DOCKET NO. 50-205

PAUL E. ROSENTHAL • CONSULTING ENGINEER

604 MISSION STREET • SAN FRANCISCO
TELEPHONE SUTTER 1-2871 POSTAL CODE 94105

March 17, 1964

Atomic Energy Commission
Washington 25, D. C.

Attention: Mr. Robert Loewenstein, Director of Licensing and Regulation

Gentlemen:

This is to request information on the projected Bodega Bay Unit No. 1, your Docket No. 50-205.

The writer is a consulting mechanical engineer experienced in the startup and debugging of industrial materials handling, control, and instrumentation systems. The Preliminary Hazards Analysis, Exhibit C of the Bodega Bay application; the Commission's Questions; Amendments No. 1 and No. 2 to Exhibit C, and TID 7024 have come to my attention.

My reading of these documents has raised a series of questions relative to the reactor safety control systems; the design of underground structures traversing fault lines to resist ground movement; and the presentation of estimates of the benefits of nuclear power to the public.

Parenthetically, you may share my surprise that private conversations with eight prominent professional engineers, six of them in responsible charge of design of major projects and one a construction manager, indicate opposition to construction of the Bodega reactor by a score of seven to one.

It is hoped that an exchange of correspondence will answer this writer's questions, or encourage answers to be developed where none now exist.

The questions which we think need discussion are:

I. What is the hazard to be guarded against?

II. How does the reactor control system protect us from the hazard?

III. Are we is possession of sufficient information as to long term reliability of the plant?

We request discussion of the following:

I. What is the hazard to be guarded against?

a. Structures: The reactor at Bodega is in a circular pit. In the event of horizontal shear forces across any subfault within the pit, the concrete lining will either have to act like a round key, preventing relative ground motion, or will yield. Are you prepared to approve a structural design which has to be "earthquake resistant" in this sense, rather than in the more familiar sense of above-ground structures resisting horizontal forces due to ground accelerations and building inertia? We here acknowledge verbal reports of design studies for the Stanford Linear Accelerator wherein an underground structure traverses a fault line. Are these design approaches sufficiently well proven in experience to form the basis of AEC approval for a reactor pit lining?

b. Reactor Operation: Is there a hazard from muclear explosion here? What are the consequences of the failure of the scram system to operate? If the core starts to melt and the fuel collects in the bottom of the core, what would happen?

II. How does the reactor control system protect us from the hazard?

a. Overcontrol Capability: From page IV-5 of Preliminary Hazards Analysis: "The total control system is designed with enough shutdown capacity so that the reactor will always be subcritical with any one control rod completely withdrawn from the core." To this reader the implication is that under some conditions complete insertion of 144 of the 145 control rods may be necessary for complete shutdown. Is this true?

b. Control System:

1. Refer to Figure III-25, PHA. How many control rods does Reactor Protection Channel #1 activate? How many control rods does Reactor Protection Channel #2 activate?

2. See PHA Figure III-14. Are the two control rod drive system solenoid valves functionally redundant? It would appear that the piping

and porting of the 2 control valves put them in a logically "OR" relationship so that a loss of voltage in either pilot solenoid circuit will initiate a scram.

3. What is the function of the 3-way solenoid valve SO/NC35 interposed between the 2" instrument air supply and the instrument air header? Is this "DC inergized to scram" solenoid powered by the station battery mentioned on PHA page III-26? Is this device considered "fail safe" and is its wiring loop to be monitored for continuity?

4. Refer to PG & E's Amendment No. 1, Page 11, answer to question #25, "Failure of power to only one bus will cause de-energization of the scram pilot valves connected to the channel served by that bus but will not result in a scram. This permits reactor operation to continue, with single channel protection provided by the unaffected channel." Under this scheme it would be possible to operate the reactor without any backup for its one functioning control channel.

How can this description be brought into line with the desire for a high-reliability scram control system? If this writer understands the wiring and piping diagrams mentioned above correctly, an alarm condition from <u>either</u> reactor protection channel will initiate a scram.

This writer would object to any unnecessary complications in an automatic control system and also would object to lockouts, bypasses, or other defeat mechanisms in the safety circuits. We wonder, then how the applicant's description of the operation of his "dual channel fail safe" control system can be made into a reality. How is the scram pilot valve to discriminate between current interruption due to bus voltage failure and current interruption due to alarm action of the automatic controls?

III. Are we in possession of sufficient information as to long term reliability of the plant?

a. <u>Control Rod Drives</u>: The control rod drives are, in this writer's opinion, moderately tricky devices, consisting of two concentric piston motions in a common exterior housing. Is there a five year record of successful operation of this device at the temperatures, pressures, and corrosion and radiation conditions to be found in the Bodega Reactor?

b. Instrumentation:

1. Is there a five year successful operating record on the instrumentation items proposed for in-core mounting, under the same conditions to be found in the Bodega Reactor?

2. Is it proposed to use any transistors or any other solid state electronic devices in surroundings in which these are significant levels of radiation? For each type proposed to be used, is there a successful five year operating record at those levels of radiation?

3. How will individual solid state devices be selected for reliability?

c. Economics: If full safety is to be achieved through the use of a "dual channel fail safe" control system, and if any failure of any component in either channel is to initiate a scram, if the entire plant has to go off the line on each scram, and if a full inspection of the plan will be necessary to determine what caused the scram, what does this do to the economics of plant operation?

d. Materials Handling and Maintenance:

1. Is there a five year record of successful operation of fuel rod, control rod, and core structure component handling, maintenance, and replacement equipment? Does this record include the successful handling of worn, bent, or corroded fuel rods and control rods?

2. Assume a condition of localized high neutron flux in the core as mentioned in the PHA. Assume localized meltdown of core components. Is there a record of successful replacement of damaged core components? Who is to determine the extent of repairs needed, and what is the amount of downtime required to reinspect and recertify the reactor as fit for service?

e. Design Stresses and Safety Factors:

Sources of information on the design of reactors for earthquake resistance seem to be written mainly by geologists or structural engineers. Their design criteria appear to be less conservative than those used in ordinary industrial equipment. For instance, Housner's "Design of Nuclear Power Reactors against Earthquakes" (Proc. 2d World Conf. on Earthquake Engineering, Tokyo, P. 134) refers to Class I parts of reactors -- those essential for safety of operation -- as areas where stresses should "remain within the elastic limits". Neglecting for the moment that moving parts often are limited by considerations of deflection rather than of strength, this writer's comment is that a much greater margin of safety appears appropriate to a reactor.

The simple analyses made in the commercial design of materials handling equipment, for instance, show a gradation of factors of safety as the amount of hazard changes. Small commercial hoists may have design stresses of one-third of the ultimate; similar equipment specifically for repair work around expensive jet aircraft will call for design stresses of one-fifth; and some parts of ladle cranes carrying molten metal in large pouring shops, where not only initial factors of safety but generous allowances for attrition due to wear are made, the design stresses can be one-tenth of the ultimate.

What is to be the factor of safety appropriate to the handling of fuel rods? It is assumed that your office goes through an extensive plan-checking procedure in approving the design work on reactors; similar plan checking in the day-to-day routine of a municipal building inspection department is based upon some applicable code. Do you have a code which governs the design of mechanical parts and reactor internals? Where did this code originate? Where it is not based upon some earlier code well proven in experience, such as the ASME Code for Pressure Vessels, how has it been experimentally verified?

Your early reply to this inquiry will be appreciated.

Very truly yours,

Paul E. Rosenthal

Paul E. Rosenthal

PER:dl

From the desk of

COMMISSIONER WILLIAM M. BENNETT

To: Dr. Glenn T. Seaborg

Date: May 21, 1964

DOCKET NO. 50-25

File Copy

DOCKETED
USAEC
Division of Licensing & Regulation
MAY 26 1964
Docket Office

RECEIVED
MAY 26 1964

Rec'd Off. Dir. of Regs.

Date ____________

Time ____________

H ST ____________ 6th ____________