UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

- - - - - - - - - - - - - - - - - - -x

In the matter of: :

METROPOLITAN EDISON COMPANY : Docket No. 50-289 (Restart)

(Three Mile Island Unit 1) :

- - - - - - - - - - - - - - - - - - :

25 North Court Street,
Harrisburg, Pennsylvania

Tuesday, December 2, 1980

Evidentiary hearing in the above-entitled matter was resumed, pursuant to adjournment, at 10:10 a.m.

BEFORE:

IVAN W. SMITH, Esq., Chairman,
Atomic Safety and Licensing Board

DR. WALTER H. JORDAN, Member

DR. LINDA W. LITTLE, Member

Also present on behalf of the Board:

MS. DORIS MORAN,
Clerk to the Board

APPEARANCES:

On behalf of the Licensee, Metropolitan Edison Company:

GEORGE F. TROWBRIDGE, Esq.
THOMAS A. BAXTER, Esq.
Shaw, Pittman, Potts and Trowbridge,
1800 M Street, N.W.,
Washington, D. C.

8012120444 T

On behalf of the Commonwealth of Pennsylvania:

ROBERT ADLER, Esq.
Assistant Attorney General,
505 Executive House,
Harrisburg, Pennsylvania
WILLIAM DORNSIFE,
Nuclear Engineer

On behalf of the Regulatory Staff:

JAMES TOURTELLOTTE, Esq.
JAMES M. CUTCHIN, IV, Esq.
Office of Executive Legal Director,
United States Nuclear Regulatory Commission,
Washington, D. C.

Petitioners for leave to intervene pro se:

STEVEN C. SHOLLY,
304 South Market Street,
Mechanicsville, Pennsylvania

C O N T E N T S

EXHIBITS

P R O C E E D I N G S

CHAIRMAN SMITH: Mr. Tourtellotte, I would like to make an announcement. We have with us this morning Mr. Ernest Hill, who is a nuclear engineer with the Lawrence-Livermore National Laboratory. Mr. Hill has been a member of the Atomic Safety and Licensing Board Panel since the early '70s, as I understand it, and he is here perhaps for the first time in an NRC adjudicative hearing, under a new provision of our rules of practice, 10 CFR 2.722, which was published in the Federal Register, 45 Fed. Reg. 62027, approximately August or September of this year. Section 6.722(b) is the section we are relying upon. That permits a presiding officer, the Board in this case, at its discretion, to call upon a member of the Atomic Safety and Licensing Board panel before the hearing to seek advice on complex matters.

In particular, in this case, Mr. Hill has been advising Dr. Jordan or will be advising Dr. Jordan as to questions to be asked witnesses to satisfy the Board's interest in certain subject matters.

There is no special significance about Mr. Hill's presence this morning, Mr. Sholly. It just happened to be he came here at this time to consult with Dr. Jordan, and there is nothing about your Contention that in itself requires his presence.

The new rule has two sections to it. The first section permits a rather wide range of consultation with other panel members. The second section, Subsection (b), is the one that we are employing. Mr. Hill's participation will be limited to advising the Board as to questions that might be asked of witnesses. We do not seek any recommendations from Mr. Hill on the resolution of issues, on findings of fact, or any of the factual issues to be resolved in this proceeding. It is merely to suggest to Dr. Jordan how he might develop the record for his purposes at this time.

Mr. Tourtellotte.

MR. TOURTELLOTTE: A couple of preliminary matters. One, the SER on management did issue and was sent out last week. Tomorrow we will have members of the staff here. As I recall, we agreed upon December 3 at 9:00 o'clock. We will have members of the staff here to go through that SER with interested parties and the Board and give a broad brush explanation of what is in the SER, and I recall that at the end of that meeting, the Board was going to establish some time, perhaps the following week, when we would get together and have an informal discovery session as we did in the emergency planning.

CHAIRMAN SMITH: I believe that we have already established that by Board order. I will check it during the next recess, but I am fairly certain that we have already done that.

MR. TOURTELLOTTE: That may well be. It is sort of fuzzy in my mind as to whether we did or whether we didn't. At any rate, that will be coming up tomorrow.

And the other thing I wanted to mention was the pieces of testimony which I indicated would not be filed on time yesterday dealt with three areas of Class 9 accidents, inadadequate core cooling, and control room design. The staff actually did file some papers yesterday, and the papers include responsive testimony we believe to UCS 13 on Class 9 accidents.

With respect to inadequate core cooling and control room design, there is also testimony or pieces of paper, maybe, I guess, partial testimony or a status report, if you will, of the other two items.

So, those, we had hoped we would have copies for you this morning, but they are on their way up and will not be here until afternoon. So in addition to serving them through the mail, we will provide both the Board and the parties present with copies of what we did file yesterday.

CHAIRMAN SMITH: Mr. Sholly, before we proceed in taking evidence, would you give a report on the substance of our telephone conversation yesterday with respect to -- well, first, Mr. Sholly called to forewarn us as to which documents would be needed so we would have them ready in the cross examination of the witnesses, and he also reported his conversations with Dr. Johnsrud of ECNP, so could you -- do you have any additional information? Could you give us an up to date report on that, Mr. Sholly?

MR. SHOLLY: I discussed it with Mr. Baxter and Mr. Cutchin this morning and told them essentially what I told you yesterday. If you want, I can repeat it.

CHAIRMAN SMITH: You have nothing new? Essentially you stated that Dr. Johnsrud is not well and does not know when she is going to be able to appear at the hearing.

MR. SHOLLY: I plan on calling her at lunch today and checking up and seeing what the status is.

CHAIRMAN SMITH: And you are prepared to proceed as lead Intervenor on the computer Contention.

MR. SHOLLY: That is correct.

CHAIRMAN SMITH: What is the remaining Contention that you have in common?

MR. SHOLLY: The in-plant instrumentation ranges.

CHAIRMAN SMITH: That is still unsettled?

MR. SHOLLY: Yes. I hope to resolve that at lunch.

CHAIRMAN SMITH: Okay.

MR. CUTCHIN: Mr. Chairman, while we are discussing this subject, we have, I understand, a status report on Dr. Johnsrud's health, but I have heard nothing with respect to Dr. Kepford's availability or non-availability.

CHAIRMAN SMITH: I do not think it is Mr. Sholly's responsibility.

MR. CUTCHIN: I realize that, sir, but I wonder if we are going to have the schedule turn on the availability of one or the other, and we might ask Mr. Sholly, if we are checking on that, to find out the status of the other participant for ECNP as well.

CHAIRMAN SMITH: You might recall, Mr. Cutchin, when the Board issued its memorandum and order with respect to dismissing some of ECNP's Contentions I believe it was this year, we noted that ECNP had not only Dr. Johnsrud but Dr. Kepford, Dr. Lockstead, and the gentleman that lives over in the vicinity of Peachbottom who is a technically trained person, plus other people.

The Board is not in a position to rule whether Dr. Johnsrud's health will affect the schedule. There is no use moving on things we don't have to. We have plenty to rule on, but we are aware that there are problems there, and we will be sensitive to the problems.

MR. CUTCHIN: Thank you, sir.

CHAIRMAN SMITH: Anything further preliminarily before we begin with the witnesses?

MR. ROBERT ADLER: Yes, Mr. Chairman. I have a matter that is preliminary to Sholly 6A. I wanted to inquire of the NRC staff whether any progress had been made in the area of obtaining testimony from Mr. Basdekas. There appears to be some connection between his concerns and ICS.

MR. CUTCHIN: Mr. Chairman, would you like me to address that again?

CHAIRMAN SMITH: Yes, you can respond.

MR. CUTCHIN: Perhaps Mr. Adler does not recollect, or I don't even remember whether he was here when I handed out the papers that Mr. Basdekas had made available and which we served on the parties and participants. The staff has no intention to offer Mr. Basdekas as a witness, and my understanding of the way it was left was that the Board would decide if it wanted to call Mr. Basdekas, and UCS, through Ms. Weiss, had asked if there were any objections to UCS' interviewing or meeting with Mr. Basdekas, and the staff had no objection, nor do I remember did the Licensee, but I have heard nothing further since those last conversations.

CHAIRMAN SMITH: Right. The Board had indicated it was going to defer its decision on whether we should bring -- whether and to what extent we should bring out Mr. Basdekas' point of view until after UCS had an opportunity to interview him and make recommendations.

However, I want to make it clear that as far as the Board is concerned, you certainly too should have access to Mr. Pasdekas and determine in advance if you wish what your interest may be in his information.

MR. ROBERT ADLER: Okay. My main purpose in raising it this morning was that there seems to be a relationship to ICS and there may be some perceived deficiency in the testimony as a result of that.

DR. JORDAN: I think you are quite correct in your observation. However, I believe there is a Contention that comes up later concerning the interaction of the safety systems with the non-safety systems which is really directly pointed toward Mr. Pasdekas' concerns.

So I think if we are going to have him here, that time would probably be the best time.

MR. BAXTER: I would note, Dr. Jordan, that is not very far away. That could be late this week or early next week.

CHAIRMAN SMITH: Anything further?

(No response.)

Whereupon,

T. GARY BROUGHTON,

was recalled as a witness by counsel for Licensee Metropolitan Edison, and having been previously duly sworn by the Chairman, was examined and testified as follows:

and Whereupon,

GERALD J. SADAUSKAS and LUTHER L. JOYNER,

called as witnesses by counsel for Licensee Metropolitan Edison, having been first duly sworn by the Chairman, were examined and testified as follows:

DIRECT EXAMINATION

BY MR. BAXTER:

Q Gentlemen, going from left to right, would each of you state your name, position and place of employment?

A (WITNESS SADAUSKAS) My name is Jerry Sadauskas. I am supervising instrumentation engineer for General Public Utilities Corporation.

A (WITNESS BROUGHTON) T. Gary Broughton. I am the control safety analysis manager for General Public Utilities.

A (WITNESS JOYNER) My name is Luther Joyner. I am a principal engineer with Babcock and Wilcox in Lynchburg.

Q I note my advice to you earlier may not be necessary as a result of the adjustments that have been made over the last weekend.

DR. JORDAN: Mainly, speak clearly.

BY MR. BAXTER: (Resuming)

Q I would like to call your attention to a document bearing the caption of this proceeding, dated September 15, 1980 entitled Licensee's Testimony of T. Gary Broughton, Gerald J. Sadauskas and Luther L. Joyner in response to

Sholly Contention No. 6A (Integrated Control System.).

Does the material associated with your name, including the attached statement of qualifications, represent testimony prepared by you or under your direct supervision for presentation at this hearing, Mr. Sadauskas?

A (WITNESS SADAUSKAS) Yes, it does.

Q Mr. Broughton?

A (WITNESS BROUGHTON) Yes.

Q Mr. Joyner?

A (WITNESS JOYNER) Yes, it does.

Q Do you have any changes or corrections to make to your testimony?

Mr. Sadauskas?

A (WITNESS SADAUSKAS) No, I do not.

Q Mr. Broughton?

A (WITNESS BROUGHTON) No.

Q Mr. Joyner?

A (WITNESS JOYNER) I have a minor change on my statement of qualifications.

Q Okay, would you point that out, please?

A (WITNESS JOYNER) Yes. Under the experience portion, second paragraph, it states I was a supervisory engineer, instrumentation and controls unit, maritime reactors. The dates should be 1972 to '76.

And in the next paragraph, program manager, product development section, the dates should be 1976 to '77.

That is the only correction required.

Q Is the testimony, Mr. Sadauskas, that you offered true and correct to the best of your knowledge and belief?

A (WITNESS SADAUSKAS) Yes, it is.

Q Mr. Broughton?

A (WITNESS BROUGHTON) Yes.

Q Mr. Joyner, as amended, is your testimony true and accurate to the best of your knowledge?

A (WITNESS JOYNER) Yes.

MR. BAXTER: Mr. Chairman, I move the receipt into evidence of the testimony and ask that it be physically incorporated into the transcript as if read.

CHAIRMAN SMITH: Seeing no objections, we will receive the testimony.

(The written direct testimony of T. Gary Broughton, Gerald J. Sadauskas and Luther L. Joyner follows:)

LIC 9/15/80

UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION

BEFORE THE ATOMIC SAFETY AND LICENSING BOARD

In the Matter of	)	
	)	
METROPOLITAN EDISON COMPANY	)	Docket No. 50-289
	)	(Restart)
(Three Mile Island Nuclear Station, Unit No. 1)	)	
	)	

LICENSEE'S TESTIMONY OF

T. GARY BROUGHTON, GERALD J. SADAUSKAS

AND LUTHER L. JOYNER

IN RESPONSE TO

SHOLLY CONTENTION NO. 6(a)

(INTEGRATED CONTROL SYSTEM)

OUTLINE

The purposes and objectives of this testimony are to respond to Sholly Contention 6(a), which asserts that prior to continued operation of TMI-1, a failure modes and effects analysis (FMEA) of the Integrated Control System (ICS) should be completed. The testimony shows that an ICS FMEA has been performed. The function and operation of the ICS are also described and the results of the ICS FMEA and complementary evaluations of field data from B&W operating plants are addressed.

INTRODUCTION

This testimony, by Mr. T. Gary Broughton, Control and Safety Analysis Manager, GPU; Mr. Gerlad J. Sadauskas, Group Leader, Instrumentation Engineering, GPU; and Dr. Luther L. Joyner, Principal Engineer, Power Systems and Controls Unit, Babcock & Wilcox Company, is addressed to the following contention:

SHCLLY CONTENTION NO. 6(a)

> It is contended that the short-term actions identified in the Commission's Order and Notice of Hearing dated 9 August 1979 are insufficient to provide the requisite reasonable assurance of operation without endangering public health and safety because they do not include the following items:
>
> a. Completion of a failure mode and effects analysis (FMEA) of the Integrated Control System.

RESPONSE TO SHOLLY CONTENTION NO. 6(a)

BY WITNESS JOYNER:

Sholly Contention 6(a) states that a failure modes and effects analysis (FMEA) of the Integrated Control System (ICS) should be completed prior to continued operation of TMI-1. Such an analysis has been performed.

The B&W ICS provides a coordinated response from the reactor/steam generator/turbine system during power operation see Figure 1. This results in a design which can readily respond to changes in demand for generated power and can accommodate various pertubations and maintain the unit in a stable power condition. During load changes or system upsets during power operation, the ICS applies signals to the major control variables (feedwater flow, steam pressure, reactor power and reactor coolant temperature) to achieve optimum overall plant response without challenge to the safety systems. The system is designed to provide automatic control during power operation, and to accept step load changes up to 10% and ramp load changes up to 5% rated power per minute. When load demand changes, the controls automatically adjust steam flow to the turbine and feedwater flow to the steam generators to maintain a constant steam pressure at the turbine throttle. Simultaneously, the system positions groups of regulating control rod assemblies to adjust reactor power and maintain a constant average coolant temperature over a load range of 15 to 100 percent power.

While the ICS was not involved in initiating the TMI-2 accident and subsequently functioned as designed, a detailed FMEA has been performed for the ICS - see Reference 1. The ICS FMEA determined the expected effects upon the B&W nuclear steam system from single failures of ICS inputs, outputs and internal modules. The analysis was complemented, as shown in Reference 1, with an evaluation of field data from all B&W operating plants, and a computer simulation to confirm the effects of various ICS failures on associated equipment.

The overall conclusion of the FMEA was the reactor core remains protected throughout any of the ICS failures studied. For those postulated ICS failures that could cause reactor trip, the safety systems operate independently of the ICS malfunction.

The overall conclusion from the operating experience evaluation was that ICS hardware performance has not led to a significant number of reactor trips. The ICS has prevented more reactor trips than it has caused and thus its net effect has been a reduction in the number of challenges to the Reactor Protection System.

BY WITNESSES BROUGHTON AND SADAUSKAS:

The B&W ICS FMEA was reviewed by GPU and found to be applicable to the TMI-1 ICS. The TMI-1 safety systems which would be actuated following ICS failures would operate independently of the ICS malfunction. The FMEA did not identify any changes required at TMI-1 to ensure the public health and safety. Implementation of the FMEA recommendations, which will result in improved reliability, improved control system performance and reduced consequences of malfunctions, is addressed in the TMI-1 Restart Report (Supplement 1, Part 3, Question 12).

BY WITNESSES BROUGHTON, SADAUSKAS AND JOYNER:

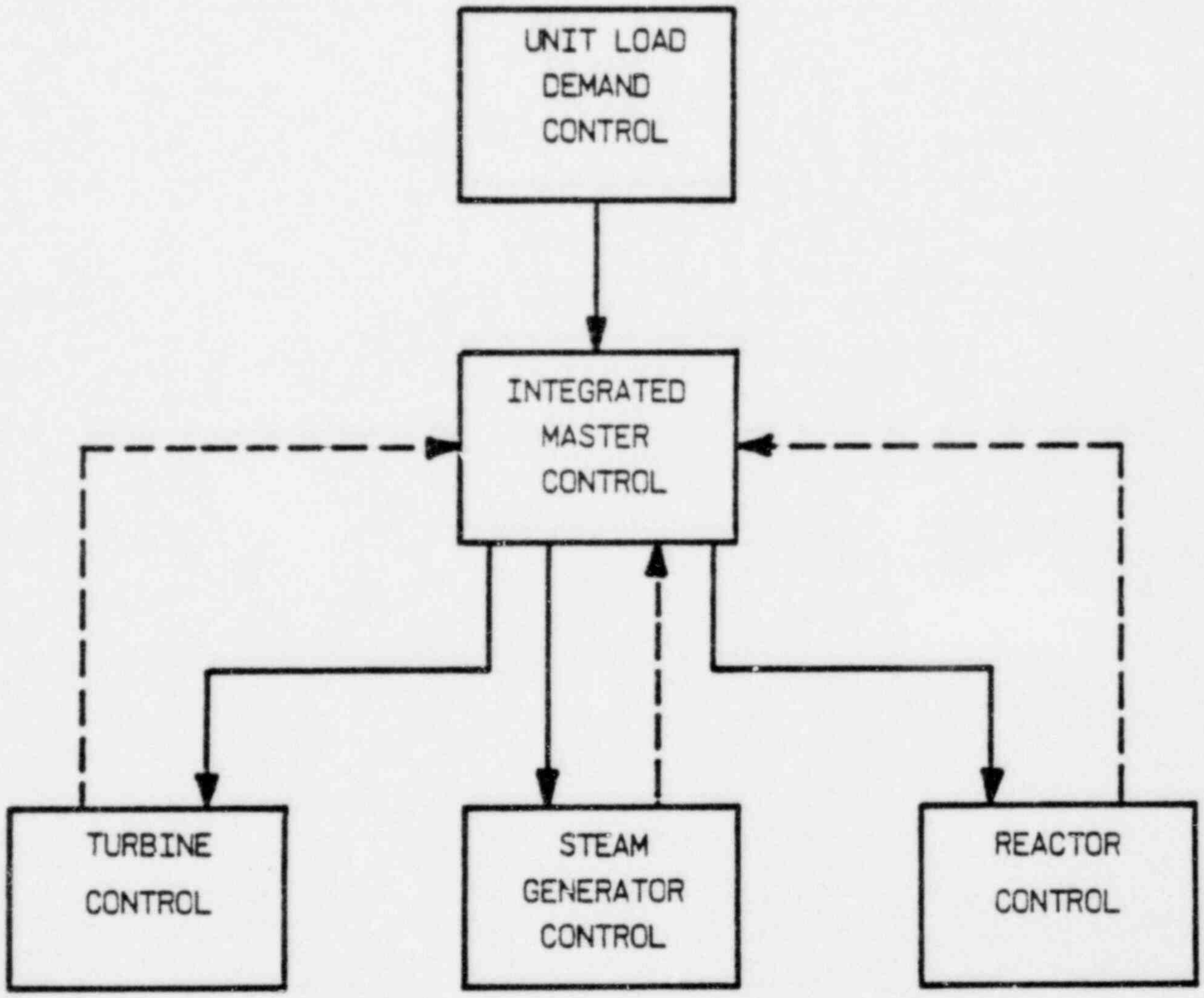
In summary with regard to Sholly Contention 6(a), an ICS FMEA has been completed.

Reference

1. Report BAW-1564, "Integrated Control System (ICS) Reliability Analysis," August, 1979.

FIGURE 1

INTEGRATED CONTROL SYSTEM



T. GARY BROUGHTON

Business Address: GPU Service Corporation
100 Interpace Parkway
Parsippany, New Jersey 07054

Education: B.A., Mathematics, Dartmouth College, 1966.

Experience: Control and Safety Analysis Manager, GPU Service Corporation, 1978 to present. Responsible for nuclear safety analysis and integrated thermal, hydraulic and control system analysis of nuclear and fossil plants. Supervised on-site technical support groups at Three Mile Island, Unit 2 during the post-accident period.

Safety and Licensing Engineer; Safety and Licensing Manager, GPU Service Corporation, 1976 to 1978. Performed and supervised nuclear licensing, environmental licensing and safety analysis for Oyster Creek, Three Mile Island and Forked River plants. Served as Technical Secretary to Oyster Creek and Three Mile Island General Office Review Boards.

Officer, U.S. Navy, 1966 to 1976. Trained at Naval Nuclear Power School, Prototype and Submarine School. Positions held include Nuclear Propulsion Plant Watch Supervisor, Instructor at D1G prototype plant and Engineering Officer aboard a fast-attack nuclear submarine.

Publications: EPRI CCM-5, RETRAN - A Program for One-Dimensional Transient Thermal-Hydraulic Analyses of Complex Fluid Flow Systems, Volume 4: Applications, December, 1978, Section 6.1, "Analysis of Rapid Cooldown Transient - Three Mile Island Unit 2", with N.G. Trikouros and J. F. Harrison.

"The Use of RETRAN to Evaluate Alternate Accident Scenarios at TMI-2", with N. G. Trikouros. Proceedings of the ANS/ENS Topical Meeting on Thermal Reactor Safety, April 1980, CONF-800403.

"A Real-Time Method for Analyzing Nuclear Power Plant Transients", with P.S. Walsh. ANS Transactions, Volume 34 TANSAD 34 1-899 (1980).

GERALD J. SADAUSKAS

Business Address: GPU Service Corporation
100 Interpace Parkway
Parsippany, New Jersey 07054

Education: A.A.S., Electrical Engineering, State University of New York at Farmingdale, 1963.
B.S., Electrical Engineering, C.W. Post College of Long Island University, 1970.
Post-graduate courses, Mechanical Engineering, State University of New York at Stony Brook, 1975 to 1977.
Post-graduate courses, Electrical Engineering, Stevens Institute of Technology, 1979 to present.

Experience: Group Leader, Instrumentation Engineering, GPU Service Corporation, 1980 to present. Responsible for establishment of instrument design criteria; preparation of conceptual designs, and verification of technical adequacy of designs; responsible for modifications of existing plant systems. The instrumentation section is also responsible for the measurement of all system parameters, signal conditioning, display and processing of system parameter information.

Senior Supervising Instrumentation and Control Engineer, Burns and Roe, Inc., 1977 to 1980. Responsibilities included implementation of TMI-2 lessons learned instrumentation requirements for the Oyster Creek and Rancho Seco nuclear power plants; was involved in the development of a Disturbance Analysis System for Nuclear Power Plants under contract with EPRI; involved in the development of an oxygen-hydrogen flame arrestor for BWR plants; served as Supervising Engineer for TMI-2 recovery, instrumentation and control systems; responsible for instrumentation and control engineering for the Forked River plant.

Instrumentation and Control Engineer, Long Island Lighting Company, 1971 to 1977. Duties included: responsible for the installation and startup of instrument and control systems at the Shoreham nuclear plant and at the Northport Unit 3 oil-fired plant; and, served as Construction Engineer for the Glenwood Landing switchyard.

Electrical Engineer, Chemical Construction Corporation, 1970 to 1971. Involved in installation of a CASO3 Venturi type flue gas scrubber at Boston Edison's Mystic Station. Designed potential electrical power and control systems, including lighting power distribution and controls.

Instrument Engineer, M.W. Kellogg Company, 1965 to 1971. Responsible for the design of instrumentation and control systems for petro-chemical plants.

Service Engineer, Bailey Meter Company, 1963 to 1965. Serviced and installed electronic and pneumatic instrument systems on oil and coal-fired boilers, marine boilers and waste heat boilers.

Professional Affiliations: Member, IEEE and IAS.

Licensed Professional Engineer, New York.

LUTHER L. JOYNER

Business Address:	Babcock & Wilcox Company Nuclear Power Generation Division P.O. Box 1260 Lynchburg, Virginia 24505
Education:	B.S., Electrical Engineering, Clemson College, 1964 M.S., Electrical Engineering, Clemson University, 1969. Ph.D., Electrical Engineering, Virginia Polytechnical Institute and State University, 1973.
Experience:	Principal Engineer, Control Analysis Unit and Power Systems and Controls Unit, Babcock & Wilcox Co., 1977 to present. Responsible for diverse problems involved with operation and control of the B&W NSS. Participated in the failure modes and effects analysis and reliability study of the Integrated Control System, including co-authoring the resulting report, BAW-1564. Supervisory Engineer, Instrumentation and Control Unit, Maritime Reactors, Babcock & Wilcox Co., 1976 to 1977. Responsible for design and procurement of a digital control system for a maritime nuclear propulsion plant. Program Manager, Product Development Section, Babcock & Wilcox Co., 1972 to 1976; Responsible for the research and development program for NSS development.
Professional Affiliations:	Member, IEEE. Registered Professional Engineer, Virginia.

MR. BAXTER: The panel is available for cross examination.

CHAIRMAN SMITH: Mr. Sholly.

DR. JORDAN: Mr. Sholly, if you do not mind, I think I would suggest that it would expedite matters if Mr. Joyner would tell us -- well, describe very briefly the integrated control system, and then following that, I think it would be very helpful if he would describe in some detail the nature of the document BAW-1564. I presume you were involved in the preparation of that document.

WITNESS JOYNER: Yes, sir.

DR. JORDAN: I notice your testimony goes into it very little. I believe there will be many questions concerning that document, and I think it would be helpful to the Board particularly if you would go through it briefly. As I say, first tell us what the ICS system does and then what -- how you went about making an analysis of the failure modes and effects analysis of the integrated control system, what you included in the analysis, and what was not included in the analysis, because I am sure that will be coming up later.

Would you mind going ahead?

WITNESS JOYNER: All right, sir.

I think to explain the ICS, it is best if you turn to my testimony, Figure 1. Figure 1 is a simplified functional block diagram description of the integrated control system. The integrated control system is a well-defined piece of equipment that is sold with the B&W product. It has a well-defi[illegible] function and is well understood by us.

The description -- the block diagram description that you have shows the major functional blocks of the ICS, and I think the thing to do perhaps is start at the bottom and work up, and if you -- if I do not do a good job, please stop me, sir.

The turbine control box on the bottom left represents those control functions that manipulate or the atmospheric and condenser dump valves and the turbine throttle valve, so that box represents those control loops that open and close those final control instruments, atmospheric dump valves, condenser dump valves, and the turbine throttle valves.

If you look at the diagram we have behind us, you can see -- if I can get up, I would point them out to you.

DR. JORDAN: Yes, explain that to me, particularly, what is the atmospheric dump valves and the other valves that you mentioned?

WITNESS JOYNER: This is the atmospheric relief valve. It is located on the steam line, and its function is to relieve steam pressure if necessary.

DR. JORDAN: To the atmosphere?

WITNESS JOYNER: That is correct, sir.

And these are the turbine bypass valves. They are also located on the steam line, and you bypass the turbine when required, dumping steam to the condenser, the desirable mode of cooling.

The other steam pressure controller is -- it would be -- is the turbine throttle valves which are located right here and not shown in this diagram.

Now, the ICS provides signals to the turbine control package. Each turbine comes with an electrical hydraulic control package that is used to open and control -- close the turbine throttle valves. The ICS sends the signals to this control system which says basically open or close the turbine throttle valves.

Now, the functions that it uses to determine when opening or closing of the valves are required, are determined by the way we operate the plant. Steam pressure is controlled constant at approximately 900 pounds over the entire load range.

DR. JORDAN: Steam pressure at the steam generator?

WITNESS JOYNER: That is the turbine throttle valve, sir. At low loads, that is the same as the steam generator pressure. At higher loads you have some drop in the line.

DR. JORDAN: So it is the pressure after the valve.

WITNESS JOYNER: It is just before the valves.

DR. JORDAN: Just before the valves.

WITNESS JOYNER: Yes. The sensor is located here, in the steam line (Indicating).

MR. BAXTER: Excuse me, Mr. Chairman.

I think for the record I would like to observe that in addition to the figure in his own testimony, Dr. Joyner has been referring to a blown up schematic of TMI Unit 1. That diagram appears in reduced form attached to Licensee's supplemental testimony of Robert W. Keaton, Joseph J. Colitz and Michael J. Ross in response to Board Question No. 6, and dated November 25, 1980, and this testimony will be offered and included in the record at a future date.

WITNESS JOYNER: So those three types of valves control steawm pressure constant over the load ranges.

CHAIRMAN SMITH: Mr. Baxter, would it be helpful, even though it is going to be added as a part of the written testimony, would it be helpful to make it an exhibit?

I think it would.

MR. BAXTER: That would be fine. We don't have the copies right now.

CHAIRMAN SMITH: Just for shorthand identification, I expect we will be using this.

(Pause)

MR. BAXTER: I would ask, then, that it be marked for identification as -- diagram foldout labeled "Simplified Schematic of TMI Unit 1," as Licensee's Exhibit No. 17.

We will provide the Reporter with the requisite copies at the next break.

CHAIRMAN SMITH: All right.

(The document referred to was marked Licensee Exhibit No. 17 for identification.)

DR. JORDAN: The pressure that you control is not the pressure at the turbine itself, neither is it the pressure at the steam generator, is that right?

WITNESS JOYNER: It is the pressure just upstream of the turbine throttle valves, and we maintain --

DR. JORDAN: Upstream of the turbine throttle valves?

WITNESS JOYNER: That is correct.

DR. JORDAN: Why is the pressure upstream from the turbine throttle valve the same as the steam generator?

WITNESS JOYNER: It is at the low loads.

DR. JORDAN: So it is essentially the steam generator pressure, minus the line drops.

WITNESS JOYNER: That is correct, sir, very small drop at low loads.

DR. JORDAN: Go ahead.

WITNESS JOYNER: That is the function of the turbine control block. It is fairly straightforward, control loop using proportional plus integral control loops and pulsers which are standard modules used in control systems.

Steam generator control box, which is in the lower center of figure 1, is used to control the flow of water to the steam generators. If you look on the diagram, you will see that you have now I think, which mimics this one, you will see for each steam generator a pair of feedwater valves and two feed pumps. I will point those out to you here.

DR. JORDAN: All right, do that.

WITNESS JOYNER: This is the startup feedwater level control valve and the main valve in parallel. The startup valve is sized to handle up to 15 percent flow. The main valve then controls flow above 15 percent, from 15 to 100 percent.

There are two main feedwater pumps located here (Indicating). These are parallel and provide flow through these valves to steam generator B. Not shown for simplicity is a similar line which comes off and provides flow to steam generator A. It also has a main and a startup feedwater control valve.

DR. JORDAN: Yes. Are you controlling on steam generator level?

WITNESS JOYNER: We control level from zero to 15 percent flow at the low level limit. Above 15 percent flow we control the rate of feedwater flow to the generators.

DR. JORDAN: Does that mean that the steam generator then sometimes run with a high level of water and at other times runs with a very low level of water in it?

WITNESS JOYNER: From zero to 15 percent the water level measurement is about 30 inches of water in the generator. As you progress up in power, that goes up to about 160 to 170 inches at 100 percent flow. Now, that is somewhat plant specific, but those are reasonable numbers for this type generator, this size.

DR. JORDAN: Only about 15 percent that the integrated control system comes in?

WITNESS JOYNER: No, sir, it controls the level from 0 to 15 percent at a constant value. Above 15 percent --

DR. JORDAN: Constant value of what?

WITNESS JOYNER: Thirty inches of water, sir.

DR. JORDAN: So during that regime, it is level control. It lets in the flow of steam --

WITNESS JOYNER: Flow of feedwater, sir.

DR. JORDAN: Flow of feedwater is controlled, and it is controlled by supplying feedwater until the pressure is adequate, or what is --

WITNESS JOYNER: Well, I think that will become clear as we progess on.

DR. JORDAN: All right, fine. I will wait.

WITNESS JOYNER: Let's just talk about the steam generator control loop. Its job is to manipulate the startup and main feedwater valves and the feed pumps so as to give the required amount of flow to the generators. Now, that is the function of that block.

If we move on over to the right, we see a block called reactor control. Its function is to control the action of the regulating rod groups in the reactor core. It issues a signal to the control rod drive system that causes insertion or withdrawal of rods from the core. It is constant speed, pull or insert, and can hold the rods at that point.

So coming out of the reactor control block is one signal that either inserts or withdraws rods.

Those three blocks, basically, constitute the heart of the control system in that they manipulate the steam valves, the feedwater pumps and valves, and the control rod signal.

If we move on up, we get to the integrated master control. Now, its function is to coordinate or integrate the operation of these three lower systems. You will see existing that box, going downward, a solid line. That line represents signals that are being sent out to each component to determine what it should deliver. In the case of the steam generator control, for example, the signal leaving the integrated master is a demand for total feedwater flow to the generators. For instance, at TMI 1, if we wanted 600 megawatts electric output from the plant, that signal would be on the order of 13 million to 14 million pounds feedwater flow power hour. That determination is made in the integrated master control. It also simultaneously sends out a signal to the reactor controller that would require approximately 75 percent neutron flux. These numbers are approximate, and if I had my calculator, I could tell you what they would be. The signal going out to the turbine controller is a demand for megawatts electric.

Now, just above the integrated master is the unit load demand control. Its basic function is to interface with the operator and to make sure that the control system does not allow the plant to operate outside of our desired envelope. For example, the operator inputs to the unit load demand control system his megawatt electric requirements, 600 megawatts, for example, comes into the unit load demand.

DR. JORDAN: What is that?

WITNESS JOYNER: That signal is input to the unit load demand system. In the system, then, we make surek that the plant is capable of delivering the megawatts that are required. For example, if we are operating with three reactor coolant pumps, we have a limit on operation of the plant, a control limit at 75 percent power.

In the unit load demand, there are status signals which tell us that we only have three reactor coolant pumps. It then limits the power -- power requests provided to the integrated master to 75 percent of the 100 percent load.

There are other limits in there, for example, main feedwater pump status. We only have one of the parallel main feedwater pumps on TMI 1, I believe we limit to like 68 percent power because that is the maximum capacity of one feed pump.

There is a limit on asymmetric rod position which I believe that limit is about 65 percent.

In a nutshell, that is the ICS, sir. It consists of not so many outputs, as you can see -- as you might expect, relatively few in number, although six or eight -- well, more than that, four feedwater valves, two feed pumps, atmospheric condenser, relief valve, turbine throttle valve, and a signal to the control rod drive system.

DR. JORDAN: Okay.

WITNESS JOYNER: I would be happy to go into any other depth you would like, sir.

DR. JORDAN: That is fine, unless some of the other parties or anyone else has a question.

All right.

WITNESS JOYNER: You had two or three questions. We began the discussion --

DR. JORDAN: Yes. This is just the start.

First I asked you to describe the integrated control system, but now I guess we are ready to get to the topic of the day, namely, the report, BAW-1564, which is a B&W document entitled "Integrated Control System Reliability Analysis."

CHAIRMAN SMITH: Mr. Sholly, do you plan to offer that document into evidence?

MR. SHOLLY: The B&W report?

CHAIRMAN SMITH: Yes.

MR. SHOLLY: I was going to just refer to it.

CHAIRMAN SMITH: Okay.

DR. JORDAN: All right.

MR. SHOLLY: I assumed the Licensee would offer it.

CHAIRMAN SMITH: If somebody is going toi do it, now is the time. If it is going to be marked for identification, this would be a good time to do it. If not, fine. I was just inquiring.

(Board conferring.)

CHAIRMAN SMITH: Well, you are free to do it.

Is there any confusion about that?

MR. SHOLLY: I did not come prepared with the requisite number of copies to do so.

CHAIRMAN SMITH: All right.

DR. JORDAN: We can go ahead.

So your testimony does not tell what you did really in making this failure modes and effects analysis, so I would like for you to tell what B&W did, how they attacked the problem, and how they arrived at the conclusion that the integrated control system has adequate reliability and would not lead to an upset on the safety systems, if indeed that is the conclusion of the report.

Does that make it clear what I would like to hear?

WITNESS JOYNER: I will start with a general description of the reliability analysis that you referred to.

I assume you have an analysis there, sir.

DR. JORDAN: Yes.

WITNESS JOYNER: The analysis that you have is basically a two-part study. The first part, Chapter 4 -- Section 4 is a failure modes and effects analysis of the integrated control system.

DR. JORDAN: One question first. Was this in response to the Commission order, long term Order No. 1?

WITNESS JOYNER: I do not believe so, sir. This was an agreement between B&W the operating plant owners, and the Commission. The documentation that I have is dated April 27, I believe, where we described to Mr. Denton what we were going to do.

MR. BAXTER: Dr. Jordan, all of the B&W operating licensees were ordered by the Commission to submit such an analysis.

DR. JORDAN: Yes, but this is also part of the Order.

MR. BAXTER: It is part of the Order in this docket as well.

DR. JORDAN: Part of the Order for what?

MR. BAXTER: In this docket as well.

DR. JORDAN: Now, I guess I want to hear from the Licensee.

Is this document the sole response to the Order Item, -- Order, Long Term Item 1? Is that correct?

MR. BAXTER: That is correct. It includes more than that.

DR. JORDAN: It does include more?

MR. BAXTER: It is the response to that Order Item.

DR. JORDAN: All right.

Okay, go ahead, please, Dr. Joyner.

WITNESS JOYNER: I am not sure I know where I was. It is a two-part report. Section 4 is a failure modes and effects analysis done along the lines of -- specified in

IEEE 352, which was the guiding document. Section 5 is a field performance survey which we did to complement the study, and the two of them together constitute the reliability study.

DR. JORDAN: All right. I think I understand the field performance survey moderately well, but I do need help in understanding the failure modes and effects analysis.

WITNESS JOYNER: All right, sir.

In the study, if you will -- let me get my copy out here. If you refer to page 4-24, this is a listing --

(Board conferring)

WITNESS JOYNER: This is a listing of all the inputs and outputs to one particular ICS.

DR. JORDAN: Where is that?

WITNESS JOYNER: Page 4-24.

DR. JORDAN: All right.

WITNESS JOYNER: If you start at the very top of page 4-24, we list the inputs to the ICS. If you go over on that table one, two -- I guess three columns, you will see an I/O column. And if in that column we have an I, it implies it is an ICS input. If we have an O, which you will see if you read down some slightly, it implies it is an output from the ICS.

DR. JORDAN: I see.

WITNESS JOYNER: What we did in the failure modes analysis was to assume the failure of each of those inputs and outputs, and then determine the effects upon the NSS. If they fail --

DR. JORDAN: The nuclear steam supply system?

WITNESS JOYNER: That is correct.

So there are three parts basically to the failure modes and effects analysis. We assumed failure of each input to the ICS for part 1. We assumed the failure of each output from the ICS for part 1. And if you will give me a minute, I will find the drawing of the ICS. That is on page 4-67. That is a functional block diagram of the ICS. My copy has a fairly fuzzy box.

DR. JORDAN: My copy is so fuzzy that I gave up trying to read it.

WITNESS JOYNER: Well, what you have is a functional equivalent of the ICS.

DR. JORDAN: Each block does not represent a component?

WITNESS JOYNER: No, sir. There are more components than functional blocks. But this kind of functional description is acceptable both, I think, intuitively, and if you read 352, IEEE 352, it even explicitly states that functional representation is adequate for complex systems.

And we assumed the failure of each block in there.

DR. JORDAN: I see. Okay.

WITNESS JOYNER: And we assumed that both failures are high. A high failure, for example, would be an output failure that caused the atmospheric dump valves to go wide open. A low failure would be a failure that caused them to go completely closed.

DR. JORDAN: How about mid-range failures?

WITNESS JOYNER: We did not do mid-range failures. Our feeling was and still is that you get the worst system -- the most important system response by failing valves and pumps full open, full closed, and those kinds of responses.

DR. JORDAN: I see.

WITNESS JOYNER: So that is the failure modes analysis.

Now, you know, as far as what we did, the field performance analysis, which is Section 5, we actually sent [illegible] engineers to each site for a period of time and I really cannot say exactly, you know, the average amount of time they stayed there, to go through the records, determine ICS field performance, and come up with Section 5 documents, description of how ICS had performed.

DR. JORDAN: What was the goal? I will probably get back into the techniques later, but what was the goal? Was it to respond to IEEE -- what was the number?

WITNESS JOYNER: Well, no, sir. IEEE 352 is the guiding standard that describes how --

DR. JORDAN: It is really -- the object was to perform this analysis, and what were you trying to demonstrate, that it was -- that it had a high degree of reliability and was highly defined, or that it would not interfere with the safety functions of the plant, namely, the engineered safety features, or just what was the goal of the study?

WITNESS JOYNER: Well, the goal was -- I flatter myself to think that the goal was not to determine that it would or would not interfere, but the goal was to determine whether or not it did, and to look for failure modes that might interfere with --

DR. JORDAN: With the engineered safety features.

WITNESS JOYNER: That is correct, or the reactor protection system.

DR. JORDAN: You particularly mentioned the protection system in many -- at many times during your -- in the document. But did you also study the other protective systems such as the emergency feedwater system or the high pressure injection system? Does it have an effect on those systems or any other safety systems?

WITNESS JOYNER: I might summarize for you the results that came to me when we were doing the analysis.

DR. JORDAN: All right.

WITNESS JOYNER: We found that there were -- or we could assume three types of failures in the ICS: those that were -- I do not call them insignificant, but ones that woulds not cause a significant upset in operation of the plant. We called those category 1 failures.

Then there were the category 2 failures where, if that failure occurred, we would expect -- could reasonably expect an upset in the system that might cause the reactor protection system to trip the plant.

DR. JORDAN: Now, you do mean the protection system that operates the control rods.

WITNESS JOYNER: That is correct, sir, and we found that there were several.

And then there were category 3 failures where we found that if that failure occurred, we could reasonably expect -- although it is not sure by any means that the plant might trip, and if it did trip, operation of some backup system such as high pressure injection or emergency feedwater would be required or could be required.

Failures are very dependent on the time in core life, the initial power level that the failure occurs at, or where the failure occurs, operator response, and many other things. But our goal was to determine whether it was reasonable to anticipate that a trip might occur, and we spelled those out in the report. In fact, they are in -- page 4-22, ICS FMEA results basically summarizes what I just stated.

CHAIRMAN SMITH: May I interrupt?

Mr. Baxter, I think that the Licensee is verging on at least a violation in spirit of the best evidence rule by having this testimony so heavily dependent upon telling about what exists in this document, that I think the responsibility of producing this in evidence is upon the Licensee.

MR. BAXTER: I have no objection, Mr. Chairman.

CHAIRMAN SMITH: It is not a question of objection. It is a question of extensive summarization of what is in an original document.

MR. BAXTER: That is correct.

CHAIRMAN SMITH: And that is a violation of the rules of evidence.

MR. BAXTER: We will provide the Reporter with copies.

Just by way of explanation, though, Mr. Chairman, the Contention that we were addressing was whether or not it was required to submit such an analysis prior to the restart of the unit, and of course we have testimony that says we have submitted such an analysis. And the testimony does summarize in brief, but the Contention was not as to the adequacy of the study that was done, but whether it had been done or not. And it was for that reason we did not initially determine to put the document in evidence.

CHAIRMAN SMITH: The study -- it is subsumed by the Contention certainly.

DR. JORDAN: It seems to me this was exactly one of the problems, that the Licensee assumed that the Contention where there was no analysis made. Here it is. There has been an analysis made, and that is the extent of the Licensee's testimony, we have done the analysis.

Now, as the Chairman says, it seems to us that it must also be demonstrated that the analysis really did meet the requirements of, if nothing else, the Order, Long Term Order 1.

MR. BAXTER: The testimony does get the overall conclusion of the analysis. I am not being resistant, I am just explaining why we made the presentation we did, based on our reading of what the issue was.

DR. JORDAN: Okay.

Well, my questioning is, I think -- well, now, which does result in bringing this in, I think is, as I said before, along the line that I am interested in myself, and I am sure that it will assist Mr., Sholly in his cross examination to get this out now. That is the reason for it now, so I guess the question is do we want the document.

CHAIRMAN SMITH: Dr. Jordan, my view is that Licensee itself is subject to objection to having his testimony received into evidence because of extensive reliance upon a written report, and if I were the Licensee, I would want to offer this report into evidence as its exhibit.

MR. BAXTER: We will --

CHAIRMAN SMITH: If you want us to give much weight to the testimony.

MR. BAXTER: We will offer the document as soon as we get the copies.

CHAIRMAN SMITH: I thought that that might occur to you.

MR. BAXTER: I thought I had said that, but --

DR. JORDAN: Mr. Joyner, I have forgotten where we stood.

WITNESS JOYNER: I have, too, sir.

DR. JORDAN: Go ahead with your explanation, unless we were in the middle of a question.

WITNESS JOYNER: I was on page 4-22.

DR. JORDAN: So you were. You were about to describe the results.

WITNESS JOYNER: And what is there is basically a statement of types of failures that we found.

Now, based on this characterization of the failures that can occur, as well as the field performance survey, we offered the recommendations that are in Section 3 of the report, and they are basically those that we feel the report indicated were desirable.

That is page 3-1 in the very front.

DR. JORDAN: Okay. Would you briefly then tell us what is in the recommendations?

WITNESS JOYNER: Well, Recommendations 1 and 2 -- Recommendation 1A is to improve the reliability of the power supply to the NNI ICS. That basically came out of the field performance survey where we saw several failures of power to the ICS.

DR. JORDAN: Does the ICS have a separate power supply?

WITNESS JOYNER: There are two power supplies to the integrated control system, and we have seen --

WITNESS SADAUSKAS: If I may interject here, on the TMI Unit 1 plant, the integrated control system is powered from a power distribution panel ATA, and this panel is fed either from an inverter 1A, which is powered from the station batteries and the engineered safeguards bus, or it can be powered from a regulated AC bus.

DR. JORDAN: I see. Is this -- and the power that is put out is 60 cycle AC. Is that what feeds the integrated control system?

WITNESS SADAUSKAS: Yes. The integrated control system at TMI Unit 1 is a Baylor Meter Company 721 system. This system operates on 120 volts, 60 cycles.

MR. SHOLLY: Might I ask a question here, Dr. Jordan?

DR. JORDAN: Go ahead.

CROSS EXAMINATION

BY MR. SHOLLY:

Q Is the ICS powered from the diesels at all, or is it just from the station batteries and the AC system?

A (WITNESS SADAUSKAS) The station batteries are charged from the engineered safeguard system and power for the ICS through the inverter is from the engineered safeguards system, ands the engineered safeguards system is on the d.esel.

MR. SHOLLY: Thank you.

DR. JORDAN: Normal operation, I presume, is from the station, regular station power.

WITNESS SADAUSKAS: It is from the regular station power of the engineered safeguard bus.

DR. JORDAN: Of the engineered safeguard bus.

WITNESS SADAUSKAS: Right.

DR. JORDAN: There are two buses, is this right? There are two buses?

WITNESS SADAUSKAS: There are redundant buses, yes, sir. The ICS is connected to one of them.

DR. JORDAN: To one of them. Switchable?

WITNESS SADAUSKAS: It is switchable.

DR. JORDAN: Why is it necessary to have a power supply of such high reliability? After all, the only time the ICS is operating, is it not, is when the station is generating power, so that you surely have -- you know you have AC power at the station at any time the ICS is operating. What is wrong with that?

WITNESS SADAUSKAS: As you said, the ICS performs a function when the unit is operating. When the unit is operating, it is important that the controls that the ICS manipulates perform, and it is for this reason that the power supply to the ICS was made quite reliable.

DR. JORDAN: Okay. That is more or less an aside.

So the first recommendation, then, was to improve the reliability of the power supply, and what -- and what -- you have in mind plans for doing that?

Go ahead, Mr. Sadauskas.

WITNESS SADAUSKAS: Currently we have implemented improvements on the power to the integrated control system. Currently, in the event that inverter 1A fails, there is a static transfer switch that will automatically transfer the source of power from the inverter to a regulated 120 volt, 60 cycle bus.

At the Oconey station, Duke Power, a failure was experienced with that switch. Metropolitan Edison has elected to install a backup device to the automatic transfer switch, and this is being implemented currently. In the event that the main source of power from the inverter fails, ands in the event that the static transfer switch fails to transfer power to the regulated bus through some failure mode, an alarm will be activated in the main control room. The operator's response to the alarm will be to manually transfer the power to the regulated bus using a new switch that is being provided in the main control room for that purpose.

DR. JORDAN: During thisd transfer, does the integrated control system remember well enough so that it does not go jerking out control rods or causing steam valves -- there must be a transient during the transfer?

WITNESS SADAUSKAS: There is probably a transient.

DR. JORDAN: Yes.

WITNESS JOYNER: I might add, sir, that normally the automatic bus transfer is designed so that it transfers fast enough that the transfer is transparent to the ICS, if it operates properly, and that is how you would expect it to operate.

BY MR. SHOLLY: (Resuming)

Q That would be in the case where a transfer is automatic, is that correct?

A (WITNESS JOYNER) Yes.

Q If it fails to transfer automatically, the operator has to take some action, and then there is a delay?

A (WITNESS JOYNER) Yes.

DR. JORDAN: All right. In answer to my question, I gather that Met Ed does have in mind what they are going to do to improve the reliability., It has not been accomplished yet, or will be, or has it?

WITNESS SADAUSKAS: The engineering design -- well, first of all, Met Ed does have in mind what we are going to do to improve the reliability. The engineering design is complete for some of the modifications, and it is actively under way for others, and at this time there have been no changes to the existing plant system.

DR. JORDAN: All right.

The next one concerns the reliability of the input signals.

Mr. Joyner, is that correct? And what are the plans for that?

WITNESS JOYNER: Well, I think it is appropriate to -- for Met Ed -- let me give you some background.

DR. JORDAN: All right.

WITNESS JOYNER: Then we can discuss it.

Table 5-3 on page 5-12, it shows the input failures that we observed had occurred, plus when the failure modes and effects analysis was performed, we determined that others could fail in an undesirable fashion.

DR. JORDAN: What?

WITNESS JOYNER: Other inputs could fail in an undesirable fashion, although we had not experienced that failure. So for tha reason we added Recommendation 1B, that we improve the reliability of certain input signals.

DR. JORDAN: I see, failures not included in Table 5-3.

WITNESS JOYNER: That is correct. They should be the reliability may need improvement, evaluating on a time specific basis.

DR. JORDAN: I see.

WITNESS JOYNER: And --

DR. JORDAN: There are plans to include those?

WITNESS JOYNER: I really think it is appropriate to talk toi the GPU people, sir.

DR. JORDAN: Go ahead.

WITNESS BROUGHTON: With respect to the reactor coolant system flow signal at TMI 1, the initial design of the equipment provided that signal into the ICS through an arrangement of a jumper and a plug. So there was a wire that connected an output of one cabinet into the input of another. Previous to t is particular analysis -- I don't know exactly the timeframe -- that equipment at TMI 1 was modified to use a different method of putting the flow signal into the ICS. The jumper was replaced with a solid wire internal to the cabinets, and the signal that was taken from the protective system, the flow signal from the protective system was -- can be taken from one of two different channels.

DR. JORDAN: For which protective system?

WITNESS BROUGHTON: The flow system pumps from the reactor protection system, a separate system from the ICS.

DR. JORDAN: By the reactor protection system you mean the system that scrams the reactor?

WITNESS BROUGHTON: Yes.

DR. JORDAN: And it automatically scrams on loss of flow of coolant, is that right?

WITNESS BROUGHTON: Yes, if the flow is reduced below a predetermined level for the existing power, that could cause a scram of the reactor. Those flow signals first go into the reactor protective system where the protection system logic decides if the reactor should be left operating at power, and then a secondary use of the flow signals is to provide information into the ICS so that from a control standpoint, it also knows what the available flow in the reactor coolant system is.

DR. JORDAN: The reason it needs to know this is because of the thing Dr. Joyner mentioned, that you may not call for full power if you only have three pumps.

Is that the reason for it?

WITNESS BROUGHTON: That is correct. There are several features within the ICS which depend on knowing what this flow is. That is one example.

DR. JORDAN: I will probably want to inquire in this in more detail later. Any time I find a connection between one of the safety systems and one of the control systems, I immediately become worried about the possibility of interactions. But we will come back to that later. I understand what it is then now.

WITNESS BROUGHTON: The modification that was made at TMI 1 to improve the reliability of this flow signal into the ICS was replacing the jumper with a cable which is permanently attached, and in addition, there is a relay which, on loss of power into the ICS channels -- excuse me, the reactor protective system channel which is generating the flow signal, this relay will cause the flow signal from the RPS to be selected to a channel which has power. So on loss of power to that flow signal, there is an automatic transfer for the ICS input to a channel which still has a valid flow signal.

DR. JORDAN: That is too complicated to understand right now. But I do not think it is important at the moment.

Where do you stand on Item C, the ICS -- this is the balance of plant system tuning, particular feedwater condensate systems, and the ICS controls.

What is being recommended there? Where do you stand?

WITNESS BROUGHTON: W have a fairly comprehensive program of maintenance and alignment at TMI 1 to deal with the ICS and to make sure that it is in fact calibrated properly and operating properly. That program is conducted whether the reactor is in operation or whether it is shut down. For example, the program is active today even though the plant is in a shutdown condition. It involves calibrating instruments which are used in sensors, checking the functioning of a loop --

DR. JORDAN: To simulate the signals.

WITNESS BROUGHTON: Yes, and evaluate the response of the components to make sure that they are proper for the signals that have been inserted.

DR. JORDAN: Yes.

WITNESS BROUGHTON: And the program goes beyond that in that it also looks at the actual components which are actuated, for example, the regulating valves for feedwater flow. Over a period of time they will begin to leak due to erosion in service, and the program rebuilds these valves on a periodic interval to ensure that the leakage across the seat is within acceptable limits for the control system.

Our experience has shown that we have not seen the same types of problems with tuning that other plants have reported, and we believe it is because of the maintenance that is performed in conjunction with the system.

DR. JORDAN: I see.

WITNESS JOYNER: I would like to add a couple of things, if I may.

Your statement about the interaction of the safety and control systems, those inputs to the ICS that originate in safety systems like the RCS flow, are completely buffered. They are -- the only interface is that that protection channel provides a flow signal to the ICS through buffer amplifiers, and it is totally isolated and independent.

DR. JORDAN: Yes, but I -- it takes an analysis of every one of those systems to make sure that you are not getting informatin from the safety system which relies -- which is then fed back to the safety system through the ICS, that there can be a feedback chain established which can be adverse. I have seen instances of it so, but I am not saying that there is one necessarily here. I am always suspicious whenever I see any interaction at all.

WITNESS JOYNER: We are, too, sir. I wanted to make that clear.

The other point is to state that these recommendations now are generic. They may or may not apply to a particular plant. In my estimation, 1C does not apply very much to TMI 1.

DR. JORDAN: Then Recommendation 2 is balance of plant.

WITNESS JOYNER: It may or may not be specific to TMI 1. In some cases, I do not believe it is particularly important.

DR. JORDAN: Concerning Item No. 2, balance of plant, are any of those applicable to TMI 1, and are there any actions being taken?

WITNESS BROUGHTON: Yes, I can comment on each of those.

The first item, main feedwater pump turbine, minimum speed control, the concern here was that if the integrated control system desires a small amoung of flow to the steam generator, it will send a signal to the feed pump which will slow it down, and it would be possible to slow the pump down low enough so that low oil pressure or some other pump protective system might cause the pump to trip to protect the pump.

At TMI 1, the main feedwater pumps have a mechanical low-speed stop which is completely separate from the ICS, and that stop is set at a high enough value so that the pump will be self-sustaining even at that low speed. So independent of the ICS control signal, a minimum speed will be maintained.

DR. JORDAN: I see. So A does not apply to TMI 1.

WITNESS BROUGHTON: That is correct.

With regard to B, a means to prevent or mitigate the consequences of a stuck open main feedwater startup valve, the concern here was that if there was a malfunction of the valve or an incorrect signal sent to the valve, that when a low flow was required to the steam generator because the valve was more fully opened than it should have been --

DR. JORDAN: That is the bypass valve?

WITNESS BROUGHTON: Yes, that is the bypass valve around the main feedwater valve; that this overfeeding could lead to undesirable high levels or perhaps overcooling of the system.

DR. JORDAN: Yes.

WITNESS BROUGHTON: Some power plants do not have the capability to stop flow in that bypass line if the valve sticks open. At TMI 1 we have a separate, motor-operated valve which is independent of the ICS which can be shut to block flow in that line. So even if we had a stuck open startup valve, we could still prevent feeding through that line.

DR. JORDAN: I see.

WITNESS BROUGHTON: The third item is a means to prevent or mitigate the consequences of a stuck open turbine bypass valve. The turbine bypass valve is the valve which would put steam into the condenser and the concern here is similar with the stuck open main feedwater startup valve. Ands at TMI 1, there are two valves, motor-operated, in series, which could be shut to isolate steam through a stuck open turbine bypass valve. So that is also an event which could be terminated by the plant as it is without further changes.

(Board conferring.)

DR. LITTLE: I am a bit confused, and I wanted to get things oriented a little bit.

I understand Mr. Sholly's Contention to indicate that a failure modes and effects analysis of the ICS at TMI 1 should be completed prior to continued operation of TMI 1, and as far as I can see in the testimony that has been provided, the documentation is BAW-1564, and then on the recommendations page, it points out that 1564 is essentially a generic report, and it indicates -- recommends that plant specific analyses should be done, and my question is, is there a plant specific analysis for TMI 1 which would be, in effect, the response to Mr. Sholly's Contention?

WITNESS SADAUSKAS: The answer to that question is yes.

DR. LITTLE: Do we have it?

WITNESS SADAUSKAS: I do not have it, no. The study was prepared under my supervision. I am quite familiar with it.

DR. LITTLE: Am I mistaken, or wouldn't that be the response? Is that the response you were looking for, the plant specific analysis?

MR. SHOLLY: I think one quick question could clear this up.

BY MR. SHOLLY: (Resuming)

Q For Dr. Joyner, is the ICS system failure modes and effects analysis done on -- is that the model that is at TMI 1? There are two models, 721 and the 820. If I recall correctly, the FMEA was done on the 820 model.

A (WITNESS JOYNER) Functionally, the ICS at all B&W units is the same, very close to the same. Some are 721 ICS hardware. Others are 820 hardware. Functionally they perform the same jobs, control the same equipment, have the same inputs, and the recommendations that we have at Section 3 are the same for both types of equipment.

MR. BAXTER: Dr. Little, the Commission's orders to the B&W operating licensees were to conduct a failure modes and effects analysis of the integrated control system, and this B&W report is the document which these operating licensees have relied upon to satisfy that Commission order item, and it is the document which the staff has reviewed, as I understand it, in their safety evaluation report, to determine whether or not there has been compliance with the Commission's order.

So the fact that B&W recommended an additional plant specific study -- and one is being undertaken -- is in a way outside or beyond, I believe, at least, our compliance with the Commission's order as we view it.

DR. LITTLE: But a number of differences were just pointed out on the recommendations. Evidently some apply and some do not here. So we are going to have to go through quite a bit of questioning, I guess, to determine just what is applicable here.

CHAIRMAN SMITH: Let's hear from Mr. Cutchin.

MR. CUTCHIN: I wanted the record to reflect as well, Mr. Chairman, that it was indeed our understanding based on the October 26, 1979 letter from then Vice President Herbein to Mr. Vollmer that the document BAW-1564 was submitted as being responsive to the long term recommended requirement No. 1 of the August 19, 1979 Commission order regarding TMI 1 restart, and it was indeed on that basis that we performed our review.

MR. BAXTER: Our witnesses testify on page 3 of their direct testimony that the FMEA was reviewed by GPU and found applicable to the TMI 1 ICS. I think the only distinction we have so far is simply Dr. Joyner's comment that it was a generic study, and he thinks 1C is less applicable to TMI 1 than it was to other units because he found that control system to be finely tuned, and to have a good record. I do not think that that means that the study itself is not applicable.

(Board conferring.)

DR. LITTLE: I will try to listen bearing those comments in mind as to what the testimony was intended to answer.

MR. SHOLLY: Mr. Chairman, if I might, I would like to repose the questions I asked because I do not think they were directly responded to. There were two of them, really.

BY MR. SHOLLY: (Resuming)

Q Which ICS model was the B&W report based on?

A (WITNESS JOYNER) It is based on the SMUD ICS.

Q Model 820?

A (WITNESS JOYNER) 820 hardware. I want to make the distinction that there is one ICS that uses 820 or 721 hardware.

Q And TMI 1 is a 721 hardware.

A (WITNESS JOYNER) That is correct.

DR. JORDAN: Okay, good.

Well, I gather, then, that it is the Licensee's position that the document BAW-1564 does satisfy the Commission's requirements.

Now, this was a long term item. Is it the Licensee's position that it is satisfied now, or that it will be satisfied sometime in the future?

MR. BAXTER: One can argue about what the Commission meant by the order. We believe, looking at the words themselves, to submit such an analysis, that we have done so. I do know that the staff safety evaluation of this order item continues on and evaluates the recommendations made by B&W and what Licensee is doing in response to those recommendations.

They conclude in that January safety evaluation that reasonable progress has been made toward following through the recommendations. I do not think there is any dispute that the analysis has been done.

DR. JORDAN: Okay. When we get to the staff, we will pose such questions as that, but I think, then, for the moment, I have no further questions on the document BAW-1564. That is by no means a claim that I understand everything in the document. I do not, and I am not going to try to understand it all right now.

So, Mr. Sholly, I guess it is up to you, then.

MR. BAXTER: While we are making a transition, Mr.

Chairman, we have provided the Reporter with thr copies of BAW Report 1564.

I would ask that it be marked for identification as Licensee's Exhibit No. 18. The document itself reflects Dr. Joyner's participation and partial authorship of it, and he has testified as to its contents. So I move its receipt into evidence.

CHAIRMAN SMITH: Any objections?

MR. SHOLLY: No objections.

MR. CUTCHIN: No objection.

CHAIRMAN SMITH: So received.

(The document referred to was marked Licensee Exhibit No. 18 for identification, and received in evidence.)

CHAIRMAN SMITH: Mr. Sholly?

BY MR. SHOLLY: (Resuming)

Q A few brief questions for Mr. Broughton and Mr. Sadauskas, and if it is any consolation to you, you can rest easy because the rest of my questions will be for Dr. Joyner.

MR. BAXTER: No, Mr. Sholly, don't counsel them that way. I would rather they not rest easy.

(General laughter.

BY MR. SHOLLY: (Resuming)

Q Within Dr. Jordan's questioning, Mr. Broughton, there was some discussion of possible feedback between the integrated control system and the reactor protection s stem as a result of the direct connection of the reactor coolant flow signal.

Has the Licensee done any evaluations of that to see if there is any possibility of a feedback?

A (WITNESS BROUGHTON) That question gets into some details of hardware that I am not personally familiar with, but the met'ods of isolating safety systems and signals from non-safety systems are ones that there are acceptable methods fc- doing that, and those methods were employed in this case. But I am not familiar enough with the hardware to be able to tell you exactly what those were.

Q Dr. Joyner, do you have anything additional to remark on that point?

A (WITNESS JOYNER) I really cannot add anything.

Q Okay.

Mr. Sadauskas, you discussed briefly about switching the engineered safeguards buses if the first on failed, and you mentioned that there are redundant buses, and that those could be switched.

Do you have any estimate of how long that might take to accomplish?

A (WITNESS SADAUSKAS) No, I do not. I -- no.

Q Any idea?

A (WITNESS SADAUSKAS) No.

Q Could you say whether it might be in terms of minutes or tens of minutes, or --

A (WITNESS SADAUSKAS) Well, it is my opinion that it would be in terms of tens of minutes.

Q During that period of time, then, would the operator be able to take manual control of the ICS?

A (WITNESS SADAUSKAS) In the event that the ICS experiences a total power failure, and that the red train from which the ICS is powered fails totally -- and I really cannot -- I find it difficult to postulate a failure like that -- the ICS would be inoperative.

Q Have you any idea as to what means operators could take during that period of time, between switching engineered safeguard buses to control the plant? I realize it might depend on what particular situation they were in at the time, but generally what I am trying to get at, are there systems that would be powered that would enable the operator to control the plant while you got ICS back on line?

A (WITNESS SADAUSKAS) Well, by control of the plant, undoubtedly the plant would not remain at power level. The engineered safeguards features systems and the reactor protection system would be operable from the redundant bus. So the plant would be in a controlled situation by virtue of the fact that those systems are operable.

DR. JORDAN: I am a little puzzled at your reticence to answer what happens if you lose power, because surely the failure modes and effects analysis, you must have followed exactly what happens if you lose power to the ICS.

What happens? You made the -- was this a fault tree kind of analysis or event tree analysis or not? What happens if you lose power?

WITNESS SADAUSKAS: No. What we did was, using the Baylor Meter Company and B&W drawings, we identified the source of power for all of the ICS components.

DR. JORDAN: The source of power?

WITNESS SADAUSKAS: The ICS receives essentially from the subdistribution system five sources of power. There is a fixed source of power that powers the cooling fans in the ICS cabinets.

DR. JORDAN: I see. So it is not a single power supply.

WITNESS SADAUSKAS: You may note I said subdistribution system. If I can run through it again, the ICS subdistribution system receives power from the 1A plant inverter, or from the regulated AC bus. From this distribution panel the power is subdivided to the ICS, and subdivided through five circuits.

DR. JORDAN: All the same voltage?

WITNESS SADAUSKAS: Yes, sir.

DR. JORDAN: Same frequency?

WITNESS SADAUSKAS: The current reading of the circuits are different.

DR. JORDAN: Than the fusing.

WITNESS SADAUSKAS: Right. In our study we considered the removal of each of the five power subfeeds to the ICS, and we did this to enable us to have an understanding of how the plant would react to an individual subfeed failure or to a major power loss.

DR. JORDAN: All right.

Does that appear in the report, the BAW, as to what happens in each one of those cases?

WITNESS JOYNER: That is not in the report, sir. That, it is my understanding, is part of your restart report.

DR. JORDAN: Are you saying that the restart report has the event tree diagram that one can follow and find what happens under each transient condition?

WITNESS SADAUSKAS: No, he is not.

DR. JORDAN: Then I -- what did Mr. Joyner say was in the restart report?

WITNESS JOYNER: Perhaps I misspoke, sir. I said it was my understanding that they had covered loss of power in the restart report. That may or may not be true. I really cannot speak for the restart report, and I should not.

DR. JORDAN: Did the failure modes and effects analysis follow what would happen upon the loss of each one of these five power supplies?

WITNESS SADAUSKAS: The --

DR. JORDAN: And what happened. I invite you to take me through the event -- what happens, event by event, upon the loss, say, as an example.

WITNESS SADAUSKAS: The result of our study, as I said, we removed the five subfeeds from the ICS, one at a time. These five subfeeds are called X power and Y power, also called Hex and Y, and these two sources primarily provide power to field mounted sensors, such as pressure transmitters or flow transmitters, things of that sort.

The other -- one of the other sources of power is the autopower system.

DR. JORDAN: What?

WITNESS SADAUSKAS: Auto.

DR. JORDAN: A-u-t-o?

WITNESS SADAUSKAS: Yes.

This essentially provides power to some computing modules, some indicators to the autotransfer relays which enable the operator to transfer the control of the various control loops from automatic to manual mode. The remaining system is the hand power system, and this system provides power for the generators that allow the operator to manually position the final control elements. In addition, it also provides power to the electrical, to pneumatic converters at the control valves. The leading source of power of the five is the auxiliary power source which is used for the emergency feedwater system. And we conducted this study to enable us first of all to understand the failure modes of the ICS system on removal of the various sources of power, the objective being to develop procedures that could be used by the control room operator in the event that one or more of these power sources was left.

As a result of our investigation, we determined that under the loss of each one of these systems that I mentioned earlier, certain indicators, transmitters, valves in the system would fail.

We have developed a list of these items, including their failure modes, and it is our plan to conduct a test, an actual test of the ICS system under controlled conditions to simulate power failure prior to the restart of the plant, to enable us to verify the results of our study.

DR. JORDAN: Does the study -- can you turn to the study and look at it and see what it predicts would happen if a particular power supply fails?

WITNESS SADAUSKAS: Yes. The study contains a list of indicators and recorders, transmitters and such that would be removed from service in the event that a power supply has failed.

DR. JORDAN: And then -- so all right, what happens to the system, the steam supply system upon failure of, let's say -- choose one.

WITNESS SADAUSKAS: On the failure of -- the system is operating in the plant at power, and operating in the automatic mode, that is, the ICS is in control of the plant.

DR. JORDAN: Good.

WITNESS SADAUSKAS: If the autopower fails, the control system will essentially fail to the manual mode in the control room, between the ICS signals that are developed in the integrated control system ands the outgoing signal to the final control element. For each of the final control elements there is a manual automatic station. This station provides the man-machine or operator interface between the integrated control system and the plant operator. In the event that the auto power fails and the -- then the system will revert to manual mode. This will be brought to the operator's attention immediately.

These automatic stations that I discussed earlier have two indicating lights on them, one from manual, one for automatic. In the event that the automatic power fails, both of these lights will be out. This will inform the operator that the system has reverted to the manual mode.

In conjunction with this, Metropolitan Edison has decided to implement a power, an ICS power monitoring system prior to restart. What this system does is it looks at each of the six major feeds to the integrated control system as well as some of the subfeeds, and it provides the operator with an enunciation and visual identification in the main control room to tell him exactly which feed has failed.

Now, once the system has reverted to the manual mode, the operator will be able to operate the final control elements by hand from the manual automatic stations not on the main control board.

DR. JORDAN: Now, you say this is something that is being planned to be implemented.

WITNESS SADAUSKAS: Yes. The engineering is well under way on the implementation of this.

DR. JORDAN: Is that in BAW-1564? Is that one of the recommendations?

WITNESS SADAUSKAS: You might consider that to be one of the recommendations of the power supply -- improved power supply reliability in the sense that it is an information system.

DR. JORDAN: I see. BAW-1564 does not spell out what is needed in the way of improved reliability.

WITNESS SADAUSKAS: I do not believe so, no, sir.

MR. SHOLLY: Dr. Jordan?

DR. JORDAN: Yes, Mr. Sholly.

MR. SHOLLY: A few questions before we move off of this particular area.

DR. JORDAN: Fine, go ahead.

BY MR. SHOLLY: (Resuming)

Q These power failures in the ICS, I believe you indicated with the manual control station, that there was a light that informsthe operator whether the system is in manual or auto control, is that correct?

A (WITNESS SADAUSKAS) Yes, that is correct.

Q And that enunciator light, does that appear on the main enunciator panel or is that down on a control panel?

A (WITNESS SADAUSKAS) We are monitoring the power feeds to the ICS system, and we provide the operator with a common alarm, if you will, that is all-inclusive, that brings to his attention via an audible and a flashing alarm from the main enunciator system that one of the ICS feeds has failed. We do not tell him with this alarm which one has failed. However, once he gets that alarm on the main control board, we are adding a series of six lights. The fail light, or the light that is indicative of which feed to the ICS has failed will de-energize, and the operator, once he becomes aware of the common alarm, the enunciator focuses attention on the light panel which will give him more definitive information. And it is our hope that from the list that we have developed, which will be substantiated by an actual field test, the operator will know which instruments in the control room are affected by this particular failure.

Q He will know that by procedures, or how will that be passed on to the operator?

A (WITNESS SADAUSKAS) Well, the list that we have now will be verified by an actual test at the Island. Following that test, the operator will receive procedures that will document the consequences in the main control room of various ICS failures, power failures.

Q And this will all be done before restart?

A (WITNESS SADAUSKAS) Yes.

Q The procedure, the tests?

A (WITNESS SADAUSKAS) Yes, the tests are scheduled before restart.

CHAIRMAN SMITH: This is in the restart report, this information you just provided?

(Pause)

WITNESS SADAUSKAS: No.

DR. JORDAN: The only reference I saw in your testimony to the restart report referred to Question 12, I believe, and that seemed to provide very little information. It was very short.

Well, are you saying that if the aut[illegible] supply were to fail, the power supply, that what would happen, there woulds be certain lights come on, there would be no pulling of control rods, no closing of feedwater valves, nothing like that happens when one of these power supplies fails? All that happens is that the operator is told to take control and there is no plant upset?

WITNESS SADAUSKAS: On the case that I cited, which was the failure of the automatic power feed to the integrated control system, the final control elements would remain in their last position. This is an inherent position of the hardware, the manual automatic stations have a memory module that monitors the automatic signal, and when the transfer is made from automatic to manual, as would be the case when automatic power fails, the final control elements would remain in that off position, with the exception -- the control rod drive system is powered exclusively from auto power, the ICS portion, and failure of auto power would not cause the rods to move.

DR. JORDAN: Okay. Go ahead, Mr. Sholly.

BY MR. SHOLLY: (Resuming)

Q Mr. Sadauskas, you mentioned, I believe, that there was a study, a site specific study, a plant specific study for TMI 1 prepared under your direction.

Is this part of what you have just been discussing?

A (WITNESS SADAUSKAS) Yes, sir, it is.

Q Is that study in a written form such that it could be submitted to the Board and the parties?

A (WITNESS SADAUSKAS) Yes, it is.

MR. SHOLLY: Mr. Chairman, I believe that that study should certainly be submitted by the Licensee. It seems to me that that is a rather important document that we should received.

WITNESS SADAUSKAS: I would like to add -- pardon me.

MR. BAXTER: I will have to confer with my client as to the status of the document. It is the result of additional work that has been done in response to a recommendation B&W made as a result of the failure modes and effects analysis which is what the Commission required.

I will not take issue with you one way or the other as to whether it is a crucial document for litigating this contention. It is not clear to me that it is, but we will confer about its status.

CHAIRMAN SMITH: Mr. Baxter, perhaps you can give us a more thorough explanation of how you view that requirement in the Commission's order, simply that a failure modes and effects analysis be done, notwithstanding how detailed it is, how reliable it is, how good it is, how bad it is, or anything else about it, just that it be done? Is that the Licensee's position in the case?

MR. BAXTER: Not quite. I think that after the accident at Unit 2, Three Mile Island, the staff perhaps for the first time gained an appreciation for interest in what the role of the ICS was in the operation of these power plants, and therefore, one of the things the Commission directed be done not prior to the restart of the other B&W units, but as a long term investigation by the staff was to look at what the failure modes and effects of these systems were, and I think it was so the staff could determine whether they precipitated, cause, aggravated or interfered with the mitigation in response to transients. Certainly I do not think it would have been acceptable for us to file two sentences or two lines. That analysis has been done, and the staff and the Licensee have both determined that the ICS is not a failure producer but is a failure mitigator.

The fact that B&W also made some recommendations for improvements in the balance of plant, by the way, not in the ICS, and that they are being pursued I think is to our credit, but I do not know it is subsumed within the Commission's initial requirement that you look at the ICS.

CHAIRMAN SMITH: Mr. Sholly was not inquiring, I don't believe, about the balance of plant, were you, Mr. Sholly?

MR. SHOLLY: I do not believe so. I think one of the things that I want to point out is that we will get to whether the failure modes and effects analysis is adequate or not. You know, I am really not too concerned about what the staff and the Licensee have concluded. I think it remains for the Board to conclude whether it is adequate or not, and if this document that Mr. Sadauskas has had prepared bears on that, then I think it is entirely relevant.

CHAIRMAN SMITH: Mr. Baxter, the Board, without having conferred with my colleagues, I think I can sense among my colleagues a feeling that we have had to try hard to develop information on this point, harder than we would have expected to.

MR. BAXTER: Mr. Chairman, I can only say the staff did supply as a reference work with their testimony the B&W report. It has never been -- I did not think unclear what we were relying on in our testimony in terms of that reference. It is not easy to anticipate what the depth or the nature of the concern is by the Board and parties. We had almost no discovery by Mr. Sholly on this Contention. That is his right, but we got some questions about the maintenance history of the system. We had no Board questions. The restart report generally responds to the order items.

CHAIRMAN SMITH: I am not referring to the testimony as it was produced. I am referring to the events of this morning. I mean, information has not seemed to flow easily.

Perhaps this would be a good time to take the lunch break, and we can all go back and think about our views on the Contention and the issue.

We will reconvene at 1:10.

(Whereupon, at 12:00 o'clock noon, the hearing in the above-entitled matter recessed, to reconvene at 1:10 o'clock p.m. the same day.)

\- - -

AFTERNOON SESSION

(1:15 p.m.)

Whereupon,

T. GARY BROUGHTON

GERALD J. SADAUSKAS

LUTHER L. JOYNER,

called as witnesses by counsel for the Licensee, having been previously duly sworn by the Chairman, were examined and testified further as follows:

CHAIRMAN SMITH: Mr. Sholly, you may proceed with your cross-examination.

MR. BAXTER: Mr. Chairman, I thought I might have heard some miscommunication during Dr. Little's examination of Mr. Sadauskas, and I have conferred with my colleagues over the lunch break and they heard the same. And I would like the opportunity to ask just a couple of clarifying questions, which I think would help the examination.

I thought, looking at the B&W recommendations on page 3-1 of Licensee's Exhibit 18, where it is recommended that the following areas be reviewed on a plant-specific basis, that Dr. Little then asked, was there an analysis, a failure modes and effects effect analysis, done of the TMI-1 integrated control system. And Mr. Sadauskas said yes to that question.

I would like to ask him whether indeed that was what he meant, and if not what he was referring to.

WITNESS SADAUSKAS: the study that we performed was an evaluation of loss of power to the ICS NNI system, and in the true context it cannot be regarded as a failure modes and effects analysis.

MR. BAXTER: And it was not an analysis of the integrated control system, but rather just of the power supply; is that correct?

WITNESS SADAUSKAS: It was an analysis of the effect of power supply failure on components of the integrated control system.

MR. BAXTER: The distinction that he made is that it is not a parallel study to the one that B&W has performed at all.

And two, I hope with that in context, I would like Dr. Joyner just briefly again to tell us what the role of the ICS is in plant performance, and what Licensee and B&W intended to show with this failure modes and effects analysis.

WITNESS JOYNER: The ICS is a non-safety grade control system. It is not responsible for protection of the plant. It aids the operator in controlling the plant to make megawatts.

The analysis that we performed was done with the goal of looking for failures that might be in the system that would cause improper operation. The ICS itself is a standard functional system that we provide with each NSS. We failed the inputs, the outputs, the functional components of the system, and looked for failures that produced undesirable transients as far as from an operational standpoint.

We were not able to find failures that would affect the operation of the safety system. When large failure occurs, we get -- or a significant failure occurs -- we get an upset in the plant, generally followed up very quickly by reactor trip.

When that occurs, the ICS role in operation and control of the plant is minimal. The rods are in the core. The turbine is tripped and the ICS really no longer is operating the plant.

Our recommendations were based upon failure modes that we thought were undesirable from an operability standpoint. We then said, these failure modes should be examined on a plant-specific basis and, if appropriate, changes performed.

That study, however, was applicable to all ICS's, because they basically have the same functional design and performance.

CHAIRMAN SMITH: Did you use the word "fail" as a verb? You "failed" the components? You disabled them?

WITNESS JOYNER: That is correct. We postulated failure high, for example, a flow transmitter may measure from zero to 7 million pounds per hour feedwater flow. We would then postulate that that transmitter failed and indicated to the ICS a flow of 7 million pounds or of zero pounds, and looked at the operation of the system when that failure occurred.

(Board conferring.)

DR. JORDAN: I was thinking in terms of the Crystal River event. Was that not a case of a failure neither high nor low, but rather a sudden change, and the ICS misoperating, calling on a higher power than should be, higher pressures therefore, and therefore the operation of the PORV -- now, was that not the type of failure which you didn't -- did you look at failures of that nature?

I asked you this morning, did you consider mid-range failures, and you said no. Does that mean therefore that failures of this type were not included in your failure modes and effect analysis?

WITNESS JOYNER: Well, we felt and I feel -- let's go back to the example of the flow transmitter. It measures zero to 7 million pounds. A mid-scale failure would then indicate 3-1/2 pounds to the ICS.

Now, I felt that a failure that indicated the largest possible flow or the minimum flow would produce the most severe plant response.

DR. JORDAN: Such as therefore a situation that they had an increase in pressure in the reactor system which would result in the operation of the PORV?

WITNESS JOYNER: Yes..

DR. JORDAN: That would be one of the possible ways it could fail, then?

WITNESS JOYNER: Well, the ICS would not fail in that manner.

DR. JORDAN: But the ICS could cause an increase in pressure. Certain failures of the ICS could call for an increase in power in the system, and therefore an increase in the pressure, which would be handled either by reactor trip or by operation of the PORV.

WITNESS JOYNER: Well, the reactor would trip when the failure occurred. It hits the high-pressure trip point, rods drop into the core, and that basically terminates the ICS or minimizes the role of the ICS in control of the plant.

DR. JORDAN: Now, it is true, I guess, that the reactor is supposed to trip before the PORV; is that correct? No, it is the other way around?

Which is it on the modified system?

WITNESS BROUGHTON: On the modified system, the reactor should trip before the PORV opens.

DR. JORDAN: Right.

WITNESS JOYNER: So we inverted the PORV.

DR. JORDAN: Is Crystal River not changed yet? I thought this was well after TMI?

WITNESS JOYNER: I think it was.

DR. JORDAN: Where did the PORV go?

WITNESS JOYNER: Well, I really -- I hesitate to discuss the Crystal River transient, because it has been a while since I looked at the scenario. I did not really work on it.

But it is my understanding that the pressure signal failed -- not the pressure signal. One of the modules in the NNI caused it to open spuriously.

DR. JORDAN: Yes. And now then -- but you say you felt it was not particularly relevant to the study that you were doing, that the Crystal River transient is not relevant to a failure modes and effects analysis of the ICS?

WITNESS JOYNER: What we identified, sir, in the failure modes and effects analysis is that the loss of power should be examined on a plant-specific basis, because we recognize the undesirability of that event.

DR. JORDAN: I see. And this has been done at TMI-1.

MR. BAXTER: Dr. Jordan, my next question was going to be to return to Mr. Sadauskas and Mr. Broughton and ask them to review again the response to B&W recommendation

1-A and what Licensee has done in response to their suggestion that NNI/ICS power supply reliability be examined on a plant-specific basis, and in particular with reference to a figure we have distributed over the luncheon break to the parties and the Board entitled "Electrical Supply to ICS/NNI System," which I would request the reporter mark for identification as Licensee's Exhibit 19.

(The document referred to was marked Licensee Exhibit No. 19 for identification.)

DR. JORDAN: You are going to bring out, then, that there is a failure modes and effects analysis specific to TMI-1?

MR. BAXTER: No, there is not a failure modes and analysis of the TMI ICS specifically.

DR. JORDAN: One of my questions is going to be specifically, then, how do you meet the long-term order item 1, because we believe that applies to TMI-1, not to the across-the-board generic analysis.

MR. BAXTER: We are posing two questions, and let's do it one at a time. The first question to the witness perhaps should be why, in their view, is the analysis performed by B&W applicable to the integrated control system at TMI-1.

My question was going to be to review for the record again what they are doing in response to B&W's recommendation on upgrading the reliability of the power supply.

Let's do them in that order, if you can. First, why is the Licensee's Exhibit 18, the B&W report, applicable to Three Mile Island Unit 1?

WITNESS BROUGHTON: The ICS which was examined by B&W and analyzed in their report is functionally the same ICS as we have at TMI-1. That is, it uses the same input signals in the ICS. It has the same major functional blocks as described in the report, and even down to the details of the individual modules which comprise those functional blocks the TMI-1 system is the same as the system examined by B&W.

The outputs of the ICS are also the same in terms of components that are controlled in the plant, based on the inputs and the logic of the ICS. So one of the things that we did when we got the B&W report was to compare the inputs, the functional description of the system, analyze it and the outputs against what actually exists at TMI-1. And that comparison indicated in some cases there might have been a minor difference between the two systems.

For example, the B&W study talks about an automatic dispatch signal and the effect that that could have on power. That is a signal that could come from a dispatcher outside the plant to change electric load. We do not use that feature in our ICS, so that was a failure that we did not need to consider since it was not specific to TMI-1.

The only difference that we found that was not of that minor nature, that it was an unused feature or the alignment was slightly different, was the difference in the power supply arrangement for the two ICS's. The power supply that we have with the TMI-1 system is one which we described earlier, and we will go into again in some more detail. And the power supply studied in the B&W report is a slightly different power supply.

As a result, we have done more looking at our individual power supplies at TMI-1, which was the first recommendation of the B&W study. So we feel that the failures identified by the B&W generic analysis in terms of which ones they are and what they would cause to have happen in the plant do accurately represent what would take place at TMI-1, because of the similarity of the functional design and the details of inputs and outputs.

MR. BAXTER: The second question, then, would be to review for the Board and the parties again what the Licensee is undertaking to do in response to B&W's recommendation to study on a plant-specific basis the NNI/ICS power supply reliability.

WITNESS SADAUSKAS: Looking at a schematic drawing called "Electrical Supply to ICS/NNI System" that we just submitted as evidence, the ICS system is shown at the bottom of the diagram, identified as "auto" and "aux," "hex," "hey," and "fan."

DR. JORDAN: Again, the acoustics in this room --

WITNESS SADAUSKAS: The ICS sub-feeder system is shown at the bottom of this diagram, and the sub-feeders are identified. There are six of them. They are fed -- the power source for the ICS system is 12-volt, 60-cycle, single-phase power.

This power is developed from the engineered safeguards bus.

DR. JORDAN: What?

WITNESS SADAUSKAS: Engineered safeguards bus, which can also be powered by the red deisel in the event that off-site power is lost.

DR. JORDAN: That is the ES bus on the right in this diagram; is that correct?

WITNESS SADAUSKAS: At the top of the diagram,, the 480-volt supply -- there is a signal on the right that means the voltage regulator goes to the ES bus.

DR. JORDAN: Okay.

WITNESS SADAUSKAS: Normally, power is fed from the 480-volt bus through the rectifier, through the inverter, it is converted to 120-volt AC that the ICS can use.

In the event that the rectifier fails, an alternate source as shown on this diagram is from the red battery. That is also converted to 120-volt, 60-cycle power that the ICS can use.

DR. JORDAN: So is it normally, then, connected to the battery in the inverter? Is that the normal operation?

WITNESS SADAUSKAS: The inverter -- the power source normally is from the AC power in the plant. We do not draw on the battery normally. The battery is drawn upon in the event that the AC system fails.

DR. JORDAN: I see.

WITNESS SADAUSKAS: In the event that the inverter fails, a static auto transfer switch that is shown on this sketch monitors the voltage level of the VBA bus as shown. And this switch is designed to provide transfer automatically to the bus on the right, labeled TRA, which is a 120-volt, single-phase regulated bus.

DR. JORDAN: Is that the one that says "new remote-operated manual transfer switch"?

WITNESS SADAUSKAS: No, it is not. It is the one that is labeled "static auto transfer switch."

DR. JORDAN: That switch is normally to the right?

WITNESS SADAUSKAS: The switch is normally to the left. The power is normally flowing from the inverter.

DR. JORDAN: Oh, I misunderstood your answer, then. I thought you -- I thought I asked if the normal power supply was from the inverter battery, and you said the normal supply was --

WITNESS SADAUSKAS: The inverter is fed from two sources. It is fed from the red battery --

DR. JORDAN: The inverter is fed to --

WITNESS SADAUSKAS: From two sources. You can see that it is fed from the red battery, and it is also fed from the 480-volt engineered safeguards bus.

DR. JORDAN: Through a rectifier.

WITNESS SADAUSKAS: That is correct.

DR. JORDAN: You are normally on a 480-volt bus?

WITNESS SADAUSKAS: That is correct.

DR. JORDAN: Rather than the battery.

WITNESS SADAUSKAS: Correct.

DR. JORDAN: I presume that is -- that switch -- no, the battery; doesn't it just ride on the rectifier?

WITNESS SADAUSKAS: The battery is being charged from the 480-volt ES bus. It is floating on the 125-volt DC system.

DR. JORDAN: So you do not have to make any changes at all if you lose the 480-volt ES bus. The battery is automatically -- it is there.

WITNESS SADAUSKAS: Yes. There is an auctioneer circuit which looks at both power sources and it transfers power to the battery in the event that the 480-volt bus fails.

DR. JORDAN: I see. So the inverter does not ride on the battery all the time, with the rectifier charging the battery. That's what it looks like in the circuit diagram there, but that is not the case; is that what you are telling me?

WITNESS SADAUSKAS: No, it is the case.

DR. JORDAN: It is?

WITNESS SADAUSKAS: The inverter can take power from the battery and convert it to AC power, or it can take rectified AC power from the 480-volt bus and convert it into AC power for use by the ICS.

DR. JORDAN: It is one or the other. It is not both. It is not both simultaneously?

WITNESS SADAUSKAS: No, it is not, that is correct.

Now, in the event that the inverter fails, the static auto transfer switch is designed to automatically transfer power from the inverter which has failed to the 120-volt single-phase regulated bus on the right. And it is a high-speed transfer, and was pointed out earlier.

We do not anticipate any transients occurring when this transfer takes place.

DR. JORDAN: All right. But this is another 480-volt engineered safety bus, presumably?

WITNESS SADAUSKAS: It is a bus independent of the inverter. It is powered from the red engineered safeguards power system, as is the --

DR. JORDAN: But there are two Class 1-E power buses, and they are both shown here, one on the left and one on the right; isn't that correct?

WITNESS SADAUSKAS: That is correct.

DR. JORDAN: Is that right?

WITNESS SADAUSKAS: That is correct, yes, sir. Now, as a result of the incident at Oconee --

DR. JORDAN: What?

WITNESS SADAUSKAS: The incident at the Oconee Nuclear Station, Duke Power, where the static auto transfer switch failed to transfer. We are aware of that incident and in order to improve the reliability of the Three Mile Island power transfer system we are installing a new remote-operated manual transfer switch, which is so labeled on this sketch.

And it is downstream of the automatic switch. In the event that the automatic switch fails to transfer, an alarm will be provided to the control room operator and the operator will manually transfer power, again to the same bus, the 120-volt bus TPA, via the new remote-operated manual transfer switch.

DR. JORDAN: That is the one that takes a little while to operate?

WITNESS SADAUSKAS: That is a manual operation, yes.

DR. JORDAN: Yes, yes.

And during that period of time when you have lost power, say from the normal -- out of the inverter or the second engineered safety bus by failure of that transfer switch, during that period once you have lost power, are you saying that the controls will remain the same, the control rod positions, the valve positions for feeding feedwater and so on? And so therefore during this period the plant will continue to operate?

WITNESS BROUGHTON: It is likely, in a case where the automatic transfer switch does not function and it requires the operator to manually transfer power, that enough time would last between the loss of power and when it was restored that the plant would go through some sort of an upset, which might very well cause a trip of the reactor.

DR. JORDAN: Yes, okay. All right.

WITNESS BROUGHTON: I would note, however, that this manual transfer switch for the new remote-operated transfer switch is located in the control room. The operator has a button in the control room that he can actuate to cause this transfer switch to move. He does not have to leave the control room to go out and manually operate breakers.

It is labeled a manual transfer switch because it takes an operator's action to cause the --

DR. JORDAN: Of course, the hope is you will be able to make the transfer, presumably, quickly enough to keep the plant on line, because after all that is your main job, to keep the plant on line.

WITNESS BROUGHTON: hat is correct. And that is function of that static auto transfer switch.

DR. JORDAN: Yes, yes.

WITNESS SADAUSKAS: The addition of the manual switch is merely a way to improve the reliability of the transfer of power.

DR. JORDAN: Say it again?

WITNESS SADAUSKAS: The addition of the manual transfer switch is merely a way to improve the reliability of the power transfer, the reliability of the power to the ICS systems.

DR. JORDAN: Yes, all right.

Do you have any further questions, Mr. Baxter?

MR. BAXTER: Does that complete your response to B&W recommendation 1-A, the status of it? Do you have anything else?

WITNESS SADAUSKAS: I have nothing further to say.

WITNESS BROUGHTON: There are other things we are doing to look at in terms of improvements of reliability of the ICS/NNI power supplies. Those are not specifically as a result of this recc mendation in the B&W report. They are more along the lines of improvements due to other events, for example the Crystal River event.

CHAIRMAN SMITH: For example what?

WITNESS BROUGHTON: We mentioned some of those earlier. But they would be --

CHAIRMAN SMITH: I did not hear your final word, that is all.

WITNESS BROUGHTON: The Crystal River 3 event was another event which brought the reliability of power into question, and as a result we are doing further studies on how to improve reliability of power.

CHAIRMAN SMITH: Could any member of the panel explain somewhat better the Crystal River event? Our understanding of it is that there was a spurious signal which actually resulted in the partial withdrawal of the control rods in the reactor.

Is that your understanding?

WITNESS JOYNER: I am not sure if the rods started out immediately or not, sir. Trip occurred very shortly after the loss of power occurred.

CHAIRMAN SMITH: There was an increase, however, in the neutron flux.

WITNESS JOYNER: The indicated neutron flux that the operator?

CHAIRMAN SMITH: In actuality.

WITNESS JOYNER: I suspect there was a small increase. I never have examined those transients. I know approximately what happened, but I'm a little bit hesitant to talk about it be.ause I might give some misinformation.

I am reasonably sure that the trip was within eight to ten seconds following loss of power.

CHAIRMAN SMITH: Is -- except, of course, the difference in the reactor, do fossil fuel plants have a similar system?

WITNESS JOYNER: They use the same kind of hardware, but of course the control system is different, as it has to be, because, you know, we have a reactor as opposed to a fossil-fired boiler. The ICS and the fossil controllers are very similar, and the ICS was indeed an evolution from control systems that controlled the operation of B&W once-through steam generators in fossil plants.

CHAIRMAN SMITH: The principal goal, then, is to go to reliability, economy and efficien ?

WITNESS JOYNER: That is correct, sir.

CHAIRMAN SMITH: I mean reliability of the plant as a whole.

WITNESS JOYNER: Right. You know, the purpose is to make megawatts. That is what we would like to optimize.

MR. BAXTER: Those are all my clarification questions. Thank you.

CHAIRMAN SMITH: Are you going to offer L-19?

MR. BAXTER: Yes. I so move.

CHAIRMAN SMITH: It is received.

(The document referred to, previously marked for identification as Licensee Exhibit No. 19, was received in evidence.)

CHAIRMAN SMITH: If I can interrupt your cross-examination, Mr. Sholly, do you have a report from Dr. Johnsrud, or can you tell us what the plans are?

MR. SHOLLY: It places me in an uncomfortable position. I can report to you that under present circumstances Dr. Johnsrud will not be able to be here.

CHAIRMAN SMITH: I don't want to --

MR. SHOLLY: She will be communicating with the Board. She indicated to me she would be getting a letter out today.

As far as where this leaves us with the in-plant instrument ranges contentions, they will not be here and I am going to have to take a close look here. Hopefully, I can do it at the afternoon break.

CHAIRMAN SMITH: To protect your interests --

MR. SHOLLY: And give you some idea of whether I wish to go forward with it or just decline cross-examining on it and move ahead.

I don't know how satisfactory that is, but that is the best I can come up with.

CHAIRMAN SMITH: I guess we are all involved in it. The Board is going to have to take a look at it.

MR. BAXTER: Mr. Chairman, I wanted to go back to that after lunch. I'm glad you brought it up. I had forgotten it.

For my planning purposes, in order to make sure we have witnesses here and keep the flow of the hearing going, I basically have to call these things two days ahead of time. And based on my preliminary discussions with Mr. Sholly, I think after the integrated control system issue the next two may go comparatively faster. And so we will be needing to make a determination, I think late today or certainly early tomorrow morning, as to where the schedule will be, if we can possibly do it.

CHAIRMAN SMITH: Mr. Sholly is going to have a busy day today. He has to have some time.

I think we all have to go back and take a look at the contention and the testimony that has been offered on it, or has been proposed. It seems to me the earliest we can take it up would be tomorrow morning, won't it, unless we take a rather long break at mid-afternoon.

MR. BAXTER: If we can take it up as the first item tomorrow morning, that would be soon enough for me.

CHAIRMAN SMITH: Okay. Would that be agreeable?

MR. CUTCHIN: To take it up tomorrow, sir? I have a similar problem, because I was going to bring it up at the same time we discussed the schedule. I have the witness available for the subject we are presently on. I have the witness available for the next issue that we are to take up.

But I have a scheduling problem with respect to the computer issue, which, if we get to it this week, there will be no problem. However, if the computer issue, which would be the issue after next, runs over into next week, the situation is this. Mr. Joyce, who is our witness on that subject, has a long-scheduled computer room review out, I believe, at Comanche Peak, and he is the team leader of a ten-man team, and it would be impossible for him to reschedule next week.

So we may run out of gas in a hurry if we start shuffling things around and be back to the UCS contentions very rapidly.

CHAIRMAN SMITH: Mr. Sholly, the Board -- I myself can call Dr. Johnsrud, or Ms. Moran can, if your relationship makes it difficult for you to be candid with the Board. Did Dr. Johnsrud authorize you to say that she would not appear this week?

MR. SHOLLY: That is correct.

CHAIRMAN SMITH: And that the relief she is seeking is going to be by letter?

MR. SHOLLY: That is also correct.

CHAIRMAN SMITH: Is there anything else she authorized you to say?

MR. SHOLLY: No, sir.

I believe if we get like a 15 or 20-minute break this afternoon, I think I can pretty well take a look at the contentions and the testimony and tell you what I want to do with them.

CHAIRMAN SMITH: All right.

MR. SHOLLY: I would like to try to get it out of the way today.

CHAIRMAN SMITH: All right. Okay, we'll take a little bit longer break and get that out of the way.

Go ahead with your cross-examination.

Off the record.

(Discussion off the record.)

CROSS-EXAMINATION -- RESUMED

BY MR. SHOLLY:

Q What I would like to do is tie together there some of the loose ends this morning before I get into some other areas.

Dr. Joyner, Dr. Jordan asked yo some questions, I believe, about the B&W analysis in terms of failing signals high and low and mid-scale failures. Are you familiar at all with a meeting summary that was prepared that dealt with a meeting that took place on October 23, 1979? It dealt with a discussion of the B&W 1564 report?

A (WITNESS JOYNER) Yes.

Q Were you not in attendance at that meeting?

A (WITNESS JOYNER) Yes, yes, I was.

MR. SHOLLY: I have a copy of the meeting summary here. I would like to have it marked for identification Sholly Exhibit 1.

(Mr. Sholly distributes documents to the Board and parties.)

(The document referred to was marked Sholly Exhibit No. 1 for identification.)

MR. SHOLLY: I should point out here, before I go on any further, that what I have handed to you deleted a repetition of the questions that are posed in the meeting summary. They are in the original document. There is an enclosure from Oak Ridge which poses the same questions which are addressed in the pages which I have distributed. So I deleted that. I did not think it was particularly necessary.

I also deleted the service lists, if that is okay with everyone. I just wanted to let you know.

DR. LITTLE: Mr. Sholly, I notice that on the list of attendees at the meeting there is -- I presume that is Mr. Joyner's name which is misspelled on the list there; is that correct?

WITNESS JOYNER: I do not know. I was at the meeting.

DR. LITTLE: It must be you, then.

MR. SHOLLY: That is why I asked. I thought it was him and it was misspelled.

WITNESS JOYNER: I don't have a list of attendees. It is handwritten?

DR. LITTLE: Last page.

MR. SHOLLY: Enclosure 2 to the original document.

WITNESS JOYNER: I don't have that.

Well, that must be me, obviously. There was no "Voyner" there.

CHAIRMAN SMITH: Someone like you.

WITNESS JOYNER: I hope not.

BY MR. SHOLLY: (Resuming)

Q If you will look at Question 2, which is at the bottom of page 2 --

A My numbers are different from yours. Okay.

Q It begins with the words, quote, "The ICS signal input failure assumptions." Is that the same question you are on now?

A (WITNESS JOYNER) I think we have different copies. I guess maybe you had better pass me a copy. I suspect it is exactly the same. It is just typed differently.

CHAIRMAN SMITH: I think it is better if you work from a copy that will be received in evidence.

WITNESS JOYNER: Okay. This is okay. Thank you.

BY MR. SHOLLY: (Resuming)

Q Question 2, the bottom of page 2.

A (WITNESS JOYNER) I have it.

Q It asks about the very issue that Dr. Jordan had asked about, the possibility for mid-scale failures. And the response indicates that the failure modes and effects analysis as performed by B&W would not highlight these types of failures because of the definition of the ICS boundary; and that there were at that point, anyway, no plans to include mid-scale failures.

Has there been any additional work done on mid-scale failures, or is any planned?

A (WITNESS JOYNER) Well, we have not expanded the work to include mid-scale failures. The most credible -- the event that would probably cause mid-scale failures is loss of power, and of course that was a recommendation of the report.

Now, in a single failure sense we believe, and I still believe, that high and low failures of inputs and outputs and modules gives a more drastic NMS response than mid-scale failures. And I really do not think that we missed any important failure modes by not assuming -- by not looking at mid-scale failures.

Q Are you familiar with the Oak Ridge review report on B&W 1564?

A (WITNESS JOYNER) Yes.

MR. SHOLLY: I would like to distribute that and have it marked for identification Sholly Exhibit 2.

(Mr. Sholly distributes documents to the Board and parties.)

(The document referred to was marked Sholly Exhibit No. 2 for identification.)

(Pause.)

BY MR. SHOLLY: (Resuming)

Q If you refer to page 20 at the bottom, Question 2 we have just been discussing is repeated, and there is a somewhat different response prepared. Apparently this one was prepared by Oak Ridge personnel, whereas the NRC meeting summary was prepared by someone from the NRC staff.

On page 21 there is a comment by Oak Ridge. It says: "We find no specific evidence to confirm this assumption." It says: "With regard to multiple-input single failures, operating experience confirms that this is a highly credible event which can result from the single failure of a power supply in the NNI in the input signal selection circuitry."

It goes on to give an example of that.

Now, I believe you indicated that you did not feel that the mid-scale failures were important, or that they would not -- that it would not lead to any additional --

A (WITNESS JOYNER) I said the case where you are most likely to get mid-scale failures is the power supply failure. And we did recommend improvements in NNI/ICS power supply.

On page 21 they say: "Operating experience confirms that this is a highly credible event which can result from the single failure of a power supply." I would question the statement "highly credible," which in my mind means -- might mean highly probable, which has not been the case at all.

But power supply failures do cause mid-scale failures. You know, we know that. And therefore we recommended improvements in that area.

Q I might ask Mr. Broughton and Mr. Sadauskas, then, what specifically has been done by the Licensee in terms of analyzing mid-scale failures or multiple failures resulting from this type of power failure?

A (WITNESS BROUGHTON) The NNI/ICS power supply reliability study that we have mentioned previously is the study which we are conducting to determine what the effects would be if various power supplies were failed. So this would include not only mid-scale failures of instruments, if that was caused by the power supply, but any other failure.

The study is in progress. There have been some conclusions reached. But in order to actually complete the study and feel confident in its results, one of the steps would be to actually go out and conduct a test in the field, where power supplies were de-energized and we could note the failures of the various components and indications.

I can review what some of the preliminary conclusions are of that study, if that would be helpful, to indicate what some of these effects would be.

Q I do not particularly think it is necessary. If the Board thinks it will help, it is fine with me.

DR. JORDAN: Yes, I would like to hear some of the conclusions of the study.

WITNESS BROUGHTON: All right. If I can refer you back to the last Licensee's exhibit, which was the Exhibit 19, the diagram of the power supplies to the NNI/ICS. At the bottom of that exhibit, we list a distribution panel ATA, and from it there are six feeders to the ICS and NNI.

We have examined what would take place if each of these feeders were lost individually, which is a possibility. And we are also looking at what would happen if there was a sustained loss of power to that complete panel.

Starting with the feeder on the extreme right, the one labeled "fan," that simply supplies power to cooling fans in equipment cabinets. So the result of a failure would be, over a prolonged period of time, increased temperatures, possible component failures, but certainly nothing immediate in terms of effect on the ICS or the NNI or the plant due to that type of failure.

The next two power supplies are labeled "HEX" and "HEY." In general, the things supplied by those power supplies are transmitters for instruments in the plant or recorders for those instruments. And the general effect of losing either HEX or HEY is that some indication may be lost. It may be an indication which is not part of the control system and therefore would not affect plant control immediately.

I think in some cases there is some indication which might be part of the control system. If that were the case, then there could be some upset in one of the loops that was involved in using that particular instrument.

The next power supply over is the one labeled "aux" and that supplies power to control the emergency feedwater system valves when those valves are being controlled by the ICS. So failure of that particular power supply when the emergency feedwater system was not in operation, when the plant is at power, for example, would have no immediate effect.

If the emergency feedwater system were in operation following operation at power, then there might be some effect on the automatic control of level using the emergency feedwater system, or perhaps on manual control of emergency feedwater using the ICS.

But at any rate, independently of this aux power to the ICS, we are installing in TMI-1 a completely separate way to control the emergency feedwater system independent of the ICS, so that if this aux power were lost automatic control would not be available for the ICS system, but there would be manual control available.

CHAIRMAN SMITH: That is a result of a Commission order in this case?

WITNESS BROUGHTON: I believe that was the source of the change. I note that appears in the order. And this change will address that item in the order, yes.

BY MR. SHOLLY: (Resuming)

Q And would the failure of the aux supply be annunciated to the operators so that they would know to undertake manual control of the feedwater?

A (WITNESS BROUGHTON) Yes. Perhaps I should have mentioned that one of the modifications we are putting into the plant before restart will be an annunciator which will indicate when power to any of these six feeders has been lost. So there will be a light and an alarm in the control room, an audible alarm which will tell the operator that he has a problem with one of these power supplies.

And in addition, there will be indicating lights which correspond to these power supplies, which will tell him whether or not that power supply is energized or de-energized. So he will be warned that he has a power supply failure and he will be able to identify which of these feeders is inoperative.

CHAIRMAN SMITH: What is happening at the plant when the auxiliary feedwater is being controlled by the ICS? What mode of operation is prevailing when that is happening?

WITNESS BROUGHTON: The emergency feedwater system would only be used when the reactor plant has been shut down. So you would not be operating the turbine. There would be a minimal number of systems operating in the steam plant and you would simply be removing residual heat.

DR. JORDAN: But there was, during previous testimony, questions concerning what might happen if we had failures on the part of the ICS system. And the question was, for example, could there be a failure of the ICS system that would call for closure of the valve in spite of the fact that the valve should be opened.

Are there failures of that type, or are there also failures of that type that would cause the opening of the valve full open and flooding of the steam generators? Have such failures been looked at?

WITNESS BROUGHTON: Those were the types of failures picked up by the failures modes and effects analysis done by B&W. Those failures might be caused by faulty input signals, faulty modules within the ICS, or faulty output signals.

Since there are only a few components that are actually controlled by the ICS, there may be several types of failures which could cause the component to malfunction. But the malfunctions you mentioned of a valve being open when it should be shut or vice versa are the types identified by the failure modes and effects analysis.

DR. JORDAN: It seems to me you are now

controlling an engineered safety feature. It is a little different. You are not -- it is a little different, you see, from the protection system. You do not try to control the protection system. You control the rods. The protection system is automatic.

You are now controlling an engineered safety feature, a system that is vital to safety. So the failures in that system can result in serious damage to either the steam generators or to the core.

WITNESS BROUGHTON: I did not mention any engineered safety feature systems that we were controlling.

DR. JORDAN: You do not consider the emergency feedwater system as an engineered safety feature?

WITNESS BROUGHTON: With respect to the emergency feedwater system and the fact that it can be controlled by the ICS --

DR. JORDAN: Do you consider that an engineered safety feature?

WITNESS BROUGHTON: I do not believe we have considered it as such, although we have said that we will be upgrading it in the future to where it is fully safety-grade and would be considered an engineered safety feature. In part of that upgrade, we will providing all control of that system independently of the ICS. That is certainly one of the things that we would have to do to make it an engineered safety feature.

DR. JORDAN: Good. And we understand that.

But I am now concerned about the possibility of ICS failures preventing that from operating, when it should be keeping the operator even from operating or overfilling the steam generator, that this -- these are -- as I say, this is an important safety system, whether you call it an engineered safety feature or not. It is a very important system for the safety of the plant.

And so here is a system that is being controlled by the ICS, and I am very much concerned about interactions between the ICS and that system and those type of failures.

Have you considered those, and what is the situation?

WITNESS BROUGHTON: Yes. Let's talk, then, for a few minutes about how --

DR. JORDAN: I believe this is plant-specific and not B&W -- the B&W system has various ways of providing engineered -- Davis Besse is different, for example, than TMI-1.

WITNESS JOYNER: Could I offer something, sir?

DR. JORDAN: Yes.

WITNESS JOYNER: The ICS controls only the auxiliary feed valves. It does not control --

DR. JORDAN: Precisely.

WITNESS JOYNER: It does not control the startup pumps or what have you. So its role is minimal in control of emergency feedwater, just control of the two valves.

DR. JORDAN: Shut or open; it is terribly important.

WITNESS JOYNER: That is correct, sir. And we could find no single failure that would cause both emergency feed valves not to provide water to the steam generator. So there was no single failure in the ICS which would prevent proper operation of the ICS.

They run on two separate generators, two level measurements, two set points, two sets of modules. So no single failure could be found that could prevent operation of both sides of the emergency feed system.

And in addition, if you have a failure and you have not lined up -- it is my understanding, and I will ask these gentlemen to correct me, because it is plant-specific. But unless you have an aux feed start, the auxiliary feedwater valves will not be lined up. So a failure in the ICS would not affect the system at all, in that the valves are not lined up to provide water to the generators unless we have an auxiliary feedwater start.

That is right, isn't it, Gary?

WITNESS BROUGHTON: I do not believe that is the case at TMI-1. But with regard to the same comments, even if the ICS were, say, to open the emergency feedwater valves when the valves should not be opened, if the pumps are not running, if the system has not started, there will not be any flow into the steam generator, so there will be no consequence to the plant as a result of that type of failure.

DR. JORDAN: Under certain circumstances, you have said that the integrated control system does control the position of the valves in the emergency feedwater system, and it controls those valves so as to set the level of the water in the steam generators to 20 percent or 50 percent or whatever the desired level is.

Are you saying that there is no failure in the system that would fail -- it would always set the level at 20 percent; no matter what the failure is, that the level automatically goes to 20 percent or whatever it --

WITNESS JOYNER: What I was saying is there is no single failure that would affect emergency feedwater control to both generators.

DR. JORDAN: To both?

WITNESS JOYNER: To both A and B generators. Each generator is provided with emergency feedwater. Each has its own valve. The ICS then controls --

DR. JORDAN: The ICS -- why can't it tell both those valves to go shut or both of the valves to go wide-open?

WITNESS JOYNER: It could, if we assumed multiple failures.

DR. JORDAN: But no single failure will do it?

WITNESS JOYNER: That is correct.

DR. JORDAN: That is what you are saying? That has been one of the consequences, then, of your failure modes and effects analysis.

WITNESS JOYNER: We found no single failure which could cause misoperation of both emergency feed systems. And as long as we get some emergency -- if we get flow to one generator, we are generally okay.

DR. JORDAN: All right. How about overfilling?

WITNESS JOYNER: There are some failures which could cause one generator to overfeed. Now, that information is readily available to the operator and the flow rate is such that he would have time to --

DR. JORDAN: He gets a warning?

WITNESS JOYNER: He gets a warning. And in addition, unless the aux feed system is started, it would not overfeed. It is a very limited amount of time. Most of the time we do not have aux feedwater. Most of the time we have main feedwater. And a failure in that case would not really affect the system.

DR. JORDAN: Yes, I am concerned about main feedwater transients.

Okay, that is enough for the moment. Go ahead, Mr. Sholly.

BY MR. SHOLLY: (Resuming)

Q Along this immediate line of single failures, I am correct that the integrated control system is not safety-grade; is that true?

A (WITNESS JOYNER) That is true.

Q Why wouldn't it be prudent, then, to assume multiple failures? If I understand NRC practice, anyway, in a system which is not safety-grade you assume multiple failures or you assume that the system fails in a combination of worst possible ways in order to do your safety analysis, or the effects analysis. Why wasn't that done in the failure modes and effects analysis?

A (WITNESS JOYNER) That was not a safety analysis, as you might note. A failure modes and effects analysis is a single failure technique, that we look at a failure and determine what the effect of that failure is on the system under study. That is the way it is done.

Q Have you done any studies at all on multiple failures regarding ICS?

A (WITNESS JOYNER) Yes, yes.

Q What did those studies involve?

A (WITNESS JOYNER) Well, they were not done for any particular reason I can recall, except knowledge on our part as to what would happen. They were operability type studies to get a feel for what the plant transient was.

Q Did the studies look at all at the safety consequences of multiple failures?

A Well, that is the safety -- the safety analysis performed for the plants looks at multiple failures. Now, this analysis was done as a single failure type analysis to determine areas where we might need to study or to make changes to the ICS, where failures were possible or had been experienced in the field.

Q This is something that concerned me very greatly in reading through the B&W 1564 and the Oak Ridge review report on 1564. And I found a number of instances in the Oak Ridge report where they referred to the lack of multiple failure analyses.

In particular, I think there are two quotes that I would like you to look at and perhaps you can get an idea of what I'm driving at. Maybe you can be a little more responsive. I may not be posing the question quite the way I want to.

If you would look on page 8, about the middle of the page, the second paragraph under "Multiple Failures." The last sentence in the first paragraph concludes what you said, that: "The failure modes and effects analysis is suited to the single failure analysis and it is not convenient for addressing multiple failures."

It goes on to say that: "The inability to address multiple failures may be sigificant, since failures can occur in the ICS without being annunciated." And the last part of the sentences says that: "Since sufficient evidence to the contrary does not exist, multiple failure-induced transients may have a significant probability."

Without analyzing that, how could you be sure, then, for instance, that multiple failures would not result in, say, both of the feedwater valves being closed, as Dr. Jordan was driving at?

A (WITNESS JOYNER) Well, when we have -- let me stress again, when we have a major upset in the system, the first or one of the first things that happens is we get a reactor trip, or we would expect a reactor trip. After that, the influence of the ICS control on plant performance is minimal.

We control feedwater and we control atmospheric dump valves, or the condenser dump valves if the condenser is available. We do not control -- manipulate control rods or the turbine.

So the effect of ICS malfunction is greatly minimized by the trip of the reactor. In any event, effects of multiple failures are bounded by the safety analysis, and we feel confident that these failures are not a significant threat to proper operation of the plant.

The safety systems are not affected by ICS failures or performance, and they operate independently following reactor trip.

DR. JORDAN: By "safety systems," are you now including emergency feedwater or not?

WITNESS JOYNER: No, sir, I am not.

DR. JORDAN: You are not. Okay.

WITNESS JOYNER: Although I might point out that emergency feedwater can be operated independently of the ICS.

BY MR. SHOLLY: (Resuming)

Q I understand what your personal or professional opinion is regarding the possible effects of multiple failures. But the Oak Ridge report specifically says, at least the way I read it, that sufficient evidence to the contrary does not exist. So they seem to be assuming, in the lack of or absence of specific evidence to the contrary, that multiple failure-induced transients may have a significant probability. And to me that is a rather significant conclusion.

I think perhaps something to explore at this point is just exactly what is done in the safety analysis you are talking about. Is that the safety analysis for the plant or for the system? Which safety analysis are you referring to?

A (WITNESS JOYNER) The plant safety analysis, you know, TMI-1 safety analysis. You know, not the ICS safety analysis. I do not know of any.

I missed your question somewhat, I think.

Q The safety analysis for TMI-1 would include analysis of multiple failures in the ICS system?

A (WITNESS JOYNER) It does not assume improper operation of non-safety systems. And I think, too, if we go back to the Oak Ridge report and look at page 15 and 16 of that report, we see a lot of agreement that the study was indeed sufficient. For instance, at the bottom of page 15, the last sentence states: "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."

And chapter 6 basically concludes, the report is adequate and sufficient for its purpose.

Q I recognize what that last sentence there that you read states. I believe if you examine it in the context of what else is said on that page and the preceding pages, you will see that they are referring to failures within the ICS as it is defined and limited in the B&W report.

In the Oak Ridge review report, it goes to some length explaining why they feel that limitation -- why it places limitations itself on the utility of the report itself.

One of the things they pointed to -- give me a moment.

(Pause.)

Q On page 13, the second paragraph, under "Operating Data," it concludes that: "Only two percent of commercial operating plant trips were caused by internal ICS failures, excluding power supplies."

I think if you look at it in that context, that external failures within the ICS certainly do not appear to constitute a significant threat. But if you read further in that paragraph on page 13, it says: "Of the remaining trips, one-third were caused by operator-technician errors and two-thirds by ICS interactions with control equipment, failures of controlled equipment, ICS inputs, including power supplies, and failures of other control systems."

This seems to be one of Oak Ridge's major criticisms of the B&W report, that it failed to consider a sufficiently large or sufficiently scoped definition of just what the ICS was, but rather defined it rather narrowly.

A (WITNESS JOYNER) Well, if you read the first five chapters -- sections, you might get that impression. I keep -- I had to read the thing three or four times myself to really get what I think was intended by the writers of this report.

Section 6, the evaluation and recommendations, is really where they say what they think. If you look at the top paragraph on page 16, paragraph 2, it says: "The FMEA would have been of greater significance if it had been expanded to use other systems with which the ICS interacts, such as non-nuclear instrumentation and its power signal sources."

Then it goes on to say, skipping a sentence: "It is not evident that redoing the analysis at this point to include this information would be worthwhile."

This is a straightforward statement of the problem -- of their conclusion, I think.

Q I understand their conclusion and I understand what they said in the first five chapters. They seem to me to be somewhat contradictory. Unfortunately, I am not technically qualified to address that. That leaves me in a bit of a fix right now.

It just seems to me that there is some contradiction between between what their statements are in the first five chapters and what their conclusions are. The conclusions do not seem to follow from their discussion, and some of their statements in the discussion seem to me to directly contradict or cast doubt on some of the testimony, and also on some of the oral testimony that has been going on today.

The discussion of multiple failures, I think, is one example.

MR. BAXTER: Mr. Chairman.

CHAIRMAN SMITH: Dr. Joyner, you indicated you had spent some time studying the report, trying to understand what was in the minds of the authors, and it was a review of your own report.

Can you give any help to Mr. Sholly in addressing -- I mean, in the first place, to understand his perception of the report? Can you give him any help along that line?

WITNESS JOYNER: I can give you what I think about the report and whether that is the correct assessment of why it seems to be contradictory or not I don't know.

CHAIRMAN SMITH: Would you object to that, Mr. Sholly?

MR. SHOLLY: No, sir.

CHAIRMAN SMITH: It seems to be what you are seeking.

MR. SHOLLY: Fine. Go ahead.

WITNESS JOYNER: If you look at the title page --

CHAIRMAN SMITH: What?

WITNESS JOYNER: The title page, page 1, where it gives the authors of the report, the top three -- Anderson, Ditto, and Stone -- they are from Oak Ridge. The next three

-- Hedrick, McBride, and Penlend -- are from SAI.

I suspect the first five factors were written by Oak Ridge and the rest by SAI.

MR. SHOLLY: When the staff gets on, I will try and remember to ask them that.

WITNESS JOYNER: I might add that there is nothing wrong with a discussion -- a report which discusses what might have been done, what could have been done, and then evaluates those alternatives and determines whether or not it really is justified.

Because we could have analyzed multiple failures does not mean it was necessarily required, or even desirable.

BY MR. SHOLLY: (Resuming)

Q Perhaps I can focus in on one part in particular in the Oak Ridge report that I feel gives me the most problems, and maybe you can comment on how you feel. That is reflected in their recommendations and conclusions. If you look at the general findings of the ORNL review, which begins on page 3, keep in mind that one of the very first things they point to, they say in the second sentence in that first paragraph, they say:

"With no other concerns expressed in the guidance given in the NRC order, the B&W analysis is more notable for what it does not include than for what it does include."

And it goes on to list perhaps half a dozen or eight different things that were not in the report, many of which seem to be rather important. And what I am trying to get to is just how useful is the FMEA which was done, when there are all these other questions remaining, some of which apparently were raised by the Commission order that the FMEA was done in response to?

A (WITNESS JOYNER) The first question, please?

Q What Commission action caused B&W to do B&W 1564?

A (WITNESS JOYNER) My understanding of the agreement between B&W and NRC is based on a memo of April 1979 from one of our people to Mr. Denton, in which we explained to him in a reasonably straightforward fashion what we would do in the reliability study.

It was not performed as the result of an NRC order referred to in that paragraph. We agreed -- and I will try to remember what we agreed to do:

One, to do a survey of field performance of the ICS;

Two, to perform a failure modes and effects analysis of the ICS, which we understand quite clearly what the ICS is. And one of the things you must do before you start on any kind of failure analysis is understand the system that you are analyzing. And it was quite clear to us what that meant.

Three, we agreed to make recommendations.

And if I think a minute, perhaps I can think of the other four. But in general -- and I can get at the break -- can determine exactly what we agreed to for you, if you would like.

But in general we met that commitment quite well, I am convinced, with the report that we prepared. We did not perform the study as a result of these -- this Commission that is being referred to. That order is May '79 and I was already at work on the report when it was done.

Q In other words, you dispute the position taken in the Oak Ridge report that the FMEA was done in response to NUREG-0560?

MR. BAXTER: Mr. Chairman, I am not sure what the relevance is of what it was done in response to. But I have got a point of clarification that may or may not help Mr. Sholly.

But the same confusion arose in the Rancho Seco case. If you look at page 2 of this Oak Ridge document, they cite as footnote 2 -- and they are citing to a sentence that says "NRC orders," and the footnote is to NUREG-0560. We find a confusion on the author's part here between that staff document, which was issued in late May, and Commission orders which had already been given to B&W Licensees. And what they are referring to in this page is the executive summary of the NRC orders.

It does not exist. It is the executive summary of NUREG--0560. So I believe throughout the document, when the Oak Ridge authors are speaking about what they view to be the Commission's directive they are really talking about that Tedesco report, the first staff study of feedwater transients, and nothing that the Commission ordered.

MR. JORDAN: I had more or less concluded the same thing, but I was going to ask specifically if that was the licensee's and the staff understanding, too. Could the staff -- are they in a position to reply right now? I think it is a fairly important point.

MR. SHOLLY: I think it is very important in order to determine whether the study met what it was supposed to or not.

MR. CUTCHIN: Let us discuss it and come back after the break, Mr. Chairman, and give you a complete answer.

CHAIRMAN SMITH: Fine.

(Board conferring.)

CHAIRMAN SMITH: While we are on this subject, is there anyone able to tell the Board what role, if any, did the ICS play in the accident at TMI-2? We were wondering how this order happened to end up in the Commission's order of August 9. Its close relationship to the high pressure injection -- I mean the auxiliary feedwater?

MR. BROUGHTON: I do not know what the reasons were for the NRC's interest in the study, but I have looked at the TMI-2 accident sequence enough to know that the ICS was not a factor in that accident. It was not an initiator and it performed as it should have throughout the time that it was called upon.

CHAIRMAN SMITH: Perhaps if it had not been expressly set forth in the order, except for its relationship to the feedwater system it would not be within the scope of this proceeding.

Mr. Sholly, do you have any feeling on this?

MR. SHOLLY: The only thing I might suggest we might find out is to go back to minutes of Commission meetings when they were debating the August 9th order, but I do not know if you are going to find anything there or not.

CHAIRMAN SMITH: It also appeared in the Davis-Besse order and the Rancho Seco order.

MR. BAXTER: Yes, sir, it is in all of them, and there was testimony by members of the Bulletins and Orders Task Force, some of whom, at least Mr. Capra will be coming up. He gave testimony at Rancho Seco as to why he thought the issue was included.

(Board conferring.)

CHAIRMAN SMITH: Are we waiting for you, do you know? What is your impression of what we are doing now, Mr. Cutchin?

MR. CUTCHIN: I understood you all were going forward and that my response to the question was that I would have to discuss it and we would respond after the break.

CHAIRMAN SMITH: That's right, you did say that.

Well, this would be a good time to take the break, then.

How much time do you think you will need, Mr. Sholly?

MR. SHOLLY: Fifteen minutes.

CHAIRMAN SMITH: All right, we will take a 15-minute break.

(Recess.)

CHAIRMAN SMITH: Mr. Sholly.

MR. SHOLLY: As far as Contention 5, which is the one that Dr. Johnsrud, ECNP was supposed to be lead intervenor on, I can proceed on questions in two specific areas, which I do not think would take -- probably less than an hour, certainly less than an hour to explore. And in order to ensure that, I will put the parties on notice as to what they are now.

One is whether the high range monitoring system will or will not be installed prior to restart, and the other I want to ask some questions about how iodine is monitored. The testimony leaves me with some questions as to how that is done, and I would like to pursue that. Beyond that I do not think I would have any other cross examination.

CHAIRMAN SMITH: I do not know whether it is necessary to have all three of the panel witnesses answer for your questions. Do you have a feeling for that? Maybe

Mr. Broughton can tell us, since you are on the panel that would be addressing that contention.

MR. BROUGHTON: I believe those two areas could probably be addressed by two of the three witnesses.

CHAIRMAN SMITH: Would you have any objection to only those witnesses on the written testimony knowledgeable in your area attending?

MR. SHOLLY: I have no problem with that.

CHAIRMAN SMITH: How about --

MR. CUTCHIN: For the staff.

CHAIRMAN SMITH: The staff's presentation is entirely on E, C and B(1)(d).

MR. CUTCHIN: No, sir. We have Mr. Stoddard and Mr. Bridges. Mr. Stoddard addresses Mr. Sholly's contention in its entirety, and if the questions are only based on Mr. Sholly's contention, it would appear to me that the only one we need bring would be Mr. Stoddard.

Now, the question would be could we get an agreement that the testimonies could be stipulated into evidence so that we do not have the problem of having to bring the witnesses up to sponsor the testimony.

CHAIRMAN SMITH: That was the gist of my question. There is no use bringing people here solely to identify an item of testimony if we are not going to examine them if you are agreeable to having the testimony stipulated.

MR. SHOLLY: I should have explained that I do not intend to cross examine the staff's witness. I think those two are directed at the licensee's witnesses. I would not object to such a stipulation.

CHAIRMAN SMITH: Would you object to having Mr. Stoddard's testimony being received by a form of affidavit?

MR. SHOLLY: That will be fine.

MR. BAXTER: We have no objection.

CHAIRMAN SMITH: You have no objection.

MR. BAXTER: That is correct.

CHAIRMAN SMITH: What is the Commonwealth's position on that?

MR. THEODORE ADLER: I have no problems with stipulating as to Mr. Stoddard's testimony. I would like to ask Mr. Broughton one question concerning the capability of those two witnesses to answer questions regarding the scope of accidents for which the radiation monitors are designed and how you define the worst case accident.

Would those two witnesses be adequate for questions in that area?

MR. BROUGHTON: I am not sure if that would be two of the witnesses or if that would require the whole panel. I would have to rereview which parts were sponsored by which witnesses.

MR. THEODORE ADLER: That is within our area of concern.

CHAIRMAN SMITH: We can leave it up to the licensee, then, to bring whomever they believe is necessary to meet these concerns, with the understanding that the missing witnesses' testimony would be stipulated.

Mr. Cutchin, the Board wanted to inquire into what the position of the parties -- we have not ourselves --

MR. CUTCHIN: Decided. You may have questions of other witnesses.

CHAIRMAN SMITH: That is possible. And we will announce that the first thing tomorrow morning.

MR. CUTCHIN: Thank you, sir.

MR. BAXTER: I am in the dark, Mr. Chairman -- maybe I am the only one -- about what we are doing about ECNP.

CHAIRMAN SMITH: We have not gotten there yet.

MR. BAXTER: Okay.

CHAIRMAN SMITH: Now, what is your position with respect to the testimony which is directed to ECNP, Contention 1(d)? Do you have any interest of your own in pursuing that aspect of the presentation?

MR. SHOLLY: I do not. That would have represented the lines along which we would have split the cross examination as we had previously discussed.

CHAIRMAN SMITH: You and a representative of ECNP?

MR. SHOLLY: That is correct. Consequently, I have really not paid much attention to what the response to ECNP's contentions were.

CHAIRMAN SMITH: So, other than just dividing the subject matter between the two intervenors, you have not worked together on a cross examination approach. You just divided the subject matter, nothing else.

MR. SHOLLY: We would have gone further, but Dr. Johnsrud's illness has prevented us from getting together.

CHAIRMAN SMITH: Yes. What is your position on that aspect of the testimony? That would be the staff's panel and the balance of licensee's testimony on the issue.

Mr. Adler?

MR. THEODORE ADLER: We have not divided our questions. We did not pay any attention to what testimony was directed at what intervenor, so I have not analyzed that. I presume, however, that I would be afforded the opportunity to cross examine on the entire piece of testimony, so I am not sure I see a problem.

CHAIRMAN SMITH: I am sorry, I missed -- I did not appreciate the import of your remarks. I did not understand you.

MR. THEODORE ADLER: Perhaps I do not understand your question.

CHAIRMAN SMITH: In looking at this I see testimony by staff witnesses Jensen, Oglewade, Bolger and Hearn relative to ECNP Contention 1(d), which is separate from the Stoddard testimony.

MR. BAXTER: Our testimony is divided also, Mr. Chairman, although it is on one piece of paper.

CHAIRMAN SMITH: Yes.

MR. THEODORE ADLER: I thought you were referring to licensee's testimony.

CHAIRMAN SMITH: I will be in a moment. I just sort of reversed the direction to keep you alert.

(Laughter.)

MR. THEODORE ADLER: I do not think I am alert enough because I do not have here both pieces of staff testimony; I only have the Stoddard testimony.

CHAIRMAN SMITH: Okay. All right. So could you be prepared in the morning to state what your position would be?

MR. THEODORE ADLER: Yes, I will.

CHAIRMAN SMITH: That is the NRC staff testimony on Contention 1(d), which was received by us October 2, 1980. As far as the portion of the licensee's testimony directed to ECNP Contention 1(d), would you state what your position would be there? That begins at page 6.

MR. THEODORE ADLER: Again, I am not sure I understand your question. Are you saying there is a problem in introducing the testimony in the absence of ECNP?

CHAIRMAN SMITH: The question would be do you have any cross examination plans for it or on it?

MR. THEODORE ADLER: The third question on page 6 would be within the area of concerns that I raised earlier. Again, I presume that licensee still wants to introduce this evidence, and if Dr. Johnsrud chooses to not avail herself of her right to confrontation, that is her decision. I presume that this evidence will be introduced and we will have an opportunity to cross examine on it.

CHAIRMAN SMITH: This is what we are addressing, whether this is going to be required if the intervenor who offered this contention does not wish to or is not going to be available for cross examination and no one else wishes to cross examine. I hesitate to have these people come here solely for the purpose of identifying the testimony and then being excused. Unless there is a worthwhile purpose of having them here, I do not think we should bring them.

MR. THEODORE ADLER: They are the same panel of witnesses as are addressing Mr. Sholly's concerns.

CHAIRMAN SMITH: Except that that was two out of the three could satisfy Mr. Sholly's concern for the licensee's panel.

MR. THEODORE ADLER: The only additional concern I had was the scope of accidents concerned.

CHAIRMAN SMITH: Okay. That should give you some guidance, then. You can present whoever you believe can cover those concerns.

MR. BAXTER: So it would be the Board's plan to proceed with the issue this week in the order we previously set?

CHAIRMAN SMITH: Yes, that is the case. I stated the Board wishes to consider after we adjourn this evening the extent to which it itself has an interest in the contentions. That is, if these contentions, for example, had been, ECNP contentions had been withdrawn earlier or if there had been a default earlier, would we have insisted on the issue being presented on our own? We have not decided that.

The ECNP contentions survived, as I recall, on the basis that there had been no discovery and therefore the licensee had not been prejudiced. Now, as compared to the other two contentions on this subject matter, which the Board itself, because it was not covered by other issues, decided should be kept in the proceeding, we have made no indication on ECNP 1(d) whether or not it involves an issue that the Board itself wishes to have explored on the record.

Do you share my memory of that?

MR. TROWBRIDGE: That is correct.

MR. CUTCHIN: The staff recalls that is the reason those two were not dismissed along with the others. Of course, what the Board, I presume, is going to do is look and see if the testimony sufficiently covers its needs and whether it would have to have that testimony expanded by the witnesses on the stand.

CHAIRMAN SMITH: That is right. It may very well also be that the Board looks at it and does not even care if the testimony is offered. Or we may say offered and we may have some questions, we may have none. I don't know. But we just have not had an opportunity to evaluate it as our own issue.

MR. CUTCHIN: That I understand, sir. Am I to understand now -- I apologize, I am a little confused -- that we would finish this issue, next take up containment isolation followed by the computer matter on Sholly 13 and ECNP 1(a), and then next we would take up Sholly 5 and ECNP 1(d)?

CHAIRMAN SMITH: Yes. We are now acting in response to the parties' urging to let them know if and to what extent they have to proceed with the testimony presenting witnesses on these issues, and with the understanding from Mr. Sholly that no one from ECNP would appear during the timeframe during which this is scheduled. ECNP is communicating with us by letter.

We are going to try to give the parties guidance as to what we believe is appropriate, but the first thing we wanted to determine was what the parties otherwise interested in the contention insist upon, and I think we have done that. We will have done that tomorrow.

The first thing we wanted to do was see what Mr. Sholly and what the Commonwealth would insist upon or request in any event in relation to these issues, and then the Board will say what it wants, if anything, and then we can deal with the problem of what seems to be an impending default or the possibility of it by ECNP.

MR. SHOLLY: Mr. Chairman, the only other thing I wondered about is my memory is confused on what Mr. Cutchin had said earlier about the availability of staff witnesses on the computer and the instrument range contention. If there can be a change made there that will accommodate the witnesses, I am amenable to that, but I would like to know ahead of time.

MR. CUTCHIN: My understanding now, Mr. Chairman, is that if there is a good chance that we will get to the computer matter this week, I have no scheduling problem. I did not, to my knowledge, have a scheduling problem with respect to the Sholly 5 and ECNP 1(d) anyhow, but my problem with respect to the computer issue is that if he does not appear this week, I will not have him available for at least another week. He will not be available next week.

CHAIRMAN SMITH: Okay. But we had anticipated the computer contention goes before 5 and ECNP 1(d).

MR. CUTCHIN: Yes, sir.

CHAIRMAN SMITH: Okay.

MR. SHOLLY: That is what my confusion was on: which was first.

CHAIRMAN SMITH: Is there anything else we need to address on this problem?

MR. CUTCHIN: Nothing further from the staff.

I had indicated, sir, that I would attempt to get an answer to the question that I understood to be posed as sort of a chicken and egg problem, perhaps, but the problem that I had understood to be posed was what was BAW 1564 submitted in response to?

I am not sure we will ever have a definite and exact answer, but it is my understanding that in the immediate aftermath of the TMI-2 accident, the licensee's people volunteered to do a failure modes and effects analysis in that same timeframe. Neither the staff nor others were absolutely sure as to whether there was some cause and effect relationship between ICS failures and what happened at TMI-2.

CHAIRMAN SMITH: At that time that was not determined.

MR. CUTCHIN: That is my understanding, and the possibility that there may have been some interrelationship since clearly the ICS controls both main and emergency feedwater are aspects of those, and since the main feedwater transient could have been theoretically caused by an ICS failure. Anyhow, I am not sure we will ever get an accurate answer there, but many things were happening in the same timeframe.

But I understand that the failure modes and effects analysis was something that was volunteered by the licensee. The Commission's orders in effect were confirmatory in nature and therefore made that volunteered analysis an order requirement, and I guess NUREG 0560 were the studies that resulted in that. They were going on at the same time.

The staff, for the reasons I just stated, thought it would be a good idea and it sort of evolved from that, but I am not sure we will get a clear answer as to what came first and so on.

CHAIRMAN SMITH: Since that time, Mr. Cutchin, has the staff been able to identify any involvement of the ICS in the accident at TMI-2?

MR. CUTCHIN: It is my present understanding that the staff does not believe that there was any cause and effect relationship between ICS problems and TMI-2. A name I stumbled over about half an hour ago was Oglevie, O-g-l-e-v-i-e.

(Board conferring.)

CHAIRMAN SMITH: The Davis-Besse order and the other B&W orders were issued initially in late spring, approximately April of '79.

MR. BAXTER: The Rancho Seco order was on May 7. I do not recall the date of the Davis-Besse order. My understanding is they were all about the first week of May.

CHAIRMAN SMITH: About the same time.

All right, Mr. Sholly, I guess you can continue your cross examination.

(Pause.)

BY MR. SHOLLY: (Resuming)

Q Dr. Joyner, we touched earlier, in my mind very briefly, on what possible differences there might be between the ICS 721 and 820 hardware, as you put it. I wonder if you would explain in a little bit more detail just what the differences are between the 721 and 820 systems.

A (WITNESS JOYNER) Both are electronic analog control lines of controlled equipment, both supplied by the same vendor of controlled equipment. Both have basically the same capabilities in that those two lines of equipment both have integrators, function generators, summers, bias modules, tristable modules, bistable modules, velocity limiting modules. That kind of equipment is standard in the control industry.

You can look in the catalogue of Bailey Controls, Foxborough, Honeywell, the people who supply analog equipment and find that kind of module. The ICS is composed of these blocks of control equipment. The difference between the two systems is how the modules themselves, the single components are designed internally. That is 99 percent of the difference in the two systems.

They are rack mounted in standard-size cabinets, about the same physical size, weight and look very similar.

Q Based on the design of those two units, would you expect any differences in performance between the 721 and 820?

A (WITNESS JOYNER) Functional performance, no.

Q No difference?

A (WITNESS JOYNER) No.

Q Would you expect any difference in failure rates, internal failure rates?

A (WITNESS JOYNER) If equally maintained, I would ex ct little difference. I believe that there have been some failures, and the reliability study pointed that out, of specific 721 modules somewhat more failure prone than others. Let me see if I can find that table.

(Pause.)

Page 5-16 in the report, the ICS Reliability Report. It lists failure rates by type of module. You can see with the exception of relays and some plus proportional, plus integral, modules have a very low failure rate. I might point out that as a statistical study of the reliability of these modules, it is probably not that valid in that the sample sizes are not really that big, and I would not want to base a scientific dec sion or engineering decision on reliability on these sample sizes.

Q I think that agrees with the Oak Ridge conclusions. They state that although the 820 appears to be more reliable, that there are insufficient data to conclude it is statistically significant; and you would agree with that?

A (WITNESS JOYNER) I agree that comparatively, to compare the 720 and 821 module reliability and to come up with a figure that would say 820 is 6.2 times more reliable than 721, that is not justified. We could probably draw the general conclusion that with the exception of a couple of modules, 721s are as reliable as 820s. I would be more prone to draw that conclusion.

I might add that as you could expect, failures were more concentrated at some plants than others. It is very heavily dependent on the kind of maintenance they receive on the equipment.

Q In the NRC meeting summary in response to question 11 which appears on page 6, there are two terms mentioned there that relate to failure rates.

A (WITNESS JOYNER) Let me find that again.

Q Question 11, page 6 of the NRC meeting summary. It is at the bottom of page 6.

(Discussion off the record.)

WITNESS JOYNER: I have one marked 6.

BY MR. SHOLLY: (Resuming)

Q I don't think the question itself is as significant as the two terms. What I wanted to do is understand what these two terms meant. They are burned-in failure rate and accelerated failure. What do those mean in the context of the discussion?

A (WITNESS JOYNER) Burned-in failure rate means the initial infant mortality that you would expect with electronic equipment. If it lasts a few months, it is likely to last quite a while.

Q Okay.

A (WITNESS JOYNER) And that is what that term means.

Q What about accelerated failure? That is used in the question.

A (WITNESS JOYNER) Normally when you look at lifetime failure rates you see that they are fairly large at the beginning of life, during the burn-in period. They then become relatively small and constant, and as you approach the end of the expected life of the equipment, you see that the failure rate turns up and you have an accelerated failure rate.

We did not see that when we looked at the reliability, at the hardware history, hardware performance in the field.

Q Do you interpret that to mean that the equipment has not reached the end of its expected lifetime or that the performance is somewhat better than expected?

A (WITNESS JOYNER) I interpret it to mean that the equipment still has quite a long, useful life left. You would expect it to last 10 to 15 years, as an estimate. I don't intend to convey it is designed for a 20-year lifetime, but after that period of time you may see certain components begin to deteriorate, like capacitors or other equipment that ages, and you would see the failure rate increase. It would not be a catastrophic-type thing in that one day you walk in and everything fails, but a burn-out, a wear-out.

Q I think perhaps the next question will be directed to Mr. Sadauskas and Mr. Broughton.

The Restart Report references the training that the operators have received in the operator accelerated training program, and this is covered, as near as I can tell, on page 6-13, which I believe is Volume 1.

I would note that under TMI Module 2 on page 6-13 of the Restart Report it indicates that the operators received four hours of training in the integrated control system. Two basic questions. Is that the extent of the operator's retraining since the accident on the ICS; and if it is not, could you explain what additional training related to that has taken place?

A (WITNESS BROUGHTON) I will have to preface my remarks by the fact that I am not deeply involved in the training program, and there are certainly things which are taking place in terms of training that I am not familiar with. But I am familiar with some of the training which is conducted in addition to the accelerated retraining program, and that is some of the training conducted at the B&W simulator.

As part of the simulator training, some of the evolutions which were conducted in the simulator do involve training on the integrated control system. There are both some classroom training in which the basic operation of the system is reviewed, and there is training within the simulator on not only normal response of the integrated control system when it is functioning properly, but there is training on things like operating the system in hand versus automatic, either as a result of failures or tests or some evolutions in which it would be preferable to control in hand rather than automatic.

Q Do you know if there has been or is there any intent to include in that training the power failure modes that were discussed earlier today, the various types of power failures and what that does and what the procedures tell the operators to do? Has that been included or will it be?

A (WITNESS BROUGHTON) When the study that we are performing is completed and all the various power failures have been identified and effects on the plant and the desired operating procedures have been developed to deal with those events, then the normal practice of the plant staff would be to train on those procedures specifically, and that training in most cases includes the background information that an operator should know as to why the procedure says to do the things that it does.

In that way it would bring in more specific results of the studies that have been performed to develop the procedures.

MR. SHOLLY: Give me a moment. I want to make sure I have covered myself up to this point.

(Pause.)

BY MR. SHOLLY: (Resuming)

Q A few more things relating to the Oak Ridge review and the B&W report.

We started briefly to get into the general findings of the ORNL review and did not get very far because we got off on a tangent on why the study was done and what the source of the orders was.

The General Findings section of the Oak Ridge report, which is on pages 3 and 4, identifies a number of limitations on the B&W report. What I want to do is go through each of those and see if you agree with them or if you take issue with them or what your position is as far as these limitations as Oak Ridge sees them.

The second paragraph, which consists of one sentence, says "The significance of the ICS to safety (Item A) is not addressed."

Do you agree that that is the case or do you have some remarks to make on that?

A (WITNESS JOYNER) No, I do not agree with that.

Q What specifically in BAW-1564 would you say meets discussing the significance --

A (WITNESS JOYNER) I am looking for the paragraph I would like to read which I think covers that. Page 2-1 in the report, second paragraph. "The overall conclusion of the FEMA is that the reactor core remains protected throughout any of the ICS failures studied." That is, I think, a safety statement. We looked for that event, were there failures that not to be the case, and we could not find any.

Q When you say you looked for those failures, you mean within the scope of how you defined what the ICS is in the report. I asked that because --

A (WITNESS JOYNER) Yes. The ICS as defined and as it exists. I am not trying to take issue, but ICS is a very definite system. It is not that we said, you know, this constitutes the ICS. That is not the case. We did not arbitrarily define it. It is well known to constitute the functions, this hardware, these inputs, these outputs, and we searched through that system for single failures that would cause the core not to be protected.

MR. JORDAN: I guess Mr. Sholly is kind of waiting for me to say something because I had picked up the microphone. I will make a comment that does not necessarily draw a conclusion but it might require a response from either Mr. Sholly or from Mr. Joyner.

I rather have a feeling that the Oak Ridge review is very broad in scope and is really, in a sense, critical of the idea of a failure modes and effects analysis that is limited to the ICS system. B&W has done a failure mode analysis of the ICS system. I believe that the ORNL review concludes that that is not a terribly significant accomplishment as regards overall safety; that the safety analysis of the type of a WASH-1400 is more productive; that a failure modes analysis of ICS does not tell you an awful lot about overall safety of the feedwater systems, the interaction of the ICS with all the other systems and so on.

For that reason, therefore, Oak Ridge is critical in that they would have liked to have seen a much broader analysis, but I believe it is probably the position of B&W that that was not called for in a failure modes analysis for ICS.

Now, would you care to address my comment? Do you think I have a proper perspective or not? Does it need modifying? If it does, I urge both you and Mr. Sholly to advise me.

WITNESS JOYNER: Well, if you read the Oak Ridge report, it definitely tends to call for more work than what was done. There is a tendency on the part of R&D academic type people to always want to do more. I do not -- I will not agree that it did not accomplish something. I think it really did.

What we failed caused feedwater perturbations. It caused reactor trips. It gave us a good insight as to what failure is due to NSS. So it was very worthwhile.

The recommendations that came out of this report are valuable, and had we not done this piece of work we would not have gotten those recommendations, which have merit and have value.

We could always have done more. In fact, we could still be working now and not have any recommendations whatsoever.

I think Oak Ridge recognized that, although if you look on page 16 in their last chapter, they say: "The FMEA would have been of greater significance if it had been expanded to include other systems," and so on and so forth. But their last sentence: "It is not evident that redoing the analysis at this point to include this information would be worthwhile.

DR. JORDAN: That is what I gather their position is, that a FMEA analysis is not going to tell you all that much about overall safety.

WITNESS JOYNER: It is not the end-all. But it does give you very useful early information on what you need to look at. And I think that is what the recommendations came out with. These are areas that we need to examine. Other areas of failures may be there, are not so important, and perhaps do not deserve the emphasis that these do.

CHAIRMAN SMITH: Is there anyplace in the Oak Ridge report standards against which the authors of the Oak Ridge report measure the failure modes and effects analysis by B&W, or does it boil down to just how they would have gone about it if they were doing it?

Are there any standards which are assigned in measuring the B&W report?

WITNESS JOYNER: Yes, sir. We agreed to perform the report along the guidelines established in IEEE Standard 372.

DR. JORDAN: 352?

CHAIRMAN SMITH: 372.

WITNESS JOYNER: 352. I am sorry. And that outlines what should be done. That was one of our agreements, that we would use that document as a guiding source of what we did.

CHAIRMAN SMITH: When Oak Ridge measures you against that document, what do they conclude?

WITNESS JOYNER: Well, I do not know that they specifically said that, sir. They did make some general comments here.

Page 15, the first full paragraph, it appears, quote: "The manufacturer contends, and we agree, that: one, the system prevents or mitigates many more upsets than it creates; and, two, the system is generally superior to manual or fragmented control schemes."

CHAIRMAN SMITH: Is it your view they are talking about safety here, rather than reliability of the plant and efficiency? In Item No. 2?

WITNESS JOYNER: From an operability standpoint, from the standpoint of keeping the plant operating.

CHAIRMAN SMITH: Capacity factor.

WITNESS JOYNER: Making megawatts, performing its intended function. It is not a safety-grade system and really does not control the safety systems that are needed for the plant.

WITNESS BROUGHTON: I think that item also says that in fact this control system does prevent challenges to the protection system, in that it mitigates upsets.

CHAIRMAN SMITH: It avoids challenges.

WITNESS BROUGHTON: It avoids challenges to protective systems. And the conclusion, after looking at the field data, was that it prevents more of those challenges to the protective systems, safety systems, than it actually creates by malfunctions which have occurred.

DR. JORDAN: Again, if you are speaking now of "protection system" meaning the scram system, I think is what we said this morning.

WITNESS BROUGHTON: That is correct. But in the mode of the ICS --

DR. JORDAN: The safety system -- I define the emergency feedwater system as part of the safety system. Then there would be no evidence one way or the other on that, as far as I know.

WITNESS BROUGHTON: No. But when the ICS is being called upon to operate to control the plant, the plant is at power. And the first safety system which it will challenge is the reactor protection system. It cannot challenge the others.

DR. JORDAN: Immediately thereafter it will be the system that has to take care of the afterheat.

WITNESS BROUGHTON: Only for some failures.

DR. JORDAN: Following a scram, some system has to take care of the afterheat.

WITNESS BROUGHTON: Yes. And the one which usually does that is the main feedwater system, controlled by the ICS.

DR. JORDAN: That is right, and it is controlled by the ICS following a scram.

WITNESS BROUGHTON: Yes.

DR. JORDAN: So I guess the question is, does it prevent challenges to the emergency feedwater system -- does it do a better job than the operator would do?

WITNESS JOYNER: I think that is their conclusion in the paragraph, sir, that it is generally superior to manual, fragmented control schemes. That is how I read that statement.

DR. JORDAN: It depends on which safety system you are talking about, I think.

MR. SHOLLY: Dr. Jordan, there is one remark that is made in the discussion portion of the Oak Ridge report which, you know, in this case is directly relevant to one of the things that is stated in the testimony and on this particular issue.

On page 3 Dr. Joyner's testimony says: "The ICS has prevented more reactor trips than it has caused, and thus its net effect has been a reduction in the number of challenges to the reactor protection system."

On page 11 of the Oak Ridge report, the last paragraph above where it says "Power Supplies" concludes that: "The B&W analysis asserts that ICS actions have averted more trips than they have caused. Although this assertion is not pertinent and is probably true, the data presented do not substantiate the assertion."

That to me seems to be somewhat in conflict with the testimony.

BY MR. SHOLLY: (Resuming)

Q When you say the ICS has prevented more reactor trips than it has caused, is that your personal opinion or is that based upon some statistical study or operating history?

A (WITNESS JOYNER) If you will turn to page 5-14 in the reliability study, Table 5-7.

Q Page -- what page was that, again?

A (WITNESS JOYNER) 5-14. That table describes runback actions at one particular plant over a five and a half-year period of operation. During that time there were a total of 37 reactor trips from all causes.

DR. JORDAN: 47?

WITNESS JOYNER: 37, sir.

During that time there were 47 successful runbacks, although I will have to say that ten percent stepload increases and decreases are not really runbacks. But those are -- at least the first three really cannot be disputed, that a successful action of the control system did prevent a trip in that case, and that is 32 of those -- turbine trip, load rejections.

At that particular plant there had been a total of

14 turbine trip or load rejections and similar events as far as the NSS is concerned. In one case the turbine throttle valve slammed shut very rapidly. That is for the turbine trip.

For the load rejection, we disconnect the electrical load from the turbine. The turbine tends to overspeed. The speed governor on the turbine closes the throttle valves rapidly, and externally you cannot tell the difference in the transient, because the throttle valve will close as rapidly, almost, as it scrams.

14 times we've run the reactor back without tripping, but not challenging the safety system.

Feedpump trips, there had been 14 of those during that five and a half year period. The ICS successfully ran the plant back to a power level less than the capacity of one feedwater without a trip.

We had had four instances of dropped control rods. The effect of dropping a control rod is to rapidly reduce the power generated in the core. The ICS must then run the feedwater flow back, steam flow back, in a smooth fashion so that the plant does not trip.

And those successful runbacks shown in that table alone are sufficient to justify the statement that it prevented more trips than it caused, because we can only definitely say that out of 310 -- in 305 reactor years, six trips have been caused by the ICS.

Now, in reality there may have been more, 20 perhaps. But in this table alone, it shows its value as a system for preventing challenges to the protection systems.

BY MR. SHOLLY: (Resuming)

Q Does that table include the experience for all the B&W plants?

A (WITNESS JOYNER) No. That is one particular plant.

Q Do you know which particular plant that is?

A (WITNESS JOYNER) Yes.

Q Which one?

A (WITNESS JOYNER) SMUD.

Q You did not examine the other plants operating?

A (WITNESS JOYNER) Yes, we examined them, but we did not tally them up like this. We could have had nine tables. Some were better than others, obviously, and we would not put the worst one in there.

But this is not atypical.

DR. LITTLE: Which plant did you say this was?

WITNESS JOYNER: SMUD, Sacramento Municipal Utility District.

BY MR. SHOLLY: (Resuming)

Q Rancho Seco?

A (WITNESS JOYNER) Rancho Seco, that is correct.

Q You mentioned that you did not put the worst one in. Do you have any idea what the worst plant --

A (WITNESS JOYNER) I really don't.

Q I don't care which plant it is. But in terms of whether it has caused more or prevented more?

A (WITNESS JOYNER) I would say in no case would it have caused more. The worst is certainly not TMI. TMI-1 was one of the better plants and had a record of running back successfully on turbine trip loss of load.

MR. SHOLLY: Did you have anything else, Dr. Jordan? I did not mean to cut you off.

DR. JORDAN: No, no. Fine.

BY MR. SHOLLY: (Resuming)

Q Getting back to the general findings of the Oak Ridge report, on page 4, the first full paragraph, it states that, quote: "Transients initiated outside the control system, whether or not successfully mitigated by the ICS, are not addressed except in tabulations of operating experience."

Do you know where in the B&W report that calculation is located?

A (WITNESS JOYNER) Yes, yes, I do. If you will turn over to page -- I am not sure I know where every one of them is located.

But for example, on page 5-11, Table 5-2. Well, really, start with Table 5-1, and we tabulated all the failures. And a failure here means a failure that caused reactor trip.

So we tabulated, beginning with 5-1, all the failures that occurred that caused reactor trip -- I'm sorry, all the reactor trips that occurred, and placed them into one of six categories, either a 1, a 2, B, C, D, or E type failure or event.

If you look over on page 5-18, Figure 5-1, you see a nice pie chart of those failures. So you can get some perspective o the relative magnitudes.

(Pause.)

Q The next paragraph on page 4 states, quote: "Identification of interactions resulting in failures in safety or non-safety systems or operator actions is notably absent."

Have you any comment on that?

(Pause.)

A (WITNESS JOYNER) I am not quite sure what interactions they would like us to define. We did not consider the effect of operator actions on the transients. It was not that kind of a study. And we did not do that.

As far as interactions resulting from failures in non-safety systems, we did look at that and we looked at failures of inputs to the ICS which would constitute failures of the other systems. We also looked at -- or we looked at failures of outputs from the ICS which exercised the pumps, valves, in a fashion similar to the way they might be exercised if they failed by themselves, and looked at the effect upon the NSS of that failure.

(Pause.)

Q In summary, the ORNL concludes, which is the last paragraph above the ORNL review plan -- it says, quote: "In summary, the report deals only with a very limited scope of failures, essentially within the ICS cabinets. The only significant measure of response is whether a reactor trip would occur. Because of this limited scope, the results are necessarily of limited value."

A (WITNESS JOYNER) Where are you, Mr. Sholly?

Q It is the fourth full paragraph on page 4.

A (WITNESS JOYNER) I was thinking maybe we were toward the end of it. Okay.

Q It is the first two sentences of that paragraph.

A Okay, sir.

Q Now, I realize that this may -- your answer probably will be tempered by what you read the FMEA as having been done for and perhaps ORNL's larger scope in which they reviewed it. Do you agree, though, that in some senses that the report is of limited value in terms of what you know the ORNL review to be looking for?

A (WITNESS JOYNER) Well, I can take that paragraph phrase by phrase, and we did go through it.

The summary -- the first phrase there, the summary, "The report deals only with a very limited scope of failures, essentially within the ICS cabinets." That is not really true, in that we did assume the failure of every input to the ICS, both high and low.

We also assumed the failure of the outputs from the ICS to the final control elements, the steam relief valves, the turbine throttle valves, the pumps, the feedwater valves, so -- and those failures could not have occurred from action other than the ICS action.

So that is not really a straightforward statement of what we did. We did more than look at failures within the ICS cabinets. That was one of the three types of failures that we looked at.

The next portion of that sentence, "The only significant measure of response is whether a reactor trip would occur." That is not really true. We categorized every failure as one of three types of failures: Categories 1, 2, and 3.

Category 2 were those failures that might reasonably cause a trip. Category 3 were those failures that might cause a trip, plus the possible need for some other type of action, operator intervention action. So that is not true.

Now, because of this limited scope, the results are of necessarily limited value. I just don't agree with that. Certainly they are limited in the overall scope of what is a value and what is not a value. But it gives the impression that we did not learn anything of value, and we certainly did.

(Pause.)

Q Let me pursue one final thing here as far as the Oak Ridge report goes. Again, I am at somewhat of a loss as to bringing together the statements in the first five sections of the report and your conclusions.

Two vital things which again get to the scope of the study, how you would perceive it and how they would perceive it, and I would like to get your reaction to those. On page 6, it is the third full paragraph under "Scope of Analysis," quote:

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

Again, it seems to cast some doubt, in my mind at least, as to the usefulness of the study, at least at Oak Ridge views it.

A (WITNESS JOYNER) I hate -- well, I don't hate. I would like to refer you to paragraph 2 at the top of page 16. They contradict themselves.

Q Absolutely.

A (WITNESS JOYNER) And I happen to know who wrote what. And you know, I happen to understand the problem. Here is a good statement, the top paragraph on page 16. I cannot say it nearly as well as they have already said it and written it down for us.

Q I think I understand what your reaction is going to be to my other example. I don't particularly see much point in pursuing it at this point.

A (WITNESS JOYNER) You know, not referring you back to 16, I do think that taking the second sentence, for example, I do believe a system should include the sensing lines, and we did include that. We looked at the input failures and evaluated their effect upon the plant. That statement is not true as it stands.

(Pause.)

MR. SHOLLY: I believe that is all the questions I have for these witnesses.

DR. LITTLE: Dr. Joyner, on page 5-14 of the B&W report, Table 5-9 on the 721 and 820 systems, do you have that?

WITNESS JOYNER: Yes, I am with you.

DR. LITTLE: I believe I understood you to say that maintenance was especially critical with the 721 system. I would like to have you elaborate on why that would be the case moreso with the 721 than the 820?

WITNESS JOYNER: Well, I may have said that, and if I did, I have no reason to believe that it is more critical on the 721 than it is on the 820.

DR. LITTLE: Is it critical on both of them?

WITNESS JOYNER: Well, "critical" is a relative term. You know, you can perform no maintenance at all, in which case it probably is important. Then you have a regularly scheduled maintenance program.

Some plants have very fine scheduled ICS maintenance programs. Others do not. And I think that that may have a lot to do with the difference in failure rates, although we did not do enough data-gathering and analysis to really go into the effect of maintenance and that kind of thing. So I cannot make a definite statement.

I do know, for instance, that at TMI-1, as an example -- I happen to know the maintenance personnel there have a regularly scheduled maintenance program. They have well qualified I&C technicians. Other plants don't have as good people and they do not have as good a record of ICS performance.

DR. LITTLE: In the analyses given in Section 5 of the B&W report, there are a number of plants listed which were studied. Do you know which ones fall into the category of having 721-type ICS systems?

WITNESS JOYNER: Oconee 1, 2, 3, and TMI-1 have 721 systems.

DR. LITTLE: Those are the ones that account for the numbers in Table 1-9?

WITNESS JOYNER: 721? That is correct.

DR. LITTLE: Okay, thank you.

(Board conferring.)

WITNESS JOYNER: A lot of the difference, too, may be due to reporting procedures. When you -- for instance, it may not be convenient for an individual to write down that he tuned the module at one plant and it may be in another. You may have strict requirements for recordkeeping at one plant and not strict at another.

We really did not go into those aspects, and I think you have to before you can draw general conclusions about the relative merits and criticality of maintenance on one system versus another.

DR. LITTLE: I was wondering if you were going to go into the fact that the 820 is a newer system and maybe has more easily maintained circuitry than the other one. Is that the case or not? That is what I gathered?

WITNESS JOYNER: It is a newer system, and it certainly appears that it is easy to maintain. But I do not think that we can really draw that conclusion.

DR. LITTLE: TMI-2 must have an 820.

WITNESS JOYNER: That is correct.

DR. LITTLE: Okay.

CHAIRMAN SMITH: Mr. Adler?

MR. THEODORE ADLER: Thank you.

BY MR. THEODORE ADLER:

Q Mr. Joyner, Mr. Sholly asked you about the difference between single failure and multiple failure analyses. I do not really want to get back into that issue. But on the bottom of page 15 of the ORNL report, that first recommendation under Section 6-2 suggests that a fault tree analysis might be used rather than a functional block diagram.

Can you explain why you elected to use a functional block diagram?

A (WITNESS JOYNER) It made the analysis much more straightforward. And I would like to refer you to IEEE 532, which you don't have a copy of.

Q Yes, I do have a copy.

A (WITNESS JOYNER) I'm sorry, you do. On page 11, for example, the first paragraph, right-hand corner. And in this section they are discussing, for those of you who do not have it, the rules for a failure modes and analysis.

MR. BAXTER: Is this Standard 352?

WITNESS JOYNER: Yes.

The sentence says: "A functional diagram may be used in the FEMA to show the functional dependencies in the system, so that the effects of failure can be traced. Fault trees may also be used. These techniques are discussed later."

BY MR. THEODORE ADLER: (Resuming)

Q I was focusing on page 16 of IEEE 352.

A (WITNESS JOYNER) 16?. Okay.

Q On the right-hand column, the second paragraph of number 2 there in the middle of the page, where it states, quote: "It is important to know the difference between the reliability of the block diagram and the fault tree diagram."

A (WITNESS JOYNER) Okay.

Q It says: "The use of fault trees stimulates the identification of possible failures and events, and a fault tree can represent all kinds of dependencies and common mode failures and events."

And then it says: "The reliability block diagram corresponds closely to the system functional diagram."

Just read that paragraph and see if it implies that you ought to use the functional block diagram to determine how the system works, and that you should use a fault tree analysis to analyze what are the potential failures of the system?

A (WITNESS JOYNER) I am not sure a functional -- reliability block diagram --

Q Perhaps --

A (WITNESS JOYNER) I would have to read the whole thing in order to make sense out of it.

Q The whole paragraph or the whole section?

A (WITNESS JOYNER) I would have to sit down and spend 20 minutes or so. My bag is not reliability analysis and I do not have that in my head.

Q Can you just respond -- let's see if this helps -- to the last sentence of that paragraph, which reads, quote: "Therefore, the fault tree represents the system in terms of the events leading to failures, and the reliability block diagram describes the system in terms of the events leading to success."

Can you comment at all on that sentence?

A (WITNESS JOYNER) Out of context, I would be hard-pressed. I would be glad to take a few minutes and read the page.

Q Go ahead. That is fine.

(Witness reviewing document.)

A (WITNESS JOYNER) I read it. If you will repeat the question, I will attempt to answer it. I am not sure I can.

Q Perhaps this will help. I am not an expert on reliability analysis, but it seems that IEEE 352(1975) is establishing a preference for the use of fault tree analysis over the functional block diagrams in terms of analyzing what the potential failures of a system that you are studying are.

And now it may be that the scope of your analysis was sufficient, but I am interested in your rationale for choosing the functional block diagram over the fault tree analysis in light of that preference.

A (WITNESS JOYNER) The rationale for choosing the functional block diagram -- and I am still unclear on this, but I can tell you why we chose the functional block diagram -- is that we had that type of diagram available in computer simulations. We could block the system out into a functional diagram and then fail each of those components on the simulation and determine the effect of its failure.

The example -- and I am really not that familiar with performing reliability analyses such as this one. But the example here is primarily for safety systems which are either go or no-go, trip-no trip. And we have systems that the magnitudes -- the time of the changes are very important.

So if we fail a block in the ICS, a function in the ICS, it is important how long that transient lasts, how rapidly pressures and temperatures change, and a lot of other things.

Q As I understand your answer, your primary reason for using functional block was that you had readily available in your computers information th t would facilitate that analysis?

A (WITNESS JOYNER) That is primarily it.

Q So when ORNL states that, quote, "The functional block FMEA approach may have been selected by some economic expedient and may not have been the optimum technique for deriving the information desired," you would agree with that?

A (WITNESS JOYNER) No, no. I think what they are saying is that we should have used -- well, let me go back and find that.

They are not saying we should have used fault trees. They are saying -- they quibble, I believe, with the particular functional block diagram that we chose. And they would like a more detailed ICS description.

Q Well, they say, "The functional block FMEA approach may have been selected." And then they say, "If further pursuit of the failure consequences of the ICS is desired, we recommend a fault tree be developed."

I presume they are saying, had they done the analysis initially, they would have used a fault tree analysis rather than the functional block diagram?

A (WITNESS JOYNER) For that one particular event they are talking about, for loss of feedwater, only for that one. This is the way I read it.

CHAIRMAN SMITH: Even though they say here that the fault tree represents -- I mean, the block diagram describes a system in terms of events -- in terms of success, in doing that you necessarily have to identify the events leading to failure, don't you?

WITNESS JOYNER: I think so, yes, sir.

Of course, I read right to the bottom sentence in one, which is a fairly straightforward --

BY MR. THEODORE ADLER: (Resuming)

Q I'm sorry?

A (WITNESS JOYNER) It is a fairly straightforward sentence. It says: "further analysis of this type may not be economically justified." The punch line.

Q Can you also turn to page 9 of IEEE 352, and also to page 4-20 of the B&W 1564?

A (WITNESS JOYNER) Okay.

Q On page 4-20 you list the display tables or the parameters described in your display tables. Comparing that with the suggested diagram in IEEE 352, I note that you have omitted two.

One is the failure mechanism, which is block number 4; and one is the method of failure detection, block number 6.

Could you explain to us why you elected not to include those in your analysis?

A (WITNESS JOYNER) I would like to preface with the statement that says "typical." There is no requirement that any given column should or should not be there.

The failure mechanism I did not personally think was really important to what we were doing. We postulated that the signals could fail high or low, for whatever reason, and looked at the effect. Now, that high failure, for example, means that the signal goes to plus 10 volts in the ICS. That can happen by shorting a lead to a 10-volt signal.

Low failure can happen by shorting a lead to a minus 10-volt signal. So, given the failures that we assume, high or low, I thought it was kind of redundant to put it in there. Plus, I did not think it contributed very much.

The method of failure detection for any particular plant, that would be perhaps different, in that the displays that the operator has, the annunciation that he has, is plant-specific.

Q Well, Mr. Sadauskas explained some of the displays for failures in the ICS system. Do you think it is important to analyze whether the operators have an adequate display of failure in the ICS system during a transient?

A (WITNESS JOYNER) That is reasonable.

Q So you feel that the individual -- the individual plant should do a specific analysis of that to supplement your FMEA?

A (WITNESS JOYNER) I do not think an individual analysis is called for. The recommendations state the failures that we feel are important. Now, when those failures are studied on a plant-specific basis the outcome perhaps would be instructions to the operator and operator training that would allow him to recognize that transient and mitigate that transient.

Q I just want to clarify your general response to some of Mr. Sholly's questions about the critique of the ORNL study. Is it your position that B&W is not going to do any further study or any further analysis in response to the ORNL study?

A (WITNESS JOYNER) I do not know how to answer that question. I read that Oak Ridge report a year ago -- 11 months ago -- and I am sure that it has affected what we have done in the past 11 months.

As far as repeating the FMEA including fault trees or expanding the scope, I do not think it is justified, and I certainly would not recommend that we do that.

Q I am not referring just to a complete repeat of the FMEA. Do you feel there are any criticisms in the ORNL study that warrant any supplemental work, or do you think that the FMEA as first produced was adequate?

A (WITNESS JOYNER) I think it is adequate. I agree with Section 6 in the report.

Q Despite the apparent differences between the first five parts and Section 6?

A (WITNESS JOYNER) Section 6 is the bottom line.

Q I am interested in your characterization of the ICS system with respect to its safety significance. Now, it is obvious that your position is that it is not and should not be a safety-grade system.

But would you agree that one of the purposes of the ICS system is to reduce the number of challenges to the plant safety systems?

A (WITNESS JOYNER) I do not think that is the purpose of it. That certainly is a design goal.

The purpose is to manipulate feedwater flow, steam flow, and reactor power.

Q When you first described this morning the operation of the ICS system, referring to your figure 1 in your testimony, you discussed the limiting conditions that might be imposed by the ICS system as a result of plant status, for example lack of one reactor coolant pump.

Are the limiting conditions that you referred to contained in the plant's technical specifications?

A (WITNESS JOYNER) Yes.

Q They are. So to that extent the ICS is useful in assuring that the plant does not exceed any of the technical specifications?

A (WITNESS JOYNER) Some are contained in the tech specs and some are not.

Q Okay.?

A (WITNESS JOYNER) I would have to change my previous statement.

Q Now, as I understand the operation of the ICS, during a transient it is necessary to isolate or to disengage the ICS from, certainly, the reactor protection system, and perhaps from some other engineered safety systems; is that correct?

A (WITNESS JOYNER) I don't understand the term "disengage ICS from RPS."

Q Well, for example, you want the control rods to become independent of ICS when they scram?

A (WITNESS JOYNER) Yes.

Q And that, I presume, is a safety-grade process?

A (WITNESS JOYNER) That action is performed by the reactor protection system, which de-energizes the control rods and they drop into the reactor core.

Q Fine. Now, my question is whether the same is true for the relationship between the ICS and two other systems that are at least related to safety. One is the emergency feedwater system and the other is control of steam generator level.

A (WITNESS JOYNER) The ICS, as we went through it this morning, the TMI ICS does have responsibility for automatic control of the steam generator levels when aux feedwater is initiated. That responsibility can be assumed by the operator and is independent of the ICS.

Q So am I correct that you require a manual override in order to take the steam generator level off the ICS control?

A (WITNESS JOYNER) That is my understanding. These gentlemen may be able to add to that.

Q Well, perhaps I should address the question to Met Ed employees.

Do you feel that it is adequate to have a safety system which may be necessary during a transient such that first you have a control by a non-safety-grade system, and if you want to go off the safety-grade system you need to have a manual override?

First, is that the status of the plant as you understand it?

A (WITNESS BROUGHTON) I think the system we are discussing here is the emergency feedwater system.

Q Well, we were discussing first -- well, both the steam generator level and the emergency feedwater system that Dr. Jordan raised earlier?

A (WITNESS BROUGHTON) All right. The steam generator level can be controlled by the ICS operating on the main feedwater control system, using the main feedwater pumps. And there are new parts of that system which are safety-grade. In fact, that is the normal method of controlling steam generator level following a trip of the reactor, is to use the ICS and to use the main feedwater system.

In the event that the main feedwater system is not available, then the emergency feedwater system could supply water to the steam generators. There are several different modes of controlling flow to the steam generators when emergency feedwater is running.

The first and the normal mode would be the ICS controlling that level on automatic.

A second mode would be control through the ICS, but with the ICS in a hand mode, rather than on automatic.

The hand mode allows the operator in the control room to control the position of the regulating valve, and thus control the flow into the generator.

A third mode of controlling steam generator level with emergency feedwater would be with a new system which is being installed at the plant, which will allow the operator to manually control steam generator level independently of the ICS. And that particular mode is an override type mode, such that regardless of what the ICS is trying to do with feedwater flow, the operator will still be able to open or shut the valve as he desires.

There are even ways of controlling level beyond those, which would require control locally at the valve from outside the control room.

Q I believe we had testimony on that when we discussed the emergency feedwater system. So the conclusion is that you either control the level through the ICS or through operator action; is that correct?

A (WITNESS BROUGHTON) That is correct.

DR. JORDAN: I did not quite understand your answer there. ICS automatic control is possible, but the emergency feedwater system operator control, manual control of the ICS system, you said, is also another mode. And a third mode is one that you are planning to put in, you say, in which the operator controls -- has the independent control of the feedwater system?

WITNESS BROUGHTON: That is correct. It would be very similar to the manual mode in the ICS or the mode that I term "hand" in the ICS, except that instead of using components that are part of the integrated control system, this new system will be completely separate from the ICS. It will use different components. It will be physically separate. It will have a different electrical power supply.

The controls will be located in the control room on the control panels, so they will be accessible to the normal operators; and by adjusting those controls, they will be able to move the feedwater regulating valves independently of what the ICS is trying to do to the valves.

DR. JORDAN: I guess I did hear you properly, and I guess I am a little surprised. I thought in the long-range there was going to be an automatic control completely outside of the ICS; isn't this correct?

WITNESS BROUGHTON: That is correct for the longer-term --

DR. JORDAN: What you are describing now is a short-range program.

WITNESS BROUGHTON: That is correct. This third mode of control, independent of the ICS, is a mode which will be in place before the plant is restarted.

DR. JORDAN: That is what I was going to ask. I see.

WITNESS BROUGHTON: The difference between that mode and what will be available in the long term is in the long term that mode of control independent of the ICS will be automatic, first of all, so it will not require the operator; and secondly, it will be safety-grade, so that it can tolerate certain failures.

DR. JORDAN: Yes, okay. I understand.

Now, the question to Mr. Joyner: The failure modes and effects analysis, which mode did it consider? Did it consider the operator control or not?

WITNESS JOYNER: It considered the automatic control.

DR. JORDAN: Only the ICS automatic control?

WITNESS JOYNER: That is correct, sir.

DR. JORDAN: And that, I believe you said, could not lead to -- no single failure could lead to overfilling of the steam generator or running dry in both steam generators?

WITNESS JOYNER: That is correct, sir.

DR. JORDAN: All right. Go ahead. I may have other questions later on, but that is fine.

MR. THEODORE ADLER: That is precisely the point that I was going to next.

BY MR. THEODORE ADLER: (Resuming)

Q I would like to refer back to your electrical supply to ICS/NNI system diagram. I have two reasons for going back here.

I believe that in response to Dr. Jordan's question you were going to the six feeders, and I think when we got to the aux feeder we got sidetracked and we never had a response to the next two, the auto and the fan. And so I do not think he got a full answer to his question.

But I also have one line of questions on the aux system. Is there any possibility of a single failure in the switch you referred to as "new remote-operated manual transfer switch"?

(Pause.)

A (WITNESS SADAUSKAS) There is a possibility. In my opinion, it is extremely remote.

Q In the event of that single failure, am I correct that all power to the ICS would be removed?

A (WITNESS SADAUSKAS) The event you are talking about would have to occur following a failure of the static auto transfer switch, which is before the manual switch.

Q I am sorry. You can explain the probability after, if you want. Can I just have a yes or no with respect to that question?

A (WITNESS SADAUSKAS) The question again, please?
Q The question is, if there were a single failure in the switch, would all power to the ICS be terminated?
A (WITNESS SADAUSKAS) The answer to that is not necessarily.
Q Okay. Can you explain that now?
A (WITNESS SADAUSKAS) If the switch is in the position that it is shown now and we are feeding the ICS system from the inverter, as is shown now, and some postulated failure occurred in the switch and the continuity was maintained in the circuit, there would be no failure to the ICS.
Q If it failed closed or in its standard position?
A (WITNESS SADAUSKAS) In the position it's in now, there is no reason to suspect that that could happen.
Q All right. So that is why you said the possibility was remote?
A (WITNESS SADAUSKAS) Yes, right.
Q Okay. In addition to that remote possibility, let's hypothesize a single failure in the static auto transfer switch, as occurred at Oconee. Then, as I understand your testimony, you would then need to switch manually to the new remote-operated transfer switch -- I am sorry, to the TPA circuit?
A (WITNESS SADAUSKAS) If on loss of power to the

ICS system, the automatic transfer switch failed to operate -- to transfer power to the regulated bus, the operator would receive an alarm in the control room. He would be required to operate the new remote-operated manual transfer switch manually from a new switch that is being installed on the main control console.

Q Right. I believe your testimony to Mr. Sholly was that that switch would take on the order of tens of minutes; is that correct?

A (WITNESS SADAUSKAS) No, that is not correct.

Q That is not? How long would it take?

A (WITNESS SADAUSKAS) A matter of minutes, perhaps.

Q Minutes. Can you describe in either of those two circumstances the potential for a single failure in the new remote box, or during those few minutes it would take to transfer can you explain the plant status, with particular focus on thos functions that ICS controls?

A (WITNESS BROUGHTON) I would like to -- I will answer that question by indicating we have already discussed what would happen if we lose fan power, HEY, HEX, and aux. The remaining area to discuss is hand and auto, and it turns out that the difference in plant response between those two failures is very similar. I think if I cover hand, then we will have covered the effect of a total loss also.

If the plant is operating at power and there is an extended loss of hand power, then the reactor could be expected to scram, to trip. There would be some feedwater control valves which would change position. Feedwater pump speed would probably change from the full-power condition, and the result would most likely be a mismatch between generated reactor power and the feedwater being sent in, probably too little feedwater and too much reactor power, resulting in a high pressure trip, high pressure scram of the reactor.

And after that, the ICS is not available to control feedwater, either main feedwater or auxiliary feedwater, if all this power has been lost. And the control then would be via the auxiliary feedwater system, using the new manual control available from the control room.

If there was another problem, like an overcooling problem, that could have occurred because of complications, it is possible that a safeguards actuation would occur, in which high pressure injection would be called upon.

Q The new manual control emergency feedwater flow from the control room, is any action required before that system is activated? And if so, how long does it take?

A (WITNESS BROUGHTON) In order for the operator to control the emergency feedwater using the new system separate from the ICS, he merely has to activate the controller on the control panel and set in a signal which is a signal to a valve.

And those actions can be taken right from the control room, and it would be within minutes, certainly, before control could be established by that means.

Q So that the actual time where the operator would lose control of emergency feedwater flow to the valves would be relatively small?

A (WITNESS BROUGHTON) Relatively small. And even for a trip of the reactor as the one I have described, it would -- there is enough inventory in the steam generators from operation at full power that several minutes remain between the time of the trip and when emergency feedwater would be required to prevent the steam generator inventory from depleting.

Q Okay. Have you completed your explanation of all six feeders?

A (WITNESS BROUGHTON) Yes. The auto feeder we briefly discussed earlier today. But the differences between loss of the auto feeder and the hand feeder are quite small.

Q Can the turbine bypass valves be controlled independently of ICS?

A (WITNESS BROUGHTON) The turbine bypass valves can be controlled in two modes from the control room. One mode is with the ICS on automatic and the second mode is with the

ICS in hand, which is similar to the hand mode for feedwater control.

There is not a third mode which would be totally independent of the ICS to control turbine bypass valves.

Q Are there a minimum number of bypass valves that are required to be operable according to the technical specifications?

A (WITNESS BROUGHTON) To my knowledge, there are not.

Q There are not.

Are there any transients that you have analyzed where it would be -- you may have answered this question. Are there any transients where it would be necessary to terminate ICS control of main feedwater?

A (WITNESS BROUGHTON) There are some ICS failures which are analyzed in the B&W report which could cause an excessive feedwater flow, and if that were the case then there are several ways to terminate the feedwater flow, some of them by using the different mode of ICS control, some of them by shutting an isolation valve in series with the valve which might be providing too much flow.

Those are the methods that come to mind to terminate flow. And flow termination would be required if excessive flow were maintained.

Q So all of those methods of termination require operator action?

A (WITNESS BROUGHTON) Yes, those would require operator action. Not all failures which produce excessive feedwater flow would require operator action to terminate. Some of those -- I can give you an example. There might be a failure within the ICS at power, for example, which caused excessive feedwater flow.

If that resulted in a trip of the reactor, there is now a different logic used to determine what proper feedwater flow is, and if that new logic being used did not have the defective component in it, then the ICS might correct the overfeeding by itself, simply because it had been shifted into a new mode of operation.

Q I presume that termination is included in the reactor trip procedures?

A (WITNESS BROUGHTON) I am not certain which procedures it is in. But my understanding of the knowledge of the operators with respect to feedwater and also turbine bypass valve problems are that they are knowledgeable of the potential for these problems and these are things that they would look for following a trip of the plant.

I am not that familiar with the procedure to say what specifically is there.

Q Are you comfortable with the reliance on operator action in a procedure that is required during the transient to disengage the ICS system?

A (WITNESS BROUGHTON) In the case where we had to, as you say, disengage the ICS, which I believe you would be referring to, using the new method of controlling independent of ICS?

Q That is correct.

A (WITNESS BROUGHTON) That could result from a loss of feedwater or some other upset. First of all, our experience has been very good with the ICS continuing to control the plant properly after a trip. So we think that the chance of having to use this new system independent of the ICS is remote.

Secondly, there are quite a few failures which might occur, which can be corrected by shifting to the alternate mode of operation of the ICS. That is, going from automatic to hand.

Thirdly, the failures which are likely to occur are ones which would affect only one of the two generators. So we would still have adequate control in the operable generator.

And in addition, the operators do -- are very attendant to feedwater, the need for feedwater after trips, and would be monitoring both steam generators. And I think it is very reasonable to assume that if there was a malfunction, that operator action could be taken to control it.

Q Would it be preferable to have the switch automatic and safety-grade?

A (WITNESS BROUGHTON) I think our commitment in the long-term to provide this type of system indicates that we think it is a desirable system to have in the plant. We do not think it is a mandatory system, but we feel the improvement in reliability and the need to rely less on the operator to intervene would be desirable.

Q Understand that I am not suggesting at all that the ICS be converted to a safety-grade system, but merely that for all cases where you switch from control by the ICS to a safety-grade system or a preferable, a more reliable control system, that that termination be accomplished by a safety-grade device or process.

A (WITNESS BROUGHTON) Well, when we have a safety-grade control system installed for emergency feedwater, that will be the only system which will control emergency feedwater. We will not use the ICS for normal mode, and then if there is an ICS failure shift in the emergency system. So when we do upgrade the system fully, it will always be separated from the ICS.

MR. THEODORE ADLER: I have no more questions.

CHAIRMAN SMITH: Mr. Cutchin?

MR. CUTCHIN: The staff has no questions of these witnesses, Mr. Chairman.

MR. SHOLLY: Just one more question. It gets back to the tens of minutes question.

BY MR. SHOLLY: (Resuming)

Q As I have the question written down here, I asked how long it would take to switch the emergency safeguards buses if the first power source failed. And you indicated that that would take tens of minutes.

A (WITNESS SADAUSKAS) I think there is a misunderstanding as to how the answer was given. My interpretation of your question was a total loss of red channel.

Q In other words, both the static transfer and the newer mode? ?

A (WITNESS SADAUSKAS) Both the 120-volt vital bus from the inverter and the 120-volt regulated bus TRA. That is what I thought you were asking. If that's not what you meant, could you ask it again please?

Q I think I was after what Mr. Adler asked. How long does it take the operator to operate that remote switch to accomplish the changeover?

A (WITNESS SADAUSKAS) Based on that question, my answer is the same: A matter of minutes.

MR. BAXTER: The same as you just gave to Mr. Adler?

WITNESS SADAUSKAS: The same as I gave to Mr. Adler, not ten minutes like I gave you earlier.

BY MR. SHOLLY: (Resuming)

Q Is it a two-position switch, you just have to throw a switch? Or is there some kind of mechanism involved, once the operator throws the switch, that has to complete the function, and that is what takes the time?

A (WITNESS SADAUSKAS) A two-position switch.

BY MR. THEODORE ADLER: (Resuming)

Q Now I think I am confused. The switch that you are referring to in response to Mr. Sholly's question, is that to a power source that is not described in this diagram?

A (WITNESS SADAUSKAS) Yes.

MR. THEODORE ADLER: Okay.

CHAIRMAN SMITH: Do you have another question, Mr. Sholly?

MR. SHOLLY: No, sir.

CHAIRMAN SMITH: Mr. Baxter?

MR. BAXTER: I have no redirect.

CHAIRMAN SMITH: Any further questions of this panel?

(No response.)

CHAIRMAN SMITH: You are excused, gentlemen.

(Witnesses excused.)

MR. CUTCHIN: Could I have three minutes before we put the staff's witness on?

CHAIRMAN SMITH: Yes.

MR. CUTCHIN: Thank you.

CHAIRMAN SMITH: Mr. Sholly, did you offer your Exhibits 1 and 2 into evidence?

MR. SHOLLY: I have not yet. Not being totally familiar with the rules of evidence, I was not sure whether I could offer them into evidence without first having the staff's witness substantiate them.

In one case, Mr. Thatcher was the author.

CHAIRMAN SMITH: You are being quite careful. We pretty much have ignored that procedural requirement in the proceeding. You mean as to authenticity of the document?

MR. SHOLLY: Yes, sir.

CHAIRMAN SMITH: We have not required that. That would -- you are literally correct. That would come up in the form of an objection to the receipt.

MR. SHOLLY: I will wait until Mr. Cutchin returns.

CHAIRMAN SMITH: All right.

(Recess.)

MR. CUTCHIN: Mr. Chairman, I would like the record to reflect the staff passed out to the Board and the parties present copies of the documents that Mr. Tourtellotte referred to this morning as having been filed by mail yesterday. These are supplied merely as a courtesy. We also supplied an updated copy of Mr. Thatcher's professional qualifications.

Whereupon,

DALE F. THATCHER,

called as a witness by counsel for the Nuclear Regulatory Commission, having first been duly sworn by the Chairman, was examined and testified as follows:

DIRECT EXAMINATION

BY MR. CUTCHIN:

Q Mr. Thatcher, do you have before you a copy of the document with the caption of this proceeding and entitled "NRC Staff Testimony of Dale F. Thatcher Relative to the Integrated Control System Failure Mode and Effect Analysis (Sholly Contention 6-A)", consisting of seven pages.

A Yes, I have that document in front of me.

Q Was that document prepared by you or under your supervision?

A Yes, it was.

Q Do you have any corrections or modifications that you would like to make to this document?

A I have two corrections to be made on page 7.

MR. CUTCHIN: These have already been put in the report as copied, Mr. Chairman.

THE WITNESS: The corrections are in the last paragraph. I will read it the way I would like to have it changed. "In addition, requirements in the emergency feedwater design and procedures that will be in place at TMI 1 will provide a fully independent method to initiate and control emergency feedwater should the ICS fail."

BY MR. CUTCHIN: (Resuming)

Q Mr. Thatcher, do you also have before you a copy of the updated professional qualifications that you prepared and which I just supplied the Board and the parties present a copy of?

A Yes, I do.

Q Does this now accurately reflect your professional qualifications including the one change to reflect your current assignment?

A Yes, it does.

Q As corrected, do the documents -- I mean are these documents true and correct to the best of your knowledge and belief?

A Yes, they are.

Q Do you adopt these documents as your testimony in this proceeding?

A Yes, I do.

MR. CUTCHIN: Mr. Chairman, I request that the documents referred to be received into evidence and that they be bound into the transcript at this point as if read, along with the outline which will accompany them but as usual will not be in evidence.

CHAIRMAN SMITH: Without objection, they will be so received.

OUTLINE

This testimony of Dale F. Thatcher contains the NRC Staff's response to Sholly Contention 6(a).

The purpose of this testimony is to demonstrate that a failure mode and effects analysis of the instrumentation and control system, as was asserted by the contention to be necessary, has been performed.

Conclusions to be drawn from this testimony:

A failure mode and effects analysis (FMEA) of the integrated control system (ICS) for TMI-1 has been completed.

The ICS for TMI-1 as presently designed has a low failure rate and does not initiate a significant number of plant upsets.

Upsets initiated by anticipated ICS failures are adequately mitigated by plant safety systems.

Modifications that have been made in emergency feedwater system design and procedures for TMI-1 provide a fully independent method to initiate and control emergency feedwater should the ICS fail.

STAFF
9/15/80

UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION

BEFORE THE ATOMIC SAFETY AND LICENSING BOARD

In the Matter of	)	
METROPOLITAN EDISON COMPANY, ET AL.	)	Docket No. 50-289 (Restart)
(Three Mile Island Nuclear Generating Station)	)	

NRC STAFF TESTIMONY OF DALE F. THATCHER
RELATIVE TO THE INTEGRATED CONTROL SYSTEM FAILURE
MODE AND EFFECT ANALYSIS

(Sholly Contention 6a)

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

A. My name is Dale F. Thatcher. I am an employee of the U. S. Nuclear Regulatory Commission assigned to the Instrumentation and Control Systems Branch.

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

A. Yes. A copy of my statement of professional qualifications is attached to this testimony.

Q 3. Please state the nature of the responsibilities that you have had with respect to the B&W Integrated Control System and Three Mile Island Unit 1.

A. After the TMI-2 event, a number of actions were initiated on the B&W designed plants. I was responsible for the review and evaluation of the actions involving the Integrated Control System. Specifically, one of the long term actions involved a study of the Integrated Control System. I was responsible for the review (in conjunction with consultants from Oak Ridge National Laboratory) of the study which was prepared by B&W.

POOR ORIGINAL

Q 4. What is the purpose of your testimony?

A. The purpose of my testimony is to respond to Sholly 6a which states:

> It is contended that the short term actions identified in the Commission's Order and Notice of Hearing dated 9 August 1979 are insufficient to provide the requisite reasonable assurance of operation without endangering public health and safety because these short term actions do not include the following items:
>
> a. Completion of a failure mode and effects analysis of the Integrated Control System.

Q 5. What is the ICS and what are its functions?

A. The ICS is the plant control system which has as its basic function the matching of generated megawatts with megawatt demand. The system philosophy is that control of the unit is achieved through feed-forward control from the unit load demand which in turn produces demands for parallel control of the turbine, reactor, and steam generators. By coordinating the flow of steam to the turbine and the rate of steam production, the ICS can match the generated megawatts to the megawatt demand.

The flow of steam to the turbine is controlled by the turbine throttle valves. The turbine header pressure is used as an index to determine whether the steam flow rate and the steam production are equal.

The rate of steam generation is controlled by varying the total amount of feedw[illegible]er and reactor power and maintaining a proper ratio between the two so [illegible] the proper steam conditions exist. The feedwater flow is controlled by [illegible]he feedwater valves and pumps, and the reactor power is controlled by moving the control rods in the reactor.

The ICS maintains constant average reactor coolant temperature between 15 and 100 percent rated power and constant steam pressure at all load conditions. Optimum unit performance is maintained by limiting steam pressure variations; by limiting the imbalance between the steam generator, turbine, and the reactor; and by limiting the total unit load demand on loss of capability of the steam generator feed system, the reactor, or the turbine generator. The control system provides limiting actions to ensure proper relationships between the generated power, turbine header pressure, feedwater flow, and reactor power.

The ICS was designed to be able to prevent a reactor trip for many anticipated plant upsets ranging from minor upsets, such as small load changes or small feedwater heating upsets, to major upsets, such as loss of one reactor coolant pump, loss of main feedwater pump, or turbine trip from 100 percent power.

Following a reactor trip, the ICS controls steam generator level at a minimum level setpoint with the startup feedwater valves to provide decay heat removal. Upon loss of both main feedwater pumps, this minimum level control is accomplished with the auxiliary feedwater valves. Should loss of all four reactor coolant pumps occur, the level is controlled at a higher level in the steam generator (i.e., 50 percent on the operating range indication) to help promote natural circulation. Following a reactor trip, the ICS also provides control of the steam pressure with the turbine bypass valves or the atmosphere dump valves (depending on the availability of the condenser and circulating water).

Q. 6 What is a FMEA?

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

Typically a FMEA has been utilized as a tool to help systematically evaluate plant protection systems (such as the reactor protection and engineered safety features actuation system) to determine if a single failure can prevent the system safety function. It is a regulatory requirement (as stated in General Design Criterion 21) that for plant protection systems no single failure shall prevent the protection function.

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

Q. 7 Has a FMEA of the TMI-1 ICS been completed?

A. B&W has performed an FMEA on the integrated control system (ICS) as part of its reliability analysis of the ICS. The other part of the reliability analysis is a review of the ICS's "Operating Experience". The FMEA and Operating Experience are documented in B&W Report BAW 1564, "Integrated Control System Reliability Analysis". This report has been adopted by the licensee as applicable to the TMI-1 facility. (Met Ed letter to NRC dated October 26, 1979).

Q 8. What were the results of this study as reported by B&W?

A. The report concluded that the reactor core remains protected for events resulting from any of the ICS failures studied (FMEA) and that the ICS hardware failures (determined from operating experience) have not led to a significant number of reactor trips.

The B&W report recognized the desirability of improving the ICS and related systems in order to improve overall plant performance. Based on the analysis, B&W made recommendations which were to be evaluated by licensees on a plant specific basis. The recommendations highlighted areas in which B&W believed improvements could potentially contribute to improved overall operation of the plant. The majority of the recommendations related to systems/components which interface with the ICS, and were not specific in nature because of the design differences which exist at the different B&W plants.

Q 9. What are the NRC staff's conclusions in this area and the bases for these conclusions?

A. Staff consultants from the Oak Ridge National Laboratory (ORNL) reviewed the B&W report for the NRC and reported their results in a Report Review, "Integrated Control System Reliability Analysis," transmitted to the Staff on January 21, 1980. ORNL concluded that, although the ICS and related control systems could be improved, the ICS itself has proven to have a low failure rate and it does not appear to precipitate a significant number of plant upsets. The examination of the failure statistics revealed that only a small number of ICS hardware malfunctions resulted in reactor trip (approximately 6 of 162). From this data, ORNL concluded that the ICS is failure tolerant to a significant degree.

ORNL agreed with the B&W conclusions regarding control system improvements, and in particular, ORNL highlighted the need for improvements with regard to the power supplies based on the past events that have resulted from NNI and/or ICS power supply failure. In addition, ORNL suggested areas for possible further study.

The staff concurs with the ORNL assessment of BAW-1564. In addition, the staff in a letter dated November 7, 1979, has requested that all licensees with B&W plants evaluate the B&W recommendations and report their follow up actions.

As reported in the staff's TMI-1 Restart SER (NUREG-0680) page C1-1, the licensee has responded to a number of the B&W recommendations. We plan to review this information to establish the adequacy of the licensee's action. This activity is part of the NRC Action Plan (NUREG-0660, Task II.K.2).

POOR ORIGINAL

Q 10. Why is startup of the TMI-1 facility permissible prior to completion of all modifications and studies.

A. The basis for the Staff's recommendation to allow start prior to the completion of all modifications and/or studies is that, although there are areas which could potentially be improved, the present ICS has proven to have a low failure rate and does not initiate a significant number of plant upsets. In addition, ORNL has concluded that the analysis (BAW-1564) shows that anticipated failures of and within the ICS are adequately mitigated by the plant safety systems, and that many potential failures would be mitigated by cross checking features of the control system without challenging the plant safety systems.

In addition, requirements in the emergency feedwater system design and procedures that ~~are~~ will be in place at TMI-1 will provide a fully independent method to initiate and control emergency feedwater should the ICS fail. (NUREG-0680, Page C1-11, Item 1b). The Staff believes that these measures provide reasonable assurance of no undue risk to the health and safety of the public.

DALE F. THATCHER
PROFESSIONAL QUALIFICATIONS
INSTRUMENTATION & CONTROL SYSTEMS BRANCH
DIVISION OF SYSTEMS SAFETY

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

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

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

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

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

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

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

CHAIRMAN SMITH: I noted a typo in the second version of the professional qualifications, the second to the last paragraph, second sentence. "Since then". It should be "since then" and not "since the". It is obvious.

THE WITNESS: Could you tell me where that was again so I can correct it?

CHAIRMAN SMITH: Second to the last paragraph, second version of your professional qualifications. The second sentence. "Since then" instead of "since the".

THE WITNESS: Thank you.

MR. CUTCHIN: Mr. Chairman. Mr. Thatcher is available for cross-examination.

CHAIRMAN SMITH: Mr. Sholly?

MR. SHOLLY: Can I move those two documents into evidence?

CHAIRMAN SMITH: Okay. Go ahead. Mr. Sholly is offering his exhibits for identification, 1 and 2, into evidence. While you were absent from the room he observed that they had not been authenticated by the proper witness and we said, well, we have not been bothering --

MR. CUTCHIN: I have no problem with their being received, Mr. Chairman.

MR. BAXTER: I will not raise an objection because in this case my witnesses have been able to address, I think, the major aspects of the report. My concern under normal circumstances, so I do not get held in setting a precedent in the future would not be authenticity but whether you could cross-examine anyone about what the document says. In this case I guess we have all had trouble interpreting what they mean, but I think we have had enough discussion by at least the Licensee's witnesses that they can be received and I do not have any objection.

CHAIRMAN SMITH: All right. So Sholly Exhibits 1 and 2 are received in evidence.

(The documents referred to, previously marked for identification as Sholly Exhibit Nos. 1 and 2, were received in evidence.)

CHAIRMAN SMITH: Do you understand the evidentiary point that was made there, Mr. Sholly? The authenticity of the document -- of documents in this case have not risen to an issue. Mr. Baxter, except for the fact that the documents were well explored and the meanings evolved, would have objected having received them into evidence without an opportunity to examine the author as to their content, but not as to authenticity.

MR. SHOLLY: I believe I understand that.

CROSS EXAMINATION

BY MR. SHOLLY:

Q Mr. Thatcher, as received in evidence, Sholly Exhibit 1, the meeting summary, you did prepare that meeting summary, is that not correct?

A That is correct.

Q And you would be familiar with the meeting summary and you were in attendance at that meeting?

A Yes, I was.

Q Before I go into a number of questions on both the meeting summary and the Oak Ridge report, I want to try and establish exactly what you know about how the Oak Ridge report was prepared, because there have been some questions as to essentially the first five sections of the Oak Ridge report as being, perhaps, contradictory to the conclusions in the sixth section of the report.

Do you know who prepared what sections of the Oak Ridge report? In other words, which sections were prepared by Oak Ridge and which were prepared by SAI?

A No, I do not differentiate or I did not differentiate between who prepared what sections.

Q You do not know?

A I do not know. No.

Q I have to come back to that later.

Referring to Question 2 and its response on pages 2 and 3 of the meeting summary, how did the ICS boundary as it was defined in the B&W report affect the FMEA as it was done? In other words, what limitations would have been placed in the FMEA by the way the ICS boundary was defined in the B&W report?

A The limitations -- we have discussed a number of limitations. I think I agree with all those citings of those limitations. However, as far as an FMEA of the ICS, there was a bound that had to be placed to perform an FMEA and I agree with the choice that B&W made, that that was the logical choice.

Q Is it your view that the Oak Ridge report authors viewed that bounding as appropriate?

A No. I think they took issue with some of the problems created in defining that particular boundary.

Q How did the staff depend on the Oak Ridge review in terms of preparing its positions on the acceptability of the B&W report? Specifically, I am concerned about how you got to the staff position from the Oak Ridge position, which appears to be in conflict.

A Well, I do not think they are really in conflict, if you agree that the bottom line is section six of the Oak Ridge report. I think, in fact, you will note that I did cite some of the findings in my testimony.

Q You agree with the Licensee, then, that the section six of the Oak Ridge report is the bottom line in terms of deciding whether the B&W report is acceptable or not?

A Yes, although we did consider some other comments made in the other sections.

Q For instance, could you give me some examples of how you considered some of those other comments?

A Well, I am trying to find an example.

Q Take your time.

A Well, I believe -- I think the question we were on there with number 2 regarding multiple failures, the staff has to made some decision as to whether we think that multiple failures are credible or not. In that particular case, the discussion of mid-scale failures and multiple failures, those two aspects manifest themselves in power supply failures which were addressed in the B&W report, not in the FMEA, but in the operating experience section, and so, given that information, we could define -- make a decision along those lines.

Q Let's move to the SER. Do you have a copy of the SER with you?

A NUREG-0680?

Q That is correct. The section dealing with the ICS failure mode and effects analysis begins with page D-1 and concludes on the next page. I would like to ask you a few questions about the SER.

First of all, did you prepare this section of the

SER?

A No, I did not.

Q Do you know who did?

A No, I do not.

Q Okay.

DR. JORDAN: This is a rather strange turn of events which I am completely puzzled out. Your witness on ICS failure mode and effect analysis was not involved in the SER and he does not know who was.

MR. CUTCHIN: That is not surprising to me, Dr. Jordan.

DR. JORDAN: All right.

(General laughter.)

MR. CUTCHIN: Mr. Thatcher was intimately involved in the failure modes and effects analysis work in that he was the technical coordinator for the Oak Ridge study and I am not sure that the SER here at this point has a great deal of substance and I think Mr. Thatcher's testimony is more substantive.

DR. JORDAN: I see. So if there are disagreements between what is in the SER and Mr. Thatcher's testimony you would say that you would rely on Mr. Thatcher's testimony.

MR. CUTCHIN: At this point in time I believe that is correct, because as I am reading here from the SER, we were indicating that there was further review under way and that we would address is further in a supplement which, I presume, is yet to come.

DR. JORDAN: Okay. Go ahead, Mr. Sholly.

BY MR. SHOLLY: (Resuming)

Q On page D-1, the third paragraph, the third sentence reads "However, we have also concluded that as a result of failures in related systems, actions of the ICS can lead to major upsets." What related systems were being referred to there?

A As I said, I did not prepare this section, but I think I can -- I hate to conjecture. I can give you my knowledge of what could have been meant by that statement.

CHAIRMAN SMITH: Let's phrase the question so it will produce something more than conjecture. Are you aware of the failure -- failures in related systems as the term is used in that sentence?

THE WITNESS: Failures in related systems, as long as related systems refer to things such as the non-nuclear instrumentation, the power distribution system -- to name two. As long as the related systems means that, then, indeed, actions of the ICS based on those failures can lead to major upsets.

CHAIRMAN SMITH: So this sentence, as far as you know, is not referring to actual historical failures of related systems. It is postulated failures?

THE WITNESS: It may well be referring to historical failures.

CHAIRMAN SMITH: Are you, yourself, familiar with such failures?

THE WITNESS: Such historical failures?

CHAIRMAN SMITH: Yes.

THE WITNESS: Yes, I am.

BY MR. SHOLLY: (Resuming)

Q Could you give an example?

A An example of -- well, I guess crystal -- I heard the word Crystal River event. That could be an example.

Q Do you feel that the B&W report, the manner in which that report was done, could have predicted the Crystal River event?

A I think so, as long as you consider the operating experience, because we did -- it was pointed out in the operating experience section -- August I think is the date on the report -- August of '79. I think I have the right year. That power supplies were indeed failure -- one of the significant failure contributors.

Q What I am trying to get at is the failure mode and effects analysis portion -- the manner in which that was done. Is it capable of predicting a failure such as the Crystal River event? Granted, once it happens obviously you know about it and can take a look at it. But what I am trying to get at is are there possibly other failures which have not occurred yet?

CHAIRMAN SMITH: I do not think you understood his answer, or at least the dates will have to be adjusted if his answer means what you thought it does. And the Crystal River event to which he is referring is February, 1980, and he has referred somewhere to August 1979 report.

MR. CUTCHIN: That is the BAW 1564, is that correct?

THE WITNESS: That is correct. And the date is August, 1979.

MR. SHOLLY: I understood that. I was going to get to that. Why --

THE WITNESS: Is there a question to me right now? I thought there was.

CHAIRMAN SMITH: No. No, there isn't. I fear I interrupted without cause, but I thought that you were suggesting that once the Crystal River transient occurred then it is incorporated in the history, and I thought you were suggesting a circular approach to it.

MR. SHOLLY: That is exactly what I was trying to get to. In other words, it seems to me that, based on a reading of the Oak Ridge report, that there were certain limitations placed on what the B&W FMEA could predict. I, first of all, would like to know whether the B&W failure mode and effects analysis could have predicted the Crystal River event and, if not, then possibly are there other events which it could not have predicted?

CHAIRMAN SMITH: There is no question --

MR. SHOLLY: I will try phrase that in terms of a question.

BY MR. SHOLLY: (Resuming)

Q Do you feel that failure mode and effects analysis as done by B&W could have predicted the Crystal River event?

A Not as done by B&W in 1564. That is not to say that a failure mode and effects analysis could not predict Crystal River.

Q But the B&W FMEA as it was done could not have predicted Crystal River?

(Pause.)

A If I could ask what portion of the Crystal River event you consider significant. The problem I have is I know about the -- certain things that happened with the control systems and -- but I guess there is some concern that they pumped water on the floor. Is that your concern?

Q What I would be referring to is the manner in which the integrated control system was involved in that particular event. Could the --

A The -- okay.

Q Let's go through a series of questions. Maybe this would be a more efficient way of doing it.

Do you know to what extent the integrated control system was involved in the Crystal River event?

A Pretty much so. I am sure if you get into very detailed questions I might not know the exact answers, but I am pretty familiar with the integrated control system's performance at Crystal River.

Q Okay. Now what -- what failures occurred in the integrated control system? Just generally.

A None that I know of other than -- no. None that I know of in the integrated control system itself. None that I know of.

Q Did the integrated control system's actions exacerbate that particular event?

The actions of the integrated control system caused what some people might consider exacerbation of the event. And that is to say that it indeed did start momentarily pulling control rods, for example.

Q Did the integrated control system also cause the PORV to open?

A No.

Q It did not. What caused the PORV to open?

A I think it was the power supply failure itself that caused the PORV to open.

Q The ICS played no role in that?

A No. I do not believe the ICS played a role in that, in the opening of the PORV.

Q It did not.

A No. The opening of the PORV was due to the mechanism in the power supply failure -- the particular mechanism in which that power supply failed.

Q You have testified that perhaps in some respects the integrated control system did exacerbate the Crystal River event. Is that sort of effect from the operation of the integrated control system capable of being predicted by the B&W failure modes and effects analysis?

A Yes, I think it is. If you take the front-end failure that the power supply loss at Crystal River created and then follow it through the FMEA of the integrated control system, you could predict that the control rods would move out, et cetera.

(Pause.)

Q To your knowledge, within the operating history of B&W plants, are there instances, events involving the integrated control system, that have occurred which would not have been predicted by B&W's failure mode and effects analysis?

A I think the failure mode and effects analysis that B&W did is an accurate reflection of what consequences occur given the failure modes postulated. That does not mean, though, that that particular tool could predict all potential consequences. I don't know --

Q In terms of insuring public health and safety, do you think the failure mode and effects analysis by itself is enough to insure the public health and safety is protected from all events involving the integrated control system?

(Pause.)

A There is a lot more to protecting the health and safety of the public than looking at the integrated control system.

Q What --

A I thought I was following your question until you said with regard to the integrated control system. Maybe if you repeat it. I was anticipating and I should not have been, but the reactor protection system has to perform the -- has to protect the public health and safety. Engineered safety features have to operate to protect the public health and safety.

Q What I am concerned about is the usefulness of the failure mode and effects analysis as it was done to assure safety and that this is one of the criticisms of the Oak Ridge report. They stated that the significance of the ICS to safety is not addressed. Granted, the Licensee's witness took issue with that. Do you take issue with that? Do you feel that the B&W report addresses the safety significance ofd the integrated control system?

A I think it does address the safety significance of the integrated control system, but there are a number of things that you have to put in context when you look at that on the surface.

There is concern that -- there are concerns that the ICS could create a loss of feedwater event and also prevent the admission of auxilliary feedwater to the steam generators, but that concern, in and of itself, is being addressed separately from any FMEA and FMEA results.

CHAIRMAN SMITH: Of the ICS.

THE WITNESS: FMEA? ICS? Yes.

CHAIRMAN SMITH: I wondered if you had completed your statement. I was suggesting a completion to your statement.

THE WITNESS: I am sorry. I can make the statement again. I mean --

DR. JORDAN: I think it would be worthwhile to state it again. What you think the --

THE WITNESS: I was trying to make the point that the concerns regarding ICS control of main feedwater and also emergency feedwater were being addressed separately from the FMEA on the ICS. That that is a separate issue because, one, by virtue of the fact of the short-term orders which require some manual actions and we heard about that from the witnesses from GTU, and in the longer term because of the recommendation that comes out of NUREG-0578, which requires a "safety grade auxilliary feedwater system". And I believe the Licensee -- both of those issues are addressed in the restart evaluation.

Now, I was going to give at least another example of how the ICS reliability study does address safety -- I am sorry, I don't remember your term, safety or health and safety of the public, and I was going to say that based on operating experience it was shown that the challenges created by that system itself are not really that great. So that says to me that the ICS does do its job, and it does not create -- does not create a large amount of challenges to the protection system in any analysis of an overall plant -- I want to say safety analysis with regard to health and safety of the public. That the concept of defense in depth is utilized by the staff. And the first line of defense as far as electrical instrumentation and control components goes is the plant control system. If that is a misbehavior -- misbehaver -- I don't know if that is a word -- the plant safety systems will be challenged frequently and any system that is challenged too frequently may, you know, fail. That is the second portion of defense in depth -- the protection system.

So that is another area where I think the reliability study did show -- what was the word -- the safety significance of the ICS, or safety consequences. I am not sure what the wording was.

BY MR. SHOLLY: (Resuming)

Q Take a look at a couple of sections of the Oak Ridge report. Take a look on page 7, the second paragraph. In particular, the last sentence states, "It would not be impossible for perculiar equipment interactions or operating conditions to place the ICS at such a disadvantage that it would respond, although, as designed in an undesirable way." This is the sort of thing that I think all day has been raising questions -- I know in my mind -- as to how useful this failure mode and effects analysis is in terms of insuring safety.

In examining the Oak Ridge report, you stated before that you took some of the concerns that the Oak Ridge review made into consideration in preparing your testimony and arriving at your positions on the FMEA. Did you consider this particular point?

A Well, this particular point I do not consider to be an indictment of the ICS itself. I think this is a restatement of the discussion we had with regard to the Crystal River event. That, given wrong inputs, that the ICS may respond in undesirable ways -- for example, pulling control rods.

Q Okay. Given that, and that is the case, do you feel that the B&W failure mode and effects analysis adequately responds to that type of concern?

A I do not think the FMEA, in and of itself, adequately -- would adequately address that. But in conjunction with the operating experience and the conclusions drawn in section six of the Oak Ridge report, that those, you know, those type of concerns are addressed

Q Do you think you would have held the same opinion before the Crystal River event?

A Well, the Crystal River event was highlighted -- to me it highlighted a separate set of concerns other than ICS. Previous to Crystal River -- and this was mentioned also -- the Oconee event, which occurred in November of 1979, occurred -- in fact November, 1979, when this report was being prepared. John Anderson and myself went down to Oconee after that event occurred. Subsequent to that event the staff issued I&E Bulletin 79-27.

Now, given, you know -- to me that addressed a separate set of concerns other than the ICS itself.

Q What I am concerned about that I think is happening, and if, after listening to my explanation you think I am misperceiving things, please clarify it.

What seems to me has happened is failure mode and effects analysis has been done on what the Oak Ridge report feels is a fairly narrow basis. There is some operating history which expands on that somewhat and the position is taken, well, this is adequate now. This addresses the failure mode and effects analysis requirement. The operating history gives us a pretty good picture of the reliability and we are pretty comfortable with that until event A comes along. That is incorporated in the operating history and now we are satisfied again until event B comes along and that is incorporated into history.

It seems to me that this is parallel with a class nine accident where a class nine accident is incredible. TMI 2 happens. Okay, all other ones are still incredible and we are back to go again. Am I misperceiving something there?

A Well, I guess I can only speak to the area of instrumentation and control, you know, systems. And if your perception is that Oconee and Crystal River -- those events -- brought in some new concerns, they were not with the ICS. You know, operating experience is a good teacher. Do you know I do not know -- you know, I do not know how to indict the FMEA on the ICS as, you know, problems with -- you know -- should have prevented the Oconee event or the Crystal River event.

Admittedly, you know -- you know, if power supply modifications could have been made, potentially they could have been prevented. But you know that is only, you know, a guess.

Q Let's move on to another line of questioning. In your testimony, at page 7, you state that the present ICS has proven to have a low failure rate and does not initiate a significant number of plant upsets. Has the staff reviewed the operational history of the ICS 721 and ICS 820 systems as presented in the Oak Ridge and the B&W reports?

A The only review of those systems was the review of the report BAW-1564.

Q You are familiar with the failure rates of those two systems?

A From the report.

Q Yes.

A Yes.

Q Does the staff take any position as to whether the 721 system is more or less acceptable than the 820 system based on the historical failure rate? Or are both of them acceptable?

A Both of them are acceptable.

Q Both are acceptable?

A Maybe I should phrase that more -- the staff does not differentiate between one being more or less acceptable than the other one.

Q In other words, you do not feel there is any significance to the differences in failure rate?

A The failure rate tabulation is not a good statistical sample to base any conclusion like that on.

Q Okay.

DR. LITTLE: Would you approve a 721 system for a new plant design?

THE WITNESS: Probably. Yes.

DR. LITTLE: All right.

BY MR. SHOLLY: (Resuming)

Q In the SER it is indicated that the Licensee has responded to a number of B&W recommendations on the ICS. Can you state whether or not Licensee has completed his response to those B&W recommendations?

A No, I cannot. I no longer have the responsibility for the review of those recommendations and the follow-up.

Q You would not be familiar with any schedule, then, that might have been established for completing those responses?

A I am familiar with -- I have discussions with some of the individuals that are responsible for follow-up in those areas. And the last indication I had, I believe, was from something that was to be presented at the ACRS meeting. I believe it was last Saturday. And according to the information I have, the responses of all B&W licensees, including Metropolitan Edison, to the recommendations of the

B&W -- BAW 1564 -- will be pursued in the first half of 1981.

You know that is not official. I am not responsible for schedules. But that is, you know, my best answer to that question.

MR. SHOLLY: Give me just a moment. Mr. Chairman, perhaps the Board will appreciate this more than the other parties. I am having trouble sorting out from everything that has happened this morning what might have been covered by this Licensee's witness. It has become increasingly difficult to be productive.

CHAIRMAN SMITH: Would you like to break for this evening? That way you can go over your notes overnight and perhaps be more efficient in the morning.

MR. SHOLLY: I think so.

CHAIRMAN SMITH: Okay. Tomorrow morning we are going to have the report on the SER supplement. You are involved in that too, aren't you?

MR. SHOLLY: Yes.

CHAIRMAN SMITH: Anything further this evening?

(No response.)

CHAIRMAN SMITH: Let's adjourn until 9:00 a.m. tomorrow morning.

(Whereupon, at 5:52 p.m., the hearing was adjourned, to reconvene at 9:00 a.m. Wednesday, December 3, 1980.)

NUCLEAR REGULATORY COMMISSION

This is to certify that the attached proceedings before the

____

in the matter of: METROPOLITAN EDISON COMPANY (TMI UNIT 1)

Date of Proceeding: December 2, 1980

Docket Number: 50-289(Restart)

Place of Proceeding: Harrisburg, Pa.

were held as herein appears, and that this is the original transcript thereof for the file of the Commission.

David G. Parker

Official Reporter (Typed)

[signature]

(SIGNATURE OF REPORTER)