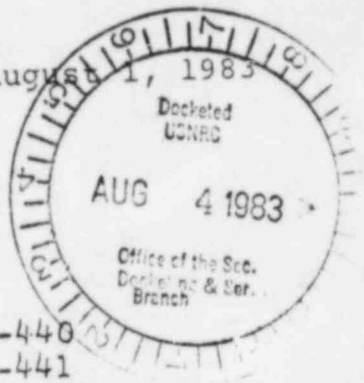
August 1, 1983

UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION

Before the Atomic Safety and Licensing Board



In the Matter of	
CLEVELAND ELECTRIC ILLUMINATING COMPANY, Et Al.	Docket Nos. 50-440 50-441
(Perry Nuclear Power Plant, Units 1 and 2)	(Operating License)

OCRE BRIEF IN SUPPORT OF THE LICENSING BOARD'S INTENT TO DECLARE A SUA SPONTE ISSUE

During the May 9, 1983 conference call the Licensing Board posed two questions to Staff and Applicants for the purpose of obtaining information which would help it "decide whether or not to declare a sua sponte issue." Tr. 809. The questions were:

(1) To what extent does the simulator training for operators of the Perry reactors include training in differentiating different kinds of instrument failures from transient or accident conditions;

(2) To the extent that some kinds of instrument failures are not simulated during training, please explain whether the omission is detrimental to the safe operations of the reactor.

NRC Staff responded to these questions on June 13 by filing the affidavit of David H. Shum. Applicants responded on July 15 by filing the affidavit of Anthony F. Silakoski. Because intervenor Ohio Citizens for Responsible Energy ("OCRE") finds these affidavits to be so vague, conclusory and lacking in factual detail as to be totally deficient, and because OCRE possesses information concerning this issue, OCRE is filing this brief supporting the Licensing Board's intent to declare a sua sponte issue. OCRE believes that the matters raised constitute a serious

D503

safety issue which should be addressed in this proceeding before PNPP can be allowed to operate.

I. Staff's Affidavit

On June 13, 1983 the Staff filed its response to the two questions posed by the Licensing Board in the form of the affidavit of David H. Shum.

The response to the first question is so vague as to be practically worthless. The Staff has essentially deferred the question to Applicants, in that the Staff assumes that simulator training will include differentiation of instrument failures from transient or accident conditions, that the plant operating procedures to be developed by Applicants should provide sufficient guidance to operators, and that other instrumentation will be available in the event of instrument failure.

The Staff's response to the second question is similarly vague. The Staff states that the omission of "some kinds of instrument failure" in simulator training will not be detrimental, but does not identify the failures so classified. The Staff then states that the worst case loss of instrumentation will be simulated during training (emphasis added). The Staff again defers to the emergency operating procedures (discussed below) as providing guidance with respect to this type of failure.

OCRE finds the term "loss of instrumentation" to be crucial. If loss means "not available", as if power is lost to an instrument channel, then it is likely that this failure would be detected as such. Much more ominous is an instrument failure which produces the display of erroneous but plausible data which might be

indicative of a transient or accident condition. Such a failure puts the operator in the position of having to decide which instrument is correct. Reliance on other indicators may or may not be helpful, depending on the degree of independence (likelihood of common-mode failures) of the monitors and the adequacy of training and diagnostic ability of the operator. Since OCRE believes that this is the whole point of the Board's inquiry, the Staff's response has provided no enlightenment on the matter.

II. Applicants' Affidavit

Applicants' response to the two questions posed by the Board, in the form of the affidavit of Anthony F. Silakoski, was filed July 15, 1983. This response did provide somewhat greater specificity as to types of instrument failures simulated.

The affidavit lists three types of instrument failures which are simulated: failure of electrical bus powering an instrument channel, failure of the process computer, and simulated break in the drywell which causes erroneous pressure readings in the control rod drive hydraulic control system. It is not clear whether any of these failures represents the "worst case loss of instrumentation" which the Staff claims will be simulated during operator training. Nor is it clear that these are the only types of instrument failures simulated. It is further unclear whether combinations of such instrument failures or of instrument failures with transient or accident conditions are ever simulated.

Of the three types of instrument failures specified, the first two appear to be of a type that is easily diagnosed. The extensive failure of electrical power (e.g., the failure of an entire electrical

division) would result in the failure of all instruments, monitoring a number of different variables, which are powered by that system. The loss of a large number of instrument would logically alert the operator to the likely cause, loss of electrical power.[1/] Less extensive electrical failures might also be readily detected, depending on its effect on the display; e.g., loss of power would cause indicator lamps and readouts to fail to light, or cause meters or recorders to display an obviously erroneous value.

The second type of failure, that of the process computer, would similarly be easily detected due to the large number of variables monitored and displayed by the computer. Observation of other displays would lead the operator to discover the computer failure.

That Applicants mention the third type of failure is interesting for two reasons. First, the significance of this parameter is not apparent. Scram system status would be more appropriately monitored by other variables, such as reactor power and control rod position.[2/] Secondly, Applicants failed to mention a most crucial variable which is affected by the condition postulated: reactor

---

1/ Applicants claim that station blackout is part of simulator training, but do not explain how an operator is to control the plant with the extensive loss of instrumentation inherent in that situation. The BWR emergency procedure guidelines do not address loss of electrical power or station blackout.

2/ CRD hydraulic system pressure is not a RPS setpoint (FSAR § 7.2.1.1). Grand Gulf (a BWR/6 like Perry) does have a limiting condition for operation that all scram accumulators be operable, and an associated surveillance requirement that the pressure of each control rod scram accumulator be verified at least once every 7 days (Grand Gulf Technical Specifications, NUREG-0926, pp. 3/4 1-8-9). An alternate source of hydraulic

(continued next page)

vessel water level. The heat from a small break LOCA in the drywell could cause erroneously high vessel level readings, at a time when monitoring of that indication is vital. (More about vessel level indication below.)

Applicants respond to the Board's second question by stating that operators are trained to compare multiple indications of plant variables and "to respond to the worst case parameter" when instrument failures create ambiguity. This is supposedly reinforced by the emergency instructions (which are discussed below). This statement, as well as the emergency instructions, gives little indication of how operators are trained to react when instrument failures create ambiguous readings that diverge toward opposite extremes, each of which is undesirable. Operator confusion may be compounded if false signals actuate or otherwise affect plant equipment, the operation of which may lend credibility to the false reading. (A specific example of this situation is described below.)

III. Adequacy of Emergency Procedure Guidelines

Since both Applicants and Staff appear to be relying extensively on the plant energency procedure guidelines as a panacea to the problem of possible operator confusion due to instrument failures, it is appropriate to examine these guidelines. The Perry-specific instructions will be prepared from the generic emergency procedure guidelines described in the General Electric Topical Report

---

2/ continued. pressure necessary for control rod insertion is provided by the control rod drive pumps. Each CRD also has an internal ballcheck valve that will allow reactor pressure (if greater than 600 psi) to insert the control rod.

NEDO-24934, "Emergency Procedure Guidelines, BWR 1-6."[3/] These generic procedures consist of two guidelines (one for RPV level control and one for containment control) and seven contigencies (level restoration, rapid RPV depressurization, core cooling without injection, core cooling without level restoration, alternate shutdown cooling, RPV flooding, and level/power control). Two additional guidelines, on combustible gas control and secondary containment control, are to be added in the future. These procedures are said to be superior to previous BWR emergency instructions in that they are symptom-based rather than event-based. The Staff in its safety evaluation of NEDO-24934 stated that "the use of symptoms rather than events as bases for actions, eliminates errors resulting from incorrect diagnosis of events, and addresses multiple failures and operator errors." (Generic Letter 83-05, dated February 8, 1983).

However, symptoms are indicated to the operator by instrumentation. The inability to diagnose instrument failures when using symptom-based procedures may prove as damaging to plant safety as the inability to diagnose events when using event-based procedures, especially since the new procedures may never be entered if the operator incorrectly interprets the instrument readings.

NEDO-24934 does provide some guidance to operators regarding instrument readings in the following general precautions:

3/ See letter dated November 16, 1982 from D. Davidson of CEI to A. Schwencer, NRC, re response to request for additional information on SER Outstanding Issue 21.

CAUTION #1

Monitor the general state of the plant. If an entry condition for either [prodedure developed from the level control guideline] or [procedure developed from the containment control guideline] occurs, enter that procedure. When it is determined that an emergency no longer exists, enter [normal operating procedure].

CAUTION #2

Monitor RPV water level and pressure and primary containment temperatures and pressures from multiple indications.

CAUTION #3

If a safety function initiates automatically, assume a true initiating event has occurred unless otherwise confirmed by at least two independent indications.

CAUTION #6

Whenever [temperature near the instrument reference leg vertical runs] exceeds the temperature in the table, the actual RPV water level may be anywhere below the elevation of the lower instrument tap when the instrument reads below the indicated level in the table.

Temperature*	Indicated Level	Instrument
any	537 in.	Shutdown Range Level (500 to 900 i
105°F	-109 in.	Wide Range Level (-150 to +60 in
310°F	19 in.	Narrow Range Level (0 to +60 in.)
379°F	239 in.	Fuel Zone Level (200 to 500 in.)

* [List in order of increasing temperature.]

CAUTION #7

[Heated reference leg instrument] indicated levels are not reliable during rapid RPV depressurization below 500 psig. For these conditions, utilize [cold reference leg instruments] to monitor RPV water level.

The guidelines further caution the operator that:

If [temperature near the cold reference leg instrument vertical runs] reaches the RPV saturation limit, enter [procedures developed from CONTINGENCY #2]. (Contigency #2 is Rapid RPV Depressurization. A plot of RPV saturation limit vs. RPV pressure is provided in step CC-2.2.2). [Note: PNPP uses only cold reference leg level instrumentation. See January 14, 1983 letter from M. Edelman of CEI to B. Youngblood, NRC, re BWROG inadequate core cooling instrumentation requirements.]

Also, if the RPV water level cannot be determined, the

operator is instructed to enter CONTINGENCY #6, RPV Flooding.

While these steps are an improvement in operator awareness of the problems existing with RPV level instrumentation, they do not totally solve the problem. The operator must rely on instrument readings before even entering the emergency procedures. The procedures can also be exited at any time, depending again on the operator's interpretation of instrument readings. The danger of an operator relying on false instruments is amply indicated by the following passages:

> The EPG provides "cautions" and instructions to the operator which are intended to allow the operator to cope with the vessel level inaccuracies or erratic indications produced by the above mentioned conditions. These instructions do not permit accurate determination of vessel level but only state that under certain conditions actual vessel level could be below the lower instrument tap when indicated vessel level is on scale. This leaves the operator without an accurate indication of vessel level under emergency conditions when he is following a procedure whose primary objective is restoration and/or maintenance of acceptable vessel level. (Report by S. Levy, Inc., SLI-8118, October 1981, p. C-4.)

> (I)f the operator fails to recognize that he has lost level indication and has a false high reading of water level, he might take action to throttle or stop ECCS systems in order to avoid filling steam lines or to reduce load on emergency power systems. In this case, the flashing or boiling in the reference legs could lead to operator actions prejudicial to plant safety . . . . We believe that operator recognition of loss of accurate level information as addressed in the emergency procedure guidelines is cumbersome at best. The operator is to relate indicated water level and drywell temperature using a table contained in a caution statement of the emergency procedures. Indicated water level values beyond the ranges shown in the table are to be mistrusted. Automation of these actions and decisions seems in order. (Memo for Roger J. Mattson from Themis P. Speis dated January 15, 1982, re Errors in BWR Vessel Water Level Indication, pp. 11 and 13.)

RPV water level is a crucial variable, with a sensing system vulnerable to recognized problems.[4/] Other plant variables are also

---

4/ For further discussion on the problems with BWR level instrumentation, see "Safety Concern Associated with Reactor

(CONTINUED NEXT PAGE)

depended upon for entry into and monitoring throughout the EPGs. These include: RPV pressure, drywell pressure, suppression pool temperature, drywell temperature, containment temperature, suppression pool level, APRM level (neutron flux), and control rod position. According to FSAR Table 7.5.1, some of these

---

4/ CONTINUED. Vessel Level Instrumentation in Boiling Water Water Reactors" by the NRC's Office for Analysis and Evaluation of Operational Data, January 1982. This report discusses possible false high level indications due to leaks in the reference leg (a number of such events have occurred; see Appendix A of the AEOD Report) which can affect control (feedwater flow) and safety systems (high-pressure ECCS) that actuate on various level signals. BWR vessel water level is measured by sensing the differential pressure across two instrument lines. One line, the reference leg, is connected to a condensing chamber connected to the reactor steam space and maintains a constant level. The other line, the variable leg, is a tap connected lower on the RPV. Typically several such taps for different level ranges share a common reference leg. Decreased level in the reference leg, due to leaks or boil-off results in false high RPV level signals. False high level indication would reduce feedwater flow into the RPV. Vessel water level would rapidly decrease; when the level reaches the low level setpoint, the operator will be confronted with both high and low level alarms.

This problem could affect safety systems as well. Aside from the obvious operator errors likely in this situation, the AEOD report indicates that GDC 24 and IEEE-279 may be violated, such that a false high level indication, coupled with a second random failure, may prevent automatic or timely actuation of safety functions, such as scram, containment isolation, and HPCS and RCIC.

Applicants (January 14, 1983 letter to B. Youngblood) claim that such a scenario (reference leg break in one division and second random failure in another) would not cause "consequences . . . of immediate concern." This conclusion of course assumes correct operator actions. Applicants also have committed to making design modifications to vessel instrument lines which purportedly reduce the effect of reference leg boil-off and flashing due to high drywell temperature. This case probably represents a worst-case "common-mode failure" of level instrumentation, since all level indicators, and signals to safety and control systems, would be falsely high. Even assuming that these mechanical fixes have eliminated this problem, operator action in the event of a reference leg break which presents conflicting information to the operator is still at issue.

variables have only two channels of safety-related display instrumentation available in the control room (notably RPV pressure, RPV vessel level, and containment pressure). This configuration leaves the operator with the task of having to decide which of two instruments is indicating correctly. Some indications, e.g., ECCS, diesel generators, emergency service water system, and combustible gas control, have no redundant instrumentation for each component or subsystem; the rationale for this is that the systems as a whole have redundancy (e.g., 2 ESWS loops, 2 diesel generators). This situation could lead an operator to declare an entire ECCS subsystem, electrical division, or ESWS loop inoperable on the basis of a faulty display, or conversely, to disable a system by operating it beyond its limits because a hazardous or faulty condition was not correctly displayed.

There may be non-safety instrumentation monitoring some of these variables, but it is questionable whether these should be relied upon during accident conditions since non-safety equipment is not environmentally qualified.

The process computer likewise may not aid the operator in the diagnosis of instrument failures. FSAR § 7.7.1.8 indicates that the process computer accepts analog signals from plant instrumentation. It appears that an instrument failure that results in an erroneous but plausible indication will merely be confirmed by the process computer as a credible reading, thereby adding to operator confusion.

IV. Human Tendencies

Even the best emergency instructions are rendered useless if they are not followed by control room operators. Swain and Guttman, in their comprehensive Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (NUREG/CR-1278, October 1980) point out that precedures are not always followed:

> A common error in human reliability analysis is to assume that available written procedures will be used and used properly. Even in work with severe penalties for nonuse or incorrect use of written procedures, nonuse and misuse have been observed. In the absense of such penalties, it is reasonable to assume a greater frequency of such practices. At every plant Brune and Weinstein visited [NUREG/CR-1368, "Development of a Checklist for Evaluating Maintenance, Test, and Calibration Procedures" (1980)], at least one manager or supervisor expressed concern that personnel might not use of follow written procedures as intended. The nonuse or misuse of written procedures is obviously related to the quality of administrative control in a plant . . . these problems are also related to the quality of the written materials themselves. (p. 14-13) 5/

Swain and Guttman offer other insights on human reliability in the area of diagnosis of instrument failures. Instrument failures, especially those in which a meter or recorder fails with the pointer reading in the normal operating band of the scale, are recognized as a contibutor to human error (p. 11-4). Pens of chart recorders are more likely to stick than pointers of panel meters (p. 11-7).

Human tendencies may override the instructions in the EPGs to monitor multiple indications of a variable. Operators have

---

5/ One would suspect that procedures which involve actions contrary to normal operator response might be less likely to be followed. The BWR emergency procedure guidelines

CONTINUED NEXT PAGE

a tendency to fixate on an anomalous display:

> In responding to a display, an operator may focus his attention on a particular display to the exclusion of all others. Often, the operator will initiate the indicated action and concentrate his attention on that display, waiting for a change in the readout. This "funneling" of attention is more likely to occur when the operator is under stress.
>
> An occasional display malfunction is "sticking": i.e., a pointer on a panel meter or a pen on a chart recorder jams for some reason and no longer yields useful information. Usually there are several redundant displays for any significant parameter, and the operator can refer to one of them for the required reading until the primary display is repaired. However, there is a strong tendency to focus on just one display without cross checking. Because of the operator's involvement in the corrective action to be taken, this is most likely to occur when the display sticks in a position indicating the need for immediate corrective action. It is less likely to occur when the sticking display does not indicate a need for immediate action because the operator will be scanning the associated displays as well. When an operator uses an instrument that has jammed without any indication to that effect, we estimate aprobability of .1 that the operator will fail to cross-check until some other indication, such as an alarm, alerts him that something is amiss. (p. 11-11)

and:

> There are several LERs of operators relying on a chart recorder indication and performing inappropriate actions because of a stuck pen. In some incidents, operators apparently relied exclusively on one display when other displays would have indicated the appropriate action required. (p. 3-26)

Still other human tendencies may lead to misdiagnosis of instrument failures. E.g., an operator's first reaction to indications of an event considered unlikely to occur (such as a design-basis LOCA) would be one of sheer disbelief, or the incredulity response. An example of this response (in a different industry) is provided:

5/ CONTINUED. contain several such actions: lowering water level to top of the active fuel to reduce power in Contingency #7, Level/Power Control; letting fuel clad temperature increase to 2000°F and then opening the safety/relief valves for steam cooling (more effective at higher clad temperatures)in Contingency #3; and terminating injection into the RPV, regardless of whether core cooling is adequate, to preserve containment integrity. Generic Letter 83-05, pp. 19, 22, 30, 39.

(I)n one refinery the first indication the control room operator had of a serious fire was that many alarms occurred and many instruments behaved abnormally. This operator's first response was to run upstairs and demand of an instrument technician, "What's wrong with my instruments?" By the time he returned to the control room, it was too late to take action that might have reduced the loss due to the fire. (p. 3-58)

The incredulity response may be reinforced by the perception that many actuations of safety-related alarms in nuclear power plants are false (p. 10-17). There also may be a bias in the operator's reaction to true alarms and instrument failures. Swain and Guttman note:

Operating personnel have two primary responsibilities: keeping the plant on-line and ensuring its safe operation. Because serious safety problems rarely occur at a plant, most of the operator's attention is directed to the instruments and controls related to the first responsibility. Interviews with operators indicate that they do not expect serious safety problems. Furthermore, they have confidence in the ability of the plant's safety systems to cope with possible safety problems automatically. These attitudes, coupled with the usual lack of practice in dealing with the unexpected, may result in reluctance on the part of an operator to take action that would interfere with keeping the plant on-line. (p. 10-16)

This bias might lead an operator to view alarms and instruments indicating serious safety problems as false alarms, while interpreting false instrument readings that would threaten continued plant operation (such as a false high RPV water level indication of incipient steamline flooding) as true. Such bias would tend to decrease plant safety.

Swain and Guttman are pessimistic about nuclear power plant operators' capabilities for coping with serious accidents, largely due to the stress and confusion in such situations (p. 10-23). A contributor to this stress is difficulty in diagnosing the emergency (p. 17-10). The operator's ability to cope with emergencies is dependent on his skill level and degree of famil-

iarity with the unusual condition, and the "extent to which the displayed information directly supports the actions the operator should take to cope with the situation." (p. 17-9)

It would thus seem that simulator training in diagnosing instrument failures would be an extremely desirable and important requirement for operator training. Staff and Applicant affidavits do not clearly indicate the adequacy or extent of this type of training, nor are the BWR emergency procedure guidelines sufficient to preclude operater misdiagnosis of instrument readings. OCRE therefore would support the Board's declaration of a sua sponte issue on this matter.

V. Standards for Sua Sponte Issues

A Licensing Board has the power to raise sua sponte any significant environmental or safety issue in operating license hearings. Consolidated Edison of New York (Indian Point, Units 1, 2, and 3), ALAB-319, 3 NRC 188, 190 (1976); Consolidated Edison of New York (Indian Point, Unit 3), CLI-74-28, 8 AEC 7 (1974). 10 CFR 2.760a provides that in an OL proceeding "(m)atters not put into controversy by the parties will be examined and decided by the presiding officer only where he or she determines that a serious safety, environmental, or common defense and security matter exists."

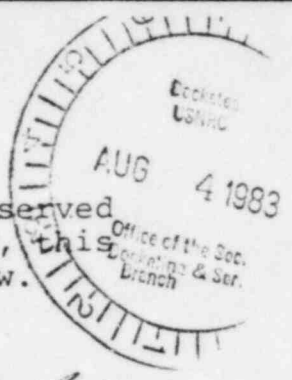
The TMI-2 accident vividly demonstrated that human error (much of which resulted from misdiagnosis of instrument readings) can rapidly exacerbate plant transients, leading to core damage and potentially devastating public health consequences. It should be noted that in "Precursors to Potential Severe Core Damage

Accidents: 1969-1979; A Status Report" (NUREG/CR-2497, June 1982) 36% of all the precursors, and 38% of the significant precursors, were found to involve human error (p. 5-18). Based on these facts and on the above analysis, OCRE would conclude that the training of operators in the diagnosis of instrument failures is indeed a serious safety matter.

It furthermore cannot be concluded that the Commission's initiatives in the human factors area since TMI will effectively reduce these problems. A General Accounting Office report, "Problems and Delays Overshadow NRC's Initial Success in Improving Reactor Operators' Capabilities" (GAO/RCED-83-4, December 15, 1982) indicates that, although the NRC has made progress in short-term actions to improve operators' abilities to cope with accidents, the NRC's efforts with respect to long-term actions have lost momentum and have been subject to delays. Simulator training has been designated as a long-term issue. See NUREG-0933, "Prioritization of Generic Safety Issues", wherein all the TMI Action Plan tasks relating to simulator training are considered covered by Item I.A.4.2, "Training Simulator Improvements - Long Term." Given the NRC's failure to effectively address long-term actions, the Commission cannot be relied upon to resolve this important problem. Plant-specific resolution therefore becomes imperative to assure that the safe operation of Perry will not be compromised by human errors resulting from inadequate training. OCRE thus urges the Board to declare a sua sponte issue regarding this matter.

Respectfully submitted,

Susan L. Hiatt



CERTIFICATE OF SERVICE

This is to certify that copies of the foregoing were served by deposit in the U.S. Mail, first class, postage prepaid, this 2nd day of August, 1983 to those on the service list below.

Susan L. Hiatt

Susan L. Hiatt
OCRE Representative
8275 Munson Rd.
Mentor, OH 44060
(216) 255-3158

SERVICE LIST

Peter B. Bloch, Chairman
Atomic Safety & Licensing Board
U.S. Nuclear Regulatory Comm.
Washington, D.C. 20555

Dr. Jerry R. Kline
Atomic Safety & Licensing Board
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Mr. Glenn O. Bright
Atomic Safety & Licensing Board
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

James M. Cutchin, IV, Esq.
Office of the Executive Legal Director
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Jay Silberg, Esq.
Shaw, Pittman, Potts, & Trowbridge
1800 M Street, NW
Washington, D.C. 20036

Docketing & Service Branch
Office of the Secretary
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Atomic Safety & Licensing Appeal Board Panel
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Terry Lodge, Esq.
McCormack, Pommeranz, & Lodge
824 National Bank Bldg.
Toledo, OH 43604