UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION

BEFORE THE ATOMIC SAFETY AND LICENSING BOARD

In the Matter of	)	
	)	
SACRAMENTO MUNICIPAL UTILITY DISTRICT	)	Docket No. 50-312 (SP)
	)	
	)	
(Rancho Seco Nuclear Generating Station)	)	
	)	

NRC STAFF TESTIMONY OF DALE F. THATCHER
RELATIVE TO THE INTEGRATED CONTROL SYSTEM

(Board Question 16)

Q 1. Please state your name and your position with the NRC.

A. My name is Dale F. Thatcher. I am an employee of the U. S. Nuclear Regulatory Commission. I was responsible for the review and evaluation of instrumentation and control systems for Babcock & Wilcox (B&W) operating reactors following the Three Mile Island Unit 2 (TMI-2) incident.

Q 2. Have you prepared a statement of professional qualifications?

A. Yes. A copy of my statement of professional qualifications is attached to the "NRC Staff Testimony of Dale F. Thatcher Relative to Direct Initiation Of Off-Normal Conditions In The Feedwater System" filed in this proceeding. There I also explain the nature of my responsibilities with respect to the Rancho Seco Nuclear Generating Station.

Q 3. What is the purpose of your testimony?

A. The purpose of my testimony is to respond to Board Question 16 which states:

Board Question 16

> SMUD, the licensee, has done insufficient analysis of the failure mode and effects analysis of the integrated control system, and therefore, Rancho Seco is unsafe and endangers the health and safety of Petitioners, constituents of Petitioners and the public.

Q 4. Describe the Rancho Seco Integrated Control System (ICS).

A. The ICS includes four subsystems. The four subsystems are the unit load demand control, the integrated master control, the steam generator control, and the reactor control. The system philosophy is that control of the plant is achieved through feed-forward control from the unit load demand control. The unit load demand control produces demands for parallel control of the turbine, reactor, and steam generator feedwater system through respective subsystems.

The integrated master control (IMC) is capable of automatic turbine valve control from minimum turbine load to full output. The steam generator control is capable of automatic or manual feedwater control from startup to full output. The reactor control is designed for automatic or manual operation above 15% output and for manual operation below 15%. The basis function of the ICS is matching megawatt generation to unit load demand. The ICS does this by coordinating the steam flow to the turbine with the rate of steam generation. To accomplish this efficiently, the following basic reactor/steam-generator requirements are satisfied:

1. The ratios of feedwater flow and Btu input to the steam generator are balanced as required to obtain the desired steam conditions.

2. Btu input and feedwater flow are controlled:

   a. To compensate for changes in fluid and energy inventory requirements at each load.

b. To compensate for temporary deviations in feedwater temperature resulting from load change, feedwater heating system upsets, or final steam pressure changes.

Q 5. What function is the Rancho Seco ICS intended to perform?

A. The ICS provides the proper coordination of the reactor, steam generator, feedwater control, and turbine under all operating conditions. Proper coordination consists of producing the best load response to the unit load demand while recognizing the capabilities and limitations of the reactor, steam generator, feedwater system, and turbine. When any single portion of the plant is at an operating limit or a control station is on manual, the ICS design uses the limit or manual station as a load reference.

The ICS maintains constant average reactor coolant (RC) temperature between 15 and 100% rated power and constant steam pressure at all loads. Optimum unit performance is maintained by limiting steam pressure variations; by limiting the imbalance between the steam generator, turbine, and the reactors; and by limiting the total unit load demand upon loss of capability of the steam generator feed system, the reactor, or the turbine generator. The ICS provides limiting actions to ensure proper relationships between the generated load, turbine valves, feedwater flow, and reactor power.

In performing its functions, the ICS interacts with, i.e., it receives inputs from and provides outputs to, a number of other related plant control systems. For example, in controlling the reactor there is interaction with control rod drive system, in controlling feedwater there is interaction with the feedwater pump control and the feedwater valve control, and in controlling the turbine there is interaction with the turbine electrohydraulic control (EHC) system and the main steam valves such as atmospheric dump valves and turbine bypass valves.

In some operating B&W plants including TMI-2 and Rancho Seco, the ICS also controls auxiliary (emergency) feedwater flow during loss of main feedwater or loss of all reactor coolant pumps via control valves responding to steam generator level signals.

Q 6. With specific reference to the TMI-2 incident, does the ICS pose a safety concern in the view of the NRC Staff with regard to its function to automatically regulate auxiliary feedwater flow?

A. At the time of the TMI-2 event, a specific safety concern was expressed with regard to the reliance on the ICS to regulate auxiliary feedwater flow for loss of main feedwater.

Q 7. What was the nature of that concern?

A. There was concern that the ICS could fail or malfunction in some manner to prevent the supply of emergency feedwater when required. Subsequent investigation suggests that the ICS at TMI-2 did perform its intended function.

Q 8. Have any steps been taken at the Rancho Seco facility to deal with the ICS concerns relative to auxiliary feedwater flow raised by the TMI-2 incident? If so, indicate what steps have been taken.

A. As a result of the Commission Order of May 7, 1979, the Rancho Seco plant was to develop and implement operating procedures for initiating and controlling auxiliary feedwater independent of ICS control. In the NRC Staff "Evaluation of Licensee's Compliance with the NRC Order dated May 7, 1979; "Docket No. 50-312, dated June 27, 1979, page 13, we concluded that the Rancho Seco plant could initiate and control auxiliary feedwater independent of ICS including starting the pumps and controlling the AFW bypass valves. Based on the measures taken at Rancho Seco to initiate and control auxiliary feedwater independent of the ICS, the Staff concluded that continued operation of Rancho Seco was acceptable.

Q 9. Will any future steps be taken at Rancho Seco facility relative to the ICS and its function to control auxiliary feedwater flow? If so, please identify what those actions will be and the time frame within which they will be completed.

A. Yes. In a letter dated October 18, 1979, J. J. Mattimoe to D. Eisenhut, the licensee committed to install a safety grade auxiliary feedwater control system independent of the ICS. The licensee has committed to implement these requirements during the 1981 refueling outage.

This would completely remove the initiation and control of the auxiliary feedwater system from ICS. In addition, the system would meet requirements equivalent to those outlined in response to Question 10 of "NRC Staff Testimony of Dale F. Thatcher Relative to Direct Initiation of Reactor Trip Upon The Occurrence of Off-Normal Conditions In The Feedwater System".

Q 10.. For each step identified in response to Question 9 above, indicate why the Rancho Seco facility may continue to operate in the interim prior to complete implementation of the action to be taken.

A. The implementation of the safety grade requirements will help ensure a highly reliable automatic initiation and control of auxiliary feedwater in the long term. However, in the interim, the procedures in place at Rancho Seco provide a fully independent method to initiate and control AFW should the ICS fail. See: "Evaluation of Licensee's Compliance with the NRC Order dated May 7, 1979," pp. 12-13 (June 27, 1979). This coupled with the improvements in overall reliability of the Rancho Seco auxiliary feedwater system (See: Testimony of Phil Matthews in Response to Board Question CEC 1-6) provides assurance that the Rancho Seco auxiliary feedwater system will perform its function as required.

Q 11. With specific reference to the TMI-2 incident, does the ICS pose a safety concern in addition to that related to auxiliary feedwater flow?

A. A general safety concern was expressed with regard to the complex role of the ICS in overall plant control, and whether or not it performs this function satisfactorily. In order to determine the potential contribution the ICS in plant upsets, the staff concluded that further investigation was needed.

Q 12. What further investigations are presently in progress?

A. The NRC Staff believed that a failure mode and effects analysis of the ICS would provide a more comprehensive understanding of this control system and provide necessary guidance for determining the need for further requirements with respect to the ICS. The licensee committed to submit a failure mode and effects analysis (FMEA) of the Integrated Control System to the NRC Staff as soon as practicable. The Commission Order of May 7, 1979 confirmed that this would be carried out in the long term.

A failure mode and effects analysis is a systematic procedure for identifying the modes of failure of a system and for evaluating their consequences. A FMEA is considered (as stated in IEEE 352-1975, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protective Systems") to be the first general step of a reliability analysis. It can potentially provide some early useful information and provide a basis for later studies and/or analyses.

Typically a FMEA has been utilized as a tool to help systematically evaluate plant safety systems (such as the reactor protection and engineered safety features actuation system) to determine if a single failure can prevent the system safety function. It is a requirement that for plant safety systems no single failure shall prevent the system safety function.

Plant control systems such as the integrated control system (ICS) have typically not been required to meet this single failure criterion. However, for any system, including a control system, a FMEA can be used to identify failure modes which could lead to undesirable consequences.

B&W has performed an FMEA on the integrated control system (ICS) as part of its reliability analysis of the ICS. The other part of the reliability analysis is a review of the ICS' "Operating Experience". The FMEA and Operating Experience are documented in B&W Report BAW 1564, "Integrated Control System Reliability Analysis".

Based on the overall reliability analysis, the report makes recommendations to be evaluated on a plant-specific basis. The recommendations highlight areas in which B&W believes improvements could potentially contribute to improved overall operation of the facility. The majority of the recommendations involved areas outside the ICS itself, and were not specific in nature because of the design differences which exist in these areas at the different plants.

Therefore, based on the recommendations, the NRC Staff requested (by letter dated November 7, 1979) that all B&W licensees evaluate the report's recommendations and include followup action plans. We are presently evaluating the responses. In addition, Oak Ridge National Laboratory (ORNL) has reviewed the B&W report for the NRC Staff and reported its results in a Report Review, "Integrated Control System Reliability Analysis," transmitted to the Staff on January 21, 1980. A copy of the ORNL report is attached to this testimony.

In addition, the NRC has one study underway entitled "Integrated Reliability Evaluation Program (IREP)." Although this program is still being developed, it does have as one of its objectives to identify the risk significance of the close-coupling of primary and secondary coolant systems and of the systems interactions originating in the Integrated Control System at B&W reactor plants. The results of this program may give some indication of the relative significance of the Integrated Control System in the overall risk from operation of B&W plants and, as a result, help determine the need for further study.

Q 13. What are the Staff conclusions in this area?

A. The Staff concluded that each plant needed to evaluate (as requested) its specific design with respect to the potential for improvement as summarized in the report by B&W.

From the ORNL Review, it appears that although the ICS and related control systems contain areas which can potentially be improved, the ICS itself has proven to have a low failure rate and it does not appear to precipitate a significant number of plant upsets. Specifically, the examination of the failure statistics revealed that only a small number of ICS malfunctions resulted in reactor trip (approximately 6 of 162). From this data, ORNL concludes that the system is failure tolerant to a significant degree.

In addition, ORNL has suggested areas for further study. We are in the process of reviewing the ORNL final report and will determine any further action to be required by the licensee.

Q 14. Based on the Staff's review, are any further steps contemplated for the Rancho Seco facility relative to the ICS?

A. The Staff's preliminary evaluation of the licensee's response (dated January 21, 1980, J. J. Mattimoe to R. Reid) to our November 7, 1979 request indicates that the licensee is implementing modifications or is in the process of evaluating modifications related to the recommendations of the B&W report (BAW-1564).

The licensee is implementing a power supply modification related to the recommendation of the B&W report. This modification is intended to increase power supply reliability and is to be completed during the January 1980 outage. Other recommendations are being evaluated by the licensee, but at this time, no specific actions have been defined.

The Staff is continuing to study and review this area as I indicated in my response to Question 13 above. However, the Staff has made no further specific recommendations in this area at this time.

Q 15. Explain why continued operation of the Rancho Seco facility is permissible prior to completion of the studies which the Staff has underway.

A. The bases for continued operation prior to the completion of all studies and/or analyses is that, although there are areas which could potentially be improved, the present ICS has proven to have a low failure rate and does not initiate a significant number of plant upsets.

In addition, ORNL has concluded that the analysis (BAW-1564) shows that anticipated failures of and within the ICS are adequately mitigated by the plant safety systems, and that many potential failures would be mitigated by cross checking features of the control system without challenging the plant safety systems.

DALE F. THATCHER

PROFESSIONAL QUALIFICATIONS

INSTRUMENTATION & CONTROL SYSTEMS BRANCH

DIVISION OF SYSTEMS SAFETY

I am a Senior Reactor Engineer in the Instrumentation and Control Systems Branch, Division of Systems Safety, Nuclear Regulatory Commission.

From May to December 1979, I was assigned to the Bulletins and Orders Task Force as a technical reviewer in the area of instrumentation and control. Just prior to this assignment I was a member of the NRR team which aided in the Three Mile Island Recovery Operation.

In the ICSB, my primary responsibility is to perform technical reviews of the design, fabrication, and operation of instrumentation and control systems for nuclear power plants. This review encompasses evaluation of applicant's safety analysis reports, generic reports and other related information on the instrumentation and control designs.

I graduated from Lehigh University with a Bachelor of Science Degree in Electrical Engineering in June 1971.

From my graduation in June 1971 until my employment at the Commission, I was an Instrumentation Engineer with Gilbert Associates, Inc., an Architect-Engineering company located in Reading, Pennsylvania. My responsibilities included the design and evaluation of various instrumentation and control systems including primarily the areas of reactor protection systems and other safety systems for various domestic nuclear power plants.

I joined the Regulatory staff of the Atomic Energy Commission in March 1974 as a Reactor Engineer. Since then, I have participated in the review of instrumentation control and electrical systems of numerous nuclear power stations and standard plant designs. In addition, I have participated in the formulation of related standards and regulatory guides.

I am a member of the Institute of Electrical and Electronics Engineers (IEEE) and have participated in the development of IEEE Standard 379-1977, "IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Class IE Systems" and other proposed standards.

INSTRUMENTATION AND CONTROLS DIVISION

Report Review:*

Integrated Control System Reliability Analysis**

Review by

J. L. Anderson S. J. Ditto R. S. Stone

Oak Ridge National Laboratory
Oak Ridge, Tennessee 37830

R. A. Hedrick A. F. McBride J. R. Penland

Science Applications, Inc.†

*Research sponsored by the Division of Systems Safety, U. S. Nuclear Regulatory Commission under Interagency Agreement No. 40-544-75 with the U. S. Department of Energy under contract W-7405-eng-26 with the Union Carbide Corporation.

**By R. L. Dungan, L. L. Joyner, G. P. Bennett, and C. W. Tally, Babcock & Wilcox, BAW-1564 (August 1979).

†Under Subcontract No. 62B13819C with the Union Carbide Corporation.

1. INTRODUCTION

The Instrumentation and Controls Division of the Oak Ridge National Laboratory (ORNL) was requested by the U. S. Nuclear Regulatory Commission (NRC) to review a report entitled *Integrated Control System Reliability Analysis*, by the Babcock and Wilcox Company (B&W).[1] In this document (hereinafter referred to as the "B&W analysis") B&W states their analysis of the effects of postulated failures in the B&W integrated control system (ICS) on the operation of the nuclear steam system (NSS). The object of the review by ORNL was to determine the adequacy of the B&W analysis.

The B&W analysis had been submitted in response to shutdown orders from the NRC to all B&W-designed plants (hereinafter referred to as the "NRC orders").[2]

The "Executive Summary" of the NRC orders directed the B&W control system analysis to address the following NRC concerns: "Plant design features unique to the B&W plants (e.g., OTSG and ICS) should be evaluated with regard to interactions in coping with transients. The mitigating systems (e.g., HPI) should also be included in the study." The NRC also directed analysis of other specific concerns in Sect. 8.2.3 of the NRC orders, which are rephrased as follows:

(a) The role of control systems (in this case the ICS) and their significance to safety.

(b) The rate at which transients initiated by control failures challenge the plant safety systems.

(c) The rate at which transients initiated outside the control system are not successfully mitigated by the control system.

(d) Identification of realistic plant interactions resulting from failure in nonsafety systems, safety systems, and operator actions. (Failure modes and effects analysis is indicated.)

---

1. R. L. Dungan, L. L. Joyner, G. P. Bennett, and C. W. Tally, *Integrated Control System Reliability Analysis*, Babcock & Wilcox, BAW-1564 (August 1979).

2. *Staff Report on the Generic Assessment of Feedwater Transients in Pressurized Water Reactors Designed by the Babcock & Wilcox Company*, U. S. Nuclear Regulatory Commission, NUREG-0560 (May 1979).

Finally, additional concerns were expressed in Appendix Y of the NRC orders, and pertinent excerpts are paraphrased as follows: The NRC staff has ascertained that B&W-designed reactors appear to be unusually sensitive to certain off-normal transient conditions originating in the secondary system. The features of the B&W design that contribute to this sensitivity are: (1) the design of the steam generators to operate with relatively small liquid volumes in the secondary side; (2) the lack of direct initiation of reactor trip upon the occurrence of off-normal conditions in the feedwater system; (3) the reliance on an integrated control system (ICS) to automatically regulate feedwater flow; (4) the actuation before a reactor trip of a pilot-operated relief valve on the primary system pressurizer (which, if the valve were to stick open, could aggravate the event); and (5) the low steam generator elevation relative to the reactor vessel, which provides a smaller driving head for natural circulation.

Because of these features, B&W-designed reactors depend greatly on the reliability and performance characteristics of the auxiliary feedwater system, the ICS, and the emergency core cooling system (ECCS) to recover from frequent, anticipated transients, such as loss of offsite power and loss of normal feedwater. This, in turn, places a large burden on the plant operators to cope with off-normal system behavior during such anticipated transients.

The administrative action required of B&W by the NRC was that "the licensee will submit a failure mode and effects analysis of the ICS to the NRC staff as soon as practicable."

2. GENERAL FINDINGS OF ORNL REVIEW

The B&W analysis[1] submitted in response to the NRC orders deals only narrowly with the ICS itself and not at all with the plant systems it controls and with which it interacts. With note of the concerns expressed and the guidance given in the NRC orders, the B&W analysis is more notable for what it does not include than for what it does include. With reference to the "Executive Summary" of the NRC orders, the B&W analysis does not deal with interactions or with transients, except those that might be initiated by limited signal or component failures (one at a time) within the ICS. Neither does the report deal with mitigating systems such as HPI, as suggested. In fact, consideration of all events is concluded with reactor trip; interactions with ECCS are not mentioned, even though to some extent the ICS (auxiliary feedwater) is a part of the ECCS.

The significance of the ICS to safety (item a) is not addressed.

The rate at which transients initiated by control failure challenge the plant safety systems (item b) is dealt with only to a limited extent. Only control failures within the ICS cabinets are considered, and then only to reactor trip. No significant control, instrument, or power failures external to the ICS cabinets are considered, even though several such failures have occurred in operating plants.

Transients initiated outside the control system (item c), whether or not successfully mitigated by the ICS, are not addressed, except in tabulations of operating experience.

Identification of interactions (item d) resulting from failures in safety or nonsafety systems or operator actions is notably absent.

Also notably absent is any consideration of the sensitivity of the B&W plant design to feedwater transients, to performance—either normal or abnormal—of the ICS, or to reliance on the pilot-operated relief valve for successful maneuvering.

In summary, the report deals only with a very limited scope of failures, essentially within the ICS cabinets; the only significant measure of response is whether a reactor trip would occur. Because of this limited scope, the results are necessarily of limited value. The following ORNL review takes into account this limited scope and attempts to evaluate the analysis presented and, also, to suggest additional work which might be needed.

3. THE ORNL REVIEW PLAN

The ORNL review plan was that first we would identify the concerns and need for a B&W analysis of the ICS. Then, from that statement of need, we would establish specific objectives for the B&W analysis report. From the statement of objectives, the B&W analysis would be evaluated relative to their methodology by which the objectives were to be achieved and to the adequacy of their implementation of the methodology.

This basic plan resulted in two classes of comments concerning the B&W analysis: "Methodology" and "Implementation." Based on these two sets of comments, major concerns were identified and evaluated, from which the adequacy of the B&W reliability analysis of the ICS was assessed. Finally, from NRC areas of concern and from the ORNL evaluation of the B&W analysis, we derived a set of recommended actions that would lead to an achievement of the original study objectives desired by the NRC.

Several questions were submitted to B&W to obtain clarification and expansion of some concerns expressed in our preliminary review of the analysis. These questions and the B&W responses are included as Appendix A.

Because of the once-through steam generator, the B&W NSS responds rapidly to secondary system perturbations. (This sensitivity was a key consideration in the analysis of the Three Mile Island accident.) In any evaluation of potential or real abnormal events, evaluation of the ICS is a principal requirement because of its influence on the course of the events. The task of evaluation of the ICS is made complicated by the following engineering considerations:

1. The complexity of the ICS due to its feed-forward approach as augmented by feedback fine tuning.

2. The complexity of the plant response to control actions.

3. The sensitivity of the plant and a definition of what constitutes failure of the ICS (e.g., instrument drift not normally associated with failure might be sufficient to initiate an ICS-induced transient).

An understanding of the sensitivity of the B&W NSS response to ICS actions enables identification of the following objectives for analysis of the B&W control system:

1. Estimate the probability that an ICS failure can initiate an accident. This estimation must be based on an objective evaluation of the system.

2. Identify design deficiencies.

3. Identify design features that influence the probability of accident initiation.

4. Evaluate the capability of the ICS to respond properly to probable events, and estimate the impact of adverse actions of the ICS.

In the following sections, we discuss the methodology selected to meet the preceding objectives (Sect. 4), discuss and evaluate the implementation of the selected methodology to evaluate the B&W ICS (Sect. 5), and recommend further work to address the role of control systems in the safety of nuclear power plants (Sect. 6).

4. METHODOLOGY SELECTION

The methodology selected for the reliability evaluation of the ICS consisted of three parts: failure modes and effects analysis (FMEA), systems simulation, and operating data collection and analysis. In concept, the FMEA is used as a predictive tool to estimate which failures within and without the ICS can lead to plant transients. A simulation model is used to study in more detail the effect of postulated failures identified by the FMEA. Finally, from collection and analysis of operating data, information is obtained for comparison of what has occurred with what has been predicted. From such comparisons, the validity of overall conclusions may be determined.

The following paragraphs identify and discuss the bases for concerns with the methodology selected.

4.1 Scope of Analysis

As part of the ongoing evaluation by the NRC staff, the initial concerns with the ICS were broadened into a more general concern about control systems and the interaction of safety and nonsafety systems as mentioned in the introduction of this review. The broader concerns were not considered explicitly in the ICS study.

Our review attempts to answer several questions. First, does the B&W analysis present a fair and complete representation of the ICS? Second, do the failures selected for analysis and the results stated provide the insight to allow valid conclusions to be drawn? Third, can this type of study, based on failures within or at the boundaries of the ICS, adequately evaluate the potential impact of the ICS on the safety of the plant? Fourth, if the answer to the previous question is "no," what other information is necessary?

We believe that the usefulness of the B&W analysis is limited because the ICS is bounded so narrowly. A control system, particularly one claimed as "integrated," should include sensing, signal conditioning, and actuating equipment and perhaps power supplies—if not primary power sources. The system being controlled includes a number of process loops that are highly interactive and which must often operate within rather narrow individual constraints. The B&W analysis does not address these interactions.

The failures selected by B&W for analysis are based on failures of functional blocks. Although it is recognized that functions can fail because of equipment failures, it is not clear that there are no undisclosed couplings or interactions of blocks. An example of common elements that may involve multiple blocks is the arrangement of power supplies and their protective features (fuses, breakers, etc.). Additionally, the B&W analysis is seldom carried beyond reactor trip, if that occurs. While it is of interest to know that a failure causes a trip, it is also of interest to know whether a trip is actually needed and whether the trip lays all problems to rest.

To some extent, the B&W analysis discusses the effect of operator posttrip action, but many of the scenarios end with the trip. Although the ICS controls the operation of equipment that is important during posttrip situations, the B&W analysis does not pursue this necessary consideration. For example, it is suspected that some possible failure modes of the ICS could inhibit initiation of auxiliary feedwater (AFW). Also some failures in the ICS possibly could initiate a loss of feedwater and also could inhibit auxiliary feedwater via the flow control valves. These possibilities are not addressed, presumably because they are plant specific.

Measures are underway to make initiation and control of AFW independent and safety grade.

Inasmuch as the ICS participates so directly in the coordination of the generation, transport, and removal of heat, it influences the behavior of the whole plant, even to the extent that it could magnify anomalous behavior that originates outside itself. Malfunctioning valves have required manual intervention for operation during startup, probably because the automatic systems (ICS) could not cope. It would not be impossible for peculiar equipment interactions or operating conditions to place the ICS at such a disadvantage that it would respond, although as designed, in an undesirable way.

A basic question, from a safety viewpoint, is the following: Can the ICS cause the plant to misbehave in a credible way so that the protection system (and ESF's) cannot adequately handle it? Hopefully the answer is no, but a corollary question might also be asked: Does the ICS increase or decrease the rate at which the protective features are being called upon to cope with real hazards? These questions are not unique to the ICS. They are concerns to be addressed in an analysis of any control system; however, they cannot be answered meaningfully by consideration of only a relatively small portion of the entire control structure, such as the ICS as limited in the B&W analysis report.

It is clear that the B&W analysis was an attempt to respond to loosely defined concerns on a short time schedule. It describes some problems that can arise, but falls short as an in-depth evaluation. The supplementary operating statistics indicate that the control system is of reasonable reliability, but they also give a somewhat hazy image of a system that has some performance deficiencies. It does not appear to be an unworkable system, but it falls short of being a strong influence for safety.

The broader concerns are summarized as follows:

1. Other control systems. These include other automatic control systems such as the nonnuclear instrumentation (NNI) makeup flow and PORV controls and turbine-generator controls. Failures within these control systems can affect the performance of the ICS and other key systems simultaneously. Of particular concern, for instance, is the postulated failure of power supplies in the NNI. In addition to automatic controls, the plant operator is himself part of a control loop between the NNI indications and the controlled components.

2. Controlled components. As identified by the historical data, plant trips are caused more by failures of controlled components than by failures of automatic control systems. As previously identified, interactions among control systems (including human operators) and controlled components may result in a transient, even though no specific equipment has failed.

3. Control system inputs. The ICS analysis considered single "high" or "low" ICS inputs. Failure of sensor signals to other control systems, including human operators, should be studied in detail. Such failures are of particular concern, since they may have a simultaneous adverse effect on ICS performance and/or the performance of other critical systems. The study should include multiple failures due to common causes (e.g., power supplies) or undetected failures. Failures of input signals at midscale should be studied because they may remain undetected and thus contribute to multiple component failures.

4.2 Multiple Failures

The FMEA is a qualitative reliability engineering technique for evaluation of the effects on system operation of single, postulated failures within the system or within subsystems interconnected to the principal system. The FMEA starts with contributing events and traces them upward through the system hierarchy to determine the overall effects. The FMEA is suited to the performance of single-failure analyses; it is not a convenient technique for addressing multiple-failure situations.

This inability to address multiple failures in the B&W ICS may be significant since, as acknowledged by B&W, failures may occur in the ICS without being annunciated, such as those of signal limiters and auctioneers. A failed auctioneer, for instance, might have no effect on ICS performance until called upon to implement a cross limit initiated by another ICS failure. Since sufficient evidence to the contrary does not exist, multiple-failure-induced transients may have a significant probability.

An alternative or augmenting technique is fault tree analysis, since fault trees are suited to handling multiple failure situations. The ICS reliability study identified major events in which the ICS could participate: loss of main feedwater, steam generator overfill, secondary depressurization through turbine bypass or atmospheric dump valves, and, possibly, combinations of these events due to instrument power failure.

It may be advisable to analyze fault trees on these major events, tracing through the system "top down" to identify the faults that could induce the specific event. This analysis would identify sets of multiple failures and estimates of their probability. Specifically, an interesting fault tree might be developed for a "top" event of loss of feedwater, using the equipment block diagram rather than the functional block diagram used in the B&W analysis. (Section 5.1.1 states the reasons for using an equipment diagram.) From the results of this analysis, one might judge whether it would be worthwhile to develop fault trees for other major events.

4.3 Participation in Feedwater Oscillations

The methodology that was selected cannot evaluate the possible involvement of the ICS with FW oscillation. At least two regimes of oscillation have been identified: one in the power range from 15 to 20%, with a period of 3 to 90 s, and a second at ~0.3 Hz, which occurs during operation up to 70% of full power in some plants. The ICS does participate in these two regimes, and it is possible that its effect could cause the plant to trip. Further, the ability of the plant systems, including the ICS, to withstand such perturbations has not been determined. It is not clear that the effect of such oscillations has been included in the plant duty cycle.

Because much is unknown concerning the dynamic response and stability of the plant control system (a broader definition of the ICS), we believe that a dynamic performance analysis should be made to better understand the dynamic characteristics, including system oscillation. Some topics suggested for study are as follows:

1. The dynamic response of FW pump control is generally slower than that of FW valves. Will transition from valve to pump control of FW cause stability problems?

2. Do the pressurizer controls attempt to mitigate or to amplify pressure oscillations? How are the pressurizer and the ICS interdependent with regard to stability?

3. Are oscillations caused or mitigated by the ICS?

4. What conditions could lead to plant instability?

4.4 System Simulation

The objective of system simulation is to evaluate the effect of postulated failures upon the NSS. This is, in concept, an excellent technique, inasmuch as evaluation using an operating plant would be prohibitively expensive and possibly dangerous. Likewise, an intuitive estimation of the effect of postulated failures on the system would be inadequate because the system response to inputs from the ICS is too complex for such a simplified technique. Thus, system simulation is an appropriate technique, with a caveat that any simulation is limited in its ability to predict system response. The strengths and weaknesses of the simulation technique chosen, POWER TRAIN IV (PT-IV), are addressed in Sect. 5.2.

5. EVALUATION OF IMPLEMENTATION OF METHODOLOGY

In this section we presume that the B&W method described in BAW-1564 is adequate for evaluation of the ICS. The results reported below evaluate the manner in which the methodology is applied to the ICS. The results of this evaluation are described in the three sections corresponding to the FMEA, POWER TRAIN simulation, and operating data.

5.1 Failure Modes and Effects Analysis

5.1.1 Functional versus hardware basis

An FMEA can be performed on either a functional flow block diagram of the ICS or an equipment block diagram. The two are not necessarily the same, and results based on the functional flow block diagram may be misleading relative to the actual configuration of hardware.

For maximum utilization of an FMEA for a real system, the FMEA should be performed on an equipment block diagram.

The functional flow FMEA provides little, if any, basis for even a judgmental estimation of failure probability. This is exemplified in Table 4-5 of the B&W analysis[1] where almost all functional failures of the ICS result in a trip. However, as implemented in ICS hardware, the functions have cross limits that can prevent trip conditions. Thus, the analysis, as presented, does not reflect beneficial features of the ICS. Specifically, fault tolerance of the system cannot be evaluated, although plant data suggest that the ICS has a considerable degree of fault tolerance. The B&W Table 4-5 shows only one of the 39 functional blocks whose failure does not produce a trip. However, operating data shows that only 6 of the 47 actual ICS equipment failures resulted in a trip.

Unless portions of an FMEA on the equipment block diagram can be performed, the impact of using the functional rather than the equipment diagram cannot be evaluated completely. As noted in Sect. 4.2, a fault tree using the equipment block diagram would have been a better method of analysis.

5.1.2 Off-normal conditions

The serious safety problems experienced in operating reactors have, in general, involved multiple failures, or sometimes a single failure compounded by operator error. Without deserting the probability-justified single-failure criterion, it would be instructive to examine the consequences of single hardware failures occurring during operation with less than a full complement of coolant pumps or with certain control functions in the manual mode. These are allowed conditions of operation; their occurrence is not uncommon. Under the same probability guidelines that mandate investigation of ATWS situations, it is not unreasonable to examine the consequences of single ICS failures during off-normal conditions of plant operation.

Where control failures are postulated under conditions of degraded heat removal capabilities, a scram may not always be the final action to be considered. If reactor cooling must be followed from full power into the shutdown mode, PT-IV does not appear to have a dynamic range to follow the decreasing power nor the command of nonlinear effects to deal with the interim transient. Additional investigation of ICS component failures under off-normal conditions would be desirable, particularly where operation is on two pumps and such ICS failures occur as a "close valve" malfunction in one steam generator's startup control valve actuator. In addition, it would be desirable to follow postscram heat removal with a blowdown-competent code, at least for a few extreme cases, in order to demonstrate the medium-term consequences of the event and the adequacy of the PT-IV predictions.

The B&W analysis asserts that ICS actions have averted more trips than they have caused. Although this assertion is not pertinent and is probably true, the data presented do not substantiate the assertion.

5.1.3 Power supplies

The evaluation of power supply failures was limited. Although a loss of input power was listed as a failure, the effects of the failure were not evaluated. Failures of power conditioning equipment internal to the ICS were not considered except for their potential contribution to "high" or "low" failures or to single internal ICS functions and to single ICS output signals. The B&W report[1] states that power supply failures could not be considered in greater detail because plant-to-plant design variations were too great, the failure modes and effects were too complex, and the time allocated for the study was too brief to permit such an analysis. In the B&W analysis, power supplies are listed as a subject for additional study.

5.1.4 Effect of postulated failures

From the limited B&W evaluation of postulated failures, it is difficult to assess the need for further evaluation or for potential design modifications. As an example, the FMEA describes the effect of steam generator overfill as "... overcooling of the primary, and possible loss of pressurizer inventory and/or level indication."* However, in the summary of an NRC-B&W Operating Plant Licensees Meeting, the effects of the

*Ref. 1, p. 4-33.

same transient were described as follows: "The resultant carry-over of liquid into the main steam lines could lead to equipment damage to both the main turbine and any auxiliary turbines (i.e., AFW pump turbines) being supplied steam from the main steam system. In addition, the carry-over could lead to excessive waterhammer. It is also possible that the weight of the water in the steam lines could cause excessive stresses on the piping system and pipe supports."[3] Regardless of how appropriate either description is, the latter description would place a greater emphasis on the potential need for remedial action.

5.2 System Simulation

A more accurate assessment of the response of a plant to ICS failures, we believe, could be achieved by simulating a failure with sufficient equipment that would be capable of following the transient resulting from the simulated failure. The equipment needed would be modules capable of responding to simulated failures of the NSS, ICS, and BOP over a wide range of parameters. Although no such global simulation capability exists, simulators that can encompass some combination of the three systems over a limited range of the parameters of interest are available.

POWER TRAIN IV (PT-IV), was chosen as the simulator and was adapted to the lower loop, once-through steam generator configuration. It has all three systems, NSS, ICS, and BOP, modeled, but its thermodynamic, fluid mechanic, heat transfer, and core power applicability ranges are restricted.

Since evaluation of the ICS deals with failures that result in large changes in process parameters, e.g., steam generator dry out or flooding, the ability of PT-IV to adequately follow the resulting transients is suspect. For example, many of the undercooling transients are stated to cause a probable overpressure reactor trip; however, due to the changing core inlet temperature, DNBR trips may be more likely. Since the parameter that guides the system directly relates to ICS action, pressure and temperature, individually, will result in different plant transients and effects on the NSS even though both may cause trip. The impact of the limitations of the PT-IV simulation on the overall results is not fully understood; however, the need for using engineering judgment relating to the PT-IV results has been indicated.

Although we would prefer a simulation tool with complete capability, in the context of state of the art, PT-IV is adequate. Its deficiencies do not greatly affect the overall results, since a reactor trip is the

---

3. R. A. Capra, "NRC Summary of Meeting Held on August 23, 1979, with the Babcock & Wilcox Operating Plant Licensees' to Discuss Recent (Post TMI-2) Feedwater Transients," (September 13, 1979), p. 8.

terminating point for the analysis. However, if a more detailed evaluation of system effects is desired, it will be necessary to develop a more sophisticated system simulation tool.

FMEA Table 4-3 is an extensive study of the impact of single ICS input failures on system behavior. Under the guidelines assumed, this was a good study, but it is questionable whether much would be gained by further pursuit of this particular approach. To begin with, a great deal of the information in Table 4-3 could be determined by a knowledgeable, a priori examination of an ICS flow sheet, without resort to simulation. Where simulation has been and should be used, it is not apparent that conditions are so far from design point that a linearized model would not be acceptable. The reason is that a reactor trip from any out-of-range variable would appear to call a halt to a study of further consequences. From a case by case examination, this response also seems justifiable; no single ICS input failure appears to cause safety problems that a scram would not cure.

5.3 Operating Data

The historical failure frequency of ICS components, the frequency of ICS initiated transients, and the actual response of operating plants to component failures were evaluated, using the records of transients at B&W operating plants. This section complies adequately with the B&W commitment. Since the scope was not limited to ICS failures, even the more general control system concerns recently raised by the NRC are addressed in the section entitled "Operating Experience."

As shown in Fig. 5.1 of "Operating Experience," only 2% of commercial, operating plant trips were caused by internal ICS failures (excluding power supplies). Of the remaining trips, one-third were caused by operator technician errors and two-thirds by ICS interactions with controlled equipment, failures of controlled equipment, ICS inputs (including power supplies), and failures of other control systems. Therefore, internal ICS failures are not a major causative factor of transients that produce trips.

The MTBF's (mean time between failures) for the ICS equipment are consistent with expected values for equipment of that generation (for both the 721 and the 820 series). The 820 series equipment appears to be much more reliable than the 721, but there are insufficient data to state that the apparent large differences are statistically significant. Although the operating data indicate a relatively low probability of ICS failure, the data should not be regarded as a source of insight into the sensitivity of the plant to the ICS.

6. EVALUATION AND RECOMMENDATIONS

6.1 Operating Experience

Reliance on the ICS or on automatic control in general to regulate feedwater and other plant parameters is not a shortcoming as might be inferred from current suspicion of the ICS; instead it is a significant asset to plant safety and availability. That the system does not perform perfectly in all situations or that it may induce plant upsets when it fails is only to be expected. Thus, one should criticize only the deficiencies and not automation in general. Customer satisfaction and acceptance of the ICS is high and at least as favorable as competitive designs.

It is clear that the ICS, either through its own failure or through its response to real or unreal plant conditions, can alter plant operation in undesirable ways. However, other effective control systems, including good and bad operators, can also do this. For example, feedwater pumps and valves, bypass valves, and atmospheric dump valves can be misoperated; control modes can be improperly altered; loop balances can be upset; and many other anomalies can be caused or exacerbated by the ICS. Neither is this surprising, nor is this necessarily a cause for alarm. The ICS has features that are effective in mitigating the effects of some of its own failures and those of its auxiliaries. These include load, rate, and cross limits, which are useful but not infallible. We find no evidence that the ICS provides more frequent or more severe challenges to the PPS (plant protection system) than other control systems of similar scope, nor do these challenges exceed the PPS capability. The coordination of nuclear power generation with load requirements under system constraints of pressure, temperature, and the like is a complicated task. The development of a system such as the ICS required consideration of many problems too complex for an operator to handle during a minor (or major) plant disturbance. The response of the ICS is far better and more predictable than that of an operator, given the same information.

While we agree that the ICS should not be classed as a protective system, we believe that there should be more concern for avoiding, as well as detecting, degradation of failures within the system. Failures in control systems do affect safety through their impacts upon the rate of challenge of the protection system. The economic costs are obvious. Better control equals better safety, but the quantification of the gain is difficult. Examination of the failure statistics in the B&W analysis (notably Table 5-8) reveals that only a small number of ICS malfunctions resulted in reactor trips (approximately 6 of 162). These data, supported by conversations with plant operators, demonstrate that the system is failure tolerant to a significant degree. This feature is also evidenced by noting the large number of postulated failures in the FMEA that could result in a reactor trip, compared with the experienced low trip rate in practice. The positive results of the FMEA and operating experience of the ICS show that the control system itself has a low failure rate and that it does not instigate a significant number of plant upsets. The analysis further shows that anticipated failures of and within the ICS are adequately mitigated by the PPS and that many potential failures would be mitigated by cross-checking features of the control system without challenging the PPS.

The manufacturer contends, and we agree, that (1) the system prevents or mitigates many more upsets than it creates, and (2) the system is generally superior to manual or fragmented control schemes. The performance deficiencies that have been suggested relate mostly to the ability or inability of the system to deal with major operational upsets, with maneuvering through different plant modes as from hot standby to low power, and with component problems such as valve leakage or pump response. Since these performance characteristics are not the subject of the B&W analysis, they are not emphasized in this review. Instead, in this review a broader scope of system performance was investigated, but to a limited extent. The following suggestions for further study are offered:

1. An analysis of overall plant stability, including the participation of the ICS in system oscillations and other specific ICS actions, such as control of feedwater after a turbine trip and other anticipated transients.

2. Development of an appropriate full-plant simulator to evaluate the interaction of the primary, secondary, and control systems.

This latter suggestion is a generic problem beyond the scope of the B&W analysis, implying a need for NRC sponsorship. The simulator would have to be an advancement over current tools, one that would combine all systems and still have an acceptable parameter and transient range. Analog systems alone are not likely to be adequate for the purpose. A hybrid system would be the most applicable computer system based on our current views of the operational upsets to be covered.

6.2 Failure Modes and Effects Analysis

Our evaluation of the FMEA as performed and reported in the B&W analysis suggests several concerns and recommendations for future investigation.

1. As discussed in Sect. 4 of this review, the functional block FMEA approach may have been selected as an economic expedient and may not have been the optimum technique for deriving the information desired. If further pursuit of the failure consequences of the ICS is desired, we recommend that a fault tree for loss of feedwater be developed, based on equipment diagrams rather than functional blocks. This would allow assessment of the significance of multiple failures and some verification of the adequacy of the use of functional block diagrams. We are satisfied that failures within the ICS itself do not constitute a significant threat to plant safety and that further analysis of this type may not be economically justifiable.

2. The FMEA would have been of greater significance if it had been expanded to include other systems with which the ICS interacts, such as the nonnuclear instrumentation (NNI) and its power and signal sources. In particular, the analysis should have considered midscale failures and off-normal initial conditions. It is not evident that redoing the analysis at this point to include this information would be worthwhile.

3. Power supply failures have caused and are continuing to cause significant plant upsets. They should be evaluated in detail, and specific recommendations for their upgrading should be reported.

4. The simulation tools used in these studies are deficient in their dynamic range and component details. Nonetheless, they served a useful purpose. It is our opinion that more detailed analyses would not provide significantly more enlightening information for purposes of the FMEA.

6.3 Comments on B&W Recommendations

6.3.1 ICS related

Our comments on the B&W recommendations are as follows:

1. NNI/ICS power supply reliability: We concur that this is an area needing attention, going somewhat beyond supply reliability per se. Although our review of this subject has not been comprehensive, problems of system arrangement and channeling and selection of input signals appear to need improvement. In at least two plants, a single power supply failure can result in a loss of virtually all signals to the ICS. Since power supply arrangements are specific for each plant, individual attention by plants is indicated.

2. Reliability of input signals from the NI/RPS system to the ICS, specifically the RC flow signal: The background for this recommendation was not described by B&W. We concur that this subject deserves attention for the same considerations as discussed in the preceding recommendation.

3. ICS/BOP system tuning, particularly feedwater condensate systems and the ICS controls: The concern behind this recommendation may be broader than tuning. We believe that the dynamic performance of these systems should be studied in relation to the entire plant response, including the effects of control limitations, such as valve and pump-speed responses, on plant stability. Since there is a tight coupling between the secondary system which is controlled by the ICS and the primary system with its important considerations of pressure and pressurizer level, including the primary system within the ICS may be worthy of investigation as a potential control improvement.

6.3.2 Balance of plant

For the balance of the plant, B&W recommends the following:

1. Equip the turbine drive in the main feedwater pump with a minimum speed control to prevent a loss of main feedwater or a loss of indication of main feedwater.

2. Install means to prevent or mitigate the consequences of a stuck-open startup valve in the main feedwater line.

3. Install means to prevent or mitigate the consequences of a stuck-open valve in the turbine bypass line.

We concur with these recommendations.

APPENDIX A: QUESTIONS AND RESPONSES

After a preliminary review of the B&W analysis, we submitted several questions to B&W to obtain an expansion or clarification of information presented in their report[1] or to obtain other information not contained in the report which may be germane to the review. B&W invited the reviewers, NRC staff members, and representatives of the Toledo Edison and Duke Power Companies to their facilities in Lynchburg, Virginia, to hear their responses to the questions. This meeting was October 23, 1979.

The questions and the reviewers interpretation of the responses follow. The reviewers have added some additional interpretations and observations summarized from the group discussion.

Q1.* *There may be a significant difference between failure modes or conditions with an FMEA that are based on functional block diagrams rather than on equipment block diagrams. Were the functional failure assumptions compared with actual equipment failure modes to assure that they are realistic and meaningful?*

R. Functional block diagrams were used to reduce the scope of the effort and allow the analysis to be accomplished in the requested time frame. As stated in their report and in discussions, B&W believes that the functional approach is adequate and that very few observations would be in error as a result of this choice.

C. An example of a possible incorrect or incomplete conclusion arising from this approach is that failure considerations of the turbine bypass valve control do not include details of whether condenser cooling is available and whether the control will be transferred to the condenser dump or to the atmospheric dump. Also not considered is operator response or interference/interaction. This example was selected because the recommendations of the B&W analysis include additional analysis of bypass valve failure.

Q2. *All assumptions of ICS signal input failure appear to be either high or low, with some attempt to identify a "worst case." Some of the operable plants under review potentially could experience midscale failures. There is some evidence that some midscale failures could be worse than high or low failures, as experienced by the plant selected as typical, Rancho Seco. Are there plans for including midscale failures in the analysis and how is the validity of the analysis compromised by not including midscale failures?*

R. B&W considers (1) midscale and multiple-input signal failures to be either outside the boundaries of the ICS or outside the scope of the review as determined by B&W, and (2) the high or low signal assumptions to be the worst case for single failures.

---

*Q, question; R, response by B&W; and C, comment by ORNL reviewers.

C. We find no specific evidence to confirm this assumption. With regard to multiple-input signal failures, operating experience confirms that this is a highly credible event which can result from the <u>single</u> failure of a power supply in the NNI in the input signal selection circuitry. An example of such a failure is the Rancho Seco event of March 20, 1978. We believe that the B&W decision not to include consideration of failures beyond the actual ICS cabinet terminals is a serious shortcoming of the analysis, especially since considerable operating experience indicates that power supplies are not reliable. B&W recommends further analysis of the ICS and NNI power supplies based on this operating experience.

Q3. *Virtually all of the events/failures considered in the analysis appear to be based on "normal" conditions, that is, when all plant equipment is functioning at nominal design points. Our limited information regarding the same operating experience suggests that many of the abnormal occurrences were the direct result of some plant equipment not functioning; for example, three primary pumps instead of four were running, one instead of two feedwater pumps was running, one or more hand/automatic stations was in manual, to name three instances. Since these seem to be the more significant initial conditions for unsatisfactory ICS performance, how is their omission justified? Were any of these "interesting" events analyzed but not reported?*

R. B&W did not miss any significant transients or protective system challenges by not including off-normal, initial conditions. No unreported analyses were performed from off-normal conditions.

C. Since B&W did not confirm this contention, we find it difficult to support. Our evaluation of plant events involving the ICS is that the majority of these events occurred from off-normal initial conditions and/or with some function(s) of the ICS in manual or tracking modes. This experience would tend to deny their assertion.

Q4. *What process was used to determine the "effect on the NSS"? Neither the technique nor the justification is included in the analysis. What verification techniques were employed for the "effects" analysis?*

R. The effects were evaluated by knowledgeable people with plant experience.

Q5. *The POWER TRAIN IV (PT-IV) code obviously has a limited ability to simulate the NSS and BOP responses. How significant is this limitation on the analysis? In particular:*

(a) Describe the extent to which the simulation was used to predict results.

(b) Describe errors and uncertainties which might have resulted from the limited dynamic range and functional detail of the simulation.

(c) Describe to what extent the simulation results were verified with plant data.

(d) *Describe the extent to which the simulation was valid or invalid for each of the individual plants and their differences, especially feedwater systems.*

(e) *Was the simulation capable of dealing with off-normal operation, such as three primary pumps or partial manual operation?*

R. PT-IV was used in about 75% of the cases to evaluate the effects on the NSS, along with supplemental "engineering judgment." This code has the following features: two steam generators modeled in continuous space and discrete time; steam lines; feedwater pumps; feedwater heaters; condenser; pressurizer; turbine dynamics; and valves. The primary system includes pump characteristics programmed from other codes as a table and appropriate transport lags (~10 s). The pressurizer modeling includes the effects of surge flows, spray flows, internal flows with condensation and flashing, heaters, and safety and power-operated relief valves. The ICS model uses a dedicated digital computer (EAI-640) and is a digital model of an analog system utilizing functional blocks. One feedwater valve model is used to represent all FW valves.

The limiting ranges of PT-IV are reported to be: primary pressure of 1500-3000 psi, secondary pressure of 500-1500 psi, temperature (primary and secondary) of 400-700°F, and feedwater temperature of 350-700°F.

The hybrid model uses two EAI-680 analog computers and one CDC-1700 digital computer. Due to computer limitations, there is not much detail of the feedwater system. A more complete model (not PT-IV) would include pump drains, flash tank levels, and condensate pumps, as well as main feed pumps. The condensate pumps have suction pressure trips that sometimes actuate when the interceptor valves close. This is not modeled. Turbine trip is the transient used to check the code with plant data. The validity of the comparison is judgmental. The model is <u>not</u> valid at low powers.

C. Within the limitations of the effects considered and the comparisons of the effects with plant data, we expect the results of PT-IV to be reasonably valid.

Q6. *The ability of the ICS to respond properly to its design basis and other probable conditions is not addressed. That is, design problems associated with normal operation or maneuvering are not included, unless a failure is assumed. This may be outside the scope of the NRC request, but the interactions of the ICS feedwater systems observed in operating plants indicate that this may be a valid concern. Were the design problems and component limitations associated with expected normal operation analyzed and documented? Are these analyses available?*

R. B&W has no strong motivation to improve the performance of the ICS. Its utility customers have no significant unresolved complaints about the ICS.

C. Subsequent discussions with three plant owners confirm this acceptance.

Q7. *Is there any connection, physical or phenomenological, between reactor protection system (RPS) sensors and ICS inputs? Which common signals, if any, initiate trip, and what is the possibility that common-signal or signal-conditioning failures could initiate a plant transient through the ICS, requiring a response of the RPS to such signals.*

R. RPS signals are used by the ICS with suitable buffering. The redundancy provided in the RPS satisfies the requirements of IEEE-279.

Q8. *FMEA categories for "causes," detection," and "propagation potential" would yield helpful information. Has this type of information been generated and is it available?*

R. Identification of component causes is not considered necessary. Detection of component failures is not warranted, considering the low failure rate. The propagation potential for failures in analog systems is difficult to predict.

Q9. *The impact of power supply failures appears to be inadequately addressed, especially considering that events of much more significance than those analyzed have occurred at operating plants. How is the omission of these considerations justified, and is more comprehensive power supply failure analysis available?*

R. Power supply reliability is a problem for the customers to resolve. It is a recognized problem that must be resolved plant by plant. This is one of the principal recommendations of the report.

Q10. *A significant number of trips appear to have occurred when portions of the system were in a manual mode of operation. What fraction of time is it estimated that control stations are in a manual mode, and what are the problems associated with this mode of operation of the ICS?*

R. No data are available for the manual operating mode. Manual modes are judged to be used most often for startup and testing. The ICS is not designed to deal with many abnormal situations (e.g., odd alignment of equipment).

Q11. *How well does historical failure data on ICS 721 and 820 compare with predictions based on nominal behavior? Is there evidence of accelerated failure?*

R. A higher "burn-in" failure rate was experienced, but it has leveled off. The long-term failure rate remains level. TMI-1 and Oconee 1, 2, and 3 are 721 models. All others are 820 models.

Q12. *Multiple failures are not annunciated. Therefore, uncorrected failures may exist until other failures occur, resulting in effective multiple failures. It appears that multiple failure situations may have* *a significant probability of occurrence. How is the omission of multiple failure considerations justified in the analysis? Might fault tree analysis have been a better technique for addressing the concerns expressed and producing the results requested?*

R. The effort required to conduct a fault tree analysis is considered excessive. The FMEA report addresses failures considered to be "important."

C. The limited scope of the FMEA casts some doubt on this position.

Q13. *The analysis does not include information to substantiate the B&W recommendation that improvement is needed in power supplies, signal selection, and signal reliability. Please supply the analysis or the information which led to this recommendation. In particular, does B&W have specific recommendations to improve the failure tolerance of the ICS?*

R. No additional data are available.

Q14. *Operating experience reports and oral information not included in the analysis suggest that the ICS and the BOP system, including the OTSG, are sensitive to "tuning" and component problems, such as feedwater valve speed and leakage. Describe the extent to which these problems are significant, how they have led to misoperation and RPS challenges, and how they might be avoided. Are "tuning" problems inherent to this type of plant, or do they represent design deficiencies which can be corrected?*

R. The adequacy of tuning is based on customer acceptance. According to Licensee Event Report statistics, B&W plants have fewer total reactor trips and fewer feedwater trips than either of the other PWR types.

Q15. *Many Licensee Event Reports, as well as this analysis, indicate that the operator is implicated in a large number of occurrences of poor ICS operation. Many of these events also involve slightly off-normal conditions such as nonstandard pump and valve alignment. Do these events represent design deficiency, operator training deficiency, or a combination of these? Does B&W have recommendations to correct these deficiencies and on what schedule can they be implemented?*

R. Most Problems occur due to maintenance, testing, or equipment problems that require manual intervention. Also, the system is not designed for fully automatic startup.

APPENDIX B: TRANSMITTAL LETTERS

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

August 22, 1979

MEMORANDUM FOR: DISTRIBUTION

FROM: R. A. Capra, B&W Project Manager, Project Management Group
Bulletins & Orders Task Force

SUBJECT: INTEGRATED CONTROL SYSTEM RELIABILITY ANALYSIS

1. As part of the long-term portion of the Commission Orders of May, 1979, each of the B&W operating plants was directed to perform a failure modes and effects analysis of the integrated control system (ICS). B&W performed this analysis for each licensee.

2. B&W has completed the analysis and forwarded ten copies of their report, "Integrated Control System Reliability Analysis - BAW1564 - August 1979," via a letter from J. H. Taylor (B&W) to D. F. Ross (NRC) dated August 17, 1979.

3. The organization who will perform the review of this document has not been determined yet; however, I am making distribution of the ten copies we have received as indicated below. I have requested that 50 additional copies be reproduced for further distribution.

R.A. Capra

R. A. Capra, B&W Project Manager
Project Management Group
Bulletins & Orders Task Force

Distribution:

[redacted]	letter only	
Novak (1)	G. Mazetis	C. Nelson
Heltemes (1)	P. Matthews	R. Ingram
Israel (1)	D. Thatcher	W. Gammill
Rosztoczy (1)	F. Ashe	D. Eisenhut
Satterfield (1)	P. Norian	S. Lewis
Capra (1)	R. Reid	L. Brenner
Docket files (1)	G. Vissing	M. Mulkey
PDR (1)	D. Garner	D. Davis
Reproduction (1)	M. Fairtile	

Babcock & Wilcox

Power Generation Group

P.O. Box 1260, Lynchburg, Va. 24505

Telephone: (804) 384-5111

August 17, 1979

Dr. D. F. Ross, Jr.
Deputy Director
Division of Project Management
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Subject: Integrated Control System Reliability Analysis

Gentlemen:

Transmitted herewith are ten copies of the Integrated Control System (ICS) Reliability Analysis, BAW-1564. B&W performed this analysis at the request of the NRC, based on concerns stemming from the TMI-2 incident. Although the ICS performed exactly as designed during the TMI-2 incident, it was brought under scrutiny since it was both the control system for Auxiliary Feedwater and one of the major differences between B&W and other PWR designs. This analysis supports B&W's previous position - the ICS is a reliable control system that promotes NSS availability by maintaining the plant on line during normal and upset conditions, providing runbacks, and minimizing reactor trips.

If you have any questions, please call (Ext. 2817).

Very truly yours,

James H. Taylor
Manager, Licensing

JHT:dsf

Encl.

cc: R. B. Borsum (B&W)
R. A. Capra (NRC)
B&W Owners Group Subcommittee (list attached)

Babcock & Wilcox

B&W Owners Group TMI-2 Subcommittee

FPC

Florida Power Corporation
P. O. Box 14042
St. Petersburg, FL 33733
Attn: E. C. Simpson (Bert)

CPC

Consumers Power Company
1945 West Parnall Road
Jackson, MI 49203
Attn: T. J. Sullivan (Terry)

DPCO

Duke Power Company
P. O. Box 33189
Charlotte, NC 28242
Attn: D. C. Holt (Dave)

GPU

GPU Service Corporation
260 Cherry Hill Road
Parsippany, NJ 07054
Attn: R. F. Wilson (Dick)

SMUD

Sacramento Municipal Utility District
6201 S Street
Sacramento, CA 95813
Attn: S. Anderson (Stan)

AP&L

Arkansas Power & Light Company
P. O. Box 551
Little Rock, AR 72203
Attn: D. G. Mardis (Dave)

TECO

Toledo Edison Company
Edison Plaza
300 Madison Avenue
Toledo, OH 43652
Attn: C. R. Domeck (Chuck)

MET ED

Metropolitan Edison Company
P. O. Box 542
Reading, PA 19603
Attn: J. F. Fritzen (Jeff)

Babcock & Wilcox

Power Generation Group

P.O. Box 1260, Lynchburg, Va. 245

Telephone: (804) 384-5111

April 28, 1979

Mr. Harold R. Denton, Director
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
7920 Norfolk Avenue
Bethesda, Maryland 20555

Mr. Denton:

Subject: Integrated Control System

As committed by Babcock & Wilcox in J. H. MacMillan's letter to you on April 26, 1979, please find attached both the schedule and scope for a Reliability Analysis of the Integrated Control System and the schedule for developing an Auxiliary Feedwater ~~Control~~ independent of the Integrated Control Ssytem.

It is our understanding that the commitment to complete these items is not a prerequisite to plant restart.

If you have any questions, please call me (Ext. 2817).

Very truly yours,

J. H. Taylor
Manager, Licensing

JHT/wl
cc: R. B. Borsum (B&W, Bethesda)

bcc: E. R. Kane
K. E. Suhrke
R. E. Ham
D. D. Fairbrother
G. J. Brazill
R. E. Wascher
J. H. MacMillan

Scope and Schedule for a Reliability Analysis of the Integrated Control System (ICS)

Purpose: To prepare an ICS Reliability Analysis including a Failure Modes and Effects Analysis (FMEA) as committed by Babcock & Wilcox. This analysis will identify sources of transients, if any, initiated by the ICS and develop recommended design improvements which may be necessary to reduce the frequency of those transients. This analysis will concentrate on ICS failure modes that could affect the feedwater system, emergency feedwater system, pressurizer level, and reactor coolant system pressure.

Scope:

(1) Two teams of engineers have been dispatched to the presently operating plants to collect data and determine the ICS's role in each transient, with particular emphasis on transients involving feedwater (FW), emergency feedwater (AFWC), pressurizer level and reactor coolant system (RCS) pressure. Data will be returned to NPGD for input into the ICS reliability analysis. Data from other plants will also be obtained with the assistance of site personnel

(2) A FMEA will be performed by NPGD to the ICS module level. The FMEA will include identification of failure modes for hardware external to the ICS. This will consist of input signals for temperature, pressure, RCS & FW flow, pump status, and power.

(3) After identification of possible failure modes, the effects of these failures on the plant will be determined by plant simulation. The emphasis will be on failures that affect or challenge the FW, AFWC, pressurizer level and pressure, PORV's, ESFAS, and safety valves.

(4) [illegible]
31 of ICS failure modes which cause undesirable responses in the ICS will be listed.

(5) Performance of the ICS during normal plant transients will be considered in the ICS analysis.

(6) IEEE 352 will be used as a guide for FMEA format and content.

<u>Schedule:</u>

(1) On-site transient data collection: 4/26/79 through 5/9/79.

(2) Definition & boundary of system to be analyzed: 4/25/79 through 5/2/79.

(3) Identification of failure modes: 5/2/79 through 5/11/79.

(4) Simulate failure-modes and determine plant effect: 5/2/79 through 5/25/79.

(5) Generation of FMEA tables: 5/9/79 through 6/1/79.

(6) Reliability report narrative: 5/2/79 through 6/11/79.

(7) Listing of potential hardware modifications: 5/16/79 though 6/20/79.

(8) Review and prepare letter report for submittal to NRC: 6/15/79 through 6/27/79.

Description: The Auxiliary Feedwater Control System (AFWCS) will be completely separated from the Integrated Control System (ICS). The general performance criteria for the AFWCS are:

(1) The AFWCS will control the auxiliary feedwater flow and deliver water to the steam generators with control features to minimize reactor coolant system fluctuations.

(2) The AFWCS will control auxiliary feedwater flow to the auxiliary feedwater nozzles of the steam generators and will be able to achieve and maintain safe shutdown from the following plant configurations:

(a) loss of main feedwater

(b) loss of forced reactor coolant flow

(3) The AFWCS will include provisions for control of main steam pressure during operation in the plant configuration modes identified in (2) above.

Criteria: The hardware in the AFWCS will conform to the following general criteria:

(1) The AFWCS will be independent of the ICS.

(2) No single random failure in the AFWCS will prevent the system from controlling the auxiliary feedwater flow to both steam generators.

(3) Standard non-1E commercial nuclear equipment will be used.

(4) The AFWCS will have provisions for manual and automatic actuation.

Schedule:

(1)	Complete design	06/01/79
(2)	Issue sytem description to NRC and Customers	06/08/79
(3)	Manufacture (based on Customer and NRC concurrence by 06/15/79)	08/10/79
(4)	Minimum shipment and installation time is 30 days. Exact installation to be scheduled by mutual agreement of the licensee and the NRC.	

APPENDIX C: UTILITY SUBMITTALS RELATING TO THE B&W RELIABILITY ANALYSIS

DUKE POWER COMPANY
POWER BUILDING
422 SOUTH CHURCH STREET, CHARLOTTE, N. C. 28242

WILLIAM O. PARKER, JR.
VICE PRESIDENT
STEAM PRODUCTION

TELEPHONE: AREA 704
373-4083

August 31, 1979

Mr. Harold R. Denton, Director
Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Attention: Mr. D. F. Ross, Jr., Director
Bulletins and Orders Task Force

Re: Oconee Nuclear Station
Docket Numbers 50-269, -270, -287

Dear Mr. Denton:

With regard to your letter dated August 21, 1979 concerning identification and resolution of long-term generic issues related to the Commission Orders of May 1979, the following information is provided:

1. Failure mode and effects analysis of the Integrated Control System.

   The Integrated Control System Reliability Analysis, submitted by Babcock and Wilcox in a letter dated August 17, 1979 has been reviewed by Duke Power Company. This document is considered to be applicable to the system at Oconee Nuclear Station.

2. Continued operator training and drilling.

   The response to this item will be submitted by September 21, 1979.

3. Upgrade of the anticipatory reactor trip to safety grade.

   No additional information requested.

4. Auxiliary/emergency feedwater system reliability analyses.

   Duke Power Company will participate in the auxiliary feedwater system reliability analyses program proposed by B&W in a letter dated August 16, 1979 from J. H. Taylor to D. F. Ross, NRC. A final report of the results of the analysis for Oconee will be provided by December 3, 1979.

ARKANSAS POWER & LIGHT COMPANY
POST OFFICE BOX 551 LITTLE ROCK, ARKANSAS 72203 (501) 371-4000

August 31, 1979

1-089-19

Director of Nuclear Reactor Regulation
ATTN: Mr. R. W. Reid, Chief
Operating Reactor Branch #4
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

POOR ORIGINAL

Subject: Arkansas Nuclear One-Unit 1
Docket No. 50-313
License No. DPR-51
Long - Term Generic Issues
Related to May 17, 1979 Order
(File: 1510)

Gentlemen:

In accordance with the request of Dr. D. F. Ross' letter of August 21, 1979, we have reviewed Enclosure 1 of that letter and provide the following responses to Items 1, 4, 5, 7 and 8.

Item 1

The failure modes and effects analysis of the Integrated Control System (ICS) was provided via letter from James H. Taylor to Dr. D. F. Ross, Jr., dated August 17, 1979. The report, entitled "Integrated Control System Reliability Analysis", also includes a reliability assessment of the ICS plant operating experience. We have reviewed this report and basically endorse it as applicable to our system. Specific areas of difference are limited and will be addressed in our response to necessary system or procedural changes, if your review should come to that conclusion. Our operating experience has lead us to believe the ICS is a reliable control system.

SMUD
SACRAMENTO MUNICIPAL UTILITY DISTRICT □ 6201 S Street, Box 15830, Sacramento, California 95813; (916) 45

August 31, 1979

Mr. D. F. Ross, Jr., Director
Bulletins and Orders Task Force
Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Docket No. 50-312
Rancho Seco Nuclear Generating
Station, Unit No. 1

Dear Mr. Ross:

The Sacramento Municipal Utility District has reviewed your letter of August 21, 1979 requesting information on several items. The following provides that information which is due today and is listed by item number of enclosure 1 to your letter.

1. On August 17, 1979 Mr. James H. Taylor of B&W transmitted the Integrated Control System Reliability analysis, BAW-1564, to you. We have reviewed this report and find it generally applicable to Rancho Seco Unit 1 and endorse the conclusions and recommendations of the report.

4. On August 16, 1979 Mr. J. H. Taylor of B&W provided you with a scope and schedule for the auxiliary feedwater system reliability analysis. Rancho Seco Unit 1 is the lead plant for this analysis which will be available by the dates provided in Mr. Taylor's letter.

5. In response to your concerns over the thermal-mechanical conditions in the reactor vessel during recovery from small breaks with extended loss of all feedwater, the District commits to have the Babcock and Wilcox Company perform an analysis on this subject. The results of this analysis should be available by December 21, 1979.

7. The District commits to provide the information listed in Attachment A to the enclosure to your letter by the following dates. These dates supersede our commitment to Harold Denton on July 26, 1979 to provide additional small break analysis information by September 15, 1979. The required analyses will be performed by the Babcock and Wilcox Company.

TOLEDO
EDISON

LOWELL E. ROE
Vice President
Facilities Development
(419) 259-5242

Docket No. 50-346

License No. NPF-3

Serial No. 538

August 31, 1979

Director of Nuclear Reactor Regulation
Attention: Mr. Robert W. Reid, Chief
Operating Reactors Branch No. 4
Division of Operating Reactors
United States Nuclear Regulatory Commission
Washington, D.C. 20555

Dear Mr. Reid:

This letter is in response to Mr. D. F. Ross's letter of August 21, 1979 (Log No.42 to all Babcock & Wilcox Operating Plants. Attachment A addresses items 1, & 4 relating to requirements of the Davis-Besse Nuclear Power Station, Unit 1 Order of May 16, 1979. Additionally, items 5, 7 and 8 of the subject letter are addressed

Very truly yours

Lowell E Roe

LER/TJM

cc:
R. A. Capra
Project Management Group
Bulletins and Orders Task Force
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Docket No. 50-346
License No. NPF-3
Serial No. 538
August 31, 1979

Attachment A

Items of NRC Letter
August 21, 1979 (TECo Log No. 423)

The item numbers below are consistent with those of Enclosure 1 of the subject letter.

Item 1 - Failure Mode and Effects Analysis of the Integrated Control System (ICS)

The ICS Reliability Analysis (BAW-1564) was published August 17, 1979. Our preliminary review has indicated general endorsement with the following deviations:

1. Page 4-1, Section 4.1.1

   Davis-Besse Unit 1 PORV setpoint is 2400 psig.
   RPS setpoints: 2300 psig/1985 psig.

2. Page 4-6, Section 4.2.3.1

   Davis-Besse rate of change is limited to 3% per minute above 90% full power and below 20% full power.

3. Page 4-9, Section 4.2.3.5

   During a reactor trip, the atmospheric vent valves are modulated when the turbine header pressure exceeds its setpoint by 155 psi. Also, the atmospheric vent valves control header pressure on loss of condenser vacuum or loss of Circulating Water pumps.

4. Page 4-9, Section 4.2.3.6

   The throttle pressure error signal is modified in the same manner as for the atmospheric vent valves but with a 50/125 psi bias versus 75/155 psi bias.

5. Page 4-11, Section 4.2.3.10

   Error must be greater than +0.95% or less than -0.95% for rod movement.

6. Page 4-11, Section 4.2.3.11

   Feedwater demand is modified when the error is greater than +10% or less than -5%. This change was to reduce feedwater input on a load rejection.

7. Page 4-47, Table 4-4, Item 5-22, Failure Mode-open

   At Davis-Besse Unit 1, the feedwater valves are about 45 to 55% open, and a signal to open these valves would overcool the RCS and result in a low pressure trip.

The above deviations are noted, but are not significant enough to affect the results and conclusions of this report.

Florida Power
CORPORATION

August 31, 1979

File: 3-0-3-a-3

Mr. D. F. Ross, Jr.
Director
Bulletins and Orders Task Force
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, DC 20555

Subject: Crystal River Unit 3
Docket No. 50-302
Operating License No. DPR-72
Identification and Resolution of Long-Term Generic Issues Related to the Commission Orders of May 1979

Dear Mr. Ross:

On August 23, 1979, Florida Power Corporation received your letter of August 21, 1979, identifying eight long-term issues related to the Order which must be resolved for Crystal River Unit 3 and the other B&W Operating Plants.

These eight (8) items were identified and briefly discussed in Enclosure 1 of your letter. In your discussion of Items 1, 4, [illegible], 7, and 8, you requested Florida Power Corporation to provide additional [illegible]rmation and our schedule for resolution of these five (5) items by August [illegible].

In that regard, Florida Power Corporation here[illegible] [illegible]its, as Attachment 1 to this letter, our response to your August 21, [illegible] [illegible]equest for additional information.

If you require further discussion concerning our [illegible]sponse, please contact us.

Very truly yours,

FLORIDA POWER CORPORATION

G. C. Moore
Assistant Vice President
Power Production

GCMekcF06(DS)

Attachment

POOR ORIGINAL

ATTACHMENT 1

Response to Ross Letter of August 21, 1979

Item 1 - Failure Mode and Affects Analysis of the Integrated Control System

On August 17, 1979, B&W submitted to you for your review, copies of the report entitled "BAW--1564, Integrated Control System (ICS) Reliability Analysis". This letter is to advise you that this report is applicable to Crystal River Unit 3. Although this was a generic report developed by B&W, and there are differences in the secondary system designs at the various B&W plants, we feel that the conclusions reached in this report can be applied to Crystal River Unit 3. Florida Power Corporation is presently reviewing the recommendations listed in Section 3 of this report to determine what possible changes are necessary at Crystal River Unit 3 to enhance reliability and safety.

Item 4 - Auxiliary/Emergency Feedwater System Reliability Upgrade

This letter is to inform you of Florida Power Corporation's commitment to the AFW/EFW System Reliability Study proposed by B&W and discussed with you and your staff on July 19, 1979, and August 9, 1979. The draft report for Crystal River Unit 3 will be submitted by October 22, 1979, and the first report will be submitted by December 3, 1979.

Item 5 - Detailed Analysis of the Thermal-Mechanical Conditions in the Reactor Vessel During Recovery from Small Breaks With Extended Loss of All Feedwater

The above analysis will be submitted by December 21, 1979.

Item 7 - Small Break LOCA Analysis

The following is our schedule of response to the six (6) items contained in Attachment A of your letter:

1) A. Report will be submitted on December [illegible] 1979.
   B. Report will be submitted on September [illegible] 1979.

2) A. Report will be submitted on September [illegible], 1979.
   B. In response to this request, we are proposing three (3) options in preference of order:

      1) Provide a statement by September [illegible] 1979, that no small break with auxiliary feedwater will pressurize the system to the PORV setpoint.

      2) Provide by December 30, 1979, a qualitative assessment of the transient.

      3) Provide core analysis by February 1, 1980, using 0.01 ft^2 break with no AFW available.

      We are presently proceeding with option #1, unless otherwise notified by the NRC by September 7, 1979.

GCMekcFU6(DS)

Table 4-5. (Cont'd)

MODULE NO.	MODULE NAME	FAILURE MODE	EFFECT ON NSS	REACTOR TRIP	REMARKS
Functional: 2 ICS: 4-2-13	Modified Turbine Header Pressure Error	High	The ICS pulser will send a continuous increase demand to the turbine EHC causing a throttle pressure decrease. The large pressure error detector transfers the turbine EHC to manual in ~5 seconds. The ICS assumes the tracking mode and the feedwater and reactor increase to meet the ~4% load increase. The erroneous modified throttle pressure error causes a mismatch between the NSS steam production and the turbine operation. The pressure decrease is limited at ~100 psi by the turbine initial pressure regulator. Reactor trip on high RC pressure is possible.	High RC Pressure	-No problem after reactor trip
		Low	Essentially the same response as Failure Mode "High" except pressure rises and is terminated by turbine by-pass valve action.	High RC Pressure if power >~40%.	-No problem after reactor trip
Functional: 3 ICS: 3-6-1	Turbine Control		Failure is very similar to failure of functional block 2, above.		