements, fire protection, health physics, and local operation actions required for event mitigation more generally. Access restriction should not excessively impede operator functions during normal operations.

9. The security system shall prevent unauthorized access to containment during power operation. Therefore, sabotage for components and systems located in containment need not be considered for power operations.

10. The sabotage design shall assure protection of the core damage prevention safety functions, i.e., reactivity control, coolant inventory control, coolant pressure control, and coolant heat removal.