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

50-302

MAY 2 8 1980

MEMORANDUM FOR: Chairman Ahearne

(Signed) William J. Dircks

THRU: William J. Dircks, Acting Executive Director for Operations, EDO

FROM: Harold R. Denton, Director, Office of Nuclear Reactor Regulation

SUBJECT: STAFF COMMENTS ON THE OPE EVALUATION OF THE IMPACT OF POST-TMI-2 NRC REQUIREMENTS ON B&W REACTORS AND THE CRYSTAL RIVER TRANSIENT

The Office of Policy Evaluation (OPE) reported to the Nuclear Regulatory Commission on the impact of Post TMI-2 NRC requirements on Babcock and Wilcox (B&W) reactors on the Crystal River transient (Reference 1). Your memorandum of April 29, 1980 asked for the staff reaction to the OPE report.

The OPE report addresses changes to operator training, procedures, instrumentation, and hardware which were made as a result of the March 28, 1979 TMI-2 accident. The general conclusion was that the changes in the area of operator training and improved procedures were "of material assistance in managing the reactor during the Crystal River transient and bringing it to a safe shutdown condition." In the area of hardware and instrumentation, the report stated that:

> Many of the NRC requirements for added instrumentation and hardware changes did not contribute significantly to the manageability of the Crystal River transient because either the new instrumentation which would have been important in a more severe accident was not called upon due to successful operator actions at the outset or equipment which could have been useful had not yet been installed.

The staff agrees with these overall conclusions.

The report did identify five areas where improvements could be made. These areas are: better coordination of NRC requirements, routine challenges to the reactor safety systems, implementation schedules, use of safety grade equipment and greater use of system engineering techniques. Each of these five items is discussed in the Enclosure.

In our review of the OPE letter, we noticed several factual errors. While these did not appear to affect either the main points of the OPE letter or our response, they are noted here for the record.

1. The most recent sequence of events from the Crystal River Unit 3 licensee indicates that HPI flow was throttled prior to restoration of instrument power, contrary to page 3 and Table 1 of the OPE report.

2. PORV position indicators are acoustic monitors, not ultrasonic as stated on page 6 of the OPE report.

3. NUREG-0667 does not recommend "dividing the power supply buses into smaller power blocks" as stated on page 7 of the OPE report.

Original Signed by
H. R. Denton

Harold R. Denton, Director
Office of Nuclear Reactor Regulation

Enclosure:
As Stated

ccs w/enclosure:
Commissioner Gilinsky
Commissioner Kennedy
Commissioner Bradford
Commissioner Hendrie
OGC
OPE
SECY

ENCLOSURE

OPE Suggested Improvement

A project-type organization should be considered for coordinating and issuing NRC requirements. This would be an individual or organization who would be completely familiar with the status of a reactor. If the project manager were also organizationally or functionally connected with regional office staff, then there would be greater likelihood that the NRC would speak with one voice to each licensee.

NRC Staff Comments

The recent reorganization of the Office of Nuclear Reactor Regulation is intended to accomplish many of the objectives of the OPE recommendation, through strengthening the role of the project manager. All project management functions both for reactors having an operating license and for reactors under licensing review have been assigned to the newly formed Division of Licensing. A project manager at headquarters is assigned to each operating nuclear reactor. It is NRR's goal to have each project manager responsible for only one plant or station. The project manager is expected to know the status of every licensing issue with respect to each of his assigned reactors. In addition, the project manager is expected to be in frequent contact with the NRC inspector assigned to that reactor. An interoffice agreement has recently been established that will further strengthen this close contact. The NRC inspector will transmit information on the status of the reactor to NRC headquarters and the project manager will clarify NRC requirements for the NRC inspector at the site.

OPE Suggested Improvement

Routine challenges to reactor safety systems should be avoided. Challenges to reactor safety systems should be used as a last line of defense rather than for routine transient control.

NRC Staff Comments

We agree with the OPE comment that unnecessary challenges to safety systems should be avoided, but this statement needs qualification. That qualification can be stated generally as follows. While a single safety system should not be depended upon as the sole line of defense between a normal operational maneuver and core melt or other damaging events, challenges to safety systems do not necessarily decrease their reliability, and it is generally preferable under abnormal conditions to depend on a highly reliable system or component rather than one which has been shown to have a relatively low reliability. As an example of this, in NUREG-0667 the staff recognized the problem and recommended attempts to limit the operator's need to use high pressure injection pumps routinely after a reactor trip. NUREG-0667 recommended that steps be taken so that following reactor trip, the pressurizer level remains on scale and system pressure remains above the HPI actuation setpoint. Meeting these two objectives is to be independent of all manual actions. However, in the situation of an abnormally high pressurizer pressure, it is our opinion that a challenge to the reactor trip system is preferable to reliance on the relatively unreliable PORV. In every case of feedwater malfunctions or integrated control system (ICS) failure, which has occurred in a B&W reactor, the reactor trip system and the emergency safety features responded correctly, while the record of the PORV is not as commendable.

NUREG-0667 recommended reversing the setpoints for reactor trip and PORV actuation. However, the change is to be made only after other changes (such as automatic closure of the PORV block valve) are studied further and resolved so as to assure higher reliability of the PORV.

OPE Suggested Improvement

More realistic implementation schedules should be established for new requirements. The Commission should instruct the staff to set implementation schedules which allow licensees as well as the NRC staff sufficient time for in-depth engineering evaluation and design, procurement of high quality equipment and its proper installation.

NRC Staff Comments

As part of the new NRR reorganization, the Safety Program Evaluation Branch has been formed. Part of the charter of this branch is to work out realistic schedules for new NRC requirements. By working with industry groups, owners groups and individual utilities, schedules that are compatible with both the requirements of the NRC and the capabilities of the nuclear power plant owners should result. To a large extent this depends on the willingness of the industry to provide realistic estimates of cost, manpower and time. It also depends on the urgency of the requirement. There can be little doubt that considerable urgency was justified in implementing short-term lessons learned from TMI. In this connection the May 1980 version of the TMI Action Plan contains an implementation policy for future TMI-related requirements that is consistent with this OPE recommendation.

It would be a mistake to blame the Crystal River event on the fact that the utility was not given sufficient time to install the saturation meter. The failed part was of poor quality, and the quality assurance of either the part or its installation was not what should be expected of equipment for any system in a nuclear power plant, whether it be control grade or safety grade. In addition, as discussed below, other causes of failure of a non-nuclear instrumentation (NNI) power supply, unrelated to the saturation meter, could have caused a similar problem at Crystal River.

OPE Suggested Improvement

Staff and industry should conduct further studies on the use of safety-grade versus non-safety-grade equipment. The initiating event at Crystal River may have been avoided if a proper Failure Modes and Effects Analysis had been performed on the installation of the saturation meter and its associated power supply.

NRC Staff Comments

The discussion of the use of safety grade equipment for various functions is an ongoing matter. One must be careful that safety grade equipment is really required and also that the safety grade "label" is kept in the proper perspective.

As discussed below, the use of safety grade equipment adds an extra burden to the licensee, economic and otherwise. Also, making a component or system safety grade does not guarantee 100% reliability.

A safety grade component has been defined by the staff (Reference 2) as one which is designed to seismic Category I (Regulatory Guide 1.29), Quality Group C or better (Regulatory Guide 1.26) and is operated by electrical instruments and controls that meet IEEE 279. In practice, the requirement is even more stringent for safety grade instrumentation and controls. The designation Class 1E is the usual designation. Class 1E implies that other standards in addition to IEEE 279 (such as environmental qualifications) are met. These requirements are quite stringent. They can significantly increase cost and procurement difficulties which can, in certain instances, lead to industry reluctance to designate a piece of equipment as safety grade.

In the context of the Crystal River Unit 3 incident several points should be made related to safety grade equipment. The licensee (FPC) was not told that the saturation meter (which was to be installed quickly) had to be control grade as was implied in the OPE letter. The instructions to the licensee (Reference 4) were that the saturation meter should be provided with temperature and pressure input from safety grade equipment and that Crystal River Unit 3 should have

> (A) "safety grade calculational devices and display (minimum of two meters) or (B) a highly reliable single channel environmentally qualified, and testable system plus a backup procedure for use of steam tables.

Further instructions stated that:

> "In the long term, the instrumentation qualifications must be required to be upgraded to meet the requirements of Regulatory Guide 1.97 (Instrumentation for Light Water Cooled Nuclear Plants to Assess Plant Conditions During and Following an Accident) which is under development."

Thus, the licensee was told that he could initially install a system that was not strictly safety grade (though it must be of high reliability) and that at a later time, when requirements have been finalized, he would then be required to upgrade the system to Regulatory Guide 1.97. That Regulatory Guide (which has not yet been released) may require a safety grade saturation meter.

The statement that if the saturation meter had been designed as safety grade, the Crystal River transient might have been avoided is true. But it is definitely not certain that it would have been avoided. Better quality components should have been used if the system was intended to be safety grade. This might have eliminated the problem. A Failure Modes and Effects Analysis (FMEA) might have been performed. This FMEA might have discovered the absence of a fuse. The fuse might (or might not) have been put at the proper location to prevent propagation of the fault. Thus, while, the use of safety grade equipment would have increased the probability that the incident would not have occurred, it is not certain that the use of safety grade equipment would have prevented the problem.

It should also be pointed out that at least part of the problem, probably the biggest part, was the faulty installation of the buffer amplifier card rack. Designating the system as safety grade would not, of itself, have assured correct installation. The conclusion on page 10 of the OPE letter states that an FMEA should have been performed on the installation of the saturation meter and its associated power supply. The purpose of a FEMA is not to identify installation problems; such analyses are aimed at design and performance. Also, while we agree that good design would have used analyses such as FMEA, such analyses would not have greatly improved the situation at Crystal River.

One of the Lessons Learned requirements for the saturation meter was that it not adversely affect the reactor protection or engineered safety features systems. At Crystal River Unit 3 no adverse effect occurred. The fault did not propagate to the safety systems. All safety systems responded as they should have.

Too much emphasis should not be placed on the subcooling meter. If the subcooling meter had not been present, a similar reactor transient might have been caused by some other fault which could have affected the ICS and caused erratic, undesirable system behavior. For example, at Rancho Seco a severe transient occurred when a light bulb was dropped into an NNI panel causing a short circuit.

Thus, the real emphasis should be placed on preventing the ICS from causing an undesirable plant response. The recommendations of NUREG-0667 are intended to accomplish this.

OPE Suggested Improvement

NRC needs to make greater use of systems engineering techniques, probabilistic analyses, event trees/fault tree methodology, and less use of deterministic methods. Also NRC requirements should be functional rather than prescriptive.

NRC Staff Comments

We agree that more extensive use should be made of probabilistic analyses and event tree/fault tree methodologies in the determination and evaluation of licensing requirements. NRR, specifically the Division of Safety Technology, will participate in the use of probabilistic analyses and event tree/fault tree methodologies to assess nuclear plant reliability and risk. To this end, NUREG-0660, "NRC Action Plans Developed as a Result of the TMI-2 Accident," includes a Reliability Engineering and Risk Assessment task that culminates in the assessment of all commercial operating reactors within the United States. The initial phase of this task involves the development of standardized procedures to evaluate all plants using probabilistic techniques. This will be done within the Interim Reliability Evaluation Program (IREP) by the NRC.

The first step in the IREP is the nearly completed evaluation of Crystal River, Unit 3, undertaken by RES. The second step is refinement of the procedures through the simultaneous evaluations of six operating nuclear plants.

These evaluations will begin the summer of 1980 and will involve both NRR and RES. It is intended that the nuclear industry will participate actively in the next phase of the national assessment and will perform the nuclear plant risk and reliability assessments utilizing the procedures developed within NRC. Efforts are underway to define and assure this industry participation.

Despite this increased emphasis on reliability and risk assessment, we do not agree that decreased use should be made of deterministic methods. Results of reliability and risk assessments can be used to identify design weaknesses and system outliers which may exist due to inadequacies in existing regulations or licensing requirements. Sufficient evidence exists to conclude that, while present licensing analysis methods provide a relatively high degree of assurance of reactor safety, nevertheless, some deficiencies do exist. Reliability and risk assessments provide a tool to identify these deficiencies and to improve the existing process. However, there is no evidence that probabilistic analyses and event tree/fault tree methodologies are sufficiently all encompassing that such assessments can be used realistically to relax any existing criteria and practices, based on defense-in-depth concepts, and judgments based on proven engineering practice.

Consider as an example the feed-and-bleed cooling option. Such a mode of operation may be found to be fully reliable from a functional viewpoint and may be within acceptable risk limits. However, if consideration is given to the operational problems involved with collecting and processing the large volume of reactor coolant which will spill in the containment, a determination may be made that the feed-and-bleed option is not acceptable and that newly designed facilities should incorporate other cooling options.

The results of reliability and risk assessment will form only one of many bases which will be used to judge design adequacy. These assessments will be based on systems engineering concepts and generally will be functional in nature. Where these assessment show that existing deterministic requirements are wrong, they will, of course, be changed.

As to the issue of functional versus prescriptive requirements, to the extent possible, the staff tries to define criteria rather than propose specific designs or procedures. When a license applicant and the NRC staff have different but equally valid ways of solving a problem, the NRC staff has traditionally allowed the applicant to implement its approach. However, the burden of proof is on the applicant to show that its approach is an equally valid method of meeting the staff criteria. In the example given in the OPE report (venting noncondensible gases from the RCS) B&W has not presented adequate support for their contention that a vent on the reactor head is not required.

REFERENCES

1. Memorandum for NRC Commissioners from Edward J. Hanrahan, Office of Policy Evaluation, USNRC, April 24, 1980.

2. Safety Discussion of 15 Technical Issues Listed in Attachment to November 3, 1976 Memo from Director, NRR to NRR Staff.

3. Buhl, A. et al, "Analysis and Evaluation of Crystal River Unit 3 Incident," NSAC-3, INPO-1, March 1980

4. Letter to J. A. Hancock, Florida Power Corporation from D. Eisenhut, USNRC, September 13, 1979.