ATTACHMENT 5

REPORT ON THE
NUCLEAR REGULATORY COMMISSION
REACTOR SAFETY REVIEW PROCESS

By

Robert D. Pollard

Project Manager

Division of Project Management

U. S. Nuclear Regulatory Commission

February 6, 1976

ILLUSTRATIVE SAFETY PROBLEMS

I. CONTAINMENT ISOLATION

The General Design Criteria set forth in Appendix A to 10 CFR Part 50 establish the "minimum requirements for the principal design criteria for water-cooled nuclear power plants". (10 CFR Part 50.34) General Design Criteria 54, 55, 56 and 57 establish minimum requirements concerning isolation of piping systems that penetrate the reactor containment. Criterion 55 and Criterion 56 specify four containment isolation valve arrangements. Each isolation valve arrangement involves a combination of locked closed isolation valves and/or automatic isolation valves to prevent the release of radioactive material. These criteria specify that one of the four valve arrangements "shall be provided -- unless it can be demonstrated that the containment isolation provisions for a specific class of lines, such as instrument lines, are acceptable on some other defined basis".

In contrast to these specific requirements, the staff is aware that many of the lines at the Indian Point 3 plant do not have isolation valve arrangements which correspond to any of the arrangements specified by Criterion 55 and Criterion 56. Furthermore, neither the staff nor the licensee has identified a "specific class of lines" that need not utilize the specified arrangements. Nor has either the staff or licensee identified "some other defined basis" on which the Indian Point 3 isolation valve arrangement can be demonstrated to be acceptable.

Rather than adhere to the requirements of the General Design Criteria, the licensee has proposed technical specifications which would permit plant operation with containment isolation valves (which have no provision for automatic closure) in their open positions. The licensee states that reliance on the reactor operator to manually initiate closure of such valves is adequate. The staff apparently gives tacit approval to this evasion of NRC regulations by stating the "We have reviewed the isolation valve arrangements for conformance to General Design Criteria 54, 55, 56 and 57, and conclude that the design meets the intent of these criteria". (Safety Evaluation of the Indian Point Nuclear Generating Unit No. 3, dated September 21, 1973).

This is one of the safety problems I became aware of as project manager for Indian Point 3. The pressure to issue a license on a schedule compatible with the applicant's desires notwithstanding, I questioned those staff personnel with specific expertise in the reactor containment area about their bases for accepting the Indian Point 3 design. Their responses indicated that: a) it was known that the design did not meet the General Design Criteria, b) the design was not different than other licensed nuclear power plants, and c) it was too late to require design changes to the plant. These experts stated that they saw

no reason to change their previous conclusions as stated in the Indian Point 3 Safety Evaluation Report and referenced above. The bases for these conclusions remain obscure if not non-existent. The staff's Safety Evaluation Report mentions the "double barrier protection -- provided so that no single valve or piping failure can result in loss of containment integrity". Also described briefly are the two groups of containment isolation valves which are closed automatically by the safety injection signal and the actuation of containment spray. No mention is made of the non-automatic containment isolation valves, the criteria used to judge the acceptability of reliance on manual operator action, or the specific "closed system" which is purported to constitute one of the barriers to escape of radioactive materials.

I believe that the provisions for containment isolation following an accident at Indian Point 3 should be evaluated or re-evaluated. If the present design and proposed technical specifications are found acceptable, the NRC should state the specific technical bases for its conclusion that the design meets the NRC regulations. Indian Point 2 should also be evaluated in this regard. It is likely that the situation there is the same as or more hazardous than the situation at Indian Point 3.

The staff should have discussed the non-automatic containment isolation valves, the nature of the "closed systems upon which the "acceptability" was partially based, and the criteria used

to judge the adequacy of manual operator action.

The Safety Evaluation Report, in discussing only those aspects of containment isolation which were not a problem and then stating the conclusion that the design meets the "intent" of the General Design Criteria, presented a more favorable picture of containment isolation than the actual design warrants. By presenting only the favorable aspects, the remainder of the licensing process, i.e., scrutiny by public, independent decisions by the licensing boards, was subverted and therefore less likely to be able to reach a sound decision based on all the facts.

II. SUBMERGED VALVES

During my assignment as project manager for the Indian Point 3 plant, the problem concerning submerged valves arose. Basically, this problem is that following an accident, much of the water from the reactor coolant system and from operation of the emergency core cooling systems collects in the containment. Recently, it has been discovered that many valves located inside the containment, including some valves intended to be used to mitigate the consequences of accidents, could become submerged and, thereby, rendered inoperable. Why the vendor, applicant or staff did not discover this problem over the past years is a question worth explaining for the future, with the aim of preventing similar fundamental oversights. For now, it is better to concentrate on determining an acceptable solution to the problem.

Con Ed has proposed a scheme to solve the problem. Basically, their proposal is to elevate only a few of the valve motors (but not the valves) above the calculated water level which is expected following an accident. For most of the valves whose motors will be sacrified, Con Ed has expressed their conclusion that this will have no adverse effect on accident consequences. Since not all the valve motors (which were previously to be relied upon to cope with the accident) will be elevated, it is necessary to modify equipment and to develop new operating procedures for the manual operator actions that are required soon after the accident. Whether the new procedures and resulting core cooling system performance using these new procedures have been evaluated as thoroughly as the original design by either the staff or the applicant is questionable. Whether the plant operators have been adequately "debriefed" on the old procedures and retrained in the use of the new procedures is also questionable.

The deficiencies in the evaluation of the revised design and operating procedures are illustrated by the following questions which have not been adequately analyzed:

a) Do the platforms used to support the elevated motors have adequate capability to withstand an earthquake? (Of course, until a decision concerning the magnitude of the earthquake that must be withstood is reached, the question of the seismic adequacy of the entire plant remains unanswerable.)

b) Is there any circumstance under which the submerged valves might be needed to cope with an accident, especially if the accident sequence does not follow the predicted sequence?

c) What "new" equipment will need to be relied on, e.g., core cooling system flow instrumentation? Has this equipment been designed, procured and installed in accordance with the regulations and standards applicable to safety equipment?

d) What are the disadvantages (and what are their significance) of using operator's trained on Unit 2 to operate Unit 3 which has had substantive design changes compared to Unit 2?

e) What other equipment besides valves will become submerged following an accident? Has the effect on safety of submerging this equipment been evaluated?

More urgent from a public safety viewpoint than the review of Indian Point 3 is the question of the status of Indian Point 2 and other operating plants. The most recent correspondence on this matter (Reference 35) of which I am aware seems to indicate that nothing will be done to alter plant design or operating procedures prior to "the first refueling outage (which) is currently scheduled to commence April 1, 1976". I consider

this to be a totally irresponsible course of action. The NRC should not allow continued operation of a plant when there is good cause to believe that an unresolved safety question exists and that the plant is not in compliance with the regulations. In fact, the regulations would appear to require a completely different course of action (see 10 CFR 50.100). Legal interpretation of the regulations notwithstanding, the proper course for a purely regulatory agency to follow is to permit operation only when there are sound technical bases to demonstrate safety of operation rather than to permit operation until the licensee or public can provide the sound technical bases for requiring immediate shutdown of the plant.

III. PUMP FLYWHEEL MISSILES GENERATED BY REACTOR COOLANT PUMP OVERSPEED

References 37 through 50 are some of the documents which discuss this unresolved safety problem

As a result of a reactor coolant system pipe rupture and the blowdown of reactor coolant through the reactor coolant pump, "the pump impeller may act as a hydraulic turbine causing the pump, motor, and the flywheel to overspeed and become potential sources of missiles". (Reference 38) This is a significant problem because of the tremendous inertial energy of the missiles, especially flywheel parts, and the difficulty of predicting the course of these missiles. Whether containment integrity can be

IV. SEPARATION OF ELECTRICAL EQUIPMENT

Much emphasis is placed on the single failure criterion in attempting to assure the public that nuclear plants are safe. Much less emphasis is given to the underlying assumptions which must be satisfied in order that the single failure criterion be a valid criterion. One of these basic assumptions is that failures will occur only in a random manner. Stated another way, the assumption is that failure (or operation) of one system or component will not affect the performance of its redundant counterpart.

One of the basic methods used to try to satisfy this assumption is to physically separate redundant equipment. The separation must be sufficient both to assure that failure of one safety system does not cause failure of the other and to assure that failures in non-safety systems do not cause failure of either safety system. A more detailed explanation of this philosophy can be found in IEEE Std 379 and the NRC standard review plan Chapter 7.

Based on my knowledge of the Indian Point 2 and 3 designs and the current separation criteria, I conclude that the physical separation provisions at Indian Point 2 and 3 are not adequate for the health and safety of the public. There is no adequate basis for concluding that a common mode failure will not result in a very serious accident other than sheer good luck. In fact,

based on the documents in the NRC files, this conclusion appears to be almost identical to the conclusions other knowledgeable staff members reached as early as 1969.

An ACRS Subcommittee meeting was held in April, 1970 and the staff made a rather detailed presentation of the poorer design aspects related to the Indian Point 2 protection and electrical systems. This included discussion of the single cable tunnel, the engineered safety feature manual actuation panel in the control room without separation in the panel, the common diesel location in a sheet metal structure, cable separation, and cable penetrations at the containment. "The Subcommittee was 'appalled' at the situation. They asked if we did not have an Oyster Creek situation in hand and whether we should not have the applicant make an independent review of his work as we required of Jersey Central." (Reference 18)

By the time the Electrical Systems Branch provided its input (Reference 22) for use in preparing a report to ACRS the electrical items which did not meet present day criteria earlier in the review, had either been "accepted", "resolved", or "approved with some reluctance", or they remained "unresolved".

The two reports to the ACRS prepared by the staff and classified as "Official Use Only" (References 26 and 28) should be reviewed by NRC to determine whether the previous bases for reluctantly accepting design deficiencies are adequate for protecting

the health and safety of the public. Based on those reports, it appears that many items were accepted solely because so many other areas of the plant were deficient that it wouldn't do much good to require upgrading only a few. In other cases, it appears that a judgment was made that the cost in time and money needed to provide substantial additional protection for the public health and safety was too great. The bases for this staff conclusion should be made public.

In the case of the separation between Unit 2 diesels, the apparent resolution is inconsistent in itself. The applicant claimed that there was no history of diesel explosions that damaged the diesel's environs. Nevertheless, a concrete wall was installed to protect the common control panel but no similar protection was installed between the diesels.

In summary, I consider the physical separation, or more accurately the lack of adequate physical separation, to be one of the significant safety hazards at Indian Point 2 and 3 which should be reconsidered. The single electric cable tunnel,*/ the cable spreading room, the containment electrical penetration area, the main control board, the safety injection pump and containment spray pump areas, and the auxiliary feedwater pump areas are among the vital areas that should be re-evaluated.

---

*/ The fact that Unit 3 has two cable tunnels is not significant because the system logic requires that two out of three systems be operable following an accident. In addition, the probiem of associated circuits was apparently not considered at all.