

A REVIEW OF
A REPORT ENTITLED
INTEGRATED CONTROL SYSTEM
RELIABILITY ANALYSIS

BAW - 1564

AUGUST 1979

by

R.L. Dungan

L.L. Joyner

G.P. Bennett

C.W. Tally

Babcock & Wilcox

REVIEW PERFORMED BY:

J.L. Anderson

S.J. Ditto

R.S. Stone

Oak Ridge National Laboratory

and

R.A. Hedrick

A.F. McBride

J.R. Penland

Science Applications, Inc.

(under subcontract to ORNL)

1.0 INTRODUCTION

The Instrumentation and Controls Division of the Oak Ridge National Laboratory has been asked by the Nuclear Regulatory Commission to review a report entitled, "Integrated Control System Reliability Analysis," BAW-1564¹ prepared by the Babcock and Wilcox Company (B&W). This document, dated August 1979, was submitted by B&W to document an evaluation of the impacts 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 is to determine the adequacy of the B&W evaluation as documented in this report.

Some of the concerns expected to be addressed by a control system analysis are expressed in the recommendations of NUREG-0560.² The executive summary states: "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." Specific concerns from Section 8.2.3 of NUREG-0560 are rephrased below:

- (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 failure challenge the plant safety systems.

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

²Staff Report on the Generic Assessment of Feedwater Transients in Pressurized Water Reactors Designed by the Babcock & Wilcox Company; U.S. NRC, NUREG-0560, May 1979.

- (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 failures in non-safety systems, safety systems, and operator actions. (Failure modes and effects analysis indicated.)

Additional concerns are expressed in the NRC shutdown orders of May 7, 1979, to B&W designed plants. (Included as Appendix Y of NUREG-0560). Pertinent excerpts from these orders are paraphrased below:

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) 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) reliance on an integrated control system (ICS) to automatically regulate feedwater flow; (4) actuation before reactor trip of a pilot-operated relief valve on the primary system pressurizer (which, if the valve sticks open, can aggravate the event); and (5) a 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 place increased reliance on the reliability and performance characteristics of the auxiliary feedwater system, the integrated control system, and the emergency core cooling system (ECCS) performance 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 in the event of off-normal system behavior during such anticipated transients.

The resulting order states:

-the licensee will submit a failure mode and effects analysis of the Integrated Control System to the NRC staff as soon as practicable.

The analysis submitted in response to this order (BAW-1564, August 1979) deals only very narrowly with the Integrated Control System itself and not at all with the plant systems it controls and with which it interacts. Considering the concerns expressed and the guidance given, the report is more notable for what it does not include than for what it includes. Referring to the executive summary of NUREG-0560, the report 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 the 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 non-safety 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 of the ICS either normal or abnormal, 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, with the only significant measure of response being whether or not reactor trip occurred. Because of this limited scope, the results are necessarily of very limited value. The following review takes into account this limited scope and attempts to evaluate the analysis presented and, also, to suggest additional work which might be needed.

The approach adopted by ORNL for this review included identification of the concerns and need for this evaluation of the Integrated Control System and, from that statement of need, to establish the specific objectives for the report. From the statement of objectives the approach used by B&W was evaluated relative to the choice of methodology to achieve the objectives and the adequacy of the implementation of that methodology. This resulted in two classes of comments upon the approach contained in BAW-1564, Methodology and Implementation. Based upon the two sets of comments, major concerns have been identified and evaluated. The results of this evaluation led to an assessment of the adequacy of the B&W reliability analysis of the ICS. Finally, the areas of concern and the evaluation of the reliability analysis have led to a set of recommendations for actions to achieve the original study objectives. A number of questions were submitted to B&W

to obtain clarification and expansion of some of our early concerns used on a preliminary review of the analysis. These questions and the responses obtained are included as Appendix A.

Due to the Once Through Steam Generator the B&W NSS exhibits very rapid response to secondary system perturbations. The sensitivity was one of the key considerations in the analysis of the Three Mile Island accident. The Integrated Control System is central to any evaluation of potential or real abnormal events due to its influence on the course of such occurrences.

This evaluation of the ICS is necessitated and complicated by:

- The complexity of the ICS due to its feed forward approach as augmented by feed back fine tuning.
- The complexity of the plant response to control actions.
- The sensitivity of the plant, the 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).

Due to the sensitivity of the B&W NSS response to ICS actions, the following objectives are identified for the analysis of the B&W control system:

- Estimate the probability that ICS failure can initiate an accident. This estimation must be based upon an objective evaluation of the system.
- Identify design deficiencies.
- Identify design features which influence the probability of accident initiation.
- Evaluate the capability of the integrated control system to respond properly to probable events and estimate the impact of adverse actions of the ICS.

A discussion of the evaluation of the choice of methodology to meet the above objectives is provided in Section 2 of this report. Section 3 provides a discussion and evaluation of how the chosen methodology was implemented in the evaluation of the B&W ICS. Section 4 summarizes recommendations for further work to address the role of control systems in the safety of nuclear power plants.

2.0 METHODOLOGY SELECTION

The methodology selected for the reliability evaluation of the ICS consisted of three parts: failure modes and effects analysis; systems simulation; and operating data analysis. In concept, the FMEA is used as a predictive tool to estimate what failures within and without the ICS can lead to plant transients. A simulation model is used to evaluate in more detail the impact of postulated failures identified in the FMEA. Finally, the operating data collection and analysis task is designed to provide the information to compare what has actually occurred with what has been predicted. From such comparisons the validity of overall conclusions may be evaluated.

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

2.1 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 "non-safety" 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 subject document present a fair and complete representation of the ICS? Second, do the failures selected for analysis and the results stated provide the necessary insight to allow valid conclusions to be drawn? Third, can this type of study, based upon failures within or at the boundaries of the ICS, adequately evaluate the potential impact of the ICS upon the safety of the plant? And, fourth, if the answer to the previous question is "no", what other information is necessary?

We believe that the usefulness of the 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 document does not address these interactions.

The failures selected for analysis are based upon failures of functional blocks. While it is recognized that functions fail because of equipment failures, it is not clear that there are not 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 results seldom are carried beyond reactor trip, if that occurs. While it is certainly of interest to know that a failure causes a trip, it would also be interesting to know whether a trip is actually needed or whether all problems are laid to rest upon its occurrence.

Although some remarks are made in the analysis regarding the effect of operator post-trip action, many of the scenarios end with the trip. The ICS is involved in operating equipment that is important during post-trip situations - but the analysis doesn't give much information here. For example, it is suspected that some failure modes of the ICS are possible which could inhibit initiation of auxiliary feedwater. Similarly, there may be a question of whether failures in the ICS could initiate a loss of feedwater event and also inhibit auxiliary feedwater via the flow control valves. This question is not addressed, presumably because it is plant specific.

Also, 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 heat generation and the heat transport and removal activities, it influences the behavior of the whole plant. It may magnify anomalous behavior that originates outside itself. Malfunctioning valves have required manual intervention in operation during startup, probably because the automatic systems (ICS) cannot cope. It would not be surprising to find that peculiar equipment lineups or operating conditions place the ICS at a disadvantage so that it responds, although as designed, in an undesirable way.

One of the basic questions, from a safety viewpoint, appears to be "can the use of the ICS cause the plant to misbehave in a credible way so that the plant protection system (and ESF's) cannot adequately handle it? Hopefully the answer is no, but a corollary question might also be asked "does the use of the ICS increase or decrease the rate at which the protective features are being called upon to cope with real hazards?" Certainly these questions are not unique to the ICS issue. They are concerns to be addressed in any control system; however, they cannot be answered meaningfully by consideration of a relatively small portion of the entire control structure such as the ICS as limited in the subject document.

It is clear that BAW-1564 was an attempt to respond to rather loosely defined concerns on a very short time schedule. It gives a picture of some of the problems that can arise but falls short of an in-depth evaluation. The supplementary operating statistics indicate a system of reasonable reliability for a control system, with a somewhat hazy image of a system

challenge
control
1/12

that has some performance deficiencies. It does not appear to be a monster, but it falls short of being a strong influence for safety.

The broader concerns are summarized below:

1. Other Control Systems: These include other automatic control systems such as the Non-Nuclear Instrumentation (NNI) makeup flow and PORV controls and turbine-generator controls. The effects of failures within these control systems can impact ICS performance and the performance of 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, failures of controlled components contribute more significantly to plant trips than 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. Sensor failures to other control systems, including human operators, should be considered in detail. Such failures are of particular concern since they may have a simultaneous adverse impact 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) and due to undetected failures. Midscale failures of inputs should be considered since they may remain undetected and thus contribute to multiple component failures.

2.2 MULTIPLE FAILURES

The failure modes and effects analysis (FMEA) is a qualitative reliability engineering tool designed to evaluate impacts on system operation of single postulated failures within the system or within systems interconnected to the subject system. The FMEA is a bottom up tool in that it takes the contributing events and traces them up through the system hierarchy to determine the overall impact. The FMEA is suited to the performance of single failure analyses. It is not a convenient tool to address multiple failure situations.

This lack of ability to address multiple failures in the B&W ICS may be significant since, as acknowledged by B&W, many failures in the ICS are not annunciated and may lie dormant. Such failures include those of signal limiters and auctioneers. A failed auctioneer, for instance, might have no impact 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 significant probability.

An alternative or augmenting technique would be that of fault tree analysis. Fault trees are suited to handling multiple failure situations. The ICS Reliability Study identified several major events in which the ICS may participate. These include: loss of main feedwater, steam generator overflow, 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 perform fault trees on these major events. This would trace through the system with a top down approach to identify the faults which would induce the specific event. This analysis would identify sets of multiple failures and estimates of their credibility. Specifically,

an interesting fault tree which might be developed is for a top event of loss of feedwater. Such a fault tree should be developed using the equipment block diagram rather than the functional block diagram used in BAW-1564 (Section 3.1.1 addresses the reasons for using equipment diagram). Results from this fault tree might be used to judge the worth of developing fault trees for the other major events.

2.3 PARTICIPATION IN FW OSCILLATIONS

The methodology selected cannot evaluate the propensity of the ICS to participate in feedwater oscillations. At least two regimes of oscillation have been identified. One occurs in the 15%-20% power range with a period of 3 to 90 seconds. The second is at approximately 0.3 Hz and occurs up to 70% power on some plants. The ICS does participate in these. It is possible that ICS participation could cause the plant to reach a trip condition. Further, the degree of stability of the plant system, including the ICS, under such situations has not been investigated. It is not clear that the impact of these oscillations has been included in the plant duty cycle.

There are a number of concerns related to the dynamic response and stability of the plant control system (a broader definition of the ICS). We believe that a dynamic performance analysis is in order to address some of these concerns, including the oscillatory tendencies. Some of the questions that have been raised are:

1. The dynamic response of feedwater pump control is generally slower than the response of the FW valves. Will transition from valve to pump control of FW lead to stability problems?
2. Do the pressurizer controls attempt to mitigate or amplify pressure oscillations? How are the pressurizer and the ICS interdependent with regard to stability considerations?

3. Are oscillations caused/mitigated by the ICS?
4. What conditions could lead to plant instability?

2.4 SYSTEM SIMULATION

The system simulation is performed to evaluate the impact 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, intuitive estimation of the impact of postulated failures on the system is expected to be inadequate due to the complexity of system response to inputs from the ICS. Thus, the systems simulation is the appropriate tool for estimation of impact of postulated failures on the system. However, any simulation is necessarily limited in its ability to predict system response. The specific simulation tool chosen, POWER TRAIN IV (PT-IV), possesses strengths and weaknesses which are addressed in the following section.

2.4.1 Simulation in Support of ICS Evaluation

Two questions can be raised concerning the function failure simulations which provided input for BAW-1564.

- (1) Are more simulations needed?
- (2) Is Power Train IV a suitable vehicle for such investigations?

FMEA Table 4-3 is an extensive study of the impact of single ICS

input failures on system behavior. So far as it goes a good job was done and under the guidelines assumed, it is questionable whether much is to 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 is not acceptable. This is because reactor trip from any out-of-range variable appears to call a halt to 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 a scram will not cure.

3.0 EVALUATION OF METHODOLOGY IMPLEMENTATION

This section presumes that the methodology as described in BAW-1564 is adequate for the evaluation of the integrated control system. 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.

3.1 FAILURE MODES AND EFFECTS ANALYSIS

3.1.1 Functional Versus Hardware Basis

The FMEA is performed based upon a functional flow block diagram of the Integrated Control System. For maximum utilization of an FMEA for a real system, the FMEA should be performed on 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. The functional FMEA provides little, if any, basis for even a judgmental estimation of failure probability. This is exemplified in Table 4-5 of BAW-1564 where almost all functional failures of the ICS result in trip. However, as implemented in ICS hardware, the functions have cross limits which 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. Table 4-5 (the ICS FMEA) of BAW-1564 shows only one of the thirty-nine functional blocks whose failure does not produce trip. However operating data shows that only six of the 47 actual ICS equipment failures resulted in 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 Section 2.2, a fault tree using the equipment block diagram would have been a better approach.

3.1.2 Off-Normal Conditions

The serious safety problems that historically have arisen 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 does not seem 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 write an end to the scenario. If reactor cooling must be followed from full power into the shutdown mode, Power Train IV does not appear to have the dynamic range to follow it down, nor the command of nonlinear effects to deal with the interim transient. Additional investigation of ICS component failures under off-normal conditions, 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, would be desirable. In addition, it would be desirable to follow post-scram 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/or the adequacy of the Power Train predictions.

The B&W report asserts that ICS actions have averted more trips than it has caused. Although this assertion is not pertinent and may be true, the data presented does not substantiate the assertion.

3.1.3 Power Supplies

The evaluation of power supply failures was very limited. Input power failure was listed as a failure but the effects of this failure remain unevaluated. Failures of power conditioning equipment internal to the ICS were not considered except for their potential contribution to "high" or "low" failures or single internal ICS functions and single ICS output signals. B&W stated that power supply failures could not be considered in greater detail due to significant plant-to-plant design variations, the complexity of the failure modes and effects and the brief span of time allocated to the study. The report lists power supplies as a subject for additional study. Appendix B of this review is a synopsis of some of the power supply problems which led to a plant upset which involved the ICS about 2 years ago at one of the B&W type plants.

3.1.4 Effect of Postulated Failures

From the limited effect evaluation, it is difficult to assess the need for further evaluation or potential design modifications. As an example, the FMEA describes the effect of a steam generator overfill as ". . . overcooling of the primary, and possible loss of pressurizer inventory and/or level indication."¹ The effects of the same transient were described in the summary of an NRC-B&W Operating Plant Licensees Meeting as "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."² Regardless of how appropriate either description is, in fact, the latter description would place a greater emphasis on the potential need for remedial action.

3.2 SYSTEM SIMULATION

In order to make an accurate assessment of the response of the plant to failures in the ICS, the best choice is a simulation of the plant capable of following the transient resulting from the prescribed failures. Such a simulation would require modules capable of producing the required response for the NSS, ICS, and BOP over a wide range of parameters. Although no such global simulation exists, simulators which encompass some combination of the three systems over a limited range of the parameters of interest are available.

The simulator chosen was POWER TRAIN IV which was adapted to the lower loop, once-through steam generator configuration. POWER TRAIN IV has all three systems, NSS, ICS, and BOP, modeled but has a restricted thermodynamic, fluid mechanic, heat transfer, and core power applicability range.

¹ ICS Reliability Study, page 4-33.

² Summary of Meeting Held on August 23, 1979, September 13, 1979, page 8.

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

It would be desirable to have a simulation tool with complete capability. However in the context of feasible state-of-the-art, POWER TRAIN IV is adequate. The obvious deficiencies will not greatly impact the overall results as reactor trip was the terminating point for the analysis. However, if more detailed evaluation of system effects is desired, it will become necessary to develop a more sophisticated system simulation tool.

3.3 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 was 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 by the Operating Experience section.

As shown in Figure 5.1 of the Operating Experience section, only 2% of the commercial operating plant trips were caused by internal ICS failures (excluding power supplies). Of the balance, one third were caused by operator technician errors and the remainder 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 producing trip.

The MTBF's for the ICS equipment are consistent with expectation for equipment of that generation (for both the 721 and the 820 series). The 820 series appears to be much more reliable than the 721. However, insufficient data exist for the apparent large differences to be statistically significant. The operating data indicate relatively low probability of ICS failure. However, these data should not be interpreted as providing great insight into the plants sensitivity to ICS actions.

4.0 EVALUATION AND RECOMMENDATIONS

Operating Experience

Reliance on the ICS or automatic control in general to regulate feedwater and other plant parameters is not a shortcoming as might have been inferred by current suspicion of the ICS, but rather is a significant asset to plant safety and availability. That the system does not perform perfectly in all situations or may induce plant upsets when it fails is only to be expected. We should be careful to focus criticism only on the deficiencies and not on 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 by responding to real or unreal plant conditions, can alter plant operation in undesirable ways. However, any other effective control system, including good and bad operators, can also do this. Feedwater pumps and valves are manipulated, bypass and atmospheric dump valves can be misoperated, control modes may be improperly altered, loop balances can be upset, and many other anomalies can be caused or exacerbated by the ICS. This is not surprising, nor is it 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 challenge to the PPS than other control systems of similar scopes, 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 or 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 quite difficult. Examination of the failure statistics in the 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 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 Plant Protection System and that many potential failures would be mitigated by the control systems cross checking features without challenging protection. It is contended by the manufacturer, and we agree, that the system prevents or mitigates many more upsets than it creates and is generally superior to manual or fragmented control schemes. Performance deficiencies which have been suggested mostly relate to the ability or inability of the system to deal with major operational upsets,

1/16/68

add

maneuvering through different plant modes as from hot standby to low power and component problems such as valve leakage or pump response. These performance characteristics are not the subject of BAW-1564 and hence are not emphasized in this review. In the course of this review a broader scope of system performance was investigated to a limited extent and 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 turbine trip and other anticipated transients.
2. Development of an appropriate full plant simulator to evaluate the interaction of primary, secondary, and control systems. This suggestion is beyond the scope of the B&W effort and is a generic problem implying need for NRC sponsorship. The simulator would have to be an advancement over current tools to 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 current views of operational upsets to be covered.

Failure Modes and Effects Analysis

Our evaluation of the FMEA as performed and reported in BAW-1564 suggests several concerns and recommendations for future investigation.

1. As discussed in Section 2.0 of this review, the functional block FMEA approach may have been selected as an economic expedient and may not be the optimum technique for deriving the information desired. If further pursuit of the failure consequences of the ICS is desired we would 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 interfaces, such as the Non-Nuclear Instrumentation and its power and signal sources. In particular, the analysis should have consideration of mid-scale failures, and off-normal initial conditions. It is not evident that re-doing 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 and should be evaluated in detail with specific recommendations for upgrade as necessary.
4. The simulation tools used in these studies possess deficiencies of dynamic range and component detail. Nonetheless, they served a useful purpose and it is our opinion that more detailed analyses would not provide significantly more enlightening? information for purpose of the FMEA.

Comments On B&W Recommendations

1. ICS Related

- a. NNI/ICS power supply reliability: We concur fully that this is an area in need of attention. The problem goes somewhat beyond supply reliability per se. While our investigation of this subject has not been comprehensive, there appear to be problems of system arrangement and channeling and selecting of input signals which are in need of improvement. In at least two plants a single power supply failure can result in loss of virtually all signals to the

ICS. Since these arrangements are plant specific, individual attention by plants is indicated. More detail on this subject is included in Appendix B.

- b. Reliability of input signals from the NI/RPS system to the ICS- specifically, the RC flow signal.

The background for this recommendation is not presented. We concur that this subject deserves attention from the same considerations as recommendation a above.

- c. ICS/BOP system tuning, particularly feedwater condensate systems and the ICS controls.

This concern may be broader than tuning. We believe that the dynamic performance of the systems should be studied carefully in relation to the total plant response. This should include the effects of control limitations such as valve and pump speed response on plant stability. Considering the tight coupling between the secondary system controlled by the ICS and the primary system with its important considerations of pressure and pressurizer level, expanding the control features of the ICS to the primary may be worthy of investigation as a potential control improvement.

2. Balance of Plant

- a. Main feedwater pump turbine drive minimum speed control - to prevent loss of main feedwater or loss of indication of main feedwater.
- b. A means to prevent or mitigate the consequences of a stuck-open main feedwater startup valve.
- c. A means to prevent or mitigate the consequences of a stuck-open turbine bypass valve.

B
a
A

*

APPENDIX A

Questions and Responses

After a preliminary review of BAW-1564, a number of questions were submitted to B&W with the intent of obtaining expansion and clarification of information presented in the report and to obtain some information not contained in the report which may be germane to the review. B&W invited the reviewers and NPC staff members to their facilities in Lynchburg, Virginia to hear their response to the questions. Toledo Edison and Duke Power Companies were represented at the meeting held October 23, 1979.

The questions and the reviewers' interpretation of the responses are described below. Some additional interpretations and observations of the reviewers are included which resulted from the discussions of the questions.

Question 1. There may be a significant difference between failure modes or conditions with an FMEA based on functional block diagrams rather than equipment block diagrams. Have the functional failure assumptions been compared with actual equipment failure modes to assure that they are realistic and meaningful?

Response 1. B&W indicated that the functional block diagrams were used rather than equipment diagrams in order to reduce the scope of the effort and allow the analysis to be accomplished in the requested time frame. B&W has stated in the report and in discussions that they believe that the functional approach is adequate and that very few observations would be in error as a result of this choice.

Comment: An example of a possibly incorrect or incomplete conclusion arising from the approach is that Turbine Bypass Valve control failure considerations do not include in detail whether condenser cooling is

available and whether control will be transferred to condenser dump or atmospheric dump. Also not considered is operator response or interference/interaction. This example was selected because the recommendations of the report include additional analysis of bypass valve failure.

Question 2. The ICS signal input failure assumptions appear to be all either "high" or "low" with some attempt to identify the "worst case." Some of the operable plants under review have the potential for mid-scale failures. There is reason to believe that some mid-scale failures may be worse than high or low failures, as experienced by the plant selected as typical, Rancho Seco. Are there plans for including mid-scale failures in the analysis and how is the validity of the analysis compromised by not including mid-scale failures?

Response 2. Mid-scale and multiple input signal failures are considered by B&W to be either outside the boundaries of the ICS or outside the scope of the review as determined by B&W. B&W considers the high or low signal assumptions to be the worst case for single failures.

Comment. 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 single failure of an NNI power failure or power failure in the input signal selection circuitry. An example of just such a failure, which should certainly be worthy of consideration, is the Rancho Seco event of March 20, 1978. The decision of B&W not to include consideration of failures beyond the actual ICS cabinet terminals we believe to be a serious shortcoming of the analysis, especially in light of the considerable operating experience indicating low power supply reliability. B&W recommends further analysis of ICS and NNI power supplies based on this operating experience.

Question 3. Virtually all of the events/failures considered in the analysis appear to be based on "normal" conditions wherein all plant equipment is functioning at nominal design points. Our limited information regarding 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 running; one instead of two feedwater pumps running; one or more hand/automatic stations in manual; etc. Since these seem to be the more significant initial conditions for unsatisfactory ICS performance, how is their omission justified? Are any of these "interesting" events analyzed but unreported?

Response 3. B&W contends that they did not miss any significant transients or protective system challenges by not including off-normal initial conditions. They also indicated that no unreported analyses have been performed from off-normal conditions.

Comment. Since B&W did not themselves confirm this contention, we find it difficult to support. Our own limited evaluation of plant events involving the ICS is that the majority of these events have 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 the assertion.

Question 4. 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?

Response 4. The effects were evaluated by knowledgeable people with plant experience.

Question 5. The POWER TRAIN code obviously has limitations to its 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 is valid or invalid for each of the individual plants and their differences, especially feedwater systems.
- e) Does the simulation have capability for dealing with off-normal operation such as three primary pumps or partial manual operation?

Response 5. Power Train IV was used in about 75% of the cases to evaluate the effects on the NSS along with supplemental "engineering judgement." Power Train IV has the following features: 2 Steam Generators modelled in continuous space, discrete time; steam lines; Feedwater pumps; Feedwater heaters; Condenser; Pressurizer; Turbine dynamics; Valves. The primary system includes pump characteristics programmed from other codes as a table and appropriate transport lags (~ 10 seconds). Pressurizer modelling includes the effects of surge flows, spray flows, internal flows with condensation and flashing, heaters, 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	1500 - 3000 psi
Secondary Pressure	500 - 1500 psi

Temperature (Pri. & Sec.)	400 - 700 °F
Feedwater Temperature	350 - 700 °F

The hybrid model uses two EAI-680 analog and one CDC-1700 digital computers. 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 modelled. Turbine trip is the transient used to check the code with plant data. The validity of the comparison is judgemental. The model is not valid at low powers.

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

Question 6. 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 supposed. This may be outside the scope of the NRC request, but the ICS feedwater systems interactions evidenced in operating plants indicate this may be of valid concern. Have the design problems and component limitations associated with expected normal operation been analyzed and documented? Are these analyses available?

Response 6. B&W currently has no strong motivation to improve the performance of the ICS. Their utility customers have no significant unresolved complaints about the ICS. Subsequent discussions with three plant owners confirm this acceptance.

Question 7. Is there any connection, physical or phenomenological, between RPS sensors and ICS inputs? Which common signals, if any, initiate trip and what is the potential for common signal or signal conditioning failures initiating a plant transient through the ICS requiring RPS response derived from that signal.

Response 7. Reactor Protection System signals are used by the ICS with suitable buffering. Adequate redundancy is provided in the RPS to satisfy the requirements of IEEE-279.

Question 8. FMEA categories for "causes", "detection", "propagation potential" would yield helpful information. Has this type information been generated and is it available?

Response 8. Identification of component causes was 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.

Question 9. 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?

Response 9. Power supply reliability is a problem for the customers to resolve. It is a recognized problem which needs to be resolved on a plant by plant basis. This is one of the principal recommendations of the report.

Question 10. A significant number of trips appear to have occurred when portions of the system were in manual. What fraction of time is it estimated that control stations are in manual, and what are the

problems associated with this mode of operation of the ICS?

Response 10. No data available on "manual" operation. Manual modes are judged to be used most for startup and testing. The ICS is not designed to deal with many abnormal situations (eg. odd equipment alignment).

Question 11. How does historical failure data on ICS 721 and 820 compare with predictions based on nominal behavior? Is there any evidence of accelerated failure?

Response 11. Some "burn-in" failure rate was experienced, but has leveled off. The long term failure rate remains level. TMI-1 and Oconee 1, 2, 3 are 721 models. All others are 820 models.

Question 12. Multiple failures are not treated although it is acknowledged by B&W that many failures are not annunciated and therefore may exist until other failures occur, resulting in effective multiple failures. It appears that multiple failure situations may have 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 and producing the results requested?

Response 12. The amount of effort required to conduct a Fault Tree analysis was considered excessive. The FMEA report addresses those failures considered to be "important."

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

Question 13. The analysis does not include information to substantiate the recommendation that improvement is needed in power supplies, signal selection and signal reliability. Please supply the analysis or information which lead to this recommendation. In particular, does B&W have specific recommendations to improve the failure tolerance of the ICS?

Response 13. No additional data is available.

Question 14. Operating experience reports and oral information not included in the analysis suggest the ICS and/or the BOP system including the OTSG is 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?

Response 14. 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.

Question 15. 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 non-standard 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?

Response 15. Most problems occur due to maintenance, testing, or equipment problems which require manual conditions. The system also is not designed for fully automatic startup.

APPENDIX B

Power Supply Considerations

Non-Nuclear Instrumentation Power Supply

The Rancho Seco reactor transient of March 20, 1978 resulted from unpredicted behavior of a Non-nuclear instrumentation power supply designated NNI-Y. A similar supply, NNI-X, continued to function and was not involved in the transient. Both NNI-X and NNI-Y are powered normally from a 120 vac vital power bus (class 1E) with automatic transfer to a non-vital bus in the event of vital bus failure. During the transient an automatic transfer occurred, but was apparently spurious, because the vital bus did not fail. Neither of the NNI systems is considered vital, even though they are powered from a vital bus for higher reliability. Some NNI-Y loads require 120 vac and are powered directly from the vital or alternate bus, but most require plus and/or minus 24 volts dc and are powered from a complex of four dc power supplies. Two of the supplies are auctioneered to produce +24 vdc and the other two to produce -24 vdc. All of the individual outputs and the auctioneered buses are monitored for undervoltage. If any individual voltage drops below 22 v an alarm is given in the control room. If either auctioneered bus drops below 22 v the 120 vac to all four supplies is interrupted by protective relays S1 and S2. Each individual supply is rated for 5 amperes and is current limited to 7 amperes under short circuit conditions. With the auctioneering arrangement, a short circuit on an auctioneered bus would be limited to 14 amperes. In addition, each supply is equipped with a crowbar circuit so that if the output voltage were to increase to 27 vdc, a short circuit would be imposed and the fault would be detected as an undervoltage alarm.

Each of the branch circuits supplied from the +24 and -24 vdc buses is individually fused at 5 amperes. It is not clear in this power supply scheme which protective feature is intended to protect which component from which difficulty. For example, it is not clear what the current limiting feature is intended to accomplish. If the current limiting is intended to protect the power supplies themselves, then it is not clear why the branch fuses are required. Conversely, if the branch fuses are intended to protect the power supplies, then it appears the current limiting feature is not needed. The two protective features together are somewhat self-defeating. The composite load on the supplies through the several branches is apparently high enough so that if a fault occurs on one branch, then, through the current limiting feature, the output voltage is reduced to the point that the current through the faulted branch may not exceed 5 amperes to blow the fuse, and the fuse does not provide the intended protection. Similarly, it is not clear whether the undervoltage monitoring feature is intended to protect the power supplies or whether it is intended to protect the supplied loads from incorrect voltage. If the undervoltage trip feature is intended to protect the loads from non-specified voltages, it is not clear this is effective because of the possible failure modes of the supplied instruments. A number of the instruments on these buses fail to mid-scale on loss of power and give no obvious indication to the operator that they have failed. From the operator's viewpoint, a partial failure or incorrect supply voltage may give a more positive indication of trouble than total supply failure. The instrument indications are ambiguous in either case. Some recommendations for improvement have been proposed by the Rancho Seco Transient Investigating Committee of the Sacramento Municipal Utility District (SMUD). One of the recommendations of this

committee is to re-size the branch fuses (presently all 5 amperes regardless of load) to values only slightly larger than the branch loads so that they would have a better chance of providing the intended protection. This proposal appears to overlook the basic incompatibility between current limiting and fusing. In our opinion, either the current limiting or the fusing should be deleted from the system in order that one or the other of the protective features can be fully effective. It is our recommendation that the current limiting feature be deleted in favor of fusing at the power supplies and in the branch circuits. It is also recommended that the function of the undervoltage trip be reviewed to determine its intended purpose and need. The alarm features are certainly desirable to alert the operators to failures. The rationale for tripping all voltage sources when one fails or is faulted is not clear to us. Since all instruments may not require all voltages supplied, there may be some advantage to tripping only the faulted supplies.

In our estimation, the SMUD recommendations may not have addressed the critical point or malperformance of the power supply complex; in particular, the conflict of performance between the current limiting and fused branches in conjunction with the undervoltage monitoring. It is our recommendation that the system modifications be approached with the following considerations:

- a. Determine if the undervoltage monitoring is designed to protect the load instruments of the power supplies. If it is intended to protect the power supplies, then a different form of protection may be appropriate. The usual over-current breakers or fuses might be used, for example. On the other hand if this feature is intended to protect the validity of information from the supplied instruments, then this function should be

reevaluated based on the failure modes of the instruments upon loss of power. Partial failure may be preferred to the total failure imposed by the undervoltage tripping of S1 and S2.

b. At one time the system separated relay loads from instrument loads by use of a separate, non-auctioneered supply. There may be several things to recommend this original arrangement, including consideration of failure modes and the possibility of noise transients generated by the relays. A more important consideration, in our view, is the arrangement of the relays which are used for instrument switching. Several of the relays are used to select either a principal or alternate instrument channel supplying signal to the Integrated Control System (ICS). The relays are arranged, one per instrument channel, so that the particular relay associated with a channel must be energized to complete the signal path to the ICS. A normally-closed contact of the relay is used to prevent the connection of the alternate instrument signal when one is already selected. If both relays are deenergized (e.g. through loss of relay power) then neither signal will be connected to the ICS even though the ICS and all instrument channels may remain functional. A better arrangement with regard to this type of failure would be to use a single relay to select one of two redundant instrument signals. Energizing the relay would select one channel and deenergizing the relay would select the other. In this way, loss of relay power could result in a preferred selection and not loss of signal. Of course this arrangement would not be helpful if power is lost to the instruments as well as to the relays.

c. Perhaps a most important consideration in improving system reliability is related to the principle of "channelization." This is a coined term not dignified with a standardized definition, but nevertheless descriptive.

Handwritten signature/initials

If all the sensors, conditioners, buffers, switching and displays associated with a particular measurement are powered from the same source (e.g. NNI-Y) and the alternate or redundant measurement is powered from a separate independent source (NNI-X), and assuming some improvement in the switching logic as discussed in item b above, then the system would be relatively immune to even large-scale power interruptions. Needless to say, such principles are normally applied to protection systems and are not considered to be required in control systems. However, if one examines the complexity of the control system power supplies, it is apparent that the amount of equipment necessary to assemble a redundant, reliable system already exists and no increase in initial capital outlay would be required. Only a willingness to extend the principles used in PPS design to control systems is lacking. Some fringe benefits would be reduced challenge to the protection system resulting from reduced probability of control system failure and the economic and political benefits associated with better plant availability.

APPENDIX C

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:

 	<u>letter only</u>	
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	

*dup of
30 0222026
lp*

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

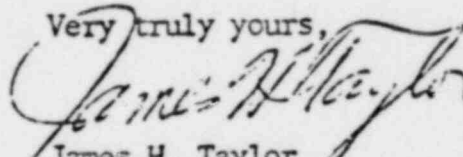
Subject: Integrated Control System Reliability Analysis

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)

*dupe of
 7908210296
 ZPP*

Babcock & Wilcox

B&W Owners Group TMI-2 SubcommitteeFPC

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)

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 System.

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/w1

cc: R. B. Borsum (BSW, Bethesda)

- bcc: E. R. Kane
- 1X. E. Suhrke
- R. E. Ham
- D. D. Fairbrother
- G. J. Brazill
- R. E. Wascher
- J. H. MacMillan

POOR ORIGINAL

DUPLICATE

*copy of 7905030352
411*

DUKE POWER COMPANY

POWER BUILDING

422 SOUTH CHURCH STREET, CHARLOTTE, N. C. 28242

WILLIAM G. PARKER, JR.
VICE PRESIDENT
STEAM PRODUCTION

August 31, 1979

TELEPHONE AREA 704
373-4093

Mr. Harold E. 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 anticipated 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 analysis 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.

POOR ORIGINAL



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

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.

POOR ORIGINAL


SMUD

SACRAMENTO MUNICIPAL UTILITY DISTRICT □ 6201 S Street, Box 15830, Sacramento, California 95813; (916) 452-3211

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.

POOR ORIGINAL



Docket No. 50-346

License No. NPF-3

Serial No. 538

August 31, 1979

LOWELL E. ROE

Vice President
Facilities Development
(419) 259-5242

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. 423) 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

LER/TJM

cc:

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

*dupe of
7909060201
2pp*

POOR ORIGINAL

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.

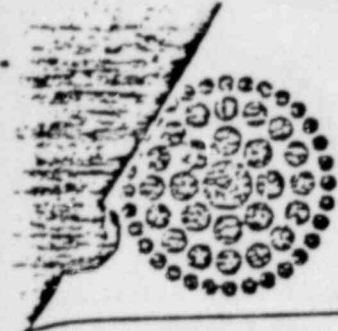
Item 1 - Failure Mode and Effects Analysis of the Integrated Control System (ICS)

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.

POOR ORIGINAL



**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, 5, 7, and 8, you requested Florida Power Corporation to provide additional information and our schedule for resolution of these five (5) items by August 31, 1979.

In that regard, Florida Power Corporation hereby submits, as Attachment 1 to this letter, our response to your August 21, 1979, request for additional information.

If you require further discussion concerning our response, please contact us.

Very truly yours,

FLORIDA POWER CORPORATION

G. C. Moore
G. C. Moore
Assistant Vice President
Power Production

*dup of 2002220225
3PP*

GCMekcF06(D5)

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 1, 1979.
B. Report will be submitted on September 20, 1979.
- 2) A. Report will be submitted on September 30, 1979.
B. In response to this request, we are proposing three (3) options in preference of order:
 - 1) Provide a statement by September 30, 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 ft² break with no AFW available.

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

Table 4-5. (Cont'd)

<u>MODULE NO.</u>	<u>MODULE NAME</u>	<u>FAILURE MODE</u>	<u>EFFECT ON NSS</u>	<u>REACTOR TRIP</u>	<u>REMARKS</u>
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.		

4-50

53

POOR ORIGINAL

Babcock & Wilcox