Docket File

MEETING SUMMARY DISTRIBUTION

SENT TO FOLLOWING LICENSEES:

Duke Power Company (Oconee 1,2and3)
Metropolitan Edison Company (TMI-1)
Florida Power Corporation (Crystal River 3)
Sacramento Municipal Utility District (Rancho Seco)
Arkansas Power & Light Company (ANO-1)
Toledo Edison Company (Davis-Besse 1)

Docket File
NRC PDR
L PDR
ORB#4 Rdg
NRR Rdg
H. Denton
E. G. Case

D. Eisenhut
R. Vollmer
W. Russell
B. Grimes
T. J. Carter
A. Schwencer
D. Ziemann
T. Ippolito
W. Gammill
L. Shao
J. Miller
AEOD

R. Reid
V. Noonan
P. Check
G. Lainas
G. Knighton
Project Manager
OELD
OI&E (3)
R. Ingram
R. Fraley, ACRS (16)
Program Support Branch
TERA
J. R. Buchanan
Meeting Summary File
NRC Participants - R. Satterfield
D. Thatcher
D. Ross
T. Novak
W. Kane
R. Capra
S. Israel
G. Mazetis
F. Ashe
J. Joyce
G. Kelly
M. Rubin
H. Silver
P. Matthews
B. Wilson
Z. Rosztoczy
P. Norian
B. Sheron
W. Jensen
S. Lewis
M. Mulkey
R. Hoefling

DEC 19 1979

Docket Nos.: 50-269, 270, 287
50-289, 50-302
50-312, 50-313
50-346

FACILITIES: Oconee Nuclear Station, Unit Nos. 1, 2 & 3 (Oconee)
Three Mile Island Nuclear Station, Unit No. 1 (TMI-1)
Crystal River Nuclear Generating Station, Unit No. 3 (CR-3)
Rancho Seco Nuclear Generating Station (Rancho Seco)
Arkansas Nuclear One, Unit No. 1 (ANO-1)
Davis-Besse Nuclear Power Station, Unit No. 1 (DB-1)

LICENSEES: Duke Power Company (DPCo)
Metropolitan Edison Company (Met-Ed)
Florida Power Corporation (FPC)
Sacramento Municipal Utility District (SMUD)
Arkansas Power & Light Company (AP&L)
Toledo Edison Company (TECo)

SUBJECT: SUMMARY OF MEETING HELD ON OCTOBER 23, 1979 WITH REPRESENTATIVES OF THE BABCOCK & WILCOX (B&W) OWNERS' GROUP, B&W AND OAK RIDGE NATIONAL LABORATORY TO DISCUSS THE "INTEGRATED CONTROL SYSTEM RELIABILITY ANALYSIS," (BAW-1564)

On October 23, 1979, members of the NRC staff (staff) and Oak Ridge National Laboratory (ORNL) and ORNL's consultants from Scientific Applications Incorporated (SAI), met with representatives of the B&W Owners' Group and B&W in Lynchburg, Virginia, to discuss the integrated control system (ICS). The reference document for the discussions was the B&W report BAW-1564 entitled "Integrated Control System Reliability Analysis," dated August 1979. During the ongoing review of this document, a set of questions was generated by ORNL/SAI which served as the meeting agenda. A copy of these questions is included as Enclosure 1. A list of attendees is provided as Enclosure 2.

BACKGROUND

As one of the long-term items of the Commission Orders of May 1979, the B&W licensees were required to submit a failure mode and effects analysis (FMEA) of the ICS. In response to this requirement, B&W submitted a generic report entitled "Integrated Control System Reliability Analysis," (BAW-1564). This report was endorsed by each of the B&W licensees as applicable to their facilities. The staff has obtained assistance in the review of this report from ORNL which, in turn, is utilizing members of SAI as subcontractors. This meeting was held to discuss the questions (Enclosure 1) prepared by ORNL and SAI based on their preliminary review of the report.

OFFICE						
SURNAME						
DATE						

8001040344

DISCUSSION

After introductory remarks by R. Finnin of B&W, R. Satterfield of NRC, and J. Anderson of ORNL, the meeting centered around a discussion of each of the questions listed in Enclosure 1. Part of the introduction was a description of the approach by ORNL/SAI to the review of the report. They stated the plan being used was to investigate what questions are answered by the report and define what questions may still have to be answered.

Specifically, ORNL/SAI's objectives will be to see if:

1. the concerns expressed by the NRC staff and ACRS have been addressed;

2. the technical content of the report is valid;

3. the conclusions are valid and useful;

4. design changes are required; and,

5. additional work should be done.

Question 1. "There may be a significant difference between failure modes or conditions with a 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: B&W expressed the opinion that the functional block approach was the most practical for the time frame and would indicate problem areas which could be developed on an equipment block basis, if necessary. They pointed out some examples where there was some follow through to the equipment failures, particularly with respect to the operating history section of the report. B&W believes it has found the "hard spots" in the ICS. These are presented in the report's conclusions and recommendations. Some discussion evolved concerning other areas which were being worked on by B&W, such as operator guidelines, particularly the Abnormal Transient Operating Guidelines (ATOG) program.

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: B&W emphasized that from a single input failure point of view the "high" or "low" were the worst cases. The failures referred to in the question were the result of multiple failures of inputs. However, as pointed out by ORNL, the multiple failure could be the result of a single power supply failure. The power supply area was highlighted as a particular concern in the report, however, this concern was based upon operating experience and not the FMEA section of the report. The FMEA as performed by B&W would not highlight these type failures because of the definition of the ICS boundary. There are presently no plans to include "mid-scale" failures.

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: B&W is of the opinion that studying of off-normal alignments would not lead to anything significant beyond what is in the report. B&W did point out that in many of the recent trips (CR-3 in particular) that the operators could have been more aware of new, post-TMI-2, reactor trip setpoints. It is B&W's opinion that these trips are operability problems not safety problems. ORNL agreed to some extent; however, while a reactor trip may be safe, it does represent a challenge to the control systems. If a control system cannot do a specific job, then there is a problem. B&W pointed to the experience that showed ICS prevented more trips than it caused.

Question 4. "What process was used to determine the "effect on the NSSS"? Neither the technique nor the justification is included in the analysis. What verification techniques were employed for the "effects" analysis?"

Response: Effects were evaluated by knowledgeable people with plant experience.

OFFICE ▶						
SURNAME ▶						
DATE ▶						

Question 5. "The POWER TRAIN code obviously has limitations to its ability to simulate the NSSS and BOP response. 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 simulaiton is valid or invalid for each of the indifidual 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: B&W pointed out that Power Train was used in about 75% of the cases; however, for post-trip cases, most of the information was developed from an engineering analysis. A general discussion of B&W's simulation followed.

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.

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: B&W explained that there is little motivation to spent a significant amount of time and money on the ICS because from plant availability there are other areas which offer more improvement. Their utility customers have no significant unresolved complaints about the ICS. There are internal B&W reports, "quick-look reports," on this subject; In addition, there is more formal work being done in the area of looking at customers' reactor trips.

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 conditioning failures initiating a plant transient through the ICS requiring RPS response derived from that signal."

Resonse: This discussion was the result of general concern with interaction between protection systems (RPS) and control systems (ICS). Based on the discussion and knowledge of B&W design, it was agreed that there is no apparent problem in this area. Although the report does not address this concern at all, RPS signals are used by the ICS with suitable buffering. Adequate redundancy is provided in the RPS to satisfy the requirements of IEEE-279.

DEC 19 1979

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

Response: Identification of component causes was not considered necessary. The categories used are based on IEEE Standard 352 The area of detection was not addressed and it was agreed that it may require a further look because of the fact that undetectable failures could exist for long periods of time and then single failures could lead to multiple failures.

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: Power supply failures were again discussed. According to B&W, further work is this area with the licensees is presently being considered. The FMEA scope did not extend to the power supplies such as those for the input instrumentaiton. Power supplied and their reliability is a problem for the customer which needs to be resolved on a plant by plant basis.

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: B&W stated that they could not analyze all combination of modes in this amount of time. We pointed out that we were asking for information to help determine which modes were more significant. Manual modes are judged to be used mostly for startup and testing.

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

Response: B&W pointed out that Oconee and TMI-1 were the plants with the 721 system. They discussed the burn-in failure rate and then the relatively constant failure rate subsequent to it.

OFFICE						
SURNAME						
DATE						

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: B&W has identified transients that have occurred, in the Operating History Section. Therefore, with respect to multiple failures the report has identified critical areas. Although this is true, an event tree of ICS may highlight other important multiple failures. This type analysis was considered to be too extensive for the time available.

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 led to this recommendation. In particular, does B&W have specific recommendations to improve the failure tolerance of the ICS?"

Response: B&W has noted that a number of events have been caused by power supply failures and other interface areas. The recommendations are based on these events and are in areas around the ICS boundary.

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: B&W explained that it is more than just ICS tuning, it is more a matter of plant tuning. If licensee complaints are experienced, more tuning may be a necessity. The area of pressurizer spray was also talked about as a way to maintain pressurizer level.

DEC 19 1979

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: Most problems occur due to maintenance, testing, or equipment problems which require manual conditions. B&W pointed out that this information should not be the sole basis for performing operator retraining. We really do not know the success rate since all we see are the unsuccessful ones. B&W is not presently investigating for these.

In addition to the questions discussed above, the following request for specific information was discussed:

1. Rancho Seco equipment block diagrams and logic diagrams. The staff should request these directly from SMUD.

2. Identification of differences in ICS design between Rancho Seco and each of the other 177FA plants. These design differences should be in the endorsement letters.

3. Identification in the FMEA of which "effects" resulted from POWER TRAIN (PT) simulation and which resulted from engineering judgement. Not pursued.

4. Information on how ICS interacts with feedwater oscillation. Real event date is particularly helpful. Real event data should come from the licensees.

5. In Table 4.4 of the report, what are specific indications to the operator display failures? The operator indications were discussed. B&W provided ICS outputs for annunciator and or computer indication.

6. What is the ICS design basis? B&W quoted the SAR Section 7.2.3.1.

7. PT-11 manual and QA File. This may be requested if the staff desires to pursue system simulation.

8. Identify the power levels at which trips occurred. A number of feedwater trips occurred around 40-50% power. This information should come from the licensees.

9. Event information on operator/technician induced trips. Need event reports.

10. Confidence levels on ICS MTBFs. A brief discussion on this topic was held.

OFFICE						
SURNAME						
DATE						

DEC 19 1979

CONCLUSION

The discussion of the report questions lead to the general conclusion that although the report appears to be accurate, it does not appear to go far enough. The B&W definition of the ICS and its boundaries tends to limit the analysis portion to relatively straight forward conclusions. However, the operating history section does indicate some of the more significant problems. It is expected that a draft report on the review of BAW-1564 will be forwarded to the NRC by ORNL in early December 1979 with a final report scheduled by the end of the year.

Original signed by:

D. Thatcher, Reactor Engineer
Systems Group
B&O Task Force
Office of Nuclear Reactor Regulation

cc: See attached sheets

OFFICE	B&O TF	B&O TF	ICSB	B&O TF		
SURNAME	RCapra:mjf	DThatcher	RSutterfield	WKane		
DATE	12/13/79	12/17/79	12/17/79	12/17/79		

ENCLOSURE 1

OAK RIDGE NATIONAL LABORATORY
OPERATED BY
UNION CARBIDE CORPORATION
NUCLEAR DIVISION

POST OFFICE BOX X
OAK RIDGE, TENNESSEE 37830

October 15, 1979

R. M. Satterfield, Chief
Instrumentation and Controls Systems Branch
Division of Systems Safety
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, DC 20555

Dear Sir:

Request for Supplemental Information:
Review of Integrated Control System Analysis
Report BAW 1564, August 1979

Review of the subject document is continuing and in the course of this review a number of questions have arisen concerning the techniques used and the results presented in the report, which we would like to have answered by B&W. In addition we have identified some subject areas in which we have not posed specific questions but would like to discuss with B&W so that we might better understand the bases and background of the information and recommendations presented. The questions and subject areas are attached.

We would like to propose that some of the ORNL and SAI staff members involved in the review visit the B&W facilities to discuss the information we seek. We believe that this would provide a more efficient exchange of information than correspondence, considering the short time allocated for this review. We request that you arrange such a meeting with B&W at your convenience.

Sincerely,

John L. Anderson
Reactor Systems Group
Instrumentation and Controls Division

JLA:cwl

cc: Director, Division of Systems Safety, NRC
Attn: B. L. Grenier
L. Beltracchi, NRC
R. Brodsky, DOE
S. J. Ditto
H. N. Hill
L. C. Oakes
F. R. Mynatt
J. R. Penland, SAI
R. S. Stone
B. Thatcher, NRC
D. B. Trauger

Questions Regarding Report BAW-1564,
Integrated Control System Reliability Analysis

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?

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?

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?

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?

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?

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?

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.

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

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?

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.

11. How does historical failure data on TCS 721 and 320 compare with predictions based on nominal behavior? Is there any evidence of accelerated failure?

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?

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?

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?

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?

SUBJECT AREAS AND SPECIFIC INFORMATION REQUESTED

* Rancho Seco equipment block diagrams and logic diagrams.

* Identification of difference in ICS between Rancho Seco and each of the other 177 FA plants.

* Identification in the FMEA of which "effects" resulted from POWER-TRAIN (PT) simulation and which resulted from engineering judgement.

* Any information on how ICS interacts with feedwater system oscillations. Any real event data would be particularly helpful.

* In Table 4.4, what are specific indications to operator for display failures?

* ICS design basis.

* PT-11 manual and QA file.

* Identification of power levels at which trips occurred.

* Event information on operator/technician induced trips.

* Confidence levels on ICS MTBFs.

Enclosure 2

ICS RELIABILITY ANALYSIS MEETING

OCTOBER 23, 1979

Ron Finnin	B&W
Art McBride	SAI
J. R. Penland	SAI
John Cole	Duke
Ron Brown	Duke
L. L. Veyner	B&W
Bob Hamm	Consumers Power Company
Larry Stalter	Toledo Edison
Gary Bennett	B&W
Stephen Ditto	ORNL
John Anderson	ORNL
Rod Satterfield	NRC
Dale Thatcher	NRC
J. D. Carlson	B&W
C. W. Cornell	B&W

Mr. William O. Parker Jr.
Vice President - Steam Production
Duke Power Company
P.O. Box 2178
422 South Church Street
Charlotte, North Carolina 28242

Mr. William Cavanaugh, III
Vice President, Generation
and Construction
Arkansas Power & Light Company
Little Rock, Arkansas 72203

Mr. J. J. Mattimoe
Assistant General Manager and
Chief Engineer
Sacramento Municipal Utility District
6201 S Street
P.O. Box15830
Sacramento, California 95813

Mr. Lowell E. Roe
Vice President, Facilities Development
Toledo Edison Company
Edison Plaza
300 Madison Avenue
Toledo, Ohio 43652

Mr. W. P. Stewart
Manager, Nuclear Operations
Florida Power Corporation

P.O. Box 14042, Mail Stop C-4
St. Petersburg, Florida 3 3733

Mr. R. C. Arnold
Senior Vice President
Metropolitan Edison Company

Parsippany, New Jersey 07054

- -

Mr. James H. Taylor
Manager, Licensing
Babcock & Wilcox Company
Power Generation Group
P.O. Box 1260
Lynchburg, Virginia 24505