ORIGINAL ACRST-1777

OFFICIAL TRANSCRIPT OF PROCEEDINGS

Agency: U.S. NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

Title: Meeting of the Advanced Pressurized Water reactor subcommittee

Docket No.

LOCATION: Bethesda, Maryland

DATE: Wednesday, January 10, 1990 **PAGES:** 1 - 254

ANN RILEY & ASSOCIATES, LTD.
1612 K St. N.W., Suite 300
Washington, D.C. 20006
(202) 293-3950

PUBLIC NOTICE BY THE

UNITED STATES NUCLEAR REGULATORY COMMISSION'S

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

DATE: Wednesday, January 10, 1990

The contents of this transcript of the proceedings of the United States Nuclear Regulatory Commission's Advisory Committee on Reactor Safeguards, (date) Wednesday, January 10, 1990, as reported herein, are a record of the discussions recorded at the meeting held on the above date.

This transcript has not been reviewed, corrected or edited, and it may contain inaccuracies.

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

***

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

Meeting of the Advanced Pressurized Water Reactor Subcommittee

Nuclear Regulatory Commission
Conference Room P-110
7920 Norfolk Avenue
Bethesda, Maryland

Wednesday, January 10, 1990

The above-entitled proceedings commenced at 8:35 o'clock a.m., pursuant to notice, J. Carroll, Subcommittee Chairman, presiding.

PRESENT FOR THE ACRS SUBCOMMITTEE:

J. Carroll	W. Kerr
C. Michelson	P. Shewmon
C. Siess	D. Ward
C. Wylie	

ALSO PRESENT:

M. El-Zeftawy, Cognizant ACRS Staff Member

L. Donatell, NRC/NRR

REPRESENTATIVES PRESENT FROM WESTINGHOUSE:

E. Burns	T. van de Venne
G. Remley	J. Easter
E. Carlin	B. Schively

PROCEEDINGS

[8:35 a.m.]

MR. CARROLL: Good morning. The meeting will now come to order. This is a meeting of the Advisory Committee on Reactor Safeguards, Subcommittee on Advanced Reactor Pressurized Water Reactors. I am J. Carroll, Subcommittee Chairman.

The other members of the ACRS in attendance today are Bill Kerr, Carl Michelson should be here shortly, Paul Shewmon, Chet Siess should be here shortly, Dave Ward and Charlie Wylie.

The purpose of this meeting is to continue our review of the Westinghouse Evolutionary Light Water Reactor SP/90.

Medhat El-Zeftawy is the cognizant ACRS staff member for this meeting. The rules for participation in today's meeting have been announced as part of the notice of this meeting previously published in the Federal Register on December 21, 1989.

A transcript of the meeting is being kept and will be made available as stated in the Federal Register notice. It is requested that each speaker first identify himself or herself and speak with sufficient clarity and volume so that he or she can be readily heard.

We have received no written comments or requests to make oral statements from members of the public.

As you can see from the agenda that has been passed

out, we have a rather full day ahead of us. We'd also like to take advantage of Paul Shewmon and Chet Siess' attendance today to cover the areas of particular interest to them, which it looks like will naturally fit into the presentation today.

We will proceed with the meeting and I'll call on Loren Donatell of the staff to begin.

[Slide.]

MR. DONATELL: Thank you, Mr. Chairman. Good morning. My name is Loren Donatell. I am the Project Manager for the SP/90 PDA. For those of you that I haven't met in the past, a brief background. I've only been with the NRC for about five months. I've been the new Project Manager for that same period of time.

Previous experience was ten-and-a-half years with Combustion Engineering. I hold a Bachelor's in nuclear engineering and eleven years enlisted nuclear Navy.

[Slide.]

MR. KERR: When you say you're the new Project Manager, does this correspond to being sent to Siberia or something?

MR. DONATELL: I think that will become clearer as we go on this morning. Every time we've gotten together in the past, there have been questions on what is a PDA. I've attempted to rough out some things here that I've been able to find out about a PDA. You have to go to a lot of sources to

find it.

First, we have issued 13 PDAs. The last was November 14, 1978. That was the Westinghouse 414. The RESAR SP/90 PDA is the first to include severe accident policy statement in the review.

This has caused a great deal of difficulty, I believe, with the staff. I believe that difficulty is still continuing and hopefully some of that will come a little clearer as we go on.

The PDA does constitute a reference design, which means that when it is enforced, it can be referenced in applications. Those applications are construction permit, manufacturing permit.

Requirements on the PDA require design detail equivalent to a Preliminary Safety Analysis Report, like 50.34. This last point is probably a little different from what we told you back in November. Charlie had mentioned that the PDA would be subject to complete review even after it is issued.

Although that is the intent of the staff, that is not strictly true. It is subject to 10CFR50.109, the backfit rule, which means that those items in the PDA that are approved when the PDA is issued fall under the backfit rule.

I apologize for essentially what we said the last time. This is a point that got lost in the weeds someplace.

[Slide.]

MR. DONATELL: I hope you will bear with me. I'm trying to fight a cold here. The current review status; you've seen this before. The only thing that is really different here is the second to the last item. The Commission has approved the June 1990 completion date for the PDA.

This came down in a staff requirements memorandum in December. I think the number is 311. I do have a copy of it which I can give you later for distribution if you don't have those things.

Essentially what it set was the priorities for the staff review of the standard designs. This is part of the problem that I am going to have on this thing.

June looks like a pretty good completion date. However, frankly, my priority is very low. I'm about number six on the list behind everybody else in the world. That gives me a little problem with the review staff and the fact that, one, I've got a low priority and I've got a near-term completion date.

To meet this, I've instituted a process that I think is rather aggressive and I hope will still get me there. It's going to change things from the traditional approach to make it by June. One of the things I am doing is I'm taking draft input from the reviewers on the open items that exist.

I'm taking that draft input and I'm writing it into the draft final SER myself. That will go back for quick

concurrence to the review staff in hopes to get the total package together for review no later than March.

Two other things that are involved here. We had mentioned before that two of the milestones that we anticipated meeting were, one, issuing a draft SER on the back end of the PRA. That was, by earlier schedules, due in November. It obviously has not been issued yet.

My intent right now, if I can get concurrence on it, is to take that information and write it into the draft final as opposed to releasing a single draft SER. That may change if I get the thing in my hands in an orderly fashion.

The other issues are the USIs and GSIs. Westinghouse, in September, submitted a very large amendment; Amendment 3 to Module II, which is regulatory conformance, which addresses all the USIs, GSIs, TMI items.

At this point in time, I think it's entirely possible that the staff will not review that amendment and that entire amendment will probably be left open in the draft final SER.

That seems to be the desires of the staff at this point in time, although I haven't gotten complete guidance on that yet. Part of the problem with this points back to one of the other slides where I said that this PDA was the first one subject to the severe accident issues.

Two years ago when this review was actually heating up, even though it's been in existence for quite a while, the

intent was that these USIs and GSIs, the input from Westinghouse would have been in our hands, I think, a little over a year ago.

So the intent was to run the SP/90 in parallel with the other reviews that were in-house at the time, holding the PDA essentially to the same standards as an FDA at that stage, which meant that the USIs and GSIs would, in fact, be reviewed and passed upon.

I also believe that, I think it was Mr. Michelson, some time ago, asked the specific question, how far is the review going to go, are you going to review the USIs and GSIs, and was told at that time that that was, in fact, going to be the case.

Again, because of the recognition of the PDA, the short term for issuance of the PDA, that is no longer the case.

MR. KERR: Mr. Donatell, I'm not sure I understand what you have just said. There seems to be some implication that the severe accident issue is the principal sticking point. Is that --

MR. DONATELL: Yes, sir. It is definitely one of the major sticking points.

MR. KERR: And the severe accident issues are not going to be reviewed at the PDA stage.

MR. DONATELL: That is essentially what I'm saying, yes. Now, they have been reviewed as a first cut through two

draft SERs at this point in time. After the two draft SERs were issued, then the amendment from Westinghouse arrived which was September, I believe, of 1989.

So the intent is to include some statements in the draft final SER and Westinghouse's input based on that amendment, but not to do a complete and thorough review.

MR. KERR: It puzzles me that one can talk seriously about reactor safety and not review the severe accident issues since this is the principal contributor to reactor risk if one believes the current state of knowledge. But I will try to preserve an open mind.

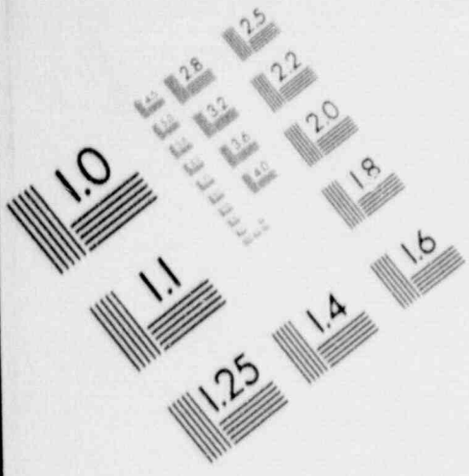
MR. DONATELL: Sir, I agree with that. Some of the things that are going on right now; there is a Commission letter that's being generated that is asking for Commission guidance on several of these severe accident issues at this point in time, either concurrence or non-concurrence with staff position.

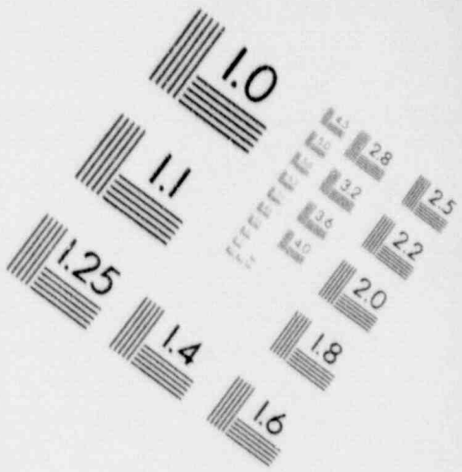
That is not in the hands of the Commission yet. It will be shortly. It will obviously take some time for them to make some decisions on this. I really believe the whole severe accident issue still is in a complete state of flux.

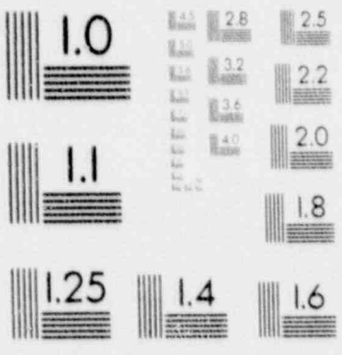
For a PDA stage, as far as the rules go, we have to address the severe accident issues in the PDA. I can't find any guidance as to what kind of depth we're looking at at the PDA stage.

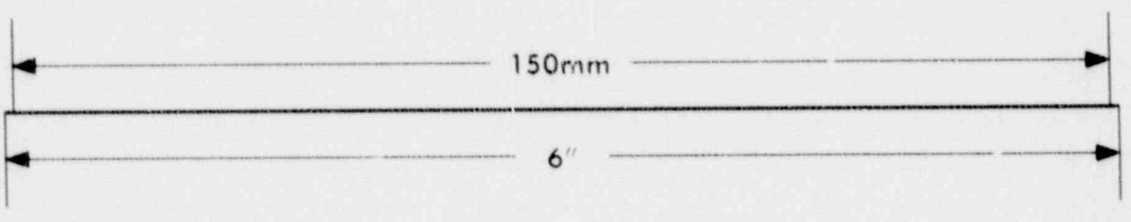
1

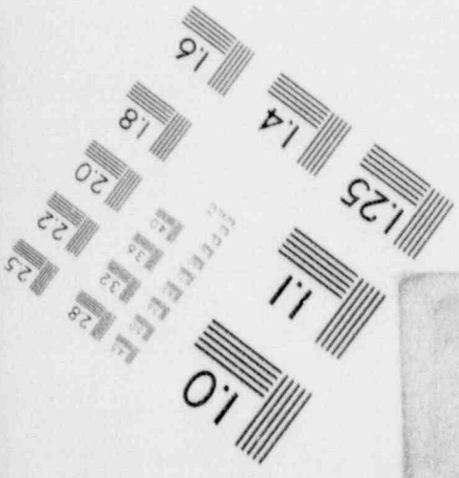
IMAGE EVALUATION TEST TARGET (MT-3)

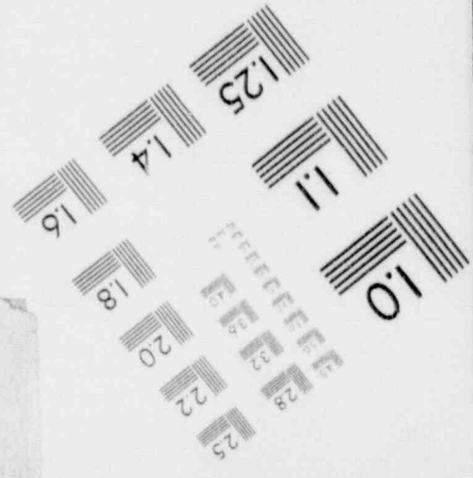






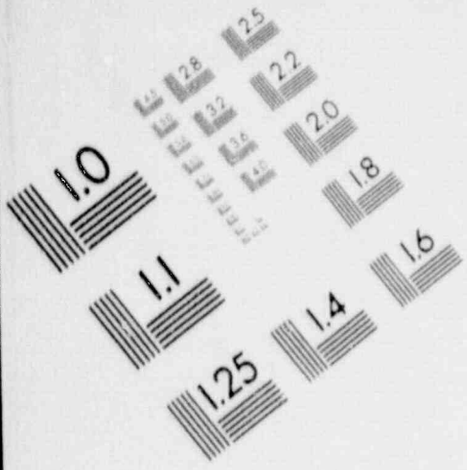


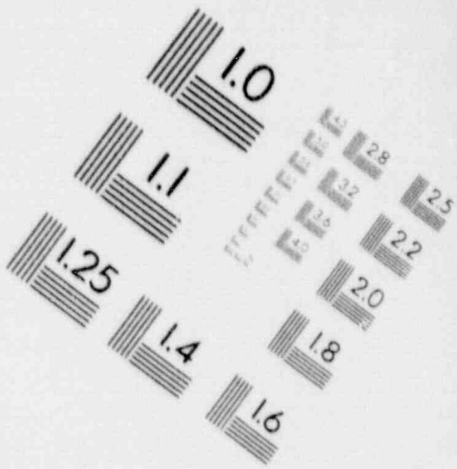


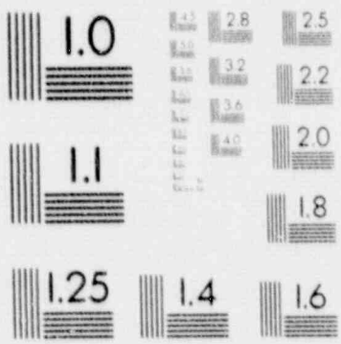


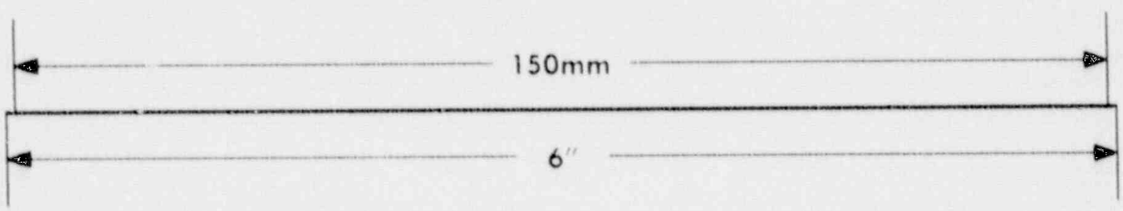
1

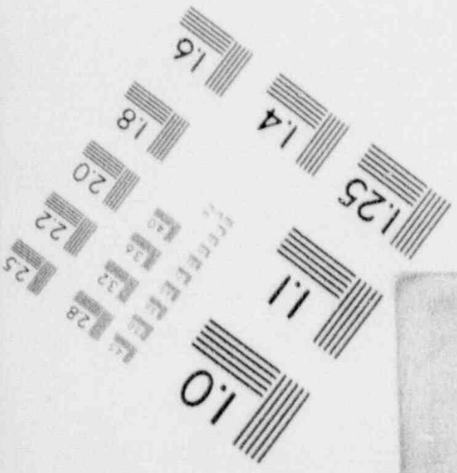
IMAGE EVALUATION TEST TARGET (MT-3)

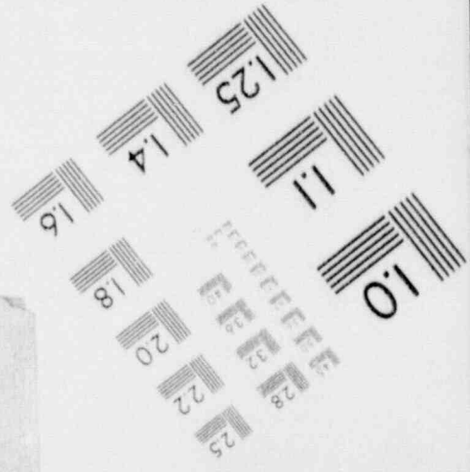


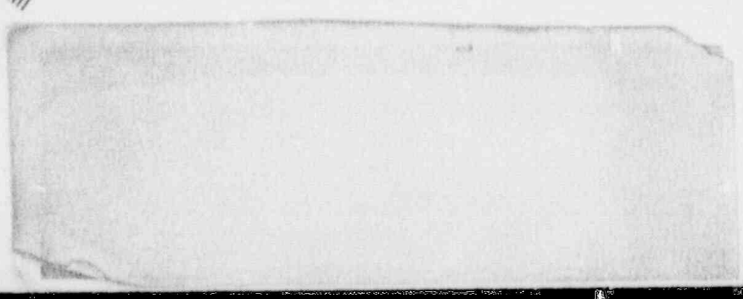






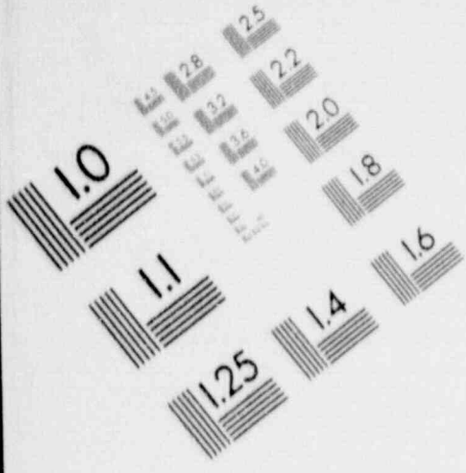


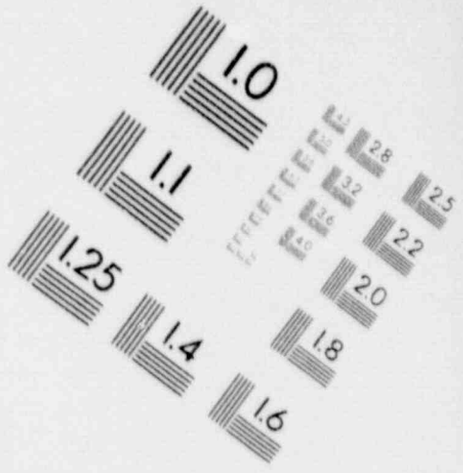


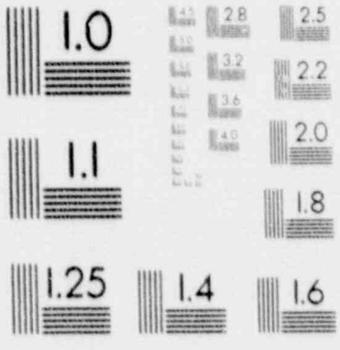


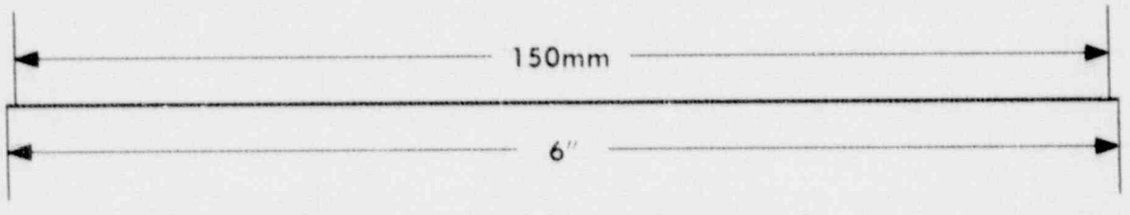
1

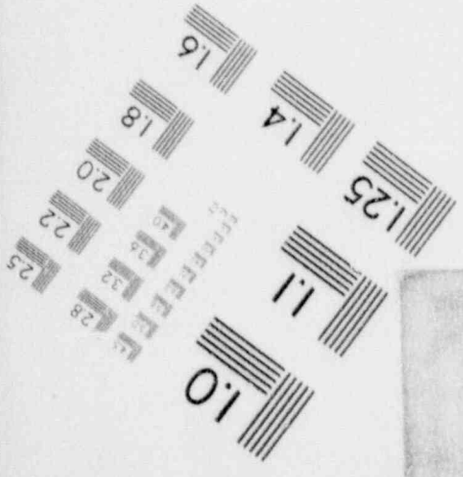
IMAGE EVALUATION TEST TARGET (MT-3)

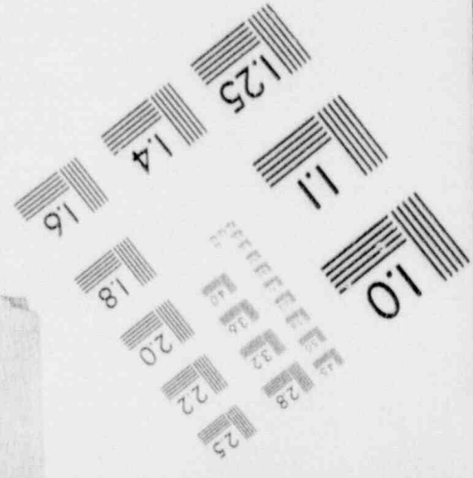






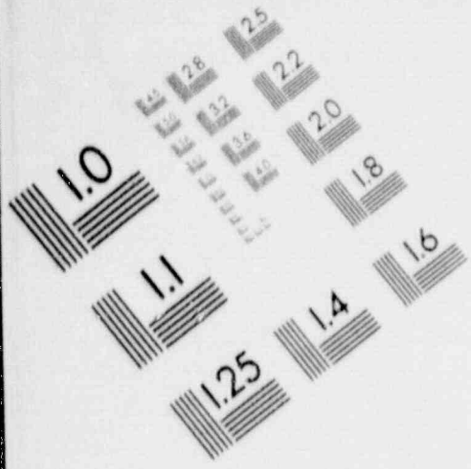


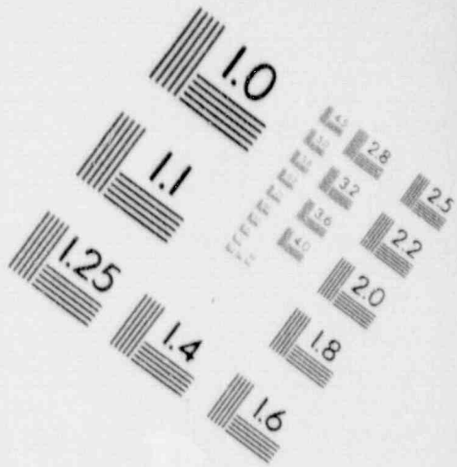


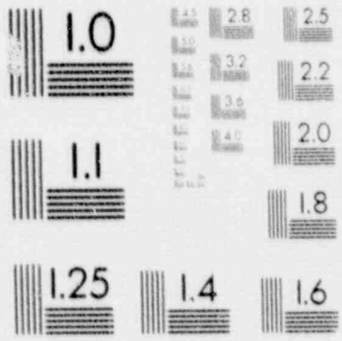


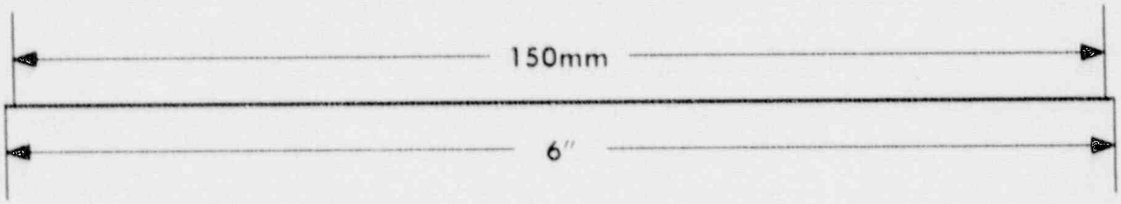
1

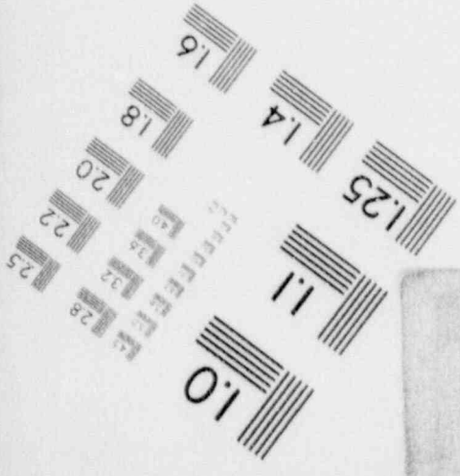
IMAGE EVALUATION TEST TARGET (MT-3)

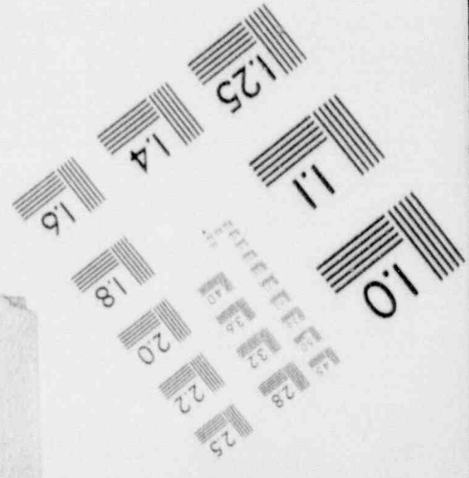












So what we're looking at is what we have historically done for a PDA and trying to factor in the new guidance under Part 52 in the new Appendix O.

MR. WARD: Excuse me. I gather your strategy here is just to -- because of what you told us about the application of the backfit rule, it makes sense.

MR. DONATELL: Yes. That is absolutely part of it, sir.

MR. WARD: Yes. So you're trying to just close out the parts of this that you're comfortable with closing out at this stage and at the level of effort you're going to put on it.

MR. DONATELL: That's correct.

MR. WARD: And the rest is just going to be left open.

MR. DONATELL: That's correct.

MR. MICHELSON: Since it's been a while since I've seen somebody proposing a PDA and the climate is changing, in today's knowledge, what do you think a PDA is granting? What is a PDA today?

MR. DONATELL: Historically, a PDA was issued, my perception and based on reading I've done, research I've done at this point in time, allowed -- once a PDA was in place, it allowed an applicant to come in and essentially apply for a construction permit based on that PDA and then to move forward

and to finalize the design as the construction progressed. The old days essentially were design and construct.

That environment has changed. The advent of Part 52 really puts PDA in an entirely different light. Frankly, it's probably a dinosaur. But it does give the applicant the ability to get a preliminary design in front of the staff for review while he is working on a final design, to get a number of items out of the way based on that staff review and approval, leading to the FDA stage.

But the only real purpose I see here is that you really are going forward to that FDA stage. You're getting work done by the agency while you are moving forward to FDA. PDA and FDA are not coupled by the rule. You do not have to have a PDA prior to submitting for an FDA.

So it's kind of one of those things that's held over, I think from the old days, but it does give the applicant some amount of leeway and ability to actually get some things moving while his design is progressing.

At this point in time, however, Westinghouse has expressed the fact that they will not go into an FDA stage until such time as they have active interest in this design. Their desires are to wind the PDA down and get it out of the way.

Also, PDA traditionally, there is a term on the PDA. The ones that we have historically issued have gone anywhere

from about five years to about two years when the PDA was active and could be utilized as a reference design.

I'm not sure how the time period was set. I suspect it was based on what the applicant's desires were or some mutual negotiation somewhere along the line. That will be another issue that we'll have to address at that stage, is the term that the PDA would be issued for.

MR. WARD: At what stage do you address that?

MR. DONATELL: We're going to have to address it obviously prior to issuance of the PDA. I think it's going to have to be something that is mutually acceptable to the agency and to the applicant.

MR. WARD: What is that likely to be -- well, I don't want to put you on the spot.

MR. DONATELL: I'll be frank. My guess is it will probably be short, but not too short; a year, two years type thing. I think that's the direction we would follow.

MR. MICHELSON: Apparently you are seeking certain commitments, design commitments at the PDA stage so that you don't have to revisit it at the FDA stage?

MR. DONATELL: That's actually the intent of the PDA, yes.

MR. MICHELSON: Can you give me some examples of things that you think without a completed design can be approved finally for this plant?

MR. DONATELL: I think if we look at the last draft SER, which was a fairly voluminous document, there were only 107 open items against that document for the PDA stage. That's all based on the standard review, plan review.

MR. MICHELSON: Is that also based on the staff no intending to revisit such issues?

MR. DONATELL: Sir, I have to assume that, in fact, is the case.

MR. CARROLL: Or if you were going to, you'd have to be able to justify your revisiting in light of the backfit rule.

MR. DONATELL: Absolutely. Something would have to be identified in the text. Dr. Murley has already said that the PDA would be issued with a number of open items. I'll get into this shortly. I've got an idea of what that number is going to be.

That means open items against the PDA, which means that if an applicant were to come in for a construction permit for this design, those items would have to be closed first prior to the construction permit being issued.

Once that is done, then they would be into the next phase, accelerating the design; making the design more rigorous; getting into the FDA stage at that point in time.

MR. MICHELSON: One other question. I gather from what you have said that you are anticipating not doing the FDA

until there is some live customer available?

MR. DONATELL: That's Westinghouse's intent.

MR. MICHELSON: Does that mean, then, that you wouldn't go through the certification process before he applied for construction?

MR. DONATELL: Well, no. You're going to have to get there.

MR. MICHELSON: No. But it takes a couple of years to certify or more. Would you wait two years before you started construction? Is that the idea?

MR. DONATELL: That really hasn't been visited.

MR. MICHELSON: I was just trying to see what --

MR. DONATELL: It would seem under the light of the new rule that that would be the prudent way to approach this thing. I frankly, and Westinghouse can add their thoughts on this, but I frankly can't see an applicant or utility requesting a construction permit, frankly, at this stage and then really going forward with the construction with all the uncertainties ahead of them.

MR. MICHELSON: Thank you.

MR. CARROLL: But that doesn't necessarily apply to a non-domestic customer.

MR. DONATELL: That's correct. If you look at our reviews, there is something that, frankly, the vendors can put in their pocket and take to a foreign customer and say this has

been done by a U.S. agency for this level.

One of the other things that -- there's another staff requirements memo -- I think it's 334 -- that the Commission has just issued. There are a number of things in there, but the thing that effects this particular project at this time is the way the Commission would like to handle draft SERs.

There are still a couple of pathways open to do this, but, one, the Commission wants all draft SERs in no time period, but prior to issuance. They want to be in that loop and they want the draft SER ahead of time essentially.

They also want the draft SER to indicate if there are any places in that draft SER that the staff has required the applicant to go beyond current rules or if there is a change in the applicant's design that would appear, and this is the way I read it, appear to go beyond certain current rules.

I think that's an extra loop in my process that's going to take time. I have no idea what that time is. I just mention that for that fact. When I get into what I propose for a schedule at this time.

MR. MICHELSON: Now, that was only in those cases wherein the staff was asking you to go beyond what you have committed to, but you might have committed to beyond current rules.

MR. DONATELL: That's right and I think there's a little uncertainty there, sir. The Commission may be concerned

if the staff is imposing, arbitrarily imposing excessive requirements on the applicant.

If the applicant comes in and overpowers an issue, to do that, his design is probably going to be significantly different from what we've seen in the past; will probably overpower the rule, also.

The question is it does deviate from the rule, even though we can say it deviates from the rule in a positive direction, but it is a deviation from current standards.

MR. MICHELSON: Of course, the Commission has already indicated they expect these next generation of reactors to be improved and have many features which are not necessarily as well done in present-day plants. So I'm trying to determine what they're worried about.

Are they worried about going beyond -- since those features haven't been prescribed yet in the regulations and, yet, they have asked for them in future plants, what are they worried about?

MR. DONATELL: You may have put your finger on it; that these things are not currently prescribed. Maybe the question is should they be.

MR. MICHELSON: Yet, they are expected, by Commission policy they're expected.

MR. DONATELL: That's right.

MR. MICHELSON: So I'm confused as to what the

earlier statements you made mean.

MR. DONATELL: Sir, I will join you.

MR. MICHELSON: But at any rate, it will get cleared up later.

MR. DONATELL: I'm also a little confused.

[Slide.]

MR. DONATELL: Open items: As I had said before, I am taking draft input from the reviewers on the open items that have been identified against the PDA at this point in time.

There were 107 of them. This is approximately where I see it today, based on the input that I have gotten. I have gotten input on everything with the exception of 15 items. I will get those shortly.

Thus far, we have found approximately 50 items that Westinghouse's last responses are acceptable to that particular open item. There are 18 items, at this point in time, that are going into the next category, if you remember back to one of the earlier meetings, that will go up to the FDA stage.

I've got two items that I've listed as greater than FDA. That's my shorthand, I guess. I apologize for that. That may be FDA. It may be greater than FDA, site-specific, identified as being site-specific. I know one of these items is design audit of reactor vessel manufacturer, which hasn't been selected. I have no idea of when that would happen. So, what timeframe that would fall in I'm really not sure.

I've got what I believe to be nine minor items that we haven't come to terms on yet. Right now, I'm looking at about 13 items as probable open items that would remain open upon issuance of the PDA, if the PDA is, in fact, issued, and that's a rough breakdown, but it gives you -- I think it gives you an idea of how far we have come on these.

MR. CARROLL: Now, that accounts for all 107 or whatever it is?

MR. DONATELL: Yes, Sir.

MR. CARROLL: Okay.

MR. MICHELSON: Now, this does not include the USIs and the GIs.

MR. DONATELL: No, Sir.

MR. MICHELSON: Okay. Which are quite a large number by themselves, and they're all, apparently, open for the moment, at least.

MR. DONATELL: Yes, Sir. That would be one major FDA item.

MR. MICHELSON: How many of those? A hundred or something?

MR. DONATELL: Well, they're -- I don't know the answer to that.

MR. MICHELSON: A large number, at least.

MR. DONATELL: Sure. There is going to be.

MR. MICHELSON: Yes, and those are the sticky ones.

MR. DONATELL: Absolutely.

MR. MICHELSON: Yes.

MR. DONATELL: Absolutely. There's no two ways about it.

MR. WARD: And it doesn't include the severe accident issues, whatever those are.

MR. DONATELL: This does not, no. The only thing -- there is one of these that is against the PRA. All right? And admittedly, by the rule, a full-blown, complete PRA is not expected at the PDA stage. That will remain open.

[Slide.]

MR. DONATELL: The schedules I have shown you in the past were, I guess, pretty neat and pretty rigorous. This is really not. It's pretty rough.

I believe I will have to come back to the Subcommittee one more time on DSER Chapter, hopefully in February. Some of the things we have to pick up are QA, waste management, radiation protection, any items that the Subcommittee wishes to revisit, pick up at that point in time, based on what we have seen over these last, really, three meetings. Okay?

My intent is to get the draft final SER on the street in March and to be able to come back to the Subcommittee in April with that draft final, full Committee in May, and wrap the thing up in June. It's a pretty rough effort. There's no

two ways about it.

I think I can get here by March. I don't know what's going to happen between here and here and what's going to change here, just based on review of said final -- draft final SER.

That's all I have, if there are any questions on that. If not, I appreciate your time.

MR. KERR: I don't have questions specifically on what you have said, but I think they bear on the review.

First, in the SER, I find frequent references to staff positions. Where could one find a listing of staff positions, since I assume one has regulations, reg guides, GSIs, USIs, SRPs, and staff positions? The others I know, but I don't know where to find staff positions.

MR. DONATELL: I think probably what you're referring to are the branch technical positions.

MR. KERR: No, those -- well, I see reference to branch technical positions, but I also see references to things -- it says, "It is the staff position that", and so, I assume there must somewhere be a listing of staff positions.

MR. DONATELL: I don't know the answer to that, if in fact there is a listing of staff positions.

MR. KERR: I mean does a staff position just sort of develop during a review process, when the staff decides that this is the way things should be?

MR. DONATELL: I think it's entirely likely that some of this may be historical positions.

MR. KERR: So, a staff position is presumably one of those things that would be reported to the Commission as going beyond --

MR. DONATELL: Yes, Sir, and that's one of the --

MR. KERR: -- the ex[illegible]ing rules.

MR. DONATELL: Yes, Sir. That's one of the quandaries that I have, again, with this draft final SER.

MR. SHEWMON: If a branch chief thinks that this is the way something should happen in his area of responsibility, does that make it a staff position which can change with the next branch chief?

MR. DONATELL: I can't answer that directly. What I can do is try to establish what that really is and try to get back to the Subcommittee with that. To say anything, on my part, would be probably personal perspective and conjecture.

MR. WARD: In some cases, I think that's just a statement of the way the staff is interpreting some more formal requirement.

MR. KERR: I assume these interpretations are not just ad hoc, however, so that there must be a list of them somewhere.

MR. DONATELL: It may be referenced to the standard review plan.

MR. WARD: They have to be ad hoc in some cases. That's what the review of the SER is all about.

MR. KERR: A staff position implies to me that the staff has consciously taken a position, through some process or other. It doesn't say it's the reviewer's position, unless each reviewer has the responsibility and the authority to take a position that is outside the regulations, and I don't -- well, I am just sort of puzzled by the phrase.

Second, I get the impression from reading the SER that reg guides, many of them, in this review are being treated as requirements. Is this a change in the staff position that reg guides are now requirements, rather than just being -- because I, for example, find language that -- "as required by reg guide" XXX.

MR. DONATELL: No, Sir. They are not requirements. The reg guides are, as I view it, points of reference in the standard review plan and guide the reviewer through his process. When he gets to a specific point in the submittal, the standard review plan should guide him through that review process, utilizing said reg guides that relate to those areas.

MR. KERR: But reg guides, I thought, were provided as guidance to licensees and that alternate approaches were, at least, possible, in principle. The language in the SER, frequently, would convince me that somebody on the staff is now treating them as requirements.

MR. DONATELL: I would have to look at that language, Sir. My view is that's inappropriate if it is indicated that way.

MR. KERR: Then, finally, from what you tell me -- this may not be an appropriate question for this review, but at least, there is some language in the SER that indicates that -- or gives lip service to the fact that a PRA is going to be required -- indeed, I guess, has been submitted -- and I would be interested in finding a copy of the criteria that are going to be used to review the required PRA and use it however it is used in the decisionmaking process. So, if such a document exists somewhere, I'd very much like to see a copy.

MR. DONATELL: I'll have to make a note on that and see what the situation is.

MR. KERR: Okay.

MR. DONATELL: PRAs are only reviewed in the Office of Research.

MR. KERR: I also note comments that say that probabilistic risk assessment can be used to eliminate requirements, and I am not sure what that means, particularly when the requirements may be reg guides, but I will have to fight that one through, I guess, by more careful examination of the SER.

It would seem to me if one is going to take a PRA seriously that when the results of a PRA show clearly that a

particular regulation doesn't make sense, it makes you give some thought to taking an exception to the regulation, but apparently, it is a staff position, as enunciated in this SER, that one cannot use reliability analysis, which I assume is what is being referred to, in an argument that says that this particular regulation doesn't make sense at this point.

MR. DONATELL: I really don't know how to respond to that.

MR. CARROLL: Other questions of Loren from members of the Subcommittee?

[No response.]

MR. CARROLL: I guess I had one point, Loren. ACRS did recently issue a letter to Taylor on the subject of the status of the ABWR review, and I think there are some items in that letter that have some relevance to this review. I think both you and Westinghouse ought to take a look at that letter and give us any comments you may have. Med can get you a copy of the letter if you haven't see it.

MR. DONATELL: At this stage, PDA stage?

MR. CARROLL: Well, ABWR is going for an FDA, but I think some of our comments are equally appropriate --

MR. DONATELL: All right, Sir.

MR. CARROLL: -- with regard to this project.

Okay. If there are no more questions, I guess we will hear from Westinghouse, and that's Ed Burns, is it?

MR. BURNS: Good morning. I'm Edward Burns, Manager of Plant Licensing at Westinghouse. It is really a novel, unique position I put myself in today, because back in 1983, when we started the SER process, I was intimately involved with writing up some of the sections, the first module on the SER, and then I moved on to operating plants for a number of years, and then just recently moved back into construction plant licensing. So now I get a chance to close out what I started a number of years ago.

[Slide.]

MR. CARROLL: And you have taken Mike Shannon's place on this project permanently?

MR. BURNS: Yes, I have.

MR. CARROLL: Where did Mike go?

MR. BURNS: Outer Siberia. He has moved to a position in licensing out at Hanford.

MR. CARROLL: Ah.

MR. BURNS: To try and get some SAR-type cognizance into that operation.

MR. CARROLL: Basically our purpose today is to continue our review that we have done through several fo the subcommittees; look at some of the additional chapters of the EDA of the SAR that we have issued, submitted; look at the auxiliary systems; get a little bit into the information systems, Chapter 7 and the control room, human factors and

that; and spend a little bit of time with Chapter 15. We'll go over plant, and some of the issues as we go through each of the individual presentations.

Several previous subcommittees have looked at the reactor itself, the system, and the emergency cooling systems, and Chapter 3, the structural systems. We don't feel it is appropriate at this stage that we will need to go into the operational or the startup type of chapters, as those are more appropriate for an FDA, or at the operations, or the site stage, when we have an applicant.

MR. KERR: What is meant by the bullet that says: "Severe accident issues and PRA were covered in September 1989 subcommittee meeting"? Does that mean that that is all we will hear about those issues?

MR. VAN DE VENNE: This is Theo van de Venne. We had a meeting in September where we took a full day to go through the severe accident issues, and I think there are like 12, or the count is always a little uncertain. It varies between 10 and 15 issues. And we made pretty extensive presentation on what the Westinghouse position was on each of those issues. And those included like station blackout, fire protection, ATWS, mid-loop operation, interfacing LOCA, debris coolability, and all those. So we covered all of those in a full-day meeting.

MR. KERR: Well, with the exception of debris

coolability, I would not consider any of those things you mentioned as severe accident issues.

MR. VAN DE VENNE: Well, we had some discussion with the staff. They were called severe accident issues. But we decided it was really a misnomer, and it would be more appropriate to call them something like policy issues. It is those top issues that I think the Commissioners are, as far as I understand, are very interested in.

MR. KERR: No, what I thought we were discussing was things that would go beyond existing design bases, and indeed, beyond most existing regulations.

MR. VAN DE VENNE: Well, for instance, mid-loop really goes beyond existing design basis. It's really never been covered. So I guess that's why it got on the list. It is issues that really in the past have not dominated the licensing process and that are very prominent now. And the name, severe accident issues, was probably a little inappropriate. But anyway, that is what they were called.

It also included hydrogen, it included containment venting, it included alternate water supply in containment. There was a whole bunch of more truly severe accident issues.

But anyway, we discussed those in a meeting in September. It took a full day.

MR. DONATELL: Excuse me. These are also the issues that will be in front of the Commission for some policy

decisions in the near future.

MR. MICHELSON: In view of what you've just said, I'm trying to sort out here, the severe accident issues are possibly in limbo for the PDA. Are these other issues which you may or may not wish to call severe accident, but which some people do call severe accident, such as large fires and so forth, these so-called external events, are they in limbo, or do you think that they are being resolved at the PDA stage, or what?

MR. VAN DE VENNE: They happen to be, in some cases, an open item. They happen to be on the 107 open list. The mid-loop is, fire protection is, station blackout is, ATWS is.

MR. MICHELSON: Okay. So it will also be held in abeyance?

MR. VAN DE VENNE: I don't know. It's really up to the staff. Our position on these is, I think, pretty clear and pretty explicit. But whether the staff is going to rule on it is another matter.

[Slide.]

MR. BURNS: I will very briefly look at the schedule that we are on. We feel that another subcommittee, if it is necessary, will work with the NRC on getting out the next batch of open items resolved, and then present it before a subcommittee, if it is needed in the next few weeks into February. But in conjunction with the draft SER, we need to

have that out, and we are looking for the ACRS subcommittee in the March and I think Loren mentioned the April time frame. We wish to support that and continue moving toward that final or full committee meeting in the April or May time frame.

Our goals that we have expressed to the NRC, and that we wish to continue working with them, is to resolve everything so that a PDA is issued by June.k

MR. KERR: Would you excuse me again? I apologize for my lack of information, but there is a reference to a review by the Advanced Plant Subcommittee of a draft SER on probabilistic safety studies. Was this a review of Westinghouse's probabilistic safety study or advanced plants generally?

MR. VAN DE VENNE: Theo van de Venne again. No, this was a review of the Westinghouse PRA or PSS, whatever it is called, in the module 16, and also review of the Brookhaven comments on that PRA.

MR. KERR: Okay. Thank you.

MR. MICHELSON: Is that to suggest then that it will not be revisited before the committee finishes its review? Because it was visited a long time ago when we knew less about what was going on than we are beginning to learn now.

MR. CARROLL: Well, I think we have to sort out what the full committee would like to hear. One option would be to make that a major item of the full committee agenda in April or

whenever.

MR. MICHELSON: Because it was some time back we looked at it, and at that time we were not as knowledgeable of what was really being proposed, since we hadn't done as much looking. That was one of the first meetings we really had where we began to get down to nuts and bolts.

MR. CARROLL: That is correct.

[Slide.]

MR. BURNS: This is just basically a reiteration of the previous slides. In the PRA and the USIs areas, we are still having an open discussion with the NRC. We have not received anything back on those. And to be fair to them, we did submit that update last Fall on the USIs/GSIs, so we couldn't place a burden on them at this stage that we cannot reasonably expect them to turn around a complete staff review.

[Slide.]

MR. BURNS: I will place a list, or a numerical summary of what we feel at this stage to be the status of the 107 open issues.

The numbers that I give here are slightly different than that that Mr. Loren Donatell presented.

Approximately half have received what we would define as a staff approval, where we have come to some type of resolution that we feel that no additional effort will be needed to resolve any technical differences between now and the

issuance of the PDA.

We list 33 as requiring additional effort. We've been working, having various telecons and discussions with the staff in recent days and weeks. And this number of 33 just recently is probably down in the low 20s. So we are trying to resolve these numbers, and we are down to approximately 20 to 22 that we feel that we will need to get continued technical discussions on in the next few weeks.

MR. MICHELSON: Could you tell us which ones are deferred to the FDA? There's only six of them, apparently, by your estimate.

MR. DONATELL: Excuse me, sir. I have got, by my count right now, about 18 of those items. I do have them by number.

MR. MICHELSON: Well, let me ask a couple of them. How about A-17? Is that one of the deferred items?

MR. DONATELL: Number 17?

MR. MICHELSON: A-17. That is system interaction.

MR. VAN DE VENNE: That is not included.

MR. MICHELSON: That is among that whole excluded group, USIs and GIs.

MR. DONATELL: All the open items with the exception of the PDA are really SRP review items.

MR. MICHELSON: Okay. That takes care of it. Thank you.

MR. KERR: Apropos of the resolution process, in the SER on Page 3-3, for example, there is a statement that the applicant uses ASN safety glasses 1, 2, 3 and non-nuclear safety as defined in the American Standards, ANSI-ANS 51.1-1983, and so on. And it appears that the staff has not accepted this. And the statement is made by whoever wrote the SER: the applicant has clearly stated in its response to these two staff questions that Westinghouse maintains its position of referencing ANSI-ANS 51.1-1983.

How do I interpret this paragraph? That Westinghouse is going to maintain that position no matter what the staff does? Or there is just going to be a difference of opinion? This is not the only place in which statements like this occur. I just use that as an example.

MR. VAN DE VENNE: I guess the difference of opinion was really on the 18.2 versus the 51.1, and the staff initially would like to continue to use 18.2 but unfortunately 18.2 is really not the current standard any more so we can't really use it. And I think what we've compromised on is that we will use the NRC classifications A, B, C, D where we can agree, we can agree on those, and then hopefully by the time the staff has reviewed 51.1, you know, we will feed that in. But really, 51.1, these safety classifications are somewhat redundant to the quality groups, they are called.

MR. KERR: I'm not asking so much for the detail on

this one. It seems to me there is an impasse here.

MR. VAN DE VENNE: No. I think we have resolved that one.

MR. KERR: Well, it says "until this issue is resolved." This is dated March of 1989. So it may be completely out of date.

MR. VAN DE VENNE: We've had discussion since that time.

MR. KERR: Okay.

MR. VAN DE VENNE: And we've agreed on using the quality groups and I think we have consistency there.

MR. DONATELL: I think if you read further you will note that this, the March '89 draft SER says this remains as an open item, which would make it part of the areas we are addressing and have been addressing since approximately mid-year.

MR. KERR: Okay. So some fraction of these statements are now, some fraction is now out of date.

MR. DONATELL: Yes, sir. That is correct.

MR. KERR: Okay. Thank you.

[Slide.]

MR. BURNS: I put up a little agenda for today, to move along into the presentations and discuss some of these open items.

This slide is a couple days old. And we have

recently, just yesterday changed it. And so this morning we will be going through the instrumentation and the information systems, the advanced control room and the human factors, to be followed after lunch by the auxiliary systems, steam and power conversion. Chapters 11 and 12 we have asked and we have agreed we will put off until a future time. So after that, we will move into Chapter 15, which will then agree with the previous agenda that Mr. Donatell placed in front of you.

MR. KERR: Let me to Chapter 11 of the SER. There is a discussion of tornado-based missiles. The last sentence of the paragraph says "However, Westinghouse has not identified where differences exist." Presumably this is differences between Reg. Guide 1.17 and the approach that Westinghouse has taken which involves using ANSI/ANS standards.

Westinghouse has not identified where differences exist and has not provided an evaluation to describe how the alternative proposal provides an acceptable method of complying with the NRC's rules and regulations.

What does the Staff mean by that statement? It would seem to me that if Westinghouse proposes an alternative, it would be up to the Staff to determine whether it was an appropriate method. It appears that the Staff is asking Westinghouse to say whether it is an appropriate method of complying.

MR. DONATELL: Excuse me, sir. I am still reading

this.

MR. KERR: Okay.

MR. DONATELL: I think in general what we are facing here, and Westinghouse can jump in if I'm wrong here, is an issue similar to some of the code issues where the Staff has a position based on an approved, accepted code or standard.

Westinghouse has come in with something different than that.

MR. KERR: But presumably though what the Staff is relying upon is the Reg. Guide 1.76. That's neither a code nor a standard.

MR. DONATELL: And as I was going on, the traditional approach is to require the Applicant to show where he varies from the existing guidance that the Staff has to make a determination whether the vendor's approach meets or exceeds the Staff requirement.

MR. KERR: Well, this says he is not provided an evaluation to describe how it provides an acceptable method.

It seems to me an acceptable method is something that only the Staff can determine and I don't see how the Applicant can determine that, but maybe I'm misunderstanding the sentence.

MR. DONATELL: I think it may be poorly worded.

I think what we are saying here is we're looking for information from Westinghouse to be able to determine whether

their approach is acceptable to the Staff.

MR. KERR: Okay. Well, to me the sentence doesn't say that.

MR. CARROLL: If you want to do something different from what's stated in a Reg. Guide you have to defend the alternative you're proposing to use.

MR. KERR: Yes, but you don't determine whether it is acceptable or not. At least I don't see how you can.

MR. CARROLL: No, I guess the acceptance has to be done on the part of the Staff. I agree with you.

MR. DONATELL: I agree, it's just poorly worded.

MR. KERR: Excuse me, please continue.

MR. BURNS: I would like to introduce Mr. Theo van de Venne to give us a little briefing on the plant arrangement, the overall design so that we can get this moving into the individual systems discussions.

MR. CARROLL: Are we somehow or other in this agenda today going to talk a little bit about some of the metallurgical issues that we gave you at the last meeting from Paul?

MR. VAN DE VENNE: On that particular question we had some written questions and I have provided some very brief answers in written form but I don't really have any overheads so we don't really have a materials specialist but, you know, we could take additional questions or I could briefly go

through the answers at any point in time.

MR. SHEWMON: It would be useful to briefly go through the answers because I think the answers are often tangential to the question.

MR. VAN DE VENNE: Well, the question maybe was not always clear.

MR. SHEWMON: The questions were more detailed than the answers is where my problem is.

MR. CARROLL: Would it be useful for the rest of us to have the questions and answers before we do that?

MR. SHEWMON: I don't think so. We have the questions. We could give them fresh sets --

MR. VAN DE VENNE: I can go maybe briefly through them right now.

Can you give me that little sheet there? I need my glasses.

MR. SHEWMON: The first question was are there any welds in the core region and the answer is they will have no welds in the core region.

MR. VAN DE VENNE: Right.

MR. SHEWMON: Is this made of ring forgings?

MR. VAN DE VENNE: It's made of ring forgings, yes.

MR. SHEWMON: So there is one circumferential weld and that is just above the middle of the --

MR. VAN DE VENNE: No, if you look at the picture I

have given you, the core is between the middle weld on the cylindrical section and the lower weld in the cylindrical section, so there is -- the active core is not -- there is no weld in the region of the active core.

MR. SHEWMON: Okay, and that forging is 162 inches high, which is 14 feet, sort of?

MR. VAN DE VENNE: Right.

MR. SHEWMON: And the reason you haven't got a vendor certified for that yet, if I understood the Staff earlier, is that nobody has ever made one of those in the United States and you aren't sure where you'll get it made?

MR. VAN DE VENNE: No, we are sure where we'll get it made because we have talked to the manufacturer and it can be made. It can be made by Japan Steel with forging.

Our partner, Mitsubishi, would manufacture the reactor vessel from forgings made by Japan Steel, so that has been checked.

MR. SHEWMON: As something which wasn't on the list, is this diameter, is there more water between the core and the vessel in this than there have been in your other?

How fast do you accumulate fluids in this compared with, say, Wolf Creek or something?

MR. VAN DE VENNE: The fluids on this design for a 40-year life is 1.4 times ten to the 19th neutrons per square centimeter.

MR. SHEWMON: So that is really no change from the previous one?

MR. VAN DE VENNE: No, it's about a factor of two lower than the current design.

The current design -- well, it depends really what we call a current design.

Our latest, like at Wolf Creek, would be around between two and a half and three for a 40-year life. Some of our older designs of course are way up there, like eight or nine or maybe even ten, so it is a significant reduction.

MR. MICHELSON: Could I ask a question on that point?

The 40-year life of course is something you can proscribe but I thought for certification when you go to FDA and certification it would be a 60-year life you design for.

MR. VAN DE VENNE: Well, yes. For 60 years --

MR. MICHELSON: Or alternatively design for annealing?

MR. VAN DE VENNE: Yes. For a 60-year life it would simply be one and a half times, of course. It would be about two. We have had some internal discussions in Westinghouse --

MR. MICHELSON: Which would be back up where we are now, roughly?

MR. VAN DE VENNE: No, two would still be far lower than any plant today.

MR. MICHELSON: Plus you've got no welds, see, in

this going through.

MR. VAN DE VENNE: And you've got no welds.

MR. MICHELSON: Do you have any idea what the Reg. Guide 199, Rev. 2 predicted shift is for that fluence?

MR. VAN DE VENNE: No, I don't know.

MR. SHEWMON: It's not at all to me that they are going to be able to avoid welding the way GE can, who comes in and says the predicted rise is 5 degrees Fahrenheit or some darn trivial number.

MR. MICHELSON: They have big gap, of course --

MR. SHEWMON: Yes, they have consciously gone to a larger gap and Westinghouse hasn't.

There's another question on the vessel material. Since its forged section that leads down into a more modern steel composition in the plate your response is that it meets the EPRI/ALWR requirements document.

Do you have any idea what that document says about the composition of the steel?

I could look it up if it's explicit.

MR. VAN DE VENNE: It's Chapter 4 of the requirements document.

I know it allows the two materials, the two possible materials for a reactor vessel and I don't really know the SA categories but they are in according with the ASME.

Then as far as impurities it allows .012 percent

phosphor and .05 copper for the base material and it allows .012 percent phosphor, .05 --

MR. SHEWMON: Is one of those sulfur or are you going to stay with phosphorus?

MR. VAN DE VENNE: That's the way it's written in that and for the weld material it's .012 phosphor, .05 vanadium and .08 percent copper. That's the way it's written.

MR. SHEWMON: That maybe is the way GE got their numbers. What they also did was to allow a 533 plate, which gives you allowable .04 sulfur, which is a very old-fashioned steel, anisotropic, low toughness. It's a miserable steel that nobody would sell you these days and so I hope that we -- let's go look at it and see.

Actually if you're in forged plates then you're down into at least a somewhat more modern composition with regard to sulfur.

There was a question here about standards for pipe joint design. Maybe you can interpret your drawing to me later and let's skip that one.

Specifications for cast stainless steel, what I am particularly interested in is the delta ferrite content, since that is what gives the aging and the loss of toughness that we are worried about.

Some of the specs will allow you to go up to 25 percent delta ferrite, which is still a lot, and that is what I

am looking for, whether you've -- do you have any idea?

MR. VAN DE VENNE: I can't answer that question. I guess the answer that we had was that in the primary loop we do not use cast piping or cast elbows. They are all forged.

The only casting that we use in the primary system is the reactor coolant pump casing, which is a single piece casting but I cannot, you know, answer to your specific question.

MR. SHEWMON: You have got here there are no welds.

MR. VAN DE VENNE: In the casting.

MR. SHEWMON: Interestingly enough, at least a generation ago the quality of the weld that -- the quality of the casting that you used there was proportional to the amount of rework and the amount of welds that somebody put in to take care of the porosity that the foundry gave you without charging you extra for it.

So then there is the question of whether they can make them any better now than they could 20 years ago but that's perhaps a separate question.

MR. VAN DE VENNE: Our latest experience is the Sizewell pumps which are being made right now, and I think people are generally pretty happy.

MR. SHEWMON: Do you have any idea how much repair work was necessary on them to get past radiography?

MR. VAN DE VENNE: No, I don't.

MR. SHEWMON: Okay. It might be interesting to learn more about that some time.

Let's go down then to -- the composition of the steel we've gone over. The steam generator materials you specified as a 690 with TT, which must be the heat treatment.

MR. VAN DE VENNE: Thermally Treated, yes.

MR. SHEWMON: And 405 stainless for the support plates.

MR. VAN DE VENNE: That's the same as our latest replacement units at, say, Indian Point and Salem.

MR. SHEWMON: I guess the only remaining item then would be the composition of the cast stainless steel which just isn't spoken to at all here.

MR. VAN DE VENNE: I will try to get that for you for the next meeting.

MR. SHEWMON: Okay, fine. Thank you.

MR. CARROLL: Or maybe over the lunch hour, huh?

MR. VAN DE VENNE: What's that?

MR. CARROLL: Or maybe over lunch hour?

MR. VAN DE VENNE: Well, I would have to make a call.

MR. SHEWMON: We have telephones here.

Let me make one other question. You have said you are going to use forged piping. Westinghouse in their older plants or most of the others had a centrifugally-cast stainless. This will now be a forged ferritic which will then

be stainless-clad?

MR. VAN DE VENNE: No, it's forged stainless.

MR. SHEWMON: The grain size in that is then small enough so that the inspection problems are not there, as there are in the -- although you haven't had as much trouble with your casts as you have with the elbows and things?

MR. VAN DE VENNE: Right, because the piping was always centrifugally cast, which I think is a better process than what they call the sand casting for the elbows.

I think most of the problems are in the elbows, really.

MR. SHEWMON: So you're still not going like the convoy plants are, which as I understand it is a forged ferritic where they have made a particular effort to get rid of welded joints in there.

You are familiar with the convoy?

MR. VAN DE VENNE: They use carbon steel with a stainless steel clad and we have over the years done a number of evaluations as to the pro's and con's and are really not all that familiar.

I think that the main incentive was that there was a general feeling that the carbon steel clad would be lower in cost and would be easier to weld to the reactor vessel but I think on balance we prefer the forged, all-stainless pipe and exactly the reasons for that I don't really know.

MR. SHEWMON: I'm sure that has merit. I guess the other question though comes into the actual number of welds, because one of the things that they have done is to try to decrease the number of welds in their primary system by getting more things forged into fewer pieces.

MR. VAN DE VENNE: They use, you know, carbon steel with a stainless steel clad, and we have over the years done a number of evaluations as to the pros and cons, you know. I'm really not all that familiar. The main incentive, I think, was that there was a general feeling that the carbon steel clad would be lower in cost and it would be easier to weld to the reactor vessel.

But I think, you know, on balance, we prefer the forged hull stainless type, and exactly the reasons for that, I don't really know.

Okay, that does it for now.

MR. WARD: Why have you left the centrifugally cast plate approach?

MR. VAN DE VENNE: No, what I'm saying is that we will go to forged pipe.

MR. WARD: Why?

MR. VAN DE VENNE: Oh, the forged pipe is even better than strictly cast from an in-service inspection point of view. It's yet another improvement. If you look at it, the worst is the sand type casting. The next best is the centrifugally cast

and then the next best is forged, all forged, from an in-service inspection point of view.

MR. SHEWMON: I think one of the reasons is that there is better homogeneity and better --

MR. VAN DE VENNE: Right.

MR. SHEWMON: -- and better for the most part, and it's also more easily inspected ultrasonically, but the homogeneity, I think, is a lot of the --

MR. WARD: It's not the same thing?

MR. SHEWMON: No. Homogeneity means that you've worked all of it, and if there are any defects there, they've shown up as cracks or something. You have, in a sense, done an original inspection.

It also refines the grain size and the inspectability usually ends up with these large grains, columnar grains that you have in the casting.

MR. VAN DE VENNE: The part of the presentation that we're talking about now is the layout, and it's really in response to a comment from Dr. Michelson the last time; that he hadn't really seen the layout, and that knowing the layout would help in getting some of the system issues better understood.

[Slide.]

MR. VAN DE VENNE: So, we're going back now to what is in Chapter 1, which is the general arrangement. The nuclear

-- what we call the nuclear power block is an integral base mat design; that is, the containment and the auxillary buildings are located on a single concrete base mat and are interconnected.

The auxillary building has all safety-related systems and equipment located in it, except the service water intake or the cooling tower, you know, as appropriate for the particular site. So, outside of this building, there is no safety-related equipment. All the tanks, storage tanks for safety-grade water are located in this building.

The containment is a spherical containment and a steel containment with a concrete shield building around it. The section you see here is the -- has the spent fuel pit and the transfer canal on one side, and it has the main steam lines over on this side. As you can see on the plan views, most of the electrical equipment is over on this side, and the mechanical equipment is over on the other side.

MR. MICHELSON: In terms of leak-before-break philosophy, where will you have the boundary on the main steam lines and the feedwater?

MR. VAN DE VENNE: Right here.

MR. MICHELSON: Okay, thank you.

MR. KERR: What is below the sphere?

MR. VAN DE VENNE: Below the sphere -- and I can show you better on a plan -- are a number of pumps, most of which

are safety-related. There are the EECS pumps, the RHR spray pumps, the emergency feedwater pumps.

MR. KERR: Are you talking about directly below? I'm thinking of what happens if one gets a melt-through the sphere.

MR. VAN DE VENNE: Here?

MR. KERR: Yes.

MR. VAN DE VENNE: This would be ground. The grade is here, so this is below ground.

MR. KERR: How much concrete between the sphere and ground?

MR. VAN DE VENNE: I think there's a minimum of three feet here and there is seven feet there, so ten feet of concrete with steel in between.

MR. KERR: Thank you.

MR. VAN DE VENNE: I'll walk through the arrangement from the bottom up.

MR. MICHELSON: Let me ask; on the bottom layout, the main feedwater and the steam; in the unlikely event you did have a larger rupture than you might speculate from pure leak-before-break theory, what provisions have you made for such larger breaks in terms of venting and whatever?

MR. VAN DE VENNE: There are very large blowout panels.

MR. MICHELSON: Will they take the circumferential rupture of the largest feedwater steam line, or something less?

MR. VAN DE VENNE: We did an analysis of that particular case, and I think that in the worst case, the pressures in the compartment are in the 20 PSI, 20-25 -- 22, I think, range, and that would cause probably deformation, but not gross failure because these walls tend to be -- those are the typical pressures you would see.

MR. MICHELSON: I'm particularly interested not necessarily in just the walls, but in penetrations through those walls that might be designed for much less and may be able to withstand much less pressure than that; you know, like any penetration that might be electrical and have a fire boundary on it, things of that sort.

Will those withstand those kinds of pressures?

MR. VAN DE VENNE: I can't answer that question at this time.

MR. MICHELSON: In other words, what is the design basis for that compartment in terms of the maximum break that you could take?

MR. VAN DE VENNE: I think --

MR. MICHELSON: And without blowing out any of the pressure boundaries -- any of the confinement boundaries?

BY MR. KRAMER:

MR. VAN DE VENNE: I think the design basis is -- and how it would have to be handled is, the design basis, I believe, is a one square foot break, which is typically what

one assumes in these, and one would have to do then a best estimate type evaluation.

MR. MICHELSON: The resulting pressures from that one square foot break would --

MR. VAN DE VENNE: No, they're on the order of 5 or --

MR. MICHELSON: Well, let me ask the question: they would not jeopardize the electrical or the ventilation or whatever?

MR. VAN DE VENNE: Those would not be jeopardized. Everything would be designed for that pressure.

MR. MICHELSON: So you design your ventilation and so forth for isolating 5 --

MR. VAN DE VENNE: Well, the ventilation is dedicated to this compartment, so it's not --

MR. MICHELSON: That, we'll get into later, yes. If it's dedicated and its rupture is in a non-obtrusive area and so forth, that's fine.

MR. VAN DE VENNE: Yes.

MR. MICHELSON: That is the philosophy then?

MR. VAN DE VENNE: That's the philosophy.

MR. MICHELSON: Where you can't take -- where you do have to have penetrations into other areas, then you're designing for this one square foot break?

MR. VAN DE VENNE: Yes.

MR. MICHELSON: Thank you. I guess that's the feedwater line that gives you the most trouble?

MR. VAN DE VENNE: No, the steam line.

MR. MICHELSON: The steam line gives you more trouble?

MR. VAN DE VENNE: Yes.

MR. MICHELSON: Even the -- that's a large feedwater line; isn't it?

MR. VAN DE VENNE: It's an 18-inch feedwater line, but it's a 32-inch steam line.

MR. MICHELSON: Now, in the unlikely event that you should experience a one square foot break, are you assuming that that break continues to have steam or water delivered to it indefinitely?

MR. VAN DE VENNE: Yes.

MR. MICHELSON: You're not taking any credit for isolations?

MR. VAN DE VENNE: No.

MR. MICHELSON: Thank you.

[Slide.]

MR. VAN DE VENNE: The lowest level in the plant is primarily dedicated to safety-related pumps. As you know, we have four subsystems in the integrated safeguard system which are -- there is one compartment dedicated to each of those, so the two Division A subsystems are here, and the two Division B

subsystems are over here, with each having a high head pump and a low head pump.

In addition, we have the emergency feedwater pumps over here and the charging pumps are located over there. The charging pumps are not safety-related, but the other pumps are. There are no connections between any of these compartments at this level, so they are all isolated from each other such that if there was flooding in one compartment, it would not affect the other ones.

There are also no penetrations between these compartments.

MR. MICHELSON: By those statements, then you mean that there is no common ventilation system that serves both compartments?

MR. VAN DE VENNE: They are all at a higher level. They are not subject to flooding.

MR. MICHELSON: No, you've got rooms with pumps. You have either heat that has to be -- either you seal the rooms up and remove all the heat internally or you circulate air through. I read the ventilation portion of the SER and it seemed to indicate that you have both types: you have circulating through and you also have closed cycle. It wasn't clear to me then; if you do have common ventilation systems circulating through, how it ties in with all the other common ventilation systems and whether, indeed, you've tied all the

rooms together.

You didn't say there was a dedicated non-safety ventilation system for each of these compartments, for instance.

MR. VAN DE VENNE: No, no. I'm say there are no interconnections at these lower levels. All the interconnections are at a higher level.

MR. MICHELSON: Well, that doesn't mean a whole lot if the steam goes up through the duct and comes back down again. Steam under pressure will move through ducts very nicely and it will move against gravity very nicely.

MR. VAN DE VENNE: Maybe we can look at this ventilation system later today.

MR. MICHELSON: Okay, but it is an important point that I would like to get clarified as to whether or not you have a non-essential ventilation system for normal operation --

MR. VAN DE VENNE: We do.

MR. MICHELSON: -- and I gathered you did, and how is it all tied together and does it, in essence, tie all these rooms together anyway?

MR. VAN DE VENNE: The emergency feed has its own dedicated ventilation system which is safety grade and is used both during normal and accident operations.

MR. MICHELSON: Now, does that mean it has no other ventilation system except --

MR. VAN DE VENNE: No.

MR. MICHELSON: It's a closed cycle within the room?

MR. VAN DE VENNE: No, it's supply and exhaust air.

MR. MICHELSON: But it is dedicated and no other ducts connect to it?

MR. VAN DE VENNE: Right, correct, and there is one for Train A and there is one for Train B. Each is separate.

MR. MICHELSON: That's on the emergency feedwater?

MR. VAN DE VENNE: That's on the emergency feedwater.

MR. MICHELSON: Now, how about on the safety injection?

MR. VAN DE VENNE: Now, the safety injection has a common ventilation system for normal operation and it has a charcoal exhaust system for post-accident operation.

MR. MICHELSON: Common means the -- it serves both Train A and Train B?

MR. VAN DE VENNE: Correct, yes.

MR. MICHELSON: So it becomes very important how you assure that there's no real inter -- systems interaction possibilities through the common ventilation system?

MR. VAN DE VENNE: Yes.

MR. MICHELSON: I don't find that anywhere. I don't find where the Staff really explored it. I think it's something that really does need to be explored.

MR. VAN DE VENNE: Okay.

[Slide.]

MR. VAN DE VENNE: At the next level, we basically have the radioactive equipment mostly in this part of the building. We have the clean equipment mostly on what I call the South part, and then the divisions between Train A and Train B are along this line.

MR. MICHELSON: In terms of the design basis for compartments, both at the lower level and at this level where you have high energy systems, or low energy -- it makes no difference -- what is the design basis for the compartments so that you are sure that an incident in one compartment does not spread to another?

MR. VAN DE VENNE: In terms of breaks, we really only assume the traditional leakage of 50 gpm.

MR. MICHELSON: Even in the non-safety areas, you're not designing for bigger than 50 gpm?

MR. VAN DE VENNE: Well, wherever there's high energy line piping, we would design for whatever that high energy line piping is. But in most cases, there is very little high energy piping because the CVCS is one area, of course, that has continuously potentially high energy piping. The CVCS has been redesigned to have the let-down heat exchange of inside containment so that the water in the auxiliary building is always cold, so that you cannot really get any energy from that.

Then the other main source of high energy piping is emergency feed, the steam admission line for the turbine-driven pumps, and that is designed for a full rupture.

MR. MICHELSON: Now, in terms of full rupture, are you taking account of or credit for isolation in that break?

MR. VAN DE VENNE: No, because it could happen upstream with the isolation valve.

MR. MICHELSON: Now, this is for the auxiliary feedwater system?

MR. VAN DE VENNE: Yes.

MR. MICHELSON: And so you're designing for continuous release for how large a break?

MR. VAN DE VENNE: That's a four-inch line, I believe.

MR. MICHELSON: Are you taking full circumferential?

MR. VAN DE VENNE: Yes.

MR. MICHELSON: And you'll design the compartments to vent properly so that they don't exceed whatever the pressure rating --

MR. VAN DE VENNE: Right.

MR. MICHELSON: -- of the concrete is and the penetrations, or whatever that might be important?

MR. VAN DE VENNE: Right.

MR. MICHELSON: Is that written down somewhere? I guess there are just too many words to look at. But that is

defined somewhere in the SAR?

MR. VAN DE VENNE: I don't really know.

MR. DONATELL: If we look at the open items for the FDA stage, there are significant open items, design scopes, pipe leakage criteria.

MR. MICHELSON: Okay.

MR. DONATELL: The stage of the design that has been submitted is not mature enough to support --

MR. MICHELSON: Okay. The staff found that there weren't enough numbers to identify this philosophy. The philosophy sounds fine; I'm just wondering if it had been documented, and apparently it's an open item.

MR. DONATELL: That's correct.

MR. MICHELSON: Now, in these compartments at this level and at other levels where you're using a common building ventilation system, in the case of an unlikely but possible fire in one of these compartments, what is your criteria for preventing smoke and heat from aggressing through the common ventilation system? There are fire dampers, I'm sure, or I assume.

MR. VAN DE VENNE: Yes. There are fire dampers, yes.

MR. MICHELSON: Now, how tight a fire dampers are you proscribing, and would that be too much prescription for a PDA? If it is, then it certainly ought to be an open item for an FDA, but if fire protection in general is an open item, I

guess, then, that this is open also. Is that the way to look at it?

MR. DONATELL: Fire protection will be addressed during the auxiliary systems portion of that. There are presently, I believe, seven open items against their submittal on fire protection. I haven't gotten input from the reviewer as to the acceptability of those responses. Hopefully, when we get into Chapter 9, we'll be able to address that.

MR. MICHELSON: But if we're going to use common ventilation systems, you don't want the smoke going from one room and the heat through -- the fire damper is designed to keep fire potential from propagating, not to keep heat and smoke from propagating at lower levels, but levels quite sufficient to actuate fire protection in other compartments, and somehow you're going to have to seal these things up enough to assure this.

Now, you're aware, of course, that things have been done at Sizewell B. I think you have significant input to it. If you read their fire protection plan for Sizewell B, you'll find some very interesting provisions.

They have recognized the problem of heat and smoke migration, they've also recognized the problem of pressure build-up just due to fire, and they have provided chimneys in their plan, in fact with relief panels, to keep the pressure build-ups from rupturing the electrical penetrations and so

forth in the rooms. I don't find any of this sort of thing in here.

I believe, before we get done at a PDA level, Westinghouse certainly ought to have given us some answers as to why what Sizewell B seems to think they need, we don't need in this country, or show that you're doing something that's comparable to take care of the problem.

MR. VAN DE VENNE: I can't address that we have everything that Sizewell has. If we had, we would --

MR. MICHELSON: It'll come up later. I don't expect you to answer that. But I'm just saying, it's an area of interest that I think puzzles me because I don't see chimneys on this plant --

MR. VAN DE VENNE: Well, there are some chimneys in this plant.

MR. MICHELSON: There are? For fire protection purposes?

MR. VAN DE VENNE: Well, the chimneys I'm really referring to are for the emergency feed, and --

MR. MICHELSON: I assume it's for the steam.

MR. VAN DE VENNE: Primarily for the steam from the emergency feed.

MR. MICHELSON: But these are fire chimneys.

MR. VAN DE VENNE: Yes.

MR. MICHELSON: These are to relieve the pressure

build-due to fire because they have made their compartments quite tight in order to assure that heat and smoke don't get out and actuate and effect other areas, and you haven't, apparently, hermetically sealed the compartments, as near as I could tell, and therefore you must answer these other things that at least the Sizewell people seem to be quite concerned about. I will look for it later when we talk about fire protection and when I see what the staff has done, but as just a forewarning, please read the report and make sure that --

MR. VAN DE VENNE: First of all, most of the Sizewell stuff came after this plant was designed -- that doesn't mean we shouldn't address it -- and there are probably some legitimate concerns.

MR. MICHELSON: Well, fire protection is one area where the staff for the agency, as a policy, has indicated they expect to see improvements.

MR. VAN DE VENNE: Yes, and I think we have made some improvements in this area.

[Slide.]

MR. VAN DE VENNE: This next drawing really is only to show the emergency water storage tank which contains the refueling water, which is located in-site containment like in an annular tank, which also, by its nature, serves as an alternate water supply in containment to assure flooding of the lower compartments.

MR. MICHELSON: Is there any need for missile protection inside a containment? Have you postulated any missiles?

MR. VAN DE VENNE: There are the typical missiles of valves and valve bodies.

MR. MICHELSON: They have not been traditionally typical missiles, of course. I don't think we postulated the valve works as a missile, although we certainly have thought about it. It's not one of the real missiles we've been designing for, or you would have to put a lot of scraps on the valves to keep the works in place.

MR. VAN DE VENNE: Well, I'd say in most cases, you can sustain a missile in containment with the kind of separation that exists.

MR. MICHELSON: So you are designing, then, for valve body works --

MR. VAN DE VENNE: Well, there is an open item related to valve bodies. There was a question.

MR. DONATELL: That's what I recall. I was just looking for it.

MR. MICHELSON: I don't think that would be normally considered a missile, but the works would, the internals.

MR. VAN DE VENNE: Well, there is a reactor coolant pump fly wheel, and --

MR. MICHELSON: That would be a missile.

MR. VAN DE VENNE: And that is being -- I think it's being analyzed to show that it's highly unlikely.

MR. MICHELSON: But valve bodies I don't believe have been postulated as missiles.

MR. VAN DE VENNE: I'm not really sure.

MR. CARROLL: Control rod drives.

MR. VAN DE VENNE: Control rod drive is a missile.

MR. MICHELSON: Yes, that's a missile. But the cover plate of a check valve could be a potential missile; the internals of a valve as retained by a bonnet could be a potential missile if the bonnet bolts failed. I wondered, are those on your list?

MR. VAN DE VENNE: I don't know. There was a question from the staff on that point.

MR. MICHELSON: Is missile protection something that will come up later?

MR. VAN DE VENNE: It was in Chapter 3.

MR. MICHELSON: We already passed it.

MR. VAN DE VENNE: Yes.

MR. MICHELSON: Okay.

MR. DONATELL: I believe we discussed it pretty much depth the last time, but I was still looking for an open item that covered it. Some of this may be out at the FDA stage.

MR. SCHIVELY: Excuse me. I think Open Issue 7 and 8 had to do with internally generated missiles, and I believe

what the open issue was, was that we had responded to questions relative to Chapter 3, Section 3-8, or whatever, and that the review was still going on.

I think that we since have received the okay, that our response to those staff questions were okay. But the open issues were -- there were two of them, I believe 7 and 8.

MR. DONATELL: I see them. Seven and 8, Internally Generated Missiles, Inside and Outside Containment, and I show them as being acceptable at this point in time.

MR. SCHIVELY: I believe that we addressed the issue of valve bodies and so forth and so on in our response to those staff questions.

MR. MICHELSON: Did you address them by indicating that you thought it was incredible, or by indicating you thought the consequence was acceptable?

MR. SCHIVELY: At this point, I'm not a structural person.

MR. MICHELSON: Okay.

MR. SCHIVELY: All I can do is go back and look or refer you to our responses.

MR. MICHELSON: No, I'll go back and look at it. Thank you.

[Slide.]

MR. VAN DE VENNE: The next elevation is the lower floor in the containment, which shows you the typical four-loop

arrangement. The component cooling heat exchangers are located here in the chilled water. It's located here. The piping is brought in through an underground tunnel, one tunnel for each train, and any flooding of the -- any break in here would drain back through the tunnel.

MR. MICHELSON: Is that again a one-square-foot break that you say will be drained back, or are you designing for bigger breaks on that system? That's a very large piping system, generally.

MR. VAN DE VENNE: It's a service water system. It pumps about 7,000 gpm, or something like that. In those type of systems, since it's unpressurized, we normally really only partial it, like a 50 gpm leak.

MR. MICHELSON: Well, it's not really unpressurized, and it may contain bellows and things like that that fail in a much different and more catastrophic fashion than do pipes. I don't know if you've got bellows, but I've seen some component cooling water systems with 15, 20 bellows in them to take care of all the various kinds of problems you have with it. With those big bellows, do you know, are you using a totally piped system here, or do you know yet?

MR. VAN DE VENNE: That really is -- I think the piping, that would be site dependent.

MR. MICHELSON: But it often ends up with bellows on that system, in which case -- and these are large pipes -- 30-

some inches.

MR. VAN DE VENNE: Thirty-two inches, or so.

MR. MICHELSON: Yes. And those big bellows, a single convolution or a couple convolutions, when they go, they go catastrophically and circumferentially. That's the way bellows fail.

MR. VAN DE VENNE: I do not believe that we have designed for a full circumferential rupture of those.

The emergency feedwater storage tank --

MR. CARROLL: What would the consequences be if you had one?

MR. VAN DE VENNE: I don't know whether -- you know, the tunnel is certainly big enough to handle 7,000 gpm. I don't know to what level you would have to float up in the room to get, you know, a natural equilibrium situation. That really is the question.

MR. MICHELSON: Or, alternatively, pressurize the room if you fill it, and if it's tight enough, you'll fill the room.

MR. VAN DE VENNE: I don't think the room with the ventilation is tight enough.

MR. MICHELSON: Yes.

MR. VAN DE VENNE: I mean, those big ducts --

MR. MICHELSON: But then you've got to chase the water from that system over to where else did the water go.

I'm not convinced from what you've said so far that you've really even considered, and I think it's something you ought to at least think about, or prove that the one-square is a reasonable break.

MR. VAN DE VENNE: Well, I think this is appropriately -- how you handle this is at the PRA stage, is that you determine -- you postulate such a break, you know, and make a certain probability, and see what the consequences are.

MR. MICHELSON: A properly done and adequately modelled PRA could certainly help you with that problem. Generally, PRAs aren't done that way, where they chase the water across the floor and down through ventilation ducts. That kind of PRA is possible, but I haven't seen it.

[Slide.]

MR. VAN DE VENNE: Most of the safety-related electrical equipment is located on this floor here. Switch gear between A and B, batteries A and B, inverters A and B, Emergency Control Room A and B, and some diesel generator equipment, auxiliary equipment A and B.

Again, each of these areas, the area A has a separate ventilation system from the area B; again, to minimize potential for propagation of smoke, fire, etcetera.

MR. MICHELSON: By separate, now, is this one of those sealed ones like the auxiliary feedwater or something else?

MR. VAN DE VENNE: It's just that one ventilation system for train A and another --

MR. MICHELSON: You're saying that the ventilation system is just dedicated to train A all the way.

MR. VAN DE VENNE: Right. All the way, yes. And the other one is dedicated to train B.

MR. MICHELSON: And there is no non-essential ventilation involved in these rooms.

MR. VAN DE VENNE: No. This is safety-related ventilation that's always running.

MR. MICHELSON: What type of transformers are you proposing in these rooms or are any located in them?

MR. VAN DE VENNE: The only transformers that are located here are the four KV to 480 volts.

MR. MICHELSON: That's a big transformer.

MR. VAN DE VENNE: Those are big transformers.

MR. MICHELSON: What type are your prescribing?

MR. VAN DE VENNE: I don't know.

MR. MICHELSON: You don't know if they're oil-filled or air cooled or freon cooled or just what?

MR. VAN DE VENNE: I don't think we have made that determination.

MR. MICHELSON: That becomes quite important, though, in terms of potential hazards in those areas.

MR. VAN DE VENNE: Yes.

MR. MICHELSON: As to what type of transformer you're going to put in it, because transformers do fail catastrophically or can fail catastrophically.

MR. CARROLL: Can and do.

MR. MICHELSON: One more question on the electrical. You showed us the floor, the layout of equipment. Is the electrical leaving that [illegible] above and below or just above the -- penetrations in both directions? In other words, they are floor penetrations and ceiling penetrations?

MR. VAN DE VENNE: They are primarily floor penetrations because most of the mechanical or most of the equipment that's being actuated is at lower levels. So most of the -- well, actually let's look at the cable routing here.

The penetration, the electrical penetrations are in this area. So they are really wall penetrations, because they tend to be at the same level as here.

As I mentioned, most of the equipment is down. So most of the power, apart from the power going to containment, most of the power goes down. Most of the input comes from above because the control room is above.

MR. MICHELSON: There is no cable spreading room.

MR. VAN DE VENNE: There is no cable spreading room.

MR. MICHELSON: Are you tending to do a lot of cable tray work within those electrical rooms?

MR. VAN DE VENNE: No. There will not be and I think

some of our people later can address that. But the number of connections to the control room is very small because of the multiplex fiber optic data transmission.

MR. MICHELSON: Yes, but you've got power equipment in those rooms, too, don't you?

MR. VAN DE VENNE: There is.

MR. MICHELSON: You've got some big boards there. There must be some big power there.

MR. VAN DE VENNE: There is power, yes.

MR. MICHELSON: And that's not multiplexed.

MR. VAN DE VENNE: Mostly AC power.

MR. MICHELSON: Yes, but it's at the 4160 level or 6900 level.

MR. VAN DE VENNE: No, no, no. That's all instrument power that goes to the control room.

MR. MICHELSON: These rooms have no switch gear in them at all.

MR. VAN DE VENNE: The control room.

MR. MICHELSON: No. I'm talking about --

VAN DE VENNE: Yes. These have the 4160 volt switch gears.

MR. MICHELSON: And those have a lot of cable trays in them or something to carry all that.

MR. VAN DE VENNE: Yes. They have cable trays above them. Yes.

MR. MICHELSON: It's a spreading room within the room.

MR. VAN DE VENNE: Right, yes. Correct.

MR. MICHELSON: And it's heavily loaded with --

MR. VAN DE VENNE: That room is heavily loaded.

MR. MICHELSON: Because there's a lot of power in that room.

MR. VAN DE VENNE: Right. There is a lot of power.

MR. MICHELSON: The instrument part is not a big contributor, but the power stuff looks like it's got to be extensive.

MR. VAN DE VENNE: Yes.

MR. MICHELSON: So the fire protection philosophy, the whole thing on hazards from that area we would certainly want to see in some detail.

[Slide.]

MR. VAN DE VENNE: The main control room is located in the corner here. The diesels are located here, A and B, again close to the switch gear.

MR. MICHELSON: And also very close to the main control room.

MR. VAN DE VENNE: One of them is, yes.

MR. MICHELSON: What is your philosophy now on protection against explosions and fires? This is really one of the principal sources of flammables in the entire plant is

around that diesel engine and diesel fires are not incredible and explosions in that room are not incredible. So what is your philosophy on confining the effects of a loss of that diesel and its consequence to the plant on the control room which is so close? It's right down the hall.

MR. VAN DE VENNE: Yes.

MR. MICHELSON: I would really think you'd want to look awfully close at how you ventilate that room, how you control the fires in that room, what you do about the explosions. I think there's a number of questions when you put a control room that close to a diesel engine, which is not traditionally done.

MR. VAN DE VENNE: On SNUPS, it's the same way.

MR. MICHELSON: Yes.

MR. VAN DE VENNE: Generally, the electrical equipment is generally concentrated and typically you will find it reasonably close.

MR. MICHELSON: But diesel compartments, by everybody's understanding, do have to be treated very carefully from the viewpoint of the hazards of the plant, unless you think there is something non-hazardous about what you're going to propose here that's different than what's done in the past.

MR. VAN DE VENNE: Of course, the diesel room has its own ventilation system, very obviously. Although the distance is maybe not very large, it's -- a fire in the room, in the

diesel room would have to be contained to that room by fire equipment regardless of really where it's located.

MR. SHEWMON: Do you, in this, specify who makes that diesel?

MR. VAN DE VENNE: Not at the PDA stage, no.

MR. SHEWMON: So this can be anybody's diesel that they think they can get for a good price and maybe reliability.

MR. VAN DE VENNE: Well, we would have to meet certain requirements under liability, sure.

MR. SHEWMON: Okay.

MR. MICHELSON: What is the oil storage for the diesel? The day tanks, I assume, are within the room.

MR. VAN DE VENNE: The day tanks are in the room and the long-term storage in the yard.

MR. MICHELSON: And you're allowing what, 700 gallons or so of oil in the room then?

MR. VAN DE VENNE: I don't know that.

MR. MICHELSON: Whatever the day tank capacity might be, whatever diesel you might be. It could be 1,000 gallons or more.

MR. VAN DE VENNE: Yes. It could be. The drain system and everything, is it dedicated or can fuel oil get in the drain systems here and thereby circulate to other parts of the plant?

MR. VAN DE VENNE: No. The drains would have to go

outside the plant.

MR. MICHELSON: And the ventilation is dedicated. Nothing else attached to it.

MR. VAN DE VENNE: The ventilation is dedicated, yes.

MR. MICHELSON: I don't find these words, but I assume what you're saying is going to show up.

MR. VAN DE VENNE: Well, there is a diesel generator ventilation system shown as one of the ventilation systems.

MR. MICHELSON: But it's never clear whether that's the only ventilation system in the room or not. These are water-cooled diesels?

MR. VAN DE VENNE: Yes.

MR. CARROLL: Rooms, really, because you've got auxiliaries on the other floor, right?

MR. VAN DE VENNE: Yes. Like the heat exchanger would be on the floor below, cooling heat exchanger.

MR. CARROLL: But this whole block that the diesels and its auxiliaries are in is also isolatable from a fire point of view.

MR. VAN DE VENNE: Right.

MR. CARROLL: Automatic fire doors that drop.

MR. VAN DE VENNE: Yes. This part is really ventilated on its own and it's normally closed off.

MR. MICHELSON: What type fire protection are you prescribing or have you?

MR. VAN DE VENNE: At this point, I don't think we have prescribed that.

MR. CARROLL: Now, the steam lines are also in close proximity to the control room, but they're inside the tunnel.

MR. VAN DE VENNE: Right.

MR. CARROLL: And it is all designed so that the possibility of filling the control room with steam from a steam line break is pretty much eliminated.

MR. VAN DE VENNE: Right.

MR. CARROLL: I think they thought that at Mojave, too.

MR. VAN DE VENNE: What's that?

MR. CARROLL: I think they thought that at Mojave, too; the Southern Cal Edison plant where they killed all the guys in the control room.

MR. VAN DE VENNE: Was that a fossil plant?

MR. CARROLL: Yes. It was a lunchroom next to the control room.

MR. VAN DE VENNE: In fact, the access to the steam tunnel is really only from the turbine building. So if any doors were to fail, it would effect the turbine building and not really this building.

MR. MICHELSON: Because of the concerns about the proximity of the diesel compartment, are you putting safety grade fire protection in there?

MR. VAN DE VENNE: No. I don't believe so and I --

MR. MICHELSON: If you don't, then you go in and do a failure modes and effect analysis on the failure of the CO2 to properly meter into the room and dump a lot more than you had planned on dumping, building up higher pressures, opening the swinging doors and spreading right on down to the lounge, which is the control room.

Things of that sort I would expect you are going to do unless you put in some highly reliable system that is assured of not over-pressurizing the compartment with the gas involved or provide relief panels or something.

Again, if you're going to put a hazard that close to the control room, you've got to give it more attention than you would if it's parked off on the side of the building in its own concrete bunker, which a lot of plants do design that way.

MR. VAN DE VENNE: At the design stage, there were a lot of discussions of removing the diesels from the integral mat for precisely that reason, because this is the way the Japanese do it in all their plants. We felt it was unusual and we would prefer to have them off the mat in their own separate buildings.

At the time, we decided, for reasons of commonality, that between the designs, that we really didn't want to change the design. But we may revisit that whole issue during the FDA stage.

MR. SHEWMON: Maybe you should get a Japanese diesel. They have unbelievable reliability.

MR. MICHELSON: Reliability here isn't really necessarily the concern, although if it's highly reliable, it means it may not explode quite as --

MR. SHEWMON: Reliability of starting isn't the concern, but reliability of performance in other ways is.

MR. MICHELSON: You don't want leakage, you don't want pipes to break, you don't want a number of things to happen or even the CO2 to go off accidentally and pressurize this whole area.

MR. VAN DE VENNE: Our partner on this design, Mitsubishi, builds their own diesels and I think they have an excellent reliability record, as you pointed out.

MR. MICHELSON: But that doesn't necessarily, at least to me, mean that it is necessarily less hazardous from the viewpoint of fire protection, because it's reliable.

MR. VAN DE VENNE: It would tend to minimize, for instance, explosion danger.

MR. MICHELSON: These are low probability events that we're dealing with, of course, and we may have not have seen them yet, although we're getting pretty close in at least one case.

Now, from the missile generation viewpoint of the diesel, what missiles are you designing for, if any?

MR. VAN DE VENNE: I think that we -- I don't know the answer to the question, but I believe that we do not assume a diesel missile.

MR. SHEWMON: Are you talking about missiles inside the room or outside the room?

MR. MICHELSON: Well, they start inside.

MR. SHEWMON: I know they do, but are you thinking of something which would penetrate the wall or not?

MR. MICHELSON: Penetrate the wall, yes. Something that can remain unconfined.

MR. SHEWMON: Is there any history of that ever happening? What do you have that's the biggest moving part there and by the time it came through the casing, could it be expected to go through the wall?

MR. MICHELSON: That's the type of analysis we need to do.

MR. CARROLL: I think people who have blown cylinder heads have.

MR. SHEWMON: I'm sure they have. I just read something recently where the operator saw the smoke coming out the top of the diesel and the report said they decided to leave the room, which I bet they did darn rapidly, and when they came back there were parts sort of all over the room.

MR. MICHELSON: This room has doors. Doors are not exactly missile barriers and there is only one more door to get

into the control room area.

MR. SHEWMON: But there are blowout panels and there are pistons moving, they come through the head.

MR. VAN DE VENNE: Any missile would tend to be radial, I think, and go either this way or --

MR. MICHELSON: When you talk about doors, you talk about things ricocheting off walls. A direct penetration of the wall, no, but certainly double doors are pretty vulnerable to things bouncing around the room.

MR. SHEWMON: Pistons bouncing off walls and then hitting doors aren't going to come down to the control room.

MR. MICHELSON: The CO2 process in the same event does come down through the hole, with a resulting fire. You've lost one of your barriers already, as a result of the missile. So, I think it needs to be addressed, and I think that's what we're asking, is where is it addressed, and if not, why not, and maybe it's incredible, although experience indicates to the contrary.

MR. SHEWMON: Systems chase around walls and out doors and down halls.

[Slide.]

MR. VAN DE VENNE: The last floor is really primarily dedicated to ventilation, which is the top floor, which has the various ventilation systems. The diesel ventilation is shown above the diesels here. The mechanical ventilation supply and

exhausts are here, and the various electrical, separate for each train and for the main control room, etcetera, are shown over the area.

MR. MICHELSON: Where are the diesel compartment ventilations again? There and there. Okay.

MR. VAN DE VENNE: Those diesels are Once-Through Cooling, so I think overpressure would primary go away through the intake and exhaust it.

MR. MICHELSON: Well, Once-Through Cooling also means, though, in case of fire, you have to isolate the Once-Through Cooling, I assume. If you're using CO2, you certainly would have to do something to shut the ventilation air off. You haven't told me yet how you do it.

So, I am not sure whether pressurization is a problem or not, but it would be if you have a provision to seal up these rooms for fire-protection purposes. Then you have to worry about pressurizing the room.

MR. VAN DE VENNE: That is general arrangement presentation. I think the next one is the I&C.

MR. MICHELSON: Excuse me. In the case of the control room, what does have to come into the control room, which is most instrument-level stuff, but probably you have to have some of them on a smaller level of control power. You know, you've got lighting systems and whatever. You've got quite a few kilowatts of energy that you need. How is it

routed in and out of the control room?

MR. VAN DE VENNE: Train A is -- this train here is brought in from below, and the other division is brought in from below here and up and over into the control room.

MR. MICHELSON: So, Train A is coming up through the floor, and Train B is coming down from the ceiling? Is that what you're saying?

MR. VAN DE VENNE: Well, from the side, really.

MR. MICHELSON: Oh, from the side.

MR. VAN DE VENNE: Yes.

MR. MICHELSON: Now, how about the non-essential but power-consuming devices within the room?

MR. VAN DE VENNE: They're mostly coming in from the turbine building, which is over -- the turbine building is located at this end here, of course.

MR. CARROLL: Okay. I think before we move to the next subject, we ought to take a break. So, let's be back at a quarter of 11.

[Brief recess.]

MR. CARROLL: Let's reconvene, and we are going to hear from Gil Remley on Chapter 7, I&C.

MR. REMLEY: My name is Gilbert Remley. I am the manager of Control and Protection System Development at Westinghouse.

We have been working on a digital I&C architecture

for a number of years in Westinghouse, and I thought it would be appropriate to briefly review the evolution of that design before I discuss the overall I&C architecture detail.

We started discussing this technology with the NRC back in 1975 on RESAR 414, and in particular, we were discussing at that time the integrated protection system design.

The integrated protection system was then and is still the heart of our I&C design, and I will talk about that more in detail a little later on.

With the review on RESAR 414, we came to a conclusion of the existing design of the integrated protection system review and completed our V&D program with NRC audits in the 1980 timeframe.

In the same timeframe, we were also working with the French. We're working on a similar system under license agreement with Westinghouse, which is known as the SPIN system.

The SPIN system represents a lot of the design concepts and the details that were implemented in the original integrated protection system design.

However, after that work, we then were jointly discussing this type of technology in England, Japan, and in Italy, and through those discussions, we decided that it would be appropriate in the mid-80s to upgrade the design to second-generation microprocessor technology, that technology being 16-

bit microprocessor technology versus 8-bit microprocessor technology.

Given the discussion we have had with those three countries, in particular, the integrated protection system has been selected as the reference design on the three plants, that being the Sizewell B plant in England -- the integrated protection system is the primary system for Sizewell B -- and the APWR design, which we are reviewing today, and on the Italian reference plant design.

MR. MICHELSON: This is all 16-bit technology?

MR. REMLEY: It's a minimum -- well, in general, it's 16-bit technology. There are certain things in slave controllers which are still 8-bit technology.

MR. MICHELSON: Okay.

MR. REMLEY: Some things which are 32-bit technology, but the heart of it is 16-bit technology.

MR. MICHELSON: Which are 32-bit?

MR. REMLEY: We use 32-bit technology in the control system --

MR. MICHELSON: Oh, you do.

MR. REMLEY: -- and in the computer system.

[Slide.]

MR. REMLEY: The elements of this design are the integrated protection system; its companion system, the integrated control system. There are remote data-acquisition

units for both safety and non-safety-type inputs. We have special monitoring systems in the design, like our flux-mapping system and other diagnostic systems -- for example, metal-impact monitor, acoustic leak detector.

MR. KERR: What would be the difference between an integrated system and a non-integrated system?

MR. REMLEY: We use the word "integrated" to mean a system that has been designed as a logic set such that its elements have been rationalized and optimized to work together, as opposed to a system that has been sort of put together ad hoc with separate units and dedicated types of equipment. Is that a sufficient answer?

MR. KERR: Well, if that's what you mean by integrated protection system, it is.

MR. REMLEY: I'm not sure I have answered the question. That's why I'm trying to make sure.

MR. KERR: I wondered what was integrated. For example, is the implication that the protection system and the control system are integrated?

MR. REMLEY: The word "integrated" means -- for example, let's try to compare it to what we had before.

MR. KERR: I think I know what the word "integrated" means. I'm trying to understand how it is used, what the implication is in this context.

MR. REMLEY: It means that the elements of the system

have been designed to logically work together in a way that's been optimized, as opposed to selecting separate systems of separate designs and linking them together.

MR. KERR: Okay. Can you give me an example?

MR. REMLEY: Yes, I can.

MR. KERR: Okay. That would be helpful.

MR. REMLEY: In the previous protection system design, we had several different design elements in the protection system. For example, we had a separate set of racks of equipment of a given technology for the nuclear instrumentation. We had another set of racks for the -- we referred to it as the process protection racks, which did all the rest of the bi-stable calculations associated with the protection functions that were not covered by the nuclear instrumentation. That was done with analog technology. Okay?

Then we had a system which we referred to as the solid-state protection system, which was a different system, which received signals from the nuclear instrumentation racks and the process protection racks and did the system-level engineered safeguards actuations calculations. That was then interfaced to a separate system that was normally provided by the architect engineer, and that technology has evolved over the years from relay-based logic up into solid-state-type logic.

MR. KERR: Okay.

MR. REMLEY: Okay. That is what we refer to as not an integrated design but a design of several separate kinds of systems. Okay?

MR. KERR: Now, what about the control system, as contrasted with your protection system? Is it roughly the same sort of design?

MR. REMLEY: That's right. The control system, in fact, uses the -- this design -- in order to achieve the goals we wanted to achieve about how we were going to produce the integrated design, we in fact designed modular elements which we could configure in a way that we'd do different functions within this design. Well, these are general-type elements in the broad applications sense, and we use these same elements over in the control system.

For example, we have a board which interfaces to an RTD, and it provides the signal conditioning for that RTD. That board is the same board in the protection system or in the control system. Okay? So, in that sense, it uses similar elements at the modular level.

MR. KERR: Okay. At some point in your presentation, are you going to say anything about the reliability goals that you have set for yourself? If you are, I'll wait until you get to that. Otherwise --

MR. REMLEY: Yes. I was going to talk about that, and I was also going to talk about the common load failures.

MR. KERR: Okay. I'll wait.

MR. REMLEY: Okay.

MR. MICHELSON: Are you going to talk later about the physical location of all these? You've drawn blue lines around. I don't know if that means their physical locations or just what, but I am quite interested in where all this equipment is located.

MR. REMLEY: I am not able to speak to the physical location of this equipment.

MR. MICHELSON: Well, it's a layout question, which I thought was the subject of our meeting today, and I am quite interested in the layout of the electrical equipment, particularly what kind of individual environmental control is provided in each of these areas in which this equipment is laid out, and I can't get any of that without getting into it, and I thought this was the meeting to do it.

MR. VAN DE VENNE: Well, maybe after we've gone through the system, I can go back and put up the layout and sort of indicate where this equipment is located.

MR. MICHELSON: Yes, because you have shown lots of good information here, but I am quite interested in where is it? Because the layout drawings don't help me any. They are not that detailed.

MR. REMLEY: It's just something I haven't studied. I can explain the capabilities of the layout but then would

have to get into the details.

MR. MICHELSON: Are we going to discuss separately the basic environmental control philosophy, because you, I am sure, recognize the importance of environmental control for these kinds of devices. Is that going to be presented today, or is that another subject, or do we have to add it as an agenda item in the future?

MR. VAN DE VENNE: Well, I may be able to address part of it. I have to better understand. Do you mean environmental control in terms of HVC?

MR. MICHELSON: Primarily. You must be concerned from two viewpoints. First of all, how do you normally keep the temperature within the allowable range of the equipment? I don't know what that is yet, but I hope to hear today.

Secondly, how do you protect that controlled environment from intrusions by other kinds of happenings, such as pipe breaks, fires, or whatever? Because this equipment is very sensitive to temperature, I think, but you're going to tell me later how it's going to be rated, what elevated temperatures it can withstand and so forth. I assume you will.

MR. REMLEY: I guess I don't agree with the statement that this equipment is very sensitive to temperature.

MR. MICHELSON: Well, that's what we'll find out. If you can stand 150-degree room temperatures, that's fine. Say so, and we'll worry much less about it. If it can only stand

104, then we'll worry a lot more.

MR. REMLEY: It's somewhere in the middle.

MR. MICHELSON: Yes. We also want to pursue carefully as to what the "somewhere in the middle" is and what it means.

MR. REMLEY: Yes. I have that data in here.

MR. MICHELSON: Okay. Good. Thank you.

MR. REMLEY: The rest of the elements of the design are the remote shutdown panel, the alarm system, the qualified display system, the main control room, and the computer system.

MR. MICHELSON: What are the little circles? Like on the blue boxes there, they seem to just terminate.

MR. REMLEY: That means isolation.

MR. MICHELSON: Does that mean you're going into multiplexing now at that point or just isolation alone?

MR. REMLEY: Both. It is fiber-optic.

MR. MICHELSON: Well, I see some, you know, where you seem to have hard lines going from one box to another. Does that mean that's hard-wired, or is that just pictorial only?

MR. REMLEY: That is pictorial only. Most everything on this diagram is indicating that it is multiplexed. There's only, really, one thing on this diagram -- there is the sensor inputs and the actuator interfaces. This is all hard-wired. There is the interface to the reactor trip switch gear from the integrated protection cabinets. That is hard-wired.

Everything else on this diagram is multiplexed.

MR. MICHELSON: From the instrument cabinets, then, which are reasonable close proximity to the device that's being monitored, is that hard-wired to some control cabinets in your integrated protection, or is that multiplexed, also?

MR. REMLEY: The sensors?

MR. MICHELSON: Yes. Well, no. You show from the sensor -- from the device itself up to that blue box. Is that blue box your so-called "sensor"?

MR. REMLEY: No. This circle with the "X" in it is the sensor. Okay? The blue box is the actuator, the logic that's associated with the equipment.

MR. MICHELSON: Right, but you're showing those boxes going to valves and pumps and so forth.

MR. REMLEY: That's right.

MR. MICHELSON: Now, that's hard-wired to the first-level box.

MR. REMLEY: This is hard-wired right here, yes.

MR. MICHELSON: Now, is it multiplexed from there to the higher level where you integrate and do some protection functions? Is that multiplexed?

MR. REMLEY: Yes, it's multiplexed, although there's --

MR. MICHELSON: So, the multiplexers are located fairly locally to the components being monitored then.

MR. REMLEY: Yes.

MR. MICHELSON: So, you must protect those multiplexers again or tell me what environments they can withstand and so forth.

MR. REMLEY: That's right.

MR. MICHELSON: Okay. Thank you.

MR. REMLEY: As I was saying, we already discussed I guess about the fact that this design uses 32-bit and 16-bit microprocessor technology. It is a distributed digital processing architecture that makes extensive use of multiplex communications. In particular, fiberoptic cabling is used.

It uses more sophisticated control and protection algorithms than in our previous designs. And we call this a fault-tolerant design.

MR. MICHELSON: What does that mean?

MR. REMLEY: Fault tolerant means that we implement the design details in a way that we consider failures when we are doing the design and we do the design in such a way that the system will degrade the preferred failure modes, and that we have redundancy built in to supplement or take over for a failed piece of equipment.

MR. MICHELSON: That is as long as the equipment is in its proper environment and so forth, it is fault healing?

MR. REMLEY: No, it even goes beyond that.

MR. MICHELSON: Well, the fault healer, the thing

that is deciding how to do the healing is also in that same adverse environment.

MR. REMLEY: You can still have a catastrophic failure and still go to a preferred failure mode.

MR. MICHELSON: By "catastrophic" you mean what, though? Catastrophic loss of environment?

MR. REMLEY: I would mean, like if I would have complete failure of all my four-channel sets of protection. the system is designed in a way that you would still trip the switch gears.

MR. MICHELSON: Let me ask it differently.

If you lost the environment, if the temperature in the room went to 180 degrees, you certainly aren't fault tolerant any more, or if you are, tell me how.

MR. REMLEY: The system has built into it continuous diagnostic.

MR. MICHELSON: But the diagnostics see 180 degrees, also. Are they working at that temperature? Unless you locate them somewhere else.

MR. REMLEY: The diagnostics don't, I mean it isn't a matter that they work, it is a matter that they shut down the system, okay, which is really what happens.

MR. MICHELSON: In other words, they are designed to fail safe under adverse environment?

MR. REMLEY: That's right.

MR. MICHELSON: Is that what you are saying?

MR. REMLEY: That's right.

MR. MICHELSON: Is that stated in the design criteria or in the SER that that is a design basis?

MR. REMLEY: The statement that we make is that the integrated protection system uses fail safe design principles in the design implementation.

MR. MICHELSON: That doesn't tell me anything about the environment question. I understand what you are saying. But it doesn't tell me about the environment.

MR. REMLEY: It's not strictly an issue of environment. There can be lots of things that cause the failures to occur besides environment.

MR. MICHELSON: Right. But I am only asking about environment in this case. And fault tolerant, that statement doesn't help me any, unless you are going to tell me that it indeed fails safe under adverse environment and then tell me what range of adverse environments it is fail safe for.

MR. REMLEY: That's what I'm telling you. It is fail safe under adverse environment.

MR. MICHELSON: Okay. We'll see later how you do that.

[Slide.]

MR. REMLEY: To compare it with our previous designs, we started, our previous designs used central processing.

We've gone to a distributed processing architecture.

Communications in general were hard-wired. In this design the communications are multiplexed, and we use fiber optics or isolation.

[Slide.]

MR. REMLEY: The previous protection and control logic was based on solid state technology and relays. Now it is digital, based on microprocessor technology.

The Westinghouse scope has gone beyond the system level actuation, as I mentioned. It also includes the component level actuation, or the engineered safeguards actuations.

The previous design had manual signal selection between the protection and control system. This is now done automatically.

The testing of the protection system in our previous design was manual. Now we have an automatic integrated tester built into the protection equipment.

MR. KERR: Excuse me. Is that in effect continuous testing?

MR. REMLEY: There are two types of tests. One is a functional test of the equipment which is what is required to be performed periodically, and that is the functional test I referred to. That is not continuous. That is something that is manually initiated and runs automatically to completion.

That is supplemented by tests that are run continuously, that we refer to as the self-diagnostics.

The one type of test is a functional test. It just ramps the process input and watches the trip actions. The other one is a type of test that is oriented toward the operation of the hardware elements. It checks that the A to D converter is operating properly. It checks that the CPU is operating properly. So it is really focused at different hardware elements.

MR. KERR: Okay. thank you.

MR. MICHELSON: The higher level power supplies for this, are they four-train power supplies, then?

MR. REMLEY: For the channel sets, yes. I think this is a four-train system for the engineered safeguards.

MR. MICHELSON: Yes. But is on the instrument and control then that it is four-train?

MR. VAN DE VENNE: Yes.

MR. REMLEY: By previous design, the protection logic was two out of four that would go to two out of three, or one out of three based on testing or failures. This design, the logic goes from two out of four to two out of three, and it includes an operational bypass.

Before, we had cabinet hardware that was of system-specific design. As I was saying, it was custom designed for every type of system.

Now, our approach is to use standard modules that we can use repetitively, then, to configure it in the way that provides the system implementation.

MR. MICHELSON: For graphic displays, do you have those dedicated one to each of the four channels?

MR. REMLEY: No.

MR. MICHELSON: You are combining then somehow. I assume they are still redundant, though.

MR. REMLEY: There is redundancy built into the safety displays. But it is not, it does not have four-way separation.

MR. MICHELSON: You mean there is more than one CRT that could read the same information, that is what you mean by redundancy built in?

MR. REMLEY: Yes. Both the calculation elements associated with the safety displays are redundant.

MR. MICHELSON: How do you isolate the graphic displays from the logic channels?

MR. REMLEY: We use the fiber optic multiplexing to do that. If we go back to the --

MR. MICHELSON: That's okay. I understand the answer.

MR. REMLEY: Okay. Just for one point of clarification, though. The displays are not, these particular displays associated with the safety information are not CRTs.

We are using plasma display technology for that.

MR. MICHELSON: Now, in older technologies, the argument on using such things as CRTs was that, well, if anything went wrong, you can always go back and read the gauges on the panels. I gather in this plant there aren't as many gauges on the panels. Is that correct?

MR. REMLEY: That is correct. There aren't as many gauges on the panels.

MR. MICHELSON: So if you lose the CRT display for any reason, you know you lost both of them, you are really going blind. Is that the situation? Or can you argue you can walk around the control room and get the information?

MR. REMLEY: I guess I would argue that, number one, you still have some dedicated indicators that are analog-type indicators.

MR. MICHELSON: Is that a sort of a minimum set, and has that been identified?

MR. REMLEY: I don't think we have designed it as a minimum set. We have designed it really as what we need to control.

MR. MICHELSON: So you are really designing as if you must have the CRTs and one of them must work. Is that right?

MR. REMLEY: Yes. But I don't want to answer is that way.

MR. MICHELSON: I guess they are seismically-

qualified CRTs and all that sort of thing.

MR. REMLEY: Yes. That is what I am trying to make sure is not misunderstood.

MR. MICHELSON: Okay.

[Slide.]

MR. REMLEY: There are two types of displays technology in this board. Well, maybe more than that even with the alarm system. But from the point of view of the safety display information, it comes through this path, what we refer to as the plant process data system, which receives any safety information or important safety information that is not directly connected into the protection system. An example of that would be the incore thermocouples.

So it receives this information from two sources. One being the direct connection to a remote data acquisition unit. And this little arrow here is indicating there is a direct connection for the important signals, up to this calculation unit, which is redundant, and also a connection to the protection system, for the remainder of the signals, comes up to these units. This is a calculation unit which is redundant. This calculation unit then interfaces into several different plasma displays that are on the control board. And they are cross coupled, so that you don't lose a display because you lose a calculation unit. You just lose that display.

Now, in addition to that, the normal data acquisition path of information is through this bus here. This system has hierarchical data highways in it. And there is a bus that runs through a data highway, which we refer to as the monitoring data highway, the data highway associated with data acquisition for the plant.

That data highway is feeding the CRT displays that are in the board. So it is a totally separate path of information for the CRT displays than is associated with the safety display information.

It also has the same degree of redundancy built into it.

MR. MICHELSON: Now, is the safety display information an adequate display if you did not have any of the other information?

MR. REMLEY: Yes.

MR. MICHELSON: And it is readable from the control room?

MR. REMLEY: Yes.

MR. MICHELSON: How do you physically separate these pathways? Are they inside of conduits, or how is that done?

MR. REMLEY: We run the fiber optic cables inside of conduits. That is our normal practice.

MR. MICHELSON: And you separate the conduits --

MR. REMLEY: That is right.

MR. MICHELSON: -- according to the trains?

MR. REMLEY: That's right.

MR. MICHELSON: This is all prescribed somewhere I guess in an SAR?

MR. REMLEY: I can't answer that.

MR. MICHELSON: The physical separation left me a little cold. But I'm sure it was all worked out. At least if we could find the basic ground rules by which it will be all physically separated, that is probably good enough.

MR. REMLEY: We have that information.

MR. MICHELSON: I just wondered where I could read it a little bit. It should be a part of the safety analysis report, I would think, since this fire in the building is one consideration, and I would like to know that I still have a minimum set of pathways still available after I heat up some area of the building, because there is a fire there. I wouldn't want to lose all these optical cables from fire in one place.

MR. REMLEY: I agree with that. Yes.

MR. MICHELSON: That physical separation criteria is defined somewhere, I assume.

MR. REMLEY: I guess I had started to move into the topic of the I&C communications network. As I was saying, what we have in front of us is a hierarchical data highway-type system for communications. And it exists at three levels.

The first level is associated with the IO itself. We use a low-level data highway-type technology for interfacing elements of the IO in the equipment to the processors. In other words, we actually start the multiplexing between the IO signal conditioning boards and the microcomputers that are doing the calculation. And the area where we do that most is, number one, in the interface between the control stations that are on the desk and the multiplexer cabinets which interface through the control highways, and in the architecture that is associated with the integrated logic cabinet that interfaces to the actuators. The reason we do hat is because this is actually a triple-redundant output from the point of view of the microcontrollers. And we bring it together to vote it on a signal conditioning board to bring the three triple-redundant elements together under one signal-conditioning board to form the single output.

MR. MICHELSON: On my drawing, and I am sure on this one, but I can't see it, those little blue boxes about the middle of your picture down at the bottom, there is a series of little circles. What do they mean?

MR. REMLEY: Is that -- I don't know where you are here.

MR. MICHELSON: I'm down at the very bottom, right there.

MR. REMLEY: Here?

MR. MICHELSON: No, no. Over to your right. There.

MR. REMLEY: That just means continued. That means that there are many of these.

MR. MICHELSON: Oh. Oh, that just means that there are a whole bunch of them.

MR. REMLEY: Yes.

MR. MICHELSON: I thought it meant there was crosstalk or something.

MR. REMLEY: No, no. It just means that it is continued.

MR. MICHELSON: Okay. Thank you.

MR. REMLEY: The next level of data highways in the system is the control highways, which exist in the protection system between the engineered safeguard system actuations, and the component level actuations, and also interface the component level actuation controls with the control board.

Okay. Those controls connect on the data highway. And this is the same in the protection system and in the control system. So that is the second level of data highway communication.

There is a separate path to the protection cabinets, the protection logic cabinets, from the remote shutdown panel, that is not data highway, but is a data link technology.

MR. MICHELSON: What does that mean; it is essentially hard-wired?

MR. REMLEY: It is not hard-wired.

MR. MICHELSON: But it is still multiplexing?

MR. REMLEY: It is still multiplexing, but it is using a different type of multiplexing.

MR. MICHELSON: Okay. I understand.

MR. REMLEY: We do use datalink technology for special applications within the design. I mentioned one of them, the interface between the remote shutdown panel and the engineered safeguards logic cabinets. Also, the connections between the protection cabinets in the engineered safeguard system level actuation calculations are fiber optic, point-to-point datalinks, Simplex datalinks.

Also, the connections between the protection system and the control system are fiber optic, point-to-point Simplex datalink. So we use the datalink technology for separation reasons, for redundancy reasons and for performance reasons. That's why we still maintain the datalink technology.

The third level of data highway technology in the design is the data acquisition function, as I was talking about. This is basically associated with getting the plant process information to the higher level systems, specifically the alarm system and the computer system and the control board displays.

[Slide.]

MR. REMLEY: The instrumentation and control cubicles

that were in the lower part of the diagram typically all look very similar. This is a picture of the integrated protection system prototype seismic cubicles.

MR. MICHELSON: Is that the solid state design there, the typical, or is that the older one?

MR. REMLEY: This is the new microprocessing design.

MR. MICHELSON: Okay, that is typical of what we would expect to see then?

MR. REMLEY: That's right.

MR. REMLEY: I guess the point I was trying to make was, there may be --

MR. WARD: That's apparently not a prototype of how they are going to be fastened to the floor?

MR. REMLEY: No.

MR. MICHELSON: I hope not.

[Slide.]

MR. REMLEY: The point I was trying to make was, all the cubicles -- and there are some exceptions to this, but all the cubicles below this line here look like what I'm about to describe.

MR. MICHELSON: No, they're located not in dedicated rooms necessarily, but out in equipment areas?

MR. REMLEY: Both.

MR. MICHELSON: Both, yes.

MR. REMLEY: The cubicles for the process protection

calculations, the control calculations, are normally located in dedicated rooms in the control room area, although, as I said, I'm not familiar with the APWR specifically. The logic cabinets are then located with the equipment, and the reason there is an advantage in doing that is because this is where you pick up the tremendous cable savings.

MR. MICHELSON: Now, all the individual power supplies for the local equipment within these multiplexing cabinets; those power supplies are all solid state type power?

MR. REMLEY: They're switching power supplies.

MR. MICHELSON: They're supplied from the DC --

MR. REMLEY: AC.

MR. MICHELSON: AC, okay, vital AC power system?

MR. REMLEY: Yes.

[Slide.]

MR. REMLEY: This is the front of the cubicle when you open the door. Typically, there are two computer subsystems in there, in these card frames, an interface panel, and separate power supply modules in a cooling assembly. One of these power supply units is associated with each of the microprocessor chassis.

So, we've gone to separate modular supplies that are associated with the computer subsystems that they service, as opposed to a centralized supply within a cubicle.

MR. MICHELSON: What's that cooling assembly mean?

MR. REMLEY: That is a blower unit that exhausts the air from the top of the cabinet. There are other fans in the cabinet that move the air up through the printed circuit boards.

MR. MICHELSON: You don't just circulate from the bottom to the top; you have fan stages through there?

MR. REMLEY: That's right.

MR. MICHELSON: But it is essentially taking air out of the room, circulating through the cabinet an exhausting again?

MR. REMLEY: That's right.

MR. MICHELSON: Thank you. What kind of kilowatts of heat are we talking about on one of these cabinets?

MR. REMLEY: I'm not sure of the answer to that.

MR. MICHELSON: You've got three bit power supplies. I'm just trying to get a feel for how big.

MR. KERR: Certainly, you aren't talking about kilowatts?

MR. MICHELSON: Power supply is in there alone, I think.

MR. REMLEY: Well, you're talking about how much energy is dissipated by the printed circuit boards.

MR. MICHELSON: Well, how much energy is used by the cabinet? That's essentially going to be removed by the air.

MR. REMLEY: Yes, same thing. Yes, that's right.

There are fans also.

MR. MICHELSON: Yes, but how much energy is supplied to the cabinet; do you have any idea?

MR. REMLEY: No, I don't know the answer to that.

MR. MICHELSON: It's surprising. That's why it's a nice number to have in front of you so you appreciate what happens when the cooling fans quit or whatever, or whenever the air in the room starts to get warm.

MR. REMLEY: Yes, since we're discussing this so much, there is redundancy in these cooling fans, okay, within the cabinet and within the fans that bring the air up through the stages. There are also temperature monitors at the top of the cabinet and at the top of the cages with the printed circuit boards.

These temperature monitors are monitored by the microprocessor subsystems themselves. There's no safety action associated, but there is an alarm function associated with those temperature monitors that they exceed the thresholds.

MR. MICHELSON: Now, on the card cages, is there more than one monitor. Did you put several monitors on each cage, or just one?

MR. REMLEY: There are two monitors on each cage.

MR. MICHELSON: Where else is the temperature monitored?

MR. REMLEY: At the top of the cubicle.

MR. MICHELSON: At the very top, okay, and there are, again, two there.

MR. REMLEY: There are two there.

MR. VAN DE VENNE: Maybe as a comment here, the cooling fans are also powered by vital AC, so there's only really one set of power coming in. If you lose the power, you lose the cooling in the cabinet, obviously.

MR. MICHELSON: Are those cooling fans considered to be vital equipment, you know, safety-grade equipment?

MR. REMLEY: Yes, those fans are --

MR. MICHELSON: The entire cabinet is safety-grade; is that right?

MR. REMLEY: That's right. It is qualified together. There is no special consideration given to the fans or anything.

[Slide.]

MR. REMLEY: If you look the cubicle from the side, again, these are the elements I've already talked about, but now there are the signal conditioning modules which perform the signal conditioning function between the field signals and the computer signals.

These boards are mounted in metal wrappers that are stacked up and when you stack them up, they form a barrier between the field wiring and the internal computer wiring, a metal barrier.

The third supply is associated with the power required for these signal conditioning modules. Although we do do some subtle change here, because these signal conditioning modules can accept dual power inputs, we actually move around some of the supplies in these units. Each one of these units can handle two supplies, so that if we remove one of these supplies, you will still have power to your signal conditioning board, but it's just a minor point.

MR. MICHELSON: These cabinets never contain more than one train of equipment or one channel; is that right?

MR. REMLEY: That's right.

[Slide.]

MR. REMLEY: This is simply the view from the rear of the cabinet. What you have here is the termination blocks and a system for interfacing the field wiring to the terminations. The cabinet can have either top or bottom entry.

MR. MICHELSON: Now, how are those terminations cooled? I guess they don't have any energy generation.

MR. REMLEY: Terminations are not cooled.

MR. MICHELSON: They're uncooled.

MR. REMLEY: They're uncooled.

MR. MICHELSON: There is some air circulation back i the cabinet from the fans?

MR. REMLEY: That's right.

MR. MICHELSON: Thank you.

MR. REMLEY: We actually have a push-pull system associated with the IO boards. I can get into that, but there's another set of fans for that.

MR. MICHELSON: Now, those little boxes also contain the -- oh, that's right, there's no multiplexing at that end?

MR. REMLEY: No, right here -- well, for sensor signals and for control signals, they are not multiplexed. They interface directly to termination blocks. But we do have datalink and data highway transceivers that also are physically -- they're the same form factor of prirted circuit board and mount in a similar type of termination frame.

So all signals that come into the and exit the cabinet, come through this part of the cabinet. Okay, so, we control the access of the field signals to this part of the cabinet.

MR. MICHELSON: You do have then some potentially sensitive devices from the viewpoint of the temperature in the area if you're going to put some of the multiplexing receivers in there. Do you monitor the temperature in that area of the cabinet?

MR. REMLEY: The receivers themselves are not in this area of the cabinet.

MR. MICHELSON: Okay.

MR. REMLEY: They're in this area of the cabinet.

MR. MICHELSON: Then they are monitored?

MR. REMLEY: Then they are monitored, yes.

MR. MICHELSON: Okay, thank you. It's just hardware terminations or interrupted terminations?

MR. REMLEY: All that's at this side is cable, but it isn't all twisted, shielded pair cable; some of it is for multiplex signals like optical cable.

MR. MICHELSON: Okay, thank you.

MR. WYLIE: These are located where?

MR. REMLEY: These cubicles?

MR. WYLIE: Yes, those cubicles.

MR. REMLEY: These cubicles can be located just about anywhere in the plant. We have some of these cubicles inside the containment for the RPI, okay. That's a very limited application. We have a lot in the main control room area, and those are the integrated protection cabinets and the integrated control cabinets.

That's mostly because of operator access. We want to provide convenient access to those cabinets. Then the other cabinets are located with the control devices themselves throughout the plant.

MR. WYLIE: Say, for your transmitters and other sensors --

MR. REMLEY: We are not trying to locate the cabinets near the transmitters. What we're trying to do is locate them near the control devices, okay.

MR. WYLIE: I mean before the inputs to your protection system, you'd have one of these cabinets somewhere.

MR. REMLEY: I'm going to show you that, yes.

[Slide.]

MR. REMLEY: The inputs to the protection system are here. Now, these cabinets, which we refer to as integrated protection cabinets, are normally located in the main control room area. They're not necessarily located, say, close to the containment, because we want to minimize this run.

MR. WYLIE: But you run in hardwire then from the --

MR. REMLEY: Yes, the signals are hardwired.

MR. WYLIE: All the way?

MR. REMLEY: All the way.

MR. WYLIE: From the transmitters in.

MR. REMLEY: Yes, we need to hardwire the transmitters because of reasons of internal separation in the design and time response requirements.

MR. MICHELSON: They're hardwired only to these cabinets though?

MR. REMLEY: Only to these cabinets; that's right.

MR. MICHELSON: I thought that next to the sensors, I thought.

MR. REMLEY: This is the sensor here.

MR. MICHELSON: You're multiplexing from those lower cabinets on up to the integrated control, I thought.

MR. REMLEY: Yes, the signal path flow though is from the sensor to the protection cabinet for the bi-stable calculation, to the engineered safeguard cabinet for the system level logic to the logic cabinet for the component interlock logic to the control device; that's the signal flow.

MR. MICHELSON: Now, which part is hardwired?

MR. REMLEY: This part is hardwired, the signal, the sensor to the integrated protection cabinet and the interface between the logic, the control logic output and the control device.

MR. MICHELSON: Right.

MR. REMLEY: Everything else is multiplexed.

MR. KERR: There is some signal processing between the sensor and the hardwire, I assume, in some cases?

MR. REMLEY: The signal processing is all done with signal conditioning modules which that are built into the front end, as I was showing, of the integrated protection cabinet.

MR. KERR: There's no signal processing at the sensor?

MR. REMLEY: No signal processing at the sensor, even -- well, there is a pre-amp associated with source range NIS that mounts on the containment wall.

MR. KERR: All right, okay.

MR. REMLEY: Other than that, all the signal processing is done on these type of signal conditioning boards

that are mounted in the protection cabinets. Now, I haven't shown the nuclear instrumentation modules.

Because of their sensitivity, they are put in special type boxes that don't look exactly like this, but conceptually, they're in the same position. They're just in isolation boxes.

MR. WYLIE: Now these panels are physically located somewhere in the vicinity of the protection system in the vicinity of the control room; right?

MR. REMLEY: That's right.

MR. WYLIE: You still have the long leads from the sensors into them?

MR. REMLEY: That's right.

MR. KERR: Now, these

[Slide.]

MR. REMLEY: This is a picture of the signal condition board inside its metal wrapper. This is the field side, and you can barely see the field terminations here. This is the computer side. As I said, these termination frames stack up, so when you see them all together, they form a barrier. This is where the power's in the ground for the board containment.

[Slide.]

MR. REMLEY: Here is the inside view from the -- looking inside the front door of the cabinet, and it's the signal conditioning board. This particular connection here is

the test bus required for the integrated functional tester.

[Slide.]

MR. REMLEY: I completed talking about the overall NC architecture, and now I was going to talk about the integrated protection system in detail. Although in your handout, before I do that, in your handout -- I guess we should back up -- I don't have an overhead for this, but there is a table which talks about the environmental characteristics of this equipment. The normal operating temperature we expect to see is 0 to 105 degrees. What this means is --

MR. MICHELSON: It says 60 to 105.

MR. REMLEY: Sorry.

MR. MICHELSON: Do you mean 0, or --

MR. REMLEY: I meant 60. I misspoke.

MR. MICHELSON: Okay.

MR. REMLEY: I misspoke.

What this means is that this is the temperature range for which we do our reliability calculations. That's what we call the normal range. We will test the equipment as a unit from 40 to 120 degrees fahrenheit, and refer to that as the abnormal range because the equipment will still operate properly. The mean time between failures may degrade, however.

Then, on an individual pipe test for the printed circuit boards, we do go over 150 degrees fahrenheit to stress the design to make sure that it still operates even at that

temperature.

MR. CARROLL: For how long?

MR. REMLEY: Excuse me?

MR. CARROLL: For how long?

MR. REMLEY: It's done actually in a switching of the environment with both temperature and humidity, and it normally lasts about two days, so it's a cycling that goes on. So, I don't know the answer to exactly how long it stays at 150 degrees fahrenheit, but it's on the order of, say, twelve hours or something, okay? But that is merely a design stress test.

MR. CARROLL: So what you're doing is going from 105 to 150 and back down again on the temperature side of it?

MR. REMLEY: That's right. And we also vary the humidity when we're doing that.

MR. CARROLL: Okay.

MR. REMLEY: The reason we quote these numbers that I have in front of me here with temperature and humidity, these have been the traditional numbers that we have used for equipment qualifications. These are the numbers that we've used traditionally, okay? We do do some excessive stress testing beyond that.

MR. MICHELSON: Let me ask you a couple of questions. The temperatures you're quoting here, the 60 to 105 and the 40 to 120, those are ambient temperatures in the room from which you are drawing the cooling air?

MR. REMLEY: That's right.

MR. MICHELSON: Not in the proximity of the component being evaluated?

MR. REMLEY: No.

MR. MICHELSON: Okay.

MR. REMLEY: We have a secondary basis of our design, which is that we will not exceed ten degrees -- now I'm going to switch units on you -- 10 degrees celsius from the input of the cabinet to the venting of the air at the top, and we will not exceed 15 degrees for any given hot spot in the cubical design.

MR. MICHELSON: What was that hot spot temperature?

MR. REMLEY: That can be 15 degrees above ambient, which is 40 degrees fahrenheit, but I -- unfortunately, I switched units on you there.

MR. WARD: We can handle that. That's all right. The hot spot is defined as the air temperature at some locality, or is it a component temperature?

MR. REMLEY: It's the air temperature, not the component temperature. The thing that causes the hot spot tends to be a hotter component. That's the reason we elevate the individual board tests that we do beyond the 120 degrees fahrenheit, because we have to adjust for the fact that we can also have the 15 degree celsius hot spot. So we test everything to that level, and then we make sure that we don't

have any hot spots that will exceed the 15 degrees.

MR. MICHELSON: Now, this 150-degree test that you do on particular boards, I gather, I'm not sure what that means, unless you are saying, in essence, that you don't even approach 150. If you talk about 120 as being your maximum ambient that you can take on an indefinite basis, then you're not really approaching -- then you said you added ten more degrees as the worst hot spot in the cabinet --

MR. REMLEY: Fifteen.

MR. MICHELSON: I thought it was ten. Okay. The worst hot spot is 15. Okay.

MR. REMLEY: Ten is just for the temperature rise in the cubic --

MR. MICHELSON: And you're not approaching -- you could be -- your hot spots could be exceeding 150 fahrenheit, then, when you've got 120 ambient.

MR. REMLEY: The actual number that we use, I think, is 164 degrees fahrenheit.

MR. MICHELSON: One-hundred and sixty-four fahrenheit?

MR. REMLEY: Yes. I need to go back and confirm that, but it takes into account the highest ambient temperature, plus the greatest temperature associated with a hot spot.

MR. MICHELSON: One other question. Now, your

humidity, as long as it's non-condensing, it can be up to 95 percent. Was that determined at 120 degrees operation ambient in the room?

MR. REMLEY: Yes, that's right. Again, the test that's run at the cubical level is a stepped test. It goes through different --

MR. MICHELSON: Well, the only test that really counts ultimately is whatever the cubical will take, because that's where the devices of concern are located, and that's where the cooling capacity, whatever it might be, is located, and that's what counts, finally, is how does a cubical survive in elevated room temperature.

MR. REMLEY: What you see in front of you is the test that we run in the cubicles as a unit, okay?

MR. MICHELSON: Now, you're using the normal cubicle fans for circulating the air, and so forth?

MR. REMLEY: That's right.

MR. KERR: And those numbers are air temperature outside the cubicle?

MR. REMLEY: These numbers are air temperature outside the cubicle, that's right, and humidity outside the cubicle. I was just trying to point out that we run additional tests that are elevated above these, but I agree with you what you're saying: the ultimate test is this.

MR. MICHELSON: Now, the 120-degree test, you claim

it will operate properly for, I guess, some period of time, although you claim that there's a loss of life.

MR. REMLEY: It will operate properly indefinitely.

MR. MICHELSON: Indefinitely.

MR. REMLEY: You will have more frequent failures, and therefore you will have to repair the equipment more often, okay?

MR. MICHELSON: Now, what kind of frequency of failure increase might I expect, or do you know, at 120?

MR. REMLEY: I don't know the answer to that.

MR. MICHELSON: In other words, if the frequency of failure was every minute, it might be a little troublesome. If it's just increased to a matter of days or weeks, it might not be so troublesome.

MR. REMLEY: It's just that we need a basis for our reliability calculations, so we choose the normal temperatures for that.

MR. MICHELSON: My thrust is more from the viewpoint of the effect of an environment and its effect on reliability.

MR. CARROLL: Not having a psychometric chart in front of me, what's the 95-degree wet bolt temperature limitation due to the 95 percent humidity?

MR. REMLEY: I think that's what you can physically achieve. You know, I don't think you can physically achieve anything beyond that.

MR. CARROLL: At 120 degrees? Sure you can.

MR. REMLEY: No, it's a --

MR. MICHELSON: I can dump steam into a room, and it'll condense out as extremely microscopic water droplets in the air.

MR. REMLEY: That is what I'm talking about. The basic ground rule here is there is no condensation because you cannot have condensation --

MR. MICHELSON: Okay. If there are no water droplets in the air suspended, then that's right.

MR. REMLEY: That's right. The basic rule is there are no water droplets.

MR. MICHELSON: Okay. Okay. But all bets are off when the water droplets appear?

MR. REMLEY: That's right.

MR. CARROLL: What do water droplets do to this equipment?

MR. REMLEY: They can short together runs on the printed circuit boards, and therefore cause them to become inoperable.

MR. MICHELSON: You are not claiming they would stand even condensing droplets? You're not designing these --

MR. REMLEY: No.

MR. MICHELSON: You could, but you're not designing them for condensation?

MR. REMLEY: That's right, we're not designing them for condensation.

MR. CARROLL: All right.

MR. REMLEY: We never have. That's always been a basis of our design, what I'm showing you here.

MR. MICHELSON: Yes, but you haven't always put these necessarily in areas where there could be a big potential for it, such as close to some of this equipment out on the plant.

MR. REMLEY: That's true. Yes.

MR. MICHELSON: That's the first, I think, although I don't know, and you can correct me if I'm wrong, but I think you're getting them pretty close to the sources of potential high humidity or water vapor.

MR. REMLEY: You're right about that.

MR. MICHELSON. In the control room, you're quite right, I don't think it's a concern.

MR. REMLEY: Okay. The remainder of what's on this chart is the seismic qualification information, and then a point about the -- even though there is no qualification requirement for electromagnetic interference, we have taken care to design for electromagnetic interference, and these are the precautions we've taken.

There is a requirement on Sizewell, and we will be testing to English specifications for electromagnetic interference tolerance.

MR. CARROLL: You mean the security guards with their walkie-talkies aren't going to trip the plant --

MR. REMLEY: That's right.

MR. CARROLL: -- a half a dozen times during start up?

MR. REMLEY: That's right.

MR. CARROLL: Good.

MR. MICHELSON: How about the electrical faults? Since some of this equipment is near fairly energetic switch gear and so forth, the propagation of electronic magnetic radiation from faults in the higher powered electrical system, is it claimed not to be a problem?

MR. REMLEY: We design our signal conditioning boards to meet IEEE surge, okay then that's where any kind of --

MR. MICHELSON 11, I think this is now electromagnetic, not arily --

MR. REMLEY: Okay. Electromagnetic -- I don't have the numbers in front of me, but the whole cubicle design is to protect against that. All the signal conditioning boards are inside the cubicle, and they're all behind this type of protection, and then if the interference is coming in through the cables, we have designed them for IEEE surge withstand.

MR. MICHELSON: In other words, you have adequate filtering in there to take this sort of thing out?

MR. REMLEY: That's right. And we also have

filtering on the power inputs.

MR. MICHELSON: One other viewpoint for solid state equipment. Do you have any understanding of what effect a fire in the vicinity would have in terms of now you've got smoke particles, perhaps ionized, entering the cooling areas in the experiments?

MR. REMLEY: We have never tested.

MR. MICHELSON: Have you ever looked at any of that possible effect?

MR. REMLEY: No.

MR. CARROLL: It probably wouldn't be good, though, would it?

MR. REMLEY: I don't think so.

MR. MICHELSON: No, I don't think you want it, but I just wondered if you had tested it.

MR. REMLEY: We have never run any tests.

MR. KERR: You mentioned that range of environmental conditions as a basis for your reliability calculations.

MR. REMLEY: Yes.

MR. KERR: What sort of goals for reliability do you expect?

MR. REMLEY: The goals that we have for the IPS design are ten to the minus seventh with respect to failures per demand on reactor trip; ten to the minus five, or three -- that's what I'm having trouble with -- with respect -- it's ten

to the minus five with respect to failures per command on engineered safeguards, actuations, and that's per train, all right? For the control system, we have a basis of ten to the minus three failures per command. That's our design basis numbers. We have done studies on the protection system that demonstrate the achieving of those goals.

MR. CARROLL: Really?

MR. REMLEY: Yes.

MR. WARD: The ten to the minus seven is per train, you said?

MR. REMLEY: No. The ten to the minus seven is with respect --

MR. WARD: To the overall system.

MR. REMLEY: To the overall reactor trip function.

MR. WARD: Okay.

MR. REMLEY: Okay. And the ten to the minus five is with respect to the operation of an engineered safeguard.

MR. WARD: Per train?

MR. REMLEY: Per train.

MR. KERR: The ten to the minus seven doesn't include the mechanical part of the trip, but just the --

MR. REMLEY: It includes the breakers. That's about all there is, right?

MR. KERR: Well, the control rods also have --

MR. REMLEY: It doesn't include the control rod.

MR. KERR: Okay.

MR. MICHELSON: This number also incorporates whatever testing and self-faulting features that are built into the system and their reliability?

MR. REMLEY: Yes. There is -- that's right, because there is credit taken for the failures that'll be detected by the diagnostics in the design, and I think the assumption that they used is 90 percent of the failures will be detected by the diagnostics. There is a, I guess, a reset function associated with the fact that you have performed the functional test of the equipment.

MR. MICHELSON: Is the self-diagnostic the main reason why you're getting this high level of reliability?

MR. REMLEY: No. The main reason is because of the fundamental architecture of the design, and I'm going to get into that a little bit down the road here. The diagnostics help, but really the fundamental architecture is the main reason.

MR. MICHELSON: Now, this is working and these numbers are all on the assumption that the environment is still proper for the equipment.

MR. REMLEY: These numbers are based on the assumption of the environment as I defined it as normal. So I'll quickly go over the integrated protection system architecture.

We have already talked about it a lot. There is an element called the integrated protection cabinets which performs basically the signal conditioning and the calculations associated with the safety functions.

These four channel sets interface to the reactor trip switch gear, which is a different configuration than we have on our existing plants, and I'll talk about that a little later. That is a direct hard wired interface.

They also interface to the engineered safeguards actuation cabinets for the system level calculations. These then interface to the logic cabinets over optical data highways. That's the overall architecture.

[Slide.]

MR. REMLEY: This diagram shows the interfaces to external systems. There are interfaces to the integrated control systems, to the main control room, and to the remote shutdown panel. This is where these interfaces come in.

[Slide.]

MR. REMLEY: This is just a different view of the architecture. There are four channel sets of protection equipment; a minimum of two trains of engineered safeguards, although the system can be expanded to handle up to four trains. The control board multiplexing, the interface of the remote shutdown panel, and the reactor trip switch gear.

MR. KERR: I assume that label at the top is just to

confuse you.

MR. REMLEY: It's an unfortunate label, yes. I didn't mean to have that on this slide.

MR. KERR: I think it's probably a clever idea.

MR. MICHELSON: Can you tell me on that drawing if I am looking at anything like a motor control center? Is one of those boxes --

MR. REMLEY: The motor control centers are down here, but they're not really on this diagram. But this cubicle would interface to a motor control center.

MR. MICHELSON: It would be very close proximity to the motor control center.

MR. REMLEY: That would be the idea. This cubicle here would be located in close proximity.

MR. MICHELSON: When I see in a layout drawing a room containing motor control centers, is it highly likely there are also some of these cubicles in there?

MR. REMLEY: Yes.

MR. MICHELSON: Thank you.

[Slide.]

MR. REMLEY: I've included in the -- excuse the diagrams. There's a little bit of a movement around of the RPI cabinets within this architecture. We can either configure the rod position indication cubicles in a safety grade configuration or in a non-safety grade configuration.

What I have up here now is the non-safety grade configuration and this is what we would implement on APWR. We can also implement a safety grade configuration which is this configuration. The only real difference is that we'll go to four-way separation instead of two-way separation and actually we use the same electronics and the same way of interfacing to the detector.

This interface here is a hard wired interface. This cubicle is inside the containment. Coming out will be multiplex datalinks.

MR. SHEWMON: Sir, let me interrupt and take you someplace else for a minute. A long time ago when things didn't have such good electronics or computer capabilities, there was a distinction between control and safety systems. Ten years ago, safety systems tended to lag behind in terms of modern components because, at least we understood, we thought we understood that the older parts, the older ways of doing things.

In fact, the NRC, about a decade ago, had a hard time reviewing the Westinghouse proposal to do some of these things because they didn't know how to evaluate the software and what might go wrong in this and that.

I guess that's a preamble to saying is there still in here a clear distinction between control and safety systems or has that all gone and been subsumed under two out of four logic

and all the same thing?

MR. REMLEY: There is still a clear distinction between control and safety systems.

MR. SHEWMON: And what we're hearing about now is the control system only.

MR. REMLEY: No. You are hearing about the safety system. I didn't mean to cause confusion. If I did with respect to the RPI interface, what I meant was that we have configurations where we can actually configure the thing to be a safety grade piece of equipment and treat it like a safety grade piece of equipment, and others where it's configured to be a piece of equipment that is an important monitoring function, which I wouldn't call a control function in any event.

MR. SHEWMON: You don't have safety system in here once. You do have control systems quite frequently.

MR. REMLEY: The discussion under integrated protection system is a discussion of the safety system.

MR. KERR: Protection is another word for safety in this presentation.

MR. REMLEY: The protection and the control functions are distinctly separated and put in separate pieces of equipment. Now, there is some sharing of information from the protection to the control system that's very closely controlled.

MR. CARROLL: As there always has been.

MR. REMLEY: As there always has been. But there is a distinct separate system.

MR. CARROLL: But what he's saying, Paul, is that they use similar components to do the two functions.

MR. REMLEY: That's right. We use similar design modules, but they are in physically separate cubicles and they are configured in a totally different way.

MR. SHEWMON: Let me ask you a different question, then. After TMI-2, there was an SPDS system specified which sort of people got implemented I hope by now but I'm not sure.

MR. CARROLL: Don't count on it.

MR. SHEWMON: Is that all subsumed into this now or is that still a separate system?

MR. REMLEY: The protection system has not the safety display system. It is the automatic safety actuations. There is information that the protection system has that is given to the display system. As I mention, that's given to the display system over a dedicated optical link here.

That's basically this sensor information. There are some additional calculations, but basically it's the processed information that's being given over to a qualified display system. But it's not a system that is part of the automatic safety functions.

In other word, this arrow goes one way; out. It's

just providing information.

MR. SHEWMON: Fine. Thank you.

MR. MICHELSON: A followup on that same thought now, just clarification. Is it true that there are no control functions performed in any of these cubicles that contain the safety-related equipment and functions? When you say they are separated, in separate cubicles, do you mean you never mix the two functions in the same cubicle?

MR. REMLEY: Yes. That is true. Now, there is only one thing about that that I think we need to discuss; the implementation of so-called qualified controls.

MR. MICHELSON: You're using the old idea of the associated circuits, yet. Is that what you're saying?

MR. REMLEY: No. There are certain control functions which I think are almost classified as safety functions now.

MR. KERR: Carl, it seems to me that we may never get away from this, but one of the very important control functions of a reactor is the ability to shut it down rapidly. You can call that protection system if you want, but the whole thing is a control system.

MR. MICHELSON: He's saying he's keeping control separate from safety and I'm trying to determine what that means.

MR. KERR: I'm simply saying that that's an artificial distinction.

MR. MICHELSON: It becomes important, though, if you start putting in some of these non-qualified control systems into cabinets that are also containing safety functions.

MR. REMLEY: We don't do that.

MR. KERR: I don't think they do that. I think the important thing is the reliability that one can achieve and you need higher reliability for some functions than others. To talk about separation or distinction is just artificial.

MR. MICHELSON: I'm not worried about reliability necessarily than the question that I'm concerned about physical separation in case of those external events.

MR. KERR: But the reason you're concerned about physical separation is because you want a highly reliable system.

MR. MICHELSON: I want one that's protected against fires in certain locations or rods or whatever.

MR. KERR: That's right.

MR. MICHELSON: That's a little different than reliability in the sense of --

MR. KERR: It's not different from reliability at all.

MR. REMLEY: Just to emphasize. There is a separate system here for plant control. I'm going to talk about that after plant protection.

[Slide.]

MR. REMLEY: The nuclear instrumentation for the integrated protection system. We have the traditional, intermediate, and source range detectors. There is four-way redundancy associated with these detectors. There is a four-section for power level detector and -- there's something missing on this picture -- I'm sorry.

There is also an N-16 detector, which I'm pretty sure is on your diagram. It's just missing from this diagram. It's a mistake. Sorry about that. But it's on your diagram.

The only electronics that's not monitored in the cubicles that I have been showing you is this source range pre-amp here which is located near the containment. These modules here are located inside the cubicles that I've been discussing.

[Slide.]

MR. REMLEY: Within the integrated protection cubicles themselves, there is separation of functions into separate microprocessor systems in the cubicles.

There is two computers associated with the reactor trip functions; two computers associated with engineered safeguards functions; a nuclear instrumentation signal-conditioning system, which isn't really a functional computer -- it's just using microprocessor technology for signal conditioning; a trip logic computer; a tester for the functional test of the equipment; and communications interface.

MR. MICHELSON: Where are those located,

approximately?

MR. REMLEY: These are located in the main control room area, these cubicles here.

MR. MICHELSON: Now, when you say "main control room area", that's not quite good enough. It's a big area there, and it might be what you call "main control room area".

MR. VAN DE VENNE: Excuse me. There are two rooms adjacent to the -- or there is really three rooms adjacent to the control room. Two of these are protection-type rooms, and one is a control-type room. These four sets are located in pairs in the two protection rooms.

MR. MICHELSON: Is that what you call the RELAT room?

MR. VAN DE VENNE: Yes. They're called, inappropriately, RELAY room.

MR. MICHELSON: It's a "T", though, and not "Y".

MR. VAN DE VENNE: There's a RELAY Room A, a RELAY Room B, and RELAY Room N. "N" is the non-nuclear and non-safety.

MR. MICHELSON: All right. I see them now. Okay.

So, the RELAY Room A is right next to the diesel engines, just a wall between them. Right?

MR. VAN DE VENNE: Correct.

MR. MICHELSON: That's what it shows on my drawing. Okay.

MR. CARROLL: Is that a piston-proof wall?

MR. MICHELSON: I don't what it's proof.

MR. VAN DE VENNE: It's very important to -- I make the point here, which I believe is an important point, is that the protection system is not a very important system from an external event point of view, because you do not rely on automatic trip in any case if you have an external event. If you had a fire, one would normally expect the operators to trip the plant.

Your protection system is really dedicated, geared toward shutting down a reactor for internal faults associated with reactor cooling conditions and main steam --

MR. MICHELSON: And that's the only thing in RELAY Room A? Is that what you're saying?

MR. VAN DE VENNE: That's right, yes, and also, the qualified data display system, Train A, the two green boxes that were up on the left here.

To the left of the control room, there were two qualified data -- what are they, Gil? Data computers? No.

MR. REMLEY: They're called qualified data acquisition.

MR. MICHELSON: They're over in the computer room?

MR. VAN DE VENNE: No. One of them is in what we called RELAY room A, and the other one is in RELAY Room B.

MR. MICHELSON: Okay.

[Slide.]

MR. REMLEY: This diagram shows the internal separation within the -- within a integrated protection cabinet channel set. So, this picture you're looking at is one of four. Okay? It's not all four. It's one of four. There is internal separation within the individual channel sets. Okay? This was an area of a lot of discussion on the 414 review with the NRC staff, and it resulted in a NUREG, NUREG 0493 for the evaluation of internal separation within this type of equipment. Okay?

There's really two levels here I'd like to discuss. The first level is that there is a separation between control protection and engineered safeguards, and that is that there is a separate computer system for communications, which is really the main interface inside the cabinet for the control system, and then there are two groups of computers for engineered safeguards and then for reactor trip calculations, and you will notice that there are two computers in each group, and the reason there are two computers in each group is we have taken the functions for reactor trip and engineered safeguards and separated them such that independent functions that operate on the same event are separated into two different computers as best we can. This isn't perfect, but we have gone through the analysis and separated these functions.

So, there's two levels here of separation. One is the control protection and engineered safeguards, and then

there is separation of functions within the two groups of computers. Okay?

MR. KERR: Give me an illustration of separation of function, please.

MR. REMLEY: Okay. Maybe that's on the next page here.

[Slide.]

MR. REMLEY: There are physically separate computer subsystems. Even though we call it by -- this is an integrated protection cabinet, it actually is a suite of cabinets and this is what it looks like. You will see the different computer subsystems that I talked about physically separated. They have their own power supply. They operate independent of the other subsystem there. Okay? They're not isolated, but they're physically separated. A failure in here is very unlikely to propagate to here.

MR. VAN DE VENNE: Let me give an example of that kind of -- I think I understand your question.

Every accident, generally, has several trip functions, and what's done here is the primary trip function is located in one computer and the backup trip function is located in the other computer, and if there is another one, it goes in the first -- some events have maybe five trip functions.

MR. KERR: Okay. So, you might have neutron power in one and overpressure in another?

MR. VAN DE VENNE: Right. Right. That's the way it's separated.

MR. KERR: Okay.

MR. REMLEY: From the point of view of the equipment, it's designed so failure don't propagate within it.

MR. MICHELSON: The power supply is one channel of power supply to each of these cabinets. Is that right? One of your divisions of DC power to each of them.

MR. REMLEY: Yes. This is a channel set. This is one of four. I'm talking about separation within a channel set, which doesn't have separation of the power coming in, because the power is done by channel set.

MR. MICHELSON: No, but these four cabinets each have their own dedicated power from a DC source. Your power supply --

MR. REMLEY: It's one source of power.

MR. MICHELSON: AC, rather, it should be.

MR. REMLEY: AC, but it's one source of AC for these four cabinets.

MR. MICHELSON: Right.

MR. REMLEY: It's another source of AC for the next four cabinets and so on.

MR. MICHELSON: Right. Okay.

MR. REMLEY: Now, within the cubicle itself, however, there is a separate power-supply module for a given subsystem.

Okay? So, a failure of a power-supply element doesn't cause more than one subsystem to fail.

[Slide.]

MR. REMLEY: Now, we have actually taken this concept all the way to the signal-conditioning modules themselves.

MR. MICHELSON: Let me ask, just as an illustrative example, in the unlikely event that you lose the power supply to this set of four cabinets, which is a common power supply, if I understood it correctly --

MR. REMLEY: Yes.

MR. MICHELSON: If you just lose it, you go dead.

MR. REMLEY: Yes.

MR. MICHELSON: What is the consequence in terms of anything that can happen out in the plant on that particular division of equipment or on the other division, for that matter? Does everything fail as is, or does everything -- I guess you'd like to say everything fails safe, whatever that might mean in a particular situation, but you've lost all your monitoring and --

MR. REMLEY: Everything has a preferred failure mode in the way we do the design. Okay?

MR. MICHELSON: On loss of power.

MR. REMLEY: On loss of power and on other events, but on loss of power, yes, and for the failure of this particular suite of cubicles, its effect on the plant is

nothing. Okay? Because this is one of four, and we need two of four before we get an actuation. So, for a particular set of cubicles here, there is no effect on the plant.

MR. MICHELSON: And these are four different locations in which these are positioned, different rooms and whatever.

MR. VAN DE VENNE: Two rooms. There's two channels in one room.

MR. MICHELSON: So, then in one room, there are two sets of these, one coming from each of -- its own AC power source --

MR. VAN DE VENNE: Yes.

MR. MICHELSON: -- but it can be affected by common influences in the room.

MR. VAN DE VENNE: Correct.

MR. MICHELSON: And now if you lose that room, for whatever reason --

MR. REMLEY: Then the system will go to its preferred failure mode.

MR. MICHELSON: Now, how does it know what its preferred failure mode is, not knowing what the event might be?

MR. REMLEY: That's a difficult question, but certainly, from the point of view of the reactor trip functions, the preferred failure mode is tripped. Okay?

MR. MICHELSON: Yes. I can understand getting the

rods in, but that's just a small part of the problem.

MR. REMLEY: Okay. I understand. Sure. You cannot predictably dynamically change the preferred failure mode. Now, we have the capability within the equipment to go -- on the engineered safeguard actuation, to go to high, low, or --

MR. MICHELSON: Well, what's bothering me, simply, is if we really -- unless we're highly confident of the ability of these cabinets to withstand what's happening in the room, you would think the cabinets would each be located in their own room with their own controlled environment, so that there isn't a cross-linking of environments between two of the four cabinets. That's the concern. That's why I am pursuing the question.

MR. VAN DE VENNE: Well, remember now, when you get down to the next level of -- the trip function is handled by the fact that it trips. The next level is ESF, and there's really only two ESF trains. So, you don't gain too much by separating these four, because you still get down to the two ESF trains for your engine safety feature.

Now, there are some fail-safe, even in ESF -- I think emergency feedwater actuation is a preferred failure mode of the system. So, you're going to get supply to the steam generators, which in the short term, for most events, is what you need. Now, remember also that if you have an external event, you don't postulate some other internal event, like --

MR. MICHELSON: Unless it's associated.

MR. VAN DE VENNE: Unless it's caused by it, but again, because the control system is yet in another room, you know, you're talking about external events occurring in --

MR. MICHELSON: Have you done such an analysis in which you have taken a catastrophic event in the room with the two cabinets and showed what the consequence is?

MR. VAN DE VENNE: We have gone through that logic, yes.

MR. MICHELSON: Where would I read about that? Is that in a NUREG or --

MR. VAN DE VENNE: That's not in any --

MR. MICHELSON: I'd like to read about it. Where do I go?

MR. REMLEY: The ESF actuation at the system level is two out of four. It's still two out of four.

MR. MICHELSON: Yes. Which two, of course, is -- hopefully, it's not the same two that are in this one room.

Where is the analysis that I might read how this is done?

I'm sure the staff has been interested in it, and they can tell me. Can the staff tell me where I can read about this -- what happens when you have a serious event in one room with two of the four cabinets in there? Has that even been looked at?

MR. NEWBERRY: This is Scott Newberry of the staff.

I don't believe that's been looked at for SP/90 at the PDA stage, no, Sir.

MR. MICHELSON: I think you would be interested in it enough to show that, yes, it's a non-problem. That's all I am asking.

MR. VAN DE VENNE: I believe the defense-in-depth analysis is part of the FDA stage. It's an open item that has to be resolved at the FDA.

MR. MICHELSON: That's something to come later. Is that what you're saying? You think it will be in there?

MR. VAN DE VENNE: Yes.

MR. CARROLL: Okay. We ought to find a convenient stopping place so we can go have some lunch.

Have you wrapped up this --

MR. REMLEY: I'm not even done with the protection system, no.

MR. VAN DE VENNE: How much longer to get the protection system, Gil?

MR. REMLEY: If I would be permitted to skip the discussion on common mode failures -- maybe I can break before that and we could discuss if we want to talk about that or not. Maybe if I can get through the switch gear, at least I have covered the protection -- reactor trip function. There's only two more things there.

[Slide.]

MR. REMLEY: I just wanted to bring up one more point with respect to this separation I was talking about. This separation actually includes the signal-conditioning modules themselves.

So, there are separate signal-conditioning modules for the separation groups that we have within the channel set. For example, there is a separate signal-conditioning module for the communications subsystem if that signal is needed for control. So, if it's needed for engineered safeguards, reactor trip, and control, there will be three separate signal-conditioning modules for the same sensor. So, the separation starts at the signal conditioning.

[Slide.]

MR. REMLEY: With respect to the reactor trip function and the interface of the trip breakers, there is an element in the system known as the trip logic computer, and we have had a lot of discussion with design -- with the NRC staff, but I'd like to quickly go over its concept.

It is basically a filter on the reactor trip function and an avalanche effect on the reactor trip function, and the way it works is that if it only gets one channel set voting to trip, none of the breakers are tripped by the trip logic computer interface to the breakers. Okay? So, it's filtering for one trip function from one channel set.

If two trip functions occur within the four channel sets, then it turns itself around and turns into an avalanche effect and actually tries to trip all eight of the breakers. Okay? So, there are eight reactor trip breakers now, configured in a two-out-four configuration, and the interface between them, which is the trip logic computer, is doing a high level, two-out-of-four vote, which is this filter avalanche effect, and then, down at the trip breakers themselves, there is a two-out-of-four vote going on. Okay?

So, this is significantly different than our current designs, and I wanted to emphasize this. Okay?

We can actually take up to -- we can guarantee we can still trip even if we fail three breakers and, possibly, up to six breakers, we could still trip. Okay? The interface to the trip breakers themselves is both through an under-voltage coil attachment for low voltage and through a shunt trip attachment.

MR. CARROLL: Now, do you also trip the feed from the MG set?

MR. REMLEY: No. We don't trip that directly.

MR. CARROLL: Can the operator trip that in the control room?

MR. VAN DE VENNE: Yes, we have made the commitment as part of the ATWS. We have made the commitment to be able to trip the MG sets from the control board.

MR. MICHELSON: Why don't you want to trip the MG

sets automatically?

MR. REMLEY: I guess the answer is we think we have a sufficiency.

MR. MICHELSON: Well, is there a technical concern about damaging something or just a little extra cost of doing it or what is the crux of the reason why you don't want to kill the power supply?

MR. KERR: Don't you remember that one of the goals, future goals, of the NRC is simplicity?

MR. MICHELSON: Well, you could argue that you could do it even simpler maybe by just killing all the power and then there is no way for the rods to hang in either, but I think you want to do both. There is no technical reason for not doing that.

MR. REMLEY: To my knowledge there is no technical problem --

MR. VAN DE VENNE: The only potential problem, and I really don't think it is a problem, but historically it's caused some problems is that you are interfacing a safety system with a non-safety piece of equipment but there are certain ways that can be done but that would be the only potential issue that I can see. Potentially you could cause more trips.

I don't know whether that is a real issue or not.

MR. CARROLL: Now these eight breakers are identical?

MR. REMLEY: Eight breakers, excuse me?

MR. CARROLL: The eight breakers are identical?

MR. REMLEY: Yes, they are identical.

MR. MICHELSON: These are still switch-gear, aren't they?

MR. CARROLL: DB 50's, I guess.

MR. REMLEY: Yes.

MR. KERR: This avalanche effect to which you referred causes all eight breakers to trip if you've got two trip signals?

MR. REMLEY: That's right. That's done at the higher level, not at the breakers themselves but it's actually done up in the IPC's.

MR. CARROLL: Okay. Does that take us to a good stopping point?

MR. REMLEY: That takes us through the breakers so I think that's good.

MR. CARROLL: All right. Let's adjourn for lunch and reconvene at 1:15.

[Whereupon, at 12:15 p.m., the meeting adjourned for lunch, to reconvene this same day at 1:15 p.m.]

AFTERNOON SESSION

[1:18 p.m.]

MR. CARROLL: Let's reconvene. Gil, do you want to continue?

[Slide.]

MR. VAN DE VENNE: Gil, I think maybe we should wait because Dr. Michelson is not here and he's the one that's most interested in the layout. So I'm sure we would have to redo it if we did it now. So why don't you just continue?

MR. REMLEY: What we'd like to do is go back and talk about the layout again and maybe give you a little bit more coherent answer than we did this morning.

Let's try going back to the overall architecture drawing for the protection system and locate the cubicles in the rooms.

[Pause.]

What I have tried to do is draw the different rooms that this equipment is in and this room here is known as Relay Room A. This room here is known as Relay Room B and they are adjacent to the control room in the diagram, okay? These rooms here with the ILCs are down in lower level, one floor down.

MR. VAN DE VENNE: Most ILCs are in the switch gear rooms.

MR. REMLEY: Switch gear rooms, okay.

Can we show maybe on the overhead, yeah.

[Pause.]

MR. VAN DE VENNE: The Relay Room "A" is here. The Relay Room "B" is here. So cables coming into A come mostly from this quadrant and into "A." They may come in at this level or to the level below which is a penetration room. Cables that come into "B" are coming this way through this corridor which goes through the main steam tunnel which is -- there is a corridor that goes right through it which is closed off.

MR. CARROLL: It's isolated from the main steam tunnel.

MR. VAN DE VENNE: It's totally isolated from the main steam tunnel.

MR. MICHELSON: Is this designed for all the same higher pressure and whatever?

MR. VAN DE VENNE: Right. Yeah.

Now cables leaving "A" primarily go down through the floor to the switch cable below where most of the ILCs are. Cables going to train "B" follow the same route that the cables came in. They go through this corridor and they go down into switch gear room "B" where most of the ILCs are.

Now, ILCs actuate switch gear primarily. Most of it's switch gear. There are also some solenoid valves that could be actuated or some -- yeah, mostly solenoids and these ILCs could be located for instance in the penetration room but

there wouldn't be many of them, maybe one, in each train.

So that's primarily how the -- now, of course the relay rooms interface with the control room basically directly. So the control room is of course the place where it all comes together.

MR. CARROLL: While we're looking at drawings, where's the remote shutdown?

MR. VAN DE VENNE: The remote shutdown panel -- actually in this case, panels -- are down here, one and three in "A" and one and three in "B." So again, cables from "A" come down. Cables to this division run horizontal above and then come down somewhere in this area and go to this. So there is a separation here, fire separation between "A" and "B."

MR. MICHELSON: Does it take two operators, one in each of those two rooms, to do the shutdown?

MR. VAN DE VENNE: Yes. The -- we've had a lot of internal discussions on the emergency panel and whether it should be in one room or in two rooms with communication between each other and it depends really -- if you postulate a fire say in here, you would normally depend on the main control room to continue to operate and you really wouldn't use this.

MR. MICHELSON: I hope that there's a real good barrier then because the main control room is immediately above that --

MR. VAN DE VENNE: Right.

MR. MICHELSON: -- area where the fire is and that means all the -- whatever penetrations of cabling through the floor and everything are, are real good.

MR. VAN DE VENNE: Yes, there has to be.

MR. MICHELSON: Yeah, yeah. Now the question though on the emergency panel rooms, you do have to position one person in each room --

MR. VAN DE VENNE: Yes.

MR. MICHELSON: -- with communication between the rooms to shut down --

MR. VAN DE VENNE: If you shut those rooms, that's what you would have to do, yes.

MR. MICHELSON: Now do you have to use both rooms?

MR. VAN DE VENNE: You could shut down a plant from one but if you had both available, I think you would do it from two.

MR. MICHELSON: The more important question is the first one then, the statement. You can shut down safely from only one of the two emergency panel rooms?

MR. VAN DE VENNE: Correct. Yeah. Because the design basis shutdown is using a single train, a single division of safety-related equipment. That's the design basis but if you have both available, you'd like for instance to feed all generators.

MR. MICHELSON: Well, I don't know what's in each of

course. In most shutdown emergency situations, there are certain things you've got to inactivate and so forth and some of that's done from that remote panel and locked out from the control room and whatever and I don't know how that's all divided up. I don't try to ask the question.

MR. VAN DE VENNE: The transfer from main to emergency control, I don't know how that's handled.

MR. REMLEY: There is no physical transfer. I mean, it's just a --

MR. MICHELSON: What do you do about the fire in the control room producing unwanted actions that you, normally in the old days we locked these out from the emergency --

MR. REMLEY: It's all done with logic inside the ILC cap and you can just tell that you're now in charge. There's no physical switching.

MR. MICHELSON: That cabinet is located where?

MR. REMLEY: Right there in the --

MR. MICHELSON: Well, that's where the fire is.

MR. REMLEY: Well then you've got the other train. If you lose that train --

MR. MICHELSON: Okay.

MR. REMLEY: To take control from the emergency shutdown panel, it's just a logic function inside the ILC. So you just tell it you're now going to control. There's no physical switch.

MR. MICHELSON: And you do that from this emergency panel?

MR. REMLEY: Yeah. You do it from the emergency panel.

MR. MICHELSON: And once having told it that, it's now -- can burn up or whatever and you're still okay.

MR. REMLEY: It's going to ignore everything above. All the signals from above it's going to ignore. It's just going to listen to the emergency shutdown panel.

MR. CARROLL: When you say "above," you mean from the control room?

MR. REMLEY: From the control room and from the automatic safety actuation. Here, let me -- what we're talking about is the direct connection, directly into the ILC here. So what I'm saying is, it's going to ignore all the higher level.

MR. CARROLL: Could you raise that a little bit?

MR. REMLEY: It's the direct connection that's indicated here into the ILC. That's the remote shutdown panel. That's the ILC. These are the system level actuations and the main control room interfaces that come in on this optical highway to the ILC. This comes around that whole thing and comes directly into the ILC. So you've direct control to the ILC and it's basically going to ignore all the higher level commands, all the other commands, if you take control here and there's no physical switch involved. It's just a logic

function.

Now, what I was going to talk about in addition to getting straight where the cubicles were, is also how the logic works. In other words, what we were postulating this morning was that we would lose, say, room "A" here, okay? What would happen? That would cause a reactor trip to occur because when we lose these two channel sets, you're going to get a two out of four configuration right at the breakers and it will trip the plant.

MR. MICHELSON: Of course, you have to demonstrate that for whatever the cause of loss might have been for all cases that you're designing for.

MR. REMLEY: Yeah. That is really analysis of the fail-safe design aspects of the IPCs.

MR. MICHELSON: Right.

MR. REMLEY: Yes. That has to be demonstrated that that's the basis that you do that, okay?

MR. MICHELSON: So it -- it takes care of itself before it's completely gone. That's what it has to do. It has to have enough logic left to know to --

MR. REMLEY: In fact, what happens is, is there is a power converter module that is the last thing before the output to the switch gear and it is being fed by a logic bus which operates dynamically. So if this logic bus is not updated by the microprocessors within several hundred milliseconds, it's

going to just take away the signal.

It's going to drop the signal, okay? That's the basic idea behind the fail-safe design.

MR. MICHELSON: But that device that does the dropping has to itself not be affected by what's causing all of this to occur.

MR. REMLEY: Yes. Yes.

MR. MICHELSON: At least long enough to safely perform an action and then quit.

MR. REMLEY: That's right, and then with respect to the engineered safeguards actuations, you still have train "B" engineered safeguard system level actuation in operation because we've taken out Room "A," okay? Now, it gets its information from Room "A" and Room "B." Two of the channel sets have optical data links that are indicated here, I guess, here and here, that come into the train "B."

Now, what's going to happen there is that those data links are also dynamic and also have checks built on them and the logic in the ESFAC actually has an automatic bypass built into it. So, it's a two out of four logic with a bypass. We've described this bypass in the RESAR 414 design. It's the same design.

So really, the logic will be, if you take out these two channel sets, you will really be in a one out of two condition with respect to the logic in train "B," okay? So

you're still in a one out of two with respect to an actuation that can come from either channel set that's left in Room "B." So it's changed the logic from two out of four to one out of two based on the fact that it detects that these two data links are failing.

Again, this has to be demonstrated to be true, that they are designed in the same way, the interface to the switch gear which is in the fail-safe way.

MR. MICHELSON: Depending on the physical arrangement of all of this, you have to show that the physical involvement of that first room does not in any way affect the functionality of the other -- the equipment in the other room, because you're counting now on a one out of two in error --

MR. REMLEY: From an I&C -- from an I&C equipment point of view, we can show that. Now, if you're talking about something going through the wall from one room to another, that's different.

MR. MICHELSON: Well, we're talking about environmental propagation through the ventilation ducts or whatever.

MR. REMLEY: Okay, something propagating. There won't be any propagation in the I&C equipment, I can make that statement.

MR. MICHELSON: Um-hum. That should certainly be the case.

MR. REMLEY: Is that a better explanation a better explanation?

MR. MICHELSON: It helps, but I'm not sure it still highlights the close proximity of the switch gear rooms to the control room and the diesel generator room to the control room and that is not settled, but I understand where this material is --

By the way, as long as we are on that subject; the diesel generator room really has barrier doors swinging open from the room? That's the way the drawing shows it. Is that really the case?

MR. VAN DE VENNE: I can't really answer that. I've noticed that, too, and that probably should be the other way around.

MR. MICHELSON: Well, at least from the viewpoint of designing those doors, it's pretty tough to design them to old much pressure if they're swinging outward. The other thing is; the relay room now, Relay Room A; how do you get into it?

There seems to be a door to the control room. Is that the only door?

MR. VAN DE VENNE: The intent is to have an equipment door that is permanently locked.

MR. MICHELSON: That's next to the stairway?

MR. VAN DE VENNE: Yes, that would become not in the corridor, but that would --

MR. MICHELSON: Well, that's not a door in a normal sense?

MR. VAN DE VENNE: No, we would consider that to be the same barrier as a wall.

MR. MICHELSON: Okay. So there is just one doorway into those rooms?

MR. VAN DE VENNE: From the main control room, yes.

MR. MICHELSON: Okay.

MR. CARROLL: That wouldn't be legal in California.

MR. VAN DE VENNE: Is that right?

MR. MICHELSON: You don't want any room with just one door; do you?

MR. VAN DE VENNE: Then as far as ventilation, I mentioned that the 2 ventilation systems for the 2 areas are separate ventilations systems, and of course, Room B, Protection Room B has to be connected to that other side of the building with that ventilation.

Train A has its own ventilation system and the main control room has its own ventilation system and Train B has its own ventilation system and there is a duct that has to be brought over from left to right, or on the picture, to connect that one room to that ventilation system.

MR. MICHELSON: Well, when you say Train B, you mean the many components of Train B, both the pumps and so forth as well electrical components?

MR. VAN DE VENNE: Yes, right.

MR. MICHELSON: Those are all inter-tied by a single duct system?

MR. VAN DE VENNE: No, that's not true because the electrical components and the I&C components are on one ventilation system. There is what we call a switch-gear room ventilation system, A and B. There is also an emergency feedwater ventilation system A and B.

MR. MICHELSON: Well, let me reduce it a little bit. In the case of a fire a switch-gear room, you will ventilate into -- in the A switch-gear room, you would get into the A Relay Room through the same duct, but you would not get into the control room?

MR. VAN DE VENNE: You would not get into the control room and you would not get into any of the B rooms.

MR. MICHELSON: Okay. I think that helps, yes, thank you. Just as a slight aside, but still on the same questioning, apparently, in part, at least, you were influenced in putting the diesels where you did because of Japanese desires or layouts or whatever.

Do the Japanese also use -- let me ask it differently. What kind of fire protection to the Japanese use and are you going to adopt the same fire protection features? See, the susceptibility of this arrangement is, in part, at least, influenced by what your fire protection philosophy is

going to be.

Are you going to use the same philosophy that they use, whatever it is?

MR. VAN DE VENNE: We haven't really reviewed that to the level of detail that we can say affirmatively, but I think eventually that the diesels will be moved for that simple reason that from a maintenance point of view or from a replacement point of view, are at a very inconvenient location because they happen to be 2 floors above grade.

MR. MICHELSON: Yes.

MR. VAN DE VENNE: We think that in the long term, we will just move them off and put them in their own building, but I don't believe that that is fire protection that's the reason there; it's maintenance.

MR. MICHELSON: For the PDA, where they are now, perhaps you're saying that by FDA, you might change it or something.

MR. VAN DE VENNE: Yes, right.

MR. MICHELSON: We'll have to assume for the moment that they stay where they are, though.

MR. VAN DE VENNE: Right, right.

[Slide.]

MR. REMLEY: I would like pick up then at the engineered safeguards actuation cabinets. These are train-oriented cabinets. All Trains -- or in this case, A and B --

receive information from the 4 channel sets over separate optical datalinks from the 4 channel sites. As a matter of fact, they actually have links from the 2 engineered safeguards computers in each channel set, so there are actually 8 optical datalinks.

The internal architecture of each engineered safeguards actuation cabinet is redundant. Maybe I will move to the next diagram to show that.

[Slide.]

MR. REMLEY: There are 2 computers basically running in parallel that do 2 out of 4 logic for the system level actuations in parallel. As I mentioned, this 2 out of 4 logic includes the concept of a bypass, so that if one of these links is lost, it assumes that that particular input is not bypassed in the logic.

This goes from a 2 out of 4 to a 2 out of 3 to a 1 out of 2 type logic as it degrades, okay? The output of these 2 subsystems then go out on the optical data highways to the logic cabinets, so there's no real signal or control interface associated with these cubicles.

MR. MICHELSON: When you say that it goes out on a highway, does that mean that it goes out on a somewhat dedicated optical fiber, or does that mean it goes into some further mixing process and the result of the mix goes out on an optical fiber? In other words, how much dedication of

individual fibers is there involved in this case?

MR. REMLEY: Okay, serial multiplexing is a time division multiplexing of data. You know, the way you convey the information from one piece of equipment to another is over a serial bit stream that changes in time.

MR. MICHELSON: Yes.

MR. REMLEY: You can have that in a dedicated communication link between one point and another, and that's usually called a point-to-point link. Now, with the data highway, you do that kind of communication, but then you also time division multiplex the points so that you can have many or several transmitters and receivers on the same physical cable.

MR. MICHELSON: Yes, the same cable is carrying a number of other circuits on a time-sharing basis.

MR. REMLEY: That's right, that's what this is.

MR. MICHELSON: Okay, that puts --

MR. REMLEY: It is effectively a single cable to start with, okay, but then it is redundant so there are two. Now, with fiber optic transmission you need a transmit and receive, as opposed to coaxial transmission where you can have the transmit and receive on the same physical cable.

So now you have 4 physical cables, okay. Now, the particular implementation --

MR. MICHELSON: You're saying you're transmitting over 2 and receiving over two?

MR. REMLEY: That's right.

[Slide.]

MR. REMLEY: Now, the particular implementation that we use is a passive transmissive star coupler which is indicated by this box here. This box then has a transmit and a receive for every node on the highway. There will be a physical pair of cables for that.

It is a radial architecture, so the number of cables ends up being, for every star coupler -- and you need 2 cables for every node on the highway. In our designs, we normally have this being redundant so you'll have 2 sets of those. The answer, I guess -- and that's a complicated answer, but the answer is that it is 2 times the number of nodes, time two, because it's redundant.

MR. MICHELSON: So you end up with a minimum of 8 cables on the highway?

MR. REMLEY: It depends on how many ILCs you have in your implementation. Normally for a safety train, we have between 8 and 10 ILCs. Okay, so let's say we have 10; that's the worse case. So, we'd have 10 -- well, let's try 8 because it will be easier to count.

Eight plus 1 more plus another one is 10 times 2 is 20 times 2, because it's redundant; it's about 40 physical cables.

MR. MICHELSON: Forty cables and how are they

physically separated from each other -- to what extent? Are they in one conduit.

MR. REMLEY: Well, normally, we put them in conduits.

MR. MICHELSON: I know, but how many conduits? All in one conduit?

MR. REMLEY: We could. The fact is that this is all one train. From a safety point of view, you could put them all in one. But that's not a normal --

MR. MICHELSON: But it is conceivable that they could be in one conduit, although what --

MR. REMLEY: It's not a good practice. We would put them in two because we would want each one being associated with each one of the transmissive stars that we're using. Two would be the logical number to me, because you do have this single point of failure here with this star.

Even though it's passive, you could physically destroy it.

MR. CARROLL: The piston coming out of the diesel generator?

MR. REMLEY: Yes.

MR. MICHELSON: I hope these aren't in the diesel room.

MR. REMLEY: No, I quickly put them up in Relay Room A and B there.

MR. MICHELSON: How susceptible, if at all -- are you

going to tell us how susceptible these cables are to elevated temperature or water surrounding the cable or that sort of thing. In other words, what do you really have to worry about in terms of external hazards?

MR. REMLEY: I can really only give you a gut feeling answer, but you know, they are glass and they're completed passive and they should be able to work under water. There's no reason I can think of why they can't work under water.

MR. MICHELSON: That's what I wondered; do you really worry about water getting into the conduit?

MR. REMLEY: No.

MR. MICHELSON: Do you worry about a fire under the conduit?

MR. REMLEY: Well, fire; if you physically --

MR. MICHELSON: If you melt the glass --

MR. REMLEY: -- separated it, you know.

MR. MICHELSON: If you don't melt the glass; if you don't get it that hot and you're a little further away from fire, is there any problem of elevated temperature up to the point of melting the fiber?

MR. REMLEY: No. The performance of the cable is not based on temperature, unless you physically destroy it.

MR. MICHELSON: There are tests that verify that that is, indeed, the case?

MR. REMLEY: Yes.

MR. MICHELSON: Thank you.

MR. REMLEY: Okay. So, the engineered safeguards actuations cabinets also have an integrated tester, which is going to perform the functional tests for this train, starting with the engineered safeguards functions, down through the logic cabinets, so all the way through to the logic. Complete test of the train, then, is done, in a functional sense, by this tester, and then there is a communications subsystem for making information from the train available to the data-acquisition equipment.

[Slide]

MR. REMLEY: This is what, physically, one of these cabinets would look like. The A computer and the B computer, which are running the same logic in parallel, the communications computers, and the tester computer.

[Slide]

MR. REMLEY: The system-level signal are then transmitted on the optical highway to the logic cubicles.

Now, I'd like to defer the discussion of the logic cubicles until the topic called the integrated logic system, which I will cover after the control system. The reason I'd like to do that is because the design is really common to both systems -- not physically common but, in concepts, common.

[Slide]

MR. REMLEY: You asked me before about the basis for

the reliability of the system, and I gave you the numbers, and I mentioned that we had done studies to verify those numbers.

So, usually, what happens is, when you get into the protection system, you end up with a discussion of a common mode failures, and I've tried to put together a thought about this, because it always comes up, and I'd like to try to give you a little bit of philosophy about the way we have approached this.

I guess the first point is we believe that there is no single solution to the problem. So, we have tried to attack it sort of in a multi-dimensional way, and I have tried to indicate here what I think are some of the key points that we built into the design to address the issue of common mode failures.

We have talked about the concept of what I call functional diversity, and that goes back to the reference to NUREG-0493, the separation between the control protection and engineered safeguards functions that are in the design. Okay? And then the further separation about the independent functions that operate on the same event being separated within the protection system. Okay? We very carefully looked at that in the design process and implementation.

We have put into our designs an integrated functional tester, and we believe there is a lot of advantage to this from the point of view of testing this equipment without requiring

to get your hands into the racks and modify the actual subsystems that are performing the safety functions. The man is not required to do that. He goes to a separate interface panel. He basically turns on a key and pushes a button and looks at a printout. So, his interaction with the safety equipment to test it is very minimal. I think this really improves the potential for problems of degradation of the protection system.

I'd like to come back to end, to the verification and validation program.

We've talked about the fact that, in the implementation, we are using fail-safe design principles with respect to how we do the implementation details. So, we're looking at the way the equipment is going to fail in a microscopic level when we're looking at how we're going to do the final implementation of the design.

MR. MICHELSON: When you look at failure modes of this equipment for degraded conditions, do you look at, for instance, experiencing degraded voltage, such as more voltage than you wanted, or less?

[Slide]

MR. REMLEY: Yes. We have a special module that is really part of the computer subsystem that is a diagnostic module that is monitoring vital information about the cabinet. One of the things that I mentioned already was temperature.

Another thing that it monitors is the voltage that's available to the computer bus. Okay? And the computer can only operate under its specification under -- you know, a certain degradation of voltage it can tolerate, but after that, its operation is not guaranteed.

So, above that threshold, this particular module is designed to reset the computer bus. Okay? So, effectively, what it does, it stops the computer from operating if it's approaching the minimum voltage that it needs to operate, and it will hold at reset until it sees the voltage goes back up to the proper level.

Now, the interface between the computer subsystem and any I/O -- we have to go on a case-by-case basis, but failsafe design principles are considered in that implementation, and it is always the case that if we lose the operation of the computer, the output will take the preferred failure mode action. Okay? So that if we stop the computer, then, for example, the interface to the switch gear is going to cause a trip.

MR. MICHELSON: If tripping is what you're interested in, that's fine.

MR. REMLEY: Yes.

MR. MICHELSON: You have a diagnostic circuit, then, that does this. The diagnostic circuit, I guess, has to be designed to operate over a much broader range of voltages, so

that it can properly function when you see the degraded voltage, since the power is all coming from the same source. In other words, the diagnostic equipment sees degraded voltage at the same time the rest of the cabinet sees it.

MR. REMLEY: Yes, that's true.

MR. MICHELSON: Is it designed, then, to operate over a broader range of voltages properly?

MR. REMLEY: Yes.

MR. CARROLL: Your example was low voltage. Does it also deal with high voltage?

MR. REMLEY: Yes. It will make sure the voltage is within a band, and if it doesn't see it, it will reset the microprocessor, and resetting the microprocessor just stops the operation. In general, we have watchdog timers that are associated with the interface to the microprocessors, and when they see the stop of operation or the stopping of the dynamic update, they'll take some preferred failure action -- a preferred action under the failure.

MR. MICHELSON: How can it take the preferred action if it's -- unless that circuit is also designed for the degraded voltage?

MR. REMLEY: That circuit would be getting its power off of another supply.

MR. MICHELSON: Yes, but all the power to the panel comes from the same source, and it's the source that's gone

bad, not the power supply in the panel.

MR. REMLEY: It doesn't make any difference. A loss of power -- we have to get into the individual boards.

MR. MICHELSON: Degraded not lost. Degraded voltage on the AC bus supplying the panel, and it also supplies the other panel, by the way. In fact, it supplies a lot of other things.

MR. REMLEY: We need to get into the design.

MR. MICHELSON: Okay, but you're accounting for all that in the circuits that monitor all of this and take appropriate actions. Those must function under the degraded voltage --

MR. REMLEY: Or they fail in a way that is safe. They either operate or they fail in a way that's safe. Okay?

MR. CARROLL: Or fail someplace in between.

MR. REMLEY: It's much easier to control these final actions than it is the operation of the computer. That's the reason -- the reason you want to shut off the computer is there are -- basically, it's very difficult to analyze how it's going to perform in a degraded voltage, so you do want to shut it off, but these other circuits, you can analyze how they are going to operate, given degraded voltage.

MR. MICHELSON: Has the staff completed its SER on the instrumentation and control portion?

MR. DONATELL: The chapter on the instrumentation and

controls is written in the draft SER. However, frankly, the important things, such as verification, validation, in-depth defense, that sort of thing, is left open to the FDA stage, and certainly, the software control and these sorts of things --

MR. MICHELSON: So, for PDA purposes, you feel the SER is finished.

MR. DONATELL: That's correct.

MR. MICHELSON: But for FDA purposes, there would be a whole lot more to do.

MR. DONATELL: Absolutely. The real work would have to be at FDA stage.

MR. CARROLL: Now, one of our colleagues, Loren, continually questions whether the staff has the capability of looking at this sort of stuff. Can you comment on that? One of our colleagues not present.

MR. DONATELL: That's probably good. No.

I asked that question -- the gentleman that was with me had to leave, but he -- his response was that, one, there are adequate standards and guides that, if designed to and followed, would meet the intent of verification and validation. In fact, in Chapter 7, one of the open items under V and V relates to one of those.

Outside of that, I think we'd have to go a lot deeper to assess whether that strong capability is really there or not.

MR. MICHELSON: I think those standards, you will find, are written in terms of maintaining normal environmental control around the equipment, which is now going to go through this -- whatever the standard says it must go through.

MR. DONATELL: I suspect that's true, yes, Sir.

MR. MICHELSON: We're not talking about that problem. I'm less concerned about it than I am when we get these external events occurring, which you do have to analyze under IPE or somewhere. It's not clear that the plant is designed for it, so it's going to be tough to show that it will --

MR. DONATELL: I think, in general, the V and V issue is a very large issue, just under normal operation, and when you start getting into a system of this type, it's going to be extremely difficult. I think that's recognized that one is going to be difficult.

Whether, at this point in time, we have people onboard that can handle that, I don't have the answer to that.

MR. CARROLL: To the extent you have looked at these issues, this was all done with inhouse NRC staff, or did you have any consultants or National Lab people working on it?

MR. DONATELL: I'd have to make a guess on that. I don't know if that particular chapter was contracted out or not. Some of the work was contracted; some was not.

MR. REMLEY: I could speak to that a little bit.

We're using the same principles for the verification

and validation that we used for the RESAR 414 system. That system was reviewed by NRC staff and with consultants from the Oak Ridge National Laboratory, when they did the review.

MR. MICHELSON: Did they include the severe environment conditions?

MR. REMLEY: No. That wasn't an issue of verification and validation. That was an issue of qualification. I do agree, though, that there is a connection that you're making associated with the integrity of the diagnostics and the details of the design in the system.

The other point I want to make is that we do address qualification when we do the design and do the qualification testing. That is traditional for our safety equipment.

We have added features in this design that we think are important in the big picture, and our experience shows us that are important, and that is this design is designed for maintenance, to minimize the amount of interaction that the I&C technician needs to have in order to maintain this equipment and to build in diagnostics in the equipment, so that he can, even externally, understand what has failed and get in there and fix it and get back out again quickly.

Again, this gets into a detailed discussion, but we have considered this in our design.

This leaves one aspect that I want to spend a little more time talking about, which is verification and validation.

MR. KERR: Excuse me, but somehow I missed the significance of the big box in the middle. I thought you were going to say more about that. Were you?

MR. REMLEY: The point was that in order to address -- it's my belief and, I think, from what I have learned working in Westinghouse, there is no single solution to the problem of common mode failures, and that's what all that is supposed to mean, is that you need to look at this problem in a global sense and you have to consider a lot of factors and there have to be tradeoffs made, sometimes, between these things when you're considering the design and trying to worry about issues of common mode failures. That's the issue with the big box in the middle.

There is a danger on getting a mindset that there is a single solution to the problem.

MR. KERR: I don't know of anybody who thinks there is a single solution. Maybe you do.

MR. REMLEY: Yes, I do. People think that this is the single solution to the problem. Okay?

MR. KERR: Let me dissociate myself from that group.

MR. REMLEY: Okay. There are people that think there are single solutions to the problem.

MR. KERR: I'm not sure there is multiple solutions to the problem.

MR. REMLEY: That may be.

MR. KERR: But I do think there isn't a single one. I do think that one needs to look at it, and this is what I was curious about. Other than being aware of it, have you done anything concrete or tangible to try to make it unlikely?

MR. REMLEY: Yes. I think what I am trying to say is that, from our experience, we believe that these are things you need to concentrate on -- now, I'm considering myself in the scope of the I&C equipment, not the whole plant, right now, when I'm talking -- to make sure you have addressed key issues associated with common mode failures. You need to look all these areas very carefully. That's what I'm saying. We believe these are important areas, and we have addressed them carefully in the design of the IPS.

MR. KERR: Now, when you do your reliability analysis, how do you account for common mode failures? Do you use the beta-factor approach, or do you ignore it?

MR. REMLEY: The numbers I quoted do not include the common mode failures. Okay?

MR. KERR: Oh, they don't?

MR. REMLEY: The 10 to the minus 7, no, for reactor trip, no, does not include common mode failures.

MR. KERR: I don't see how you could attach a lot of credibility to the numbers if they don't include some consideration of common mode failures.

At this level of reliability, common mode failures

may be the most important contributor.

MR. REMLEY: I agree with that. But you still need to do the other analysis that shows your basic design is okay.

MR. KERR: Well, that doesn't show that your basic design is okay.

MR. REMLEY: With respect to the overall architecture. I think you need to do that other analysis, which doesn't really factor in common mode failure, because, to me -- and I'm not saying you don't do the analysis that does factor in common mode failure, but you don't want to mix the two things together because I think you'll create a lot of confusion.

You need an analysis which is strictly based on random failures of components. I believe you need that.

MR. KERR: Of course, but you also need to look carefully at what you think the contribution to common mode failures is likely to be.

MR. REMLEY: I agree with that, too.

MR. KERR: Have you done that?

MR. REMLEY: Yes.

MR. KERR: In a quantitative way?

MR. REMLEY: No. We have done it in a qualitative way and this is what I'm trying to talk about now. It's qualitative.

MR. KERR: Okay. Qualitative --

MR. REMLEY: Based on our experience.

MR. KERR: Qualitatively, how much change do you think it will produce --

MR. REMLEY: You're asking me to interpret qualitative into quantitative and I'm not prepared to do that.

MR. KERR: Do you think it will reduce the -- will increase the unavailability by a factor of ten, two orders of magnitude?

MR. REMLEY: My belief is it's two orders of magnitude, but I can't -- I would have a very difficult time justifying that.

MR. KERR: I'm not asking for a rigorous.

MR. REMLEY: My belief is it's two orders of magnitude.

MR. CARROLL: Now, this got to be an issue with Brookhaven on looking at the PRA, right?

MR. REMLEY: I can't answer that.

MR. VAN DE VENNE: Yes. It got to be an issue -- if you go back to the PRA, the -- I still believe that if you look at the numbers carefully that the IPS is really not that limiting within certain assumptions. On ATWS, it's still the mechanical liability of the rods that finally is going to get you and it really doesn't make too much difference whether the trip function is ten to the minus five or ten to the minus six because there is a backup trip from the operator.

And even if you assume fairly poor operator reliability, it's the mechanical liability of the rods that's going to get you. Now, the only other area that you have that is very sensitive is emergency feed or the whole issue of decay heat removal.

Because the emergency feed is really or the feedwater to the generator is -- the first line of defense is the startup feedwater system which is actuated from the control system. So you've got one set of reliability there.

Your second actuation is the emergency feed from the ESF actuation. That's your second level of defense. Your third level of defense is your emergency feed actuation from AMSAC, which you didn't put in there for that purpose, but it's there.

In other words, AMSAC, on yet another input signal, will start the emergency feed. On top of that, you have a possibility of operators starting emergency feed and you have an operator initiating feed and bleed.

So you've got so many levels of defense there that even if one is only like ten to the minus three, all of them together, I think, still can get you to adequate decay heat removal.

Most other events that you protect against are a low power build, the mechanical systems aren't really that reliable. So they are not limiting from an emergency -- from

an actuation point of view.

MR. CARROLL: Have you come to closure with Brookhaven on this issue or is it still --

MR. VAN DE VENNE: Not really, no. Not really.

MR. CARROLL: That was my question. V and V, oh boy.

MR. KERR: Excuse me. I think those comments are relevant, but they are relevant only if you're convinced that the trip system is fairly reliable. You're assuming that it's considerably more reliable than is the mechanical system.

Now, that is true only if you have properly taken into account common mode failures for the trip system. Perhaps you have, but it does not make sense to just assume that you have because your random failures give you a high number.

MR. VAN DE VENNE: The thing is, though, in the PRA for -- we assumed the trip reliability and it was three times ten to the minus five, which is really not all that optimistic, I believe, personally.

We can argue whether that's optimistic or not, but that's not --

MR. KERR: The problem with three times ten to the minus five is that neither you nor I can never demonstrate that it's achieved.

MR. VAN DE VENNE: Yes.

MR. KERR: Let's take --

MR. VAN DE VENNE: And based on that, the ATWS

contribution is pretty small. It could get even worse than that and still not be very dominating. It's only a few percent of the total, I think. Then when you go from the ATWS to the containment failure frequency, which is really what you're after, it's a very low probability.

The things that really kill you in the PRA are station blackout and loss of cooling. I'm purely relying on operator action during those events. Those are really the things in PRA that when you look at the bottom line, what is containment failure frequency, I believe 98.some percent is due to those two events.

So that's really the bottom line. Those are the two events you have to work on. Also, when you get to external events, that's really what it's going to be. It's going to be operator action and it's not these systems.

The information systems are important. The operator has to see what's going on. But the automatic actions --

MR. KERR: That assumes that that shutdown frequency or shutdown unavailability is somewhere around ten to the minus five.

MR. REMLEY: Yes.

MR. KERR: If it is, then I agree. What you say makes sense.

MR. REMLEY: On blackout, the first thing that happens is the rods are going to go in because there's no

power.

[Slide.]

MR. REMLEY: I guess on verification and validation, I would first like to start out with at least the definitions of the words the way I am going to use them and the way we use them in Westinghouse. And I think they are consistent with the definitions that are in the standards.

So verification is the process of determining that the successive steps in the design process are correct. And that is, that they meet the requirements as defined in the previous step. So it is a step by step activity.

Whereas validation is taking the final product and seeing that it meets the original requirements that you set out for the system.

[Slide.]

MR. REMLEY: There are a significant number of standards in this area. And these are the ones that we've considered in our program, as a minimum, in the program that we put together for the integrated protection system.

MR. KERR: With the exception of 730, and I guess 1012, I was going to say those really deal primarily with hardware.

MR. REMLEY: No. Most of these are oriented, I think every one of them is oriented towards software base systems.

MR. KERR: But they don't tell how to verify

software, do they? They tell how to put it together.

MR. REMLEY: You are right in the sense that they tend to lean a lot toward constraints on the design that will lead to a product which is a more verifiable product. That's true. But they also give you some guidance as to what you should do in verification.

I mean, I will agree that there is a lot of flavor of constraints on the design in these standards.

MR. KERR: Does Westinghouse have any good ideas independently of these standards as to how they can make certain that their software is always going to do what it is designed to do, or does it depend on the standards?

MR. REMLEY: No, we have put together a separate, we have used the standards as a basis to produce our own programs.

[Slide.]

MR. REMLEY: And we have something called the I&C development engineering D&D program, which really captures our philosophy, we've written this ourselves. And then in addition to that, we have individuals plans for a specific system.

For example, in the integrated protection system we have a software verification plan and a hardware verification plan and a system verification plan and a system validation plan. We have written all these ourselves, to do the specifics of how we are going to do it.

MR. KERR: Correct me if my memory is wrong. It may

be. But it seems to me that it was a Westinghouse program, or was it a program used on Westinghouse plants with seismic designs, which after a good many years was discovered to have errors in it which caused a lot of concern about a fairly large number of plants.

MR. WARD: Stone and Webster.

MR. KERR: Okay. So Stone and Webster didn't have your expertise available to validate and verify their software.

MR. REMLEY: I can't answer that. I don't know.

We used the standards. We reviewed them. But we put our own programs, or say philosophy, and individual plans together. So we do do all that planning in addition to reviewing the standards. And these plans are available to NRC to review.

MR. CARROLL: Now, in the course of putting this together, did you do anything like a peer review?

MR. REMLEY: Yes.

[Slide.]

MR. REMLEY: In the philosophy of verification, you have to understand that you have to design something to be verifiable and you also have to do the verification during the process. It is very difficult to do the verification after the fact, for a couple of reasons.

One is that your verification isn't interjected in the right time to do any good. And you may not have produced

the information necessary to do the verification. And you may have violated some basic principles that allow you to do the verification. For example, you may have used interrupts in your software.

Those factors require that your verification proceed somewhat in parallel with your design, and that you put together a design process that is verifiable.

[Slide.]

MR. REMLEY: And the process that we use is depicted in this figure. And the verification process is running in parallel to this.

So the first thing we do is we write in our requirements phase. It has these five phases. The requirements phase, the design phase, the specification phase, an implementation phase and an integration phase.

Now, what happens with verification is that each one of these steps has to be verified. In other words, this design phase has to be verified against what was done in the requirements step. And the specification phase has to be verified against what was stated in the design phase; and the implementation has to be verified against what is stated in the specification phase.

MR. CARROLL: Okay. If the same cowboys are doing each of these phases --

MR. REMLEY: No. The verification group is an

independent group from the design group.

MR. CARROLL: Okay.

MR. REMLEY: Now, the design concept of peer reviews is totally within design space. Okay? But the idea of reviews by verification, if you want to put it that way, at each step, is what I have been talking about, which is somewhat a peer review, because the thing is it is done by an independent team.

MR. CARROLL: How independent? Is it two groups who have coffee together in the cafeteria?

MR. REMLEY: Yes. We allow them to have coffee together in the cafeteria.

We believe that it is important for them to communicate, although we keep it as a structure independent. In other words, they have a separate manager, they are a separate team. Okay? But we believe the communication is important.

I think our experience has shown, because we have had our software independently analyzed by people outside of Westinghouse. One at the request of NRC, another one at the request of CEGB. And one of the most difficult things we always have is the fact that there seems to be a problem if people don't understand the design. So if they can't communicate with the designers, it does seem to be a problem. That barrier is difficult, because they have to know enough about the design to analyze it.

MR. CARROLL: Who did the NRC have look at it?

MR. REMLEY: NRC asked Boeing Aerospace to look at some of our regional software.

In my opinion -- I never got a view from NRC -- in my opinion, the most difficult part about that was Boeing had a small piece to do and they didn't understand the context of the whole IPS, and they were very confused because of the small piece they had to do, without understanding the context of it. And a lot of the questions that I got were associated with the fact that well, why did you do it this way; and you have to understand we did it this way because of this other thing you didn't understand.

MR. CARROLL: And what was the bottom line of all of that? Did they think you had done a good job?

MR. REMLEY: Yes. With NRC we finally reached agreement that everything seemed to be okay.

MR. CARROLL: How about CEGB?

MR. REMLEY: CEGB is still running their independent design assessment. That's not complete yet.

Now, the original assessment done by NRC independently with Boeing was done on the eight-bit microprocessor design and now we've doing it on the 16-bit design.

This diagram, then, depicts the process we follow for system hardware and software.

And you can see that we don't really distinguish too much, although I agree there ends up being a lot of emphasis on the software. But we actually do a hardware verification in parallel to the software verification, and also we include the system verification steps.

[Slide.]

MR. REMLEY: As I mentioned, we also have a plan for each one of these.

[Slide.]

MR. REMLEY: Now, with respect to the software, we have done a lot of work on trying to, let's say, put a process together that has the ability to quantify what the verifiers are doing. And this is an improvement in my opinion over the verification program we were in on the 414 software. And the way we are doing this is by more extensive use of automatic tools.

If you look at an approach to software verification, you can think of it in terms of things that you want to do statically and things that you want to do dynamically. Now, the difference is that static is just looking at the documents in the code; and dynamically is actually running tests on the code.

And then there are two ways you can do that. You can do it manually or you can do it in an automated way.

We did a lot of manual kind of testing and inspection

in the original 414 software design. We did some here. But what we've tried to move down here, so we are getting more coverage in these four blocks. So there are induced static analyzers for our code that can audit the code and do analyses of complexity and data flow. And this is done automatically, although it is a static analysis. The code doesn't do anything. You are just looking at a piece of, you are running a piece of paper, if you will, through this auditor. It is not actually running in the microprocessor.

In the area of automated dynamic testing, we have put together a system which can monitor the way the tests are run on the code itself, and it analyzes the test coverage. And what it gives you is test metrics of the output. And you can guarantee that all the program logics were executed, all the branches were taken, and something called linear code sequence and jump was done.

So what it does, it gives you an independent way to audit the quality of the verification testing, because it puts out these test metrics. In addition, it gives the verifier a goal, because his goal is to reach 100 percent equivalent on his tests. And what that means is he either has to get 100 percent coverage on his test, or he has to understand why. In some cases, you can't do it. But then he can explain why he was not able to put together a test case that got him 100 percent coverage on a module. I'm at a module level. I'm not

talking about the whole system at once. You have to do this on a software module, and then build it up into a system.

We can get 100 percent coverage on our tests with this kind of an approach. And I think this is probably the biggest thing that we have improved on since the 414 design, is this automatic dynamic testing.

MR. KERR: What sort of language do you use in this process?

MR. REMLEY: We are using PLM-86 primarily. Sometimes we have to go to assembly line. PLM-86 is the Intel Language, because we are using the Intel family of microprocessors, the 80-86 family. Sometimes we use assembly language. That is only if necessary, based on timing problems usually, or diagnostics usually have to be written in assembly language. It's very difficult to write diagnostics in a high-level language.

There is some PLM-51 in some microcontroller chips that we are using also. But a very minimum amount of that. Primarily PLM-86.

MR. KERR: In the total design, or at some point, are you going to give any consideration to making it difficult for a meddler to file up the system?

MR. REMLEY: Well, the eventual product is all hardware. The software itself ends up physically on a PROM. And so, and by its nature, you cannot modify that, without

going back through a rather complex set of tools to get you to that PROM, which are really with Westinghouse.

And on top of that, there are operational checks built into that PROM. For example, we run checks on tests, as we operate it. So if something would happen, if somebody would put the PROM in a PROM burner and burn a few extra bits in there, and you put it in the system, it just would fail to check some tests.

So from the point of view of the software itself, there is really no access to the PROM. It is kind of a different thing. And if you actually do something to the PROM to compromise its integrity, the diagnostics in the system will detect it right away.

MR. CARROLL: Even if somebody at Westinghouse as smart as you are about this became disgruntled or something and wanted to really mess up a bunch of nuclear plants?

MR. REMLEY: No. That's true. An intelligent attack is difficult here. We are talking about not something like that.

We have, you know, a configuration management system for the revisions of the software that we have in the system, and that is under a single point of control. And there is a review associated with that. But that has limitations on what it could filter.

MR. SHEWMON: You said the software was burned into

PROMs. And I grant that would be hard to change. But I find it difficult to believe that you have nothing on a hard disk that gets loaded in, because now if you ever want to change your software, you have to replace all the PROMs.

MR. REMLEY: No, normally our practice would be, and this is what we worked out, is that we will provide a master set of PROMs to the utility. And when PROM fails, the procedure would be to go to the master set of PROMs, get the master copy, put it in a PROM burner, copy it, and then burn the new PROM, put the master back and replace the PROM in the board.

So there is no reason, from the point of view of maintaining the equipment, to go back to the quote "software source."

MR. SHEWMON: And there is no reason to ever change the program?

MR. REMLEY: Not unless you change the functions, no. The calibration of the program, we've structured the code in a say that the calibration data is separated from the code so that when you recalibrate the system, you do not have to change the code to do that.

We have provided a maintenance interface, and you basically update E-squared-PROM, which contains calibration constants, if you need to.

Some of this calibration, we think is never going to

change, but there should be no reason to go back to the software source to maintain the system.

Now, if you change a function, you've got to go back to the software source.

MR. WARD: You have not said much about the on-line diagnostics, other than the check, some tests, that sort of thing. Is that because with these burned-in programs you don't consider that as important as it might be?

MR. REMLEY: No. We consider it very important. We have diagnostics starting even with the analogue circuits that we have interfacing between the microcomputers and the sensors. We start our diagnostics as close to the screws and into the cabinets as we can get them.

In other words, we actually have diagnostics on our analogue circuits to assure that we're converting the signal properly. So we actually compensate for drift in the analogue circuits with our diagnostics. If the drift gets too far, we make the quality of the input bad to the system.

Those diagnostics proceed all the way through the A to D converter, through the communication of information through memories, into the operation of the microprocessors. We have diagnostics on the CPU instruction set, diagnostics on the PROM, diagnostics on the RAM.

It would take a long discussion to explain all the diagnostics. It's rather extensive and we consider it very

important. The problem is you have to be worried about the amount of time you spend executing the diagnostics versus how much time you spend executing the safety functions.

MR. WARD: Yes.

MR. REMLEY: Because you can get hung up in spending all your time executing diagnostics.

MR. WARD: Yes. What is it typically?

MR. REMLEY: We spend roughly ten percent of the time on the diagnostics. We structure them in a way that we can run them partially. We run partial sets of -- like, we don't test all the RAM, because these microcomputers execute in a loop that's about 100 milliseconds. So it's very fast.

So we'll execute a set of diagnostics on a portion of the RAM every loop and not try to run diagnostics on the entire RAM in the system, and the same with the PROM and the same with the instruction sets.

So what we have done is we've kind of layered the diagnostics so that we can go through a table of them in a way from top to bottom. So in a matter of a few seconds, we'll cover the whole thing, but it allows us to make sure that we don't compromise the safety function.

MR. CARROLL: Back to my earlier question. You're telling me some mischievous person at Westinghouse, if he was really smart enough, could --

MR. REMLEY: Basically, if the person could convince

the chief programmer, who we have set up as the guy who is working on the configuration management, and he doesn't change all the software, he doesn't program all the software, but he is the reviewer. If he can convince the chief programmer that what he did was okay, he can get the change into the system. That's what it would come down to.

MR. CARROLL: That would effect multiple plants.

MR. REMLEY: Plus, the change would have to be verified. But you're talking about some intelligent thing here and that's really difficult defending it. You'd have to convince the chief programmer and you'd have to get it through verification.

MR. CARROLL: Okay.

MR. DONATELL: Excuse me. Gil, do you have any idea how much longer your presentation is going to take?

MR. REMLEY: I will stop anytime you want me to.

MR. DONATELL: We are rapidly approaching the point that we probably won't get into some of the other stuff and I just want to go forward and complete I&C.

MR. REMLEY: I'm coming to the end of the protection system. It depends on what you want to hear, I guess.

MR. CARROLL: Shall we wrap this one up today? Is that the wishes of the Committee? Let's take as much time as we need, then.

MR. REMLEY: Fine. The only other thought that I

wanted to put together. We've talked a lot about verification and now the final point is about validation. We believe that the only way to achieve proper validation is to construct a representative set of the equipment and give it very realistic tests.

[Slide.]

MR. REMLEY: So what we've done is put together a very extensive prototype for running our validation tests. This prototype consists of an entire channel set and train of equipment, such as reactor trip switch gear and RPI cabinet, the whole control system, a representative piece of the rod control system, which I haven't talked about yet, which is a new design, and its associated logic cabinets.

The interfaces to the control desk and also we've included the flux mapping system in this, but that's not a safety system, but it does gather information. It's important to the protection system.

So the real emphasis behind our validation is to build an extensive prototype that is as close to the design as we can make it, the actual design we plan to put in the plant. There may be some modifications later on, but it is something that's very close to what you call pre-production model. It allows us to do some very extensive testing in a validation sense.

I've completed the discussion of verification and

validation, if you want to ask me anymore questions on that.

MR. KERR: Have you encountered any surprises in the process?

MR. REMLEY: Well, you have to understand that this was actually the second time we've done this. We had a lot of insight from the eight-bit design. I don't think we've encountered any surprises. I think what we've done is improved upon things that we learned we could improve upon from the eight-bit design for this design.

In addition to that, we had, in the interim between the eight-bit design and this design, we had an activity where we designed something that's a commercial system that Westinghouse markets, which is called the Westinghouse Distributive Processing Family.

We worked on that design in the interim. So I think what we've done is we've just improved things. You get more insight into details and this is really a third generation design in that sense. It would have been very surprising to run into surprises at this stage.

I think what happens is you look back and you say I think I could have done that better and you do that.

MR. CARROLL: We, ACRS, met with our Canadian counterparts a few months back and learned of many concerns that they're having in Canada about the equivalent of your IPS for their latest generation of plants. I guess it's

Darlington.

They just have not convinced themselves that they know how to V and V something that has that kind of safety significance. It does have a higher degree of safety significance with their reactors than it does with a Westinghouse PWR.

Are you familiar with the problems up there or the concerns?

MR. REMLEY: No, I'm not. I guess I could just make the statement that you have to start out at the beginning with the knowledge and the intent that you're going to verify something when you're doing the design.

It is very difficult, in my opinion, to do something after the fact. If that's the situation they're in, I can understand that.

MR. CARROLL: I think they started doing it in parallel with the design, but then questioned how good a job they had done. But they, of course, do have a great deal of experience with computer-based control systems up there on their CANDU reactors and this is the first shift-over into putting it into the world of protection.

MR. REMLEY: I'm can sort of speculate here. I would starting asking on some really fundamental principles that we, through our experience, believe you have to restrict yourselves to at the beginning; otherwise, your verification is going to

be next to impossible.

For example, do they basically prohibit the use of interrupts? That's a key question at the beginning. If the answer to that is no, then I think you're going to end up with a job that you can never convince yourself that you've done a verification. That's the key one.

Have they produced the documentation in a way that independent people can review it and check it? That's another one. There are some real fundamental points you need to look at to kind of come to a judgment of whether you think the job is doable or not, at least in my opinion.

MR. WARD: I think they're puzzling a little more over -- they have -- perhaps for good reasons, they're trying to have two entirely independent shutdown systems, RAM systems, protection systems. They're trying to make them not only independent, but they're trying to make them diverse; not only in hardware, but in software to the point of having different organizations.

MR. REMLEY: In lieu of V and V or with V and V? Is the first software there in lieu of V and V?

MR. CARROLL: With V and V.

MR. WARD: No, no. With V and V on each system.

MR. REMLEY: That makes the problem more difficult. You know what happens is you find that probably one is better than another. Then you say, well, why am I doing this one over

here if I've already decided that that one is better. Well, I'm doing it because it's different.

Frankly, it's never been a philosophy that's appealed to us at Westinghouse.

MR. WARD: Yes, but you haven't figured out where you stand on common mode failures, either.

MR. REMLEY: Have they? I find it very difficult to accept the rationale that something is different, that something that is different is going to protect you against something you haven't thought about, which is basically what you just said.

MR. CARROLL: Let's say before we continue with this, let's talk about what we're going to do with the remaining hour-and-a-half this afternoon. How long do you think your presentation is going to take?

MR. REMLEY: We have covered a lot of the material already that I had in here. The only thing left that may be of importance here is the control system and how it's designed. Then maybe I could just leave it there. We've already talked about the qualified display processing system and some other things that you asked me questions about already.

So I could cover the control system. I think really I will have covered the material --

MR. CARROLL: How long should that take?

MR. REMLEY: I could get through it in 15 minutes, I

think. How's that?

MR. CARROLL: With our help.

MR. REMLEY: With your help, yes.

MR. CARROLL: Then is it logical to follow that with the human factors discussion?

MR. REMLEY: Yes.

MR. CARROLL: Does that relate?

MR. REMLEY: Very, yes. I think it is.

MR. CARROLL: Do you have some idea of what that entails in time?

MR. EASTER: Again, with your help, we could do it in less than an hour.

MR. CARROLL: So that pretty much takes us to 4:00.

MR. EASTER: I would guess so. Yes, sir. And we've got to have a break. Does that help you, Loren, in terms of staff?

MR. DONATELL: Yes, sir. I appreciate it. Thank you.

[Slide.]

MR. REMLEY: Now I'd like to talk about the integrated control system. As I've said before, this is a completely separate system from the protection system, although it is based on the same technology and uses a lot of the elements that the protection system uses at a module level.

It consists of basically three elements; the

modulating control section, which we call the integrated control cabinets; a logic bus, which is similar to the data highway that I talked about in the protection system; the rod control system and then the logic cabinets associated with the on-off controls.

The modulating controls are handled directly from the integrated control cabinets.

[Slide.]

MR. REMLEY: I would like to now focus on the design of the integrated control cabinets which are the cabinets which handle the modulating control.

MR. MICHELSON: Now, these are all non-safety?

MR. REMLEY: These are all non-safety.

MR. MICHELSON: Thank you.

MR. REMLEY: But they are performing the NSSS controls.

[Slide.]

MR. REMLEY: Again, the structure of the cubicle looks like what I showed you before, but the internal architecture is now different. Within each cubicle, the design basis is that there is no single point of failure in the electronics. That includes the signal conditioning modules.

This is done by producing an active and a standby computer subsystem, plus its associated signal conditioning modules for process inputs and for control outputs. The reason

you have to go to an active standby kind of structure is because in modulating control, you have to deal with integrating controllers, and the system cannot run in parallel.

It actually has to be in control or not be in control; because if it's trying to run in parallel and it's really not in control, its controller will just integrate off. So what we do is, we run with an active and a standby controller.

Now, there are a few points to be discussed about this that may be different from classical systems. The active and the standby roles are interchangeable. Upon detection of a failure, the control is automatically transferred from the active to the standby.

There also can be a manual control from the active to a standby and each controller has entirely separate units.

MR. WARD: Detection of a failure means through the diagnostic programs?

MR. REMLEY: That's right; we're essentially using the same diagnostics that are in the IPS, and what we're doing with them here is we're using them to switch from the active to the standby roles.

MR. MICHELSON: When the switch is performed, is there an annunciation or some attention brought to somebody?

MR. REMLEY: There is a status panel on the computer subsystems themselves that tell you the state of them.

MR. MICHELSON: How often do you think you might look at the status panel since it's a non-safety piece of equipment?

MR. REMLEY: Well, the information is available on the monitoring highway, but to be honest, we haven't discussed what we might do with that information yet.

MR. MICHELSON: It's available, you're saying, but not brought to anybody's attention except on the monitoring panel?

MR. REMLEY: At this point in time, that's true.

MR. MICHELSON: Now, if you also have lost -- if you have already flipped the standby two weeks ago and now your standby goes out, there's no fail safe consideration or anything because this is non-safety?

MR. REMLEY: Well, fail safe, yes -- I'm having trouble with --

MR. MICHELSON: Well, I don't know what happens when the standby has also failed, because I didn't notice that the usual system has also failed.

MR. REMLEY: If the standby has failed, it won't switch to the standby.

MR. MICHELSON: No, it has to quit or -- I don't know what it does next. That's what the question is.

MR. CARROLL: He has two failures.

MR. MICHELSON: Spread by a couple of loops or --

MR. REMLEY: It's only single failure proof, so you

postulate two failures that will take it down.

MR. CARROLL: He says that the original, or what was the active, went down two weeks ago. Nobody knew that --

MR. REMLEY: Yes, that's right.

MR. CARROLL: Now, the standby, which became the active, goes down; what happens to the valve or the solenoid or whatever?

MR. REMLEY: Well, it's going to lose the output and it's going to do whatever it does when it loses the control signal.

MR. MICHELSON: Presumably that's not a safety concern?

MR. REMLEY: No.

MR. MICHELSON: It's a non-safety component here.

MR. REMLEY: That's right.

MR. MICHELSON: But it could be the feedwater valve, I assume?

MR. REMLEY: It could be.

MR. MICHELSON: Oftentimes, I think we begin to realize that the feedwater valves, the big ones, are pretty important. Have they be elevated to some other consideration, or are they still a part of the non-safety consideration?

MR. REMLEY: They have not been elevated to some other consideration.

MR. MICHELSON: So you're not worrying about all the

feedwater lines wide open, overfeeding the generator because you've got another control somewhere?

MR. REMLEY: I'm having trouble here. We built a system that's an order of magnitude better than any system in operation today and you're telling me it's not good enough.

MR. MICHELSON: I'm not going to go every day and look at that status panel. If it's non-safety, I might never look at it.

MR. REMLEY: But all you're talking about is the fact that somebody's got to be aware of the fact that when something fails, they have to go fix it. I presume that's proper operating procedure; that people don't just let things --

MR. CARROLL: I think what's troubling us is that you made it very nebulous as to how somebody finds this out.

MR. REMLEY: The way they find it out is to go to cubicle once and a while and look at the state of the status panel.

MR. KERR: Whether we like it or not, the general design criteria do specify that the operation of control systems must be such that they do not disable reactor protection systems. Presumably there is a backup that will take care of this.

MR. REMLEY: I would consider it to be good operating procedure for somebody to make sure they understand the status of this equipment all the time.

MR. WARD: Would there, for example, be some administrative control, tech spec or procedures that would permit only X hours, days, shifts, or something of operation on this?

MR. REMLEY: Certainly not, because today, you only have a system that can have a single point of failure, so you don't have any tech spec that says --

MR. MICHELSON: I thought the feedwater system had been reevaluated though because of its implications on steam generator overfill and so forth?

MR. REMLEY: I don't know that.

MR. MICHELSON: It's in another category. It's recognized not to be safety grade, per se, but it has, I thought, some safety grade controls on it. It's the same way with the steam generators themselves. The level of controls have been changed to safety grade for this very reason, although they didn't used to be necessarily safety grade.

I just wondered if feedwater was getting any different treatment than you're describing here.

MR. CARROLL: Apparently it is fail as is or fail closed.

MR. MICHELSON: Being non-safety, I don't know if they've done any of that. That's what I was asking; certain components, even though they're categorized as non-safety components, do they get certain extra consideration, an example

being feedwater control?

MR. REMLEY: With respect to how the control is done, both the automatic and the manual controls are implemented in the digital controllers, okay? Manual control is an operating control mode. Backup for availability is provided through the system redundancy.

This kind of architecture allows you to continuously have process information available -- continuously meaning given that you've only had a single failure to the operator. There are several types of tracking in the design. There's tracking between the active and the standby controller/

There is tracking associated with the automatic/manual control mode, and there is set-point tracking for the changing at set-points.

MR. MICHELSON: Do you have redundant fans and so forth like you describe for your safety grade cabinets?

MR. REMLEY: Yes, all the physical aspects of this cubicle are the same as the safety grade cabinet.

MR. MICHELSON: Temperature monitoring also?

MR. REMLEY: Temperature monitoring, the fans, the EMI glass; there's no physical attribute of this cabinet that's different than the safety cabinet.

MR. MICHELSON: It's made the same way and everything. I assume it's off the same production line and they just call it non-safety because it doesn't need to be

safety.

MR. REMLEY: That's right.

MR. CARROLL: What's the difference in price?

[Laughter.]

MR. MICHELSON: There shouldn't be any.

MR. REMLEY: I'm not authorized to give that information.

MR. MICHELSON: It's just a paper difference, I guess.

MR. CARROLL: What is the availability of your diagnostic system?

MR. REMLEY: Our basis for the availability of this system is 10 to the minus 3 failures per demand. Now, the diagnostic system is integrated inside of these controllers. Conservatively, we have assumed that our diagnostics can detect 90 percent of the failures in the electronics. We have done some analysis work to justify that, although that is a subjective area.

I would give you the answer of 90 percent as the effective diagnostics.

MR. KERR: Now, the diagnostic system that says that something has gone wrong is a diagnostic system in each of the two controllers, active and standby? That is, is it possible for the diagnostic system to go wrong and to say that, let's say, Control System No. 1 has failed when it really hasn't

failed?

MR. REMLEY: That's possible, but unlikely.

MR. KERR: -- and then to look at Control System No. 2, which is identical to Control System No. 1 and conclude that it has failed also.

MR. REMLEY: Because of the same air condition occurred or something?

MR. KERR: Yes.

MR. REMLEY: I can say that -- I mean, that may be possible.

MR. KERR: What I am asking is; does the same diagnostic system look at both?

MR. REMLEY: It's not the same diagnostic system, because they're basically put in each system separately, but it's the same diagnostics. It's the same algorithm.

MR. KERR: You could have a failure in one of the diagnostic systems and then the second diagnostic system in the standby system would say it was operating okay.

MR. REMLEY: Yes, it's a separate set. It isn't independent of both and therefore, if it makes a mistake, it takes down both. It isn't that way.

MR. WARD: Unless there's a common mode of failure.

MR. REMLEY: Unless it's a common mode of failure; that's right.

MR. MICHELSON: Are you evaluating these systems

under USI 847 which is the Safety Implications of Control Systems?

MR. REMLEY: I think we do, right? Yes.

MR. MICHELSON: There, do you consider again the possibility of external events affecting these control systems with adverse effects thereby on safety systems? Is that a part of your analysis?

MR. REMLEY: I would think so, yes.

MR. MICHELSON: So we can expect to see the effects of fire on these cabinets or in the rooms and pipe breaks and whatever, as external events somewhere analyzed and the effects shown, when they do the USI which I gather will be FDA stage?

[Slide.]

MR. REMLEY: Well, I guess, you know, maybe I said it indirectly, but I will say it for emphasis: there is no direct wire between the control board and this valve. Its manual control is not a form of redundancy in this design; it is an operating control mode.

MR. MICHELSON: What were you saying? You can't go to some switch and operate the valve; is that what you're saying?

MR. REMLEY: On the desk; that's right.

MR. MICHELSON: You cannot go to a switch on the desk --

MR. REMLEY: Oh, you can operate it at the desk.

What I'm saying is; one of these two computers has to be working to do that.

MR. MICHELSON: Oh, yes, yes, sure.

MR. REMLEY: You can certainly go to a dedicated switch on the board and operate this valve under manual control. You can certainly do that.

MR. MICHELSON: As long as the computer is working.

MR. REMLEY: As long as one of those computers is working.

MR. MICHELSON: If the computer goes out, then you're saying there isn't any way, short of turning the hand wheel or something, to get it to go.

MR. REMLEY: If both of them go. You have to lose two.

[Slide.]

MR. REMLEY: This is just a diagram of the physical implementation of all the controllers. They are divided up into subsystems. There is the power control, the feedwater control and then two other control groups in the systems.

One of the important features of this design is that there is a signal selector, automatic signal selector included in the design and it provides a functional filter between the protection system which has four-way redundant process inputs and the control system. We've provided electrical isolation by using optical datalinks and the functional isolation is

provided by the signal selector.

It is designed such that it can take a failure in the protection system in one channel set while another channels set is under test. It can actually take two failures in the protection system and still provide the control system with a valid signal.

MR. MICHELSON: The control systems can be located in the same room with the protection system cabinets; is that right?

MR. REMLEY: It probably could be but it's not normal practice to do that.

MR. MICHELSON: Okay, you keep the control in separate rooms from the protection.

MR. REMLEY: Yes.

MR. MICHELSON: Okay. Thank you.

MR. KERR: In the control, does the control system that you have for feedwater permit you to start the plant at zero power and automatically control feedwater until you get to full power?

MR. REMLEY: Yes, we have expanded the control ranges with improved digital control algorithms and I'm not quite sure if we can go from zero power automatically. Can we with that algorithm? Okay, zero power.

I know we've brought it down to lower power but I wasn't sure it was zero power.

MR. CARROLL: But you're doing this with different combinations of pumps and valves.

MR. REMLEY: Yes, that's right.

MR. KERR: You really make me feel good about American technology because for years I said that I was sure it was possible to do this.

MR. REMLEY: Yes.

MR. KERR: If somebody would just do it, and you can. That's great.

[Slide.]

MR. REMLEY: Okay, the next piece of the control system is the rod control system which is a very special design system that interfaces to the control cabinets that we have upgraded to also be a microprocessor-based design.

Basically what is microprocessor in this design is the logic here that's associated with moving the rods, okay? It is also completely redundant. There's no single point of failure and it interfaces with individual power cabinets that have microcontrollers that receive signals from the logic cabinets and then these microcontrollers control thiristors which then move the control rod drive mechanisms.

So what we've done is we've upgraded this design to be consistent with the rest of the technology in the I&C architecture and put in place the same principles that we could with respect to fault tolerance and that is no single point of

failure down to the actual control mechanism itself.

MR. MICHELSON: One might ask, as long as you were going solid states the whole way, why do you still use switch gear breakers?

MR. CARROLL: Too much current.

MR. MICHELSON: No, you can get solid state --

MR. REMLEY: Yeah, I don't know. Yeah, I've heard that question. Personally, I don't know that --

MR. MICHELSON: They may have -- one time and decided not to use it.

MR. REMLEY: Yeah. Solid state breakers.

MR. MICHELSON: Yeah, you can --

MR. REMLEY: I'm not sure that they're fail-safe. I think that's one of the problems.

MR. MICHELSON: Well, I don't know. I was just wondering why. I'm sure there are good reasons. I just wondered if you could give us -- reason.

MR. REMLEY: I cannot give you reasons right now. We have considered it though.

[Slide.]

MR. REMLEY: There is equipment designed that is common to the protection and the control and we sort of separate it off to talk about it in a separate way although it's not physically associated. It's just a way the design operates and we refer to that as the integrated logic system.

As I mentioned before, there are two trains of the integrated logic system associated with the IPC, A and B, and these are physically completely separate trains and then we have a non-safety train of logic. They're basically three elements to this design, that is, a control board multiplexer, a data highway and logic cabinets. There's a set for train A, train B, or train N or the non-safety train.

The cubicle that is the logic interface looks like the rest of the cubicles. It's just in a special configuration for the logic system. I think it's interesting to consider the way this system interfaces to the main control board. There are actually two levels of multiplexing that are going on in the main control board. There is a set of electronics that's actually resident in the disk and these are associated with each train in the non-train equipment.

Then there are also internally redundant. So the only hard wires are between the hand switches and these multiplexer units and these -- I think I have a picture of them. Oh, well.

MR. MICHELSON: What kind of voltage levels do those hand switches operate at?

MR. REMLEY: I'm not sure. It's low level DC voltage, like 15 volts.

MR. MICHELSON: Fifteen?

MR. REMLEY: Yeah, I'm pretty sure like that but I'd

have to verify that but it is low level DC voltages. I mean I can say that for sure. There's no power signals in this disk.

MR. MICHELSON: I assumed not but I was asking.

MR. REMLEY: Yeah. The only concern I have is telling you exactly what the voltage is. Well, anyway.

MR. MICHELSON: The multiplexing units have to operate at about -- off 110 AC?

MR. REMLEY: Yeah. These units here are coming in with AC power. These units here, yes, these are also -- have power supplies in their AC part.

MR. MICHELSON: The power supply, what kind of power delivery levels are we talking about to one of those units?

MR. REMLEY: There's actually a power supply module in the disk that's converting the AC to DC and that's receiving 110.

MR. MICHELSON: How many does it serve?

MR. REMLEY: It is dedicated to a train.

MR. MICHELSON: So it can be 20, 30, 40 of those components?

MR. REMLEY: Oh, no. See the -- okay, let me try to explain the way this works. The reason there's two levels is we need -- this in fact at this level is a gateway between the computer -- or the control desk and the individual data highways, okay, and there's basically a hand switch multiplexer unit within each module -- desk module -- that is connected

through a data link here to the gateway to the highway. So there are basically as many datalinks here as there are desk sections that need to interface to the controls on that highway.

That would be say on the order of 10, okay. So this set of multiplexers here is localized to a desk section and generally gets multiplied by the number of sections which is about 10. So the number of boards in each -- for a logic station, you can have four stations per board and for a control station, you can have two stations per board. So the number of boards that you need for a given section generally fits into one 19-inch rack without any difficulty.

So there's not a lot of power --

MR. MICHELSON: Let me tell me just what the question is.

MR. REMLEY: Okay.

MR. MICHELSON: The question is, some people think that there's no energetic sources within the control panel itself, the main bench board. Indeed though, I think you have to have power supplies for these components and those operate at a 110, several ampere kind of levels.

MR. REMLEY: Yes.

MR. MICHELSON: Now on the supply side --

MR. REMLEY: That's right.

MR. MICHELSON: And indeed, that's a fairly energetic

source and it can start a fire in the bench board and so on.

MR. REMLEY: Oh, yeah. Okay.

MR. MICHELSON: Therefore, you can't just say I've got all 24-volt stuff. I'm not going to have any fire problems, all milliamp circuits. It really isn't. There is plenty of power in the cabinets yet and that's what I was looking for.

MR. REMLEY: That's true but I think the key thing is it isn't power that's running out to the controls.

MR. MICHELSON: No, but we'd like to see how you address the possibility that things goes up in flames and what effect it has. Some people have been taking all the barriers out of the boards and so forth.

MR. REMLEY: Well, it is, you know. We still want to maintain some separation here.

MR. MICHELSON: You put barriers between each section all the way up?

MR. REMLEY: Well, the problem is -- you run into a conflict that Jim Easter can discuss next, you know, what you want to do in human factors space versus what is nice to do from the point of view of separation of the electronics because there's certain layouts which are better from a human factors point of view that you have to look at a trade-off with respect to the separation issues. Now, we believe that we can deal with this a lot better now because we do have these low level

signals and we think we don't -- think the separation requirements are easier to handle.

MR. MICHELSON: But we still have high level power supplies.

MR. REMLEY: Yeah, but that's not all over the place. That's coming into one area.

MR. MICHELSON: No, no. If it starts burning, it makes smoke and smoke gets into components and how do you protect the other components?

MR. REMLEY: But again, it's not all over the board. It's in one space.

MR. MICHELSON: No, that's right.

MR. KERR: No fuses?

MR. MICHELSON: It depends. It depends on the design and fuses -- not fuses -- small circuit breakers are not equivalent and you don't know whether that works or not. They don't have high reliability in the sense of ten to the minus four or something.

MR. KERR: Fuses are pretty reliable.

MR. MICHELSON: No, these aren't fuses though.

MR. KERR: Yeah but you could use fuses.

MR. MICHELSON: Oh, yeah. You could require they double fuse the thing if you want to but I don't think they're requiring that.

MR. REMLEY: We have circuit breakers --

MR. MICHELSON: You're just using a circuit breaker and those are not anywhere near as reliable.

MR. REMLEY: I'm almost there.

MR. CARROLL: We want to get into human factors.

MR. REMLEY: Yeah. The point is that what we've done is we've decoupled then the train architecture from the way we want to lay out the control board.

That concludes my discussion on the control system. Okay?

MR. CARROLL: That concludes your entire discussion? There is a few more sections --

MR. REMLEY: Yeah, I know but I think we talked about those.

MR. CARROLL: To some degree, they get picked up in human factors?

MR. REMLEY: Yeah, the layout of the control board and that stuff will, plus we've talked about the qualified data processing system and the computer system and I touched a little bit on the special monitoring systems already. So I don't think there's anything that I haven't at least talked about to some extent.

MR. MICHELSON: Within the main control room panel, I see just from flipping pages, there are a number of devices there that have rather large energy requirements and you see a couple of them --

MR. REMLEY: Yes, the CRTs and the plasma displays.

MR. MICHELSON: Somewhere and someday when we talk about fire protection, you're going to address fire in this main bench board because it's either that or show why it's a non-problem to have a fire in that main bench board. You're getting everything awful close together and I'm not sure how many barriers there are -- environmental barriers within that cabinet. It's not clear and you point out the problems of putting too many in. So we'll talk about that on some other occasion.

MR. VAN DE VENNE: In one of the responses to the fire protection, we have stated that the probability of a fire is probably lower but cannot be excluded so we still have the evacuation panels. That's the backup, basically.

MR. MICHELSON: Yeah, but you have to show what happens between the time that you start getting the fire and the time you start actuating the evacuation panels and the fire's in this area.

MR. VAN DE VENNE: Again, if the fire's in the main control room, the protection system should shut the plant down. There is plenty of time to --

MR. MICHELSON: The design system will get the rods in, I suspect, but I'm not -- I'm talking about opening relief valves, all the other things that can occur later on.

MR. REMLEY: I believe that we can show that the

electronic design is such that we're not going to generate spurious actuations. You may not be able to control anything from that desk but nothing's going to happen as a result of a fire in that desk because again, if the diagnostics built into this equipment, it's difficult to create this intelligent action that's going to create something.

Again, that requires a detailed demonstration.

MR. MICHELSON: Yes.

MR. CARROLL: Okay, let's take a break until 3:15 and we'll pick up human factors.

[Recess.]

MR. CARROLL: Let's reconvene.

[Slide.]

MR. EASTER: Okay. My name's Jim Easter. Very briefly, I've been working for Westinghouse for about 25 years. I am not, by training, either an psychologist or a human factor specialist. My background is in mechanical engineering and nuclear engineering, and I would say that my perspective here is really one of systems. The question of human factors and applied psychology as it relates to the job of trying to integrate the human -- and I use that in a rather loose sense, I guess -- to include the human, maybe is a better way of saying it, into the design and operation of the control board, to support humans that are expected to support that staff and to keep the plant up and going.

So in terms of the theory of human factors, etcetera, I don't claim myself to be a specialist in that area. My emphasis has primarily been in control board design and the subsequent design of interfaces that relate to that.

[Slide.]

MR. EASTER: By way of introduction, I'll try to move this pretty quickly and make a couple of points about process, etcetera, that are really, I think, the backbone of what we're trying to do. The latter half of the presentation kind of winds up showing you some place where we are right now relative to what equipment design, and display design, and alarm system design looks like, but I think the main emphasis ought to be on the first half, which talks about the processes that we're into from the point of view of design engineering, and the treatment that we give to those processes.

We've been at this a little bit less than the time that the I&C designers have been at the idea of microprocessors in the plant. We've been at this design a little bit longer than the Three Mile Island anniversary -- a little more over a decade.

The idea was, as the I&C moved into the microprocessing and computer-based arena, to take advantage, in terms of the managing interface, of what exactly that meant in terms of adding capability and improving the ability of the human to be a part of the system and not have to be a collector

and an interpreter of what was going on, and have to work with the interface system as a separate system, but rather to be able to treat the interface system as a truly transparent interface.

That got us into some thoughts along these lines, of thinking about the raw data from a number of different kinds of sources, trying to organize that data into some kind of a knowledge structure, and the actual interface is some kind of a graphic blackboard, so that, in effect, what we're doing is creating a database or a knowledge structure, and then letting the human, in effect, be the inference engine, if you want to adopt the AI terminology for expert systems.

In that way, we get, hopefully, things that the computer can do well and things that, at least in terms of the understanding and interpretation of plant processes, that the human can do well.

[Slide.]

MR. EASTER: One of the main points I wanted to make this afternoon is the idea of design process here. Over the last ten years, we've tried to develop this process and to make it a systematic form of our total engineering process for a plant, and it starts with the inclusion of experience that we've had collectively over the last 20 years with operating plants.

The main emphasis, though, that we have done over the

last ten years is to try to understand something about the human decisionmaking processes, and closely associated with that, to begin to think about how to represent the plant in a functional way, as opposed to simply in a physical way.

One of the things I think we all learned from Three Mile Island, documented in reports, is that the decisionmaking issues are essential, and the decisionmaking issues really get done better if people can understand functionality in addition to, but not to the exclusion of, physical connection. So a lot of our emphasis has been in this kind of an area.

Downstream with that, we end up writing task analyses for people that are involved, and those people are not only control room operators, but it turns out that when you begin to think about what happens relative to accident management, the people set grows with the accidents.

One of the things I'm currently very much involved with is a design of a plant computer replacement system that will use a lot of these ideas in a European facility. I spent about three weeks sitting with the entire operations organization.

One of the things you learn is that one of the big problems they have, and it's probably shown up some in our emergency drills, is this idea of synchronization between people. As an accident grows, you bring in more and more people, and the question that interrupts operators and

interrupts subsequent people that could be used to more effectively help with accident management is simply the idea of trying to synchronize those new people.

What can a computer system do to help that synchronization; what we have to understand about the way the computer system and the interface are created so that those people become a productive asset to the people that are managing the accident, and not something of a distraction.

So we have to write these task analyses. We worry about the task allocation between man and machine. Although the guidelines currently are not terribly clear in terms of task allocation, experience is helpful here.

We then look at the issues of alarm system design, display design, and control systems layout based on these functional issues. We then work out a workstation design, and finally a control board layout.

This is, in a sense, a first cut at it in preparation for doing the traditional functional requirements and design basis documentation. So, in effect, this first part of the process is really a first attempt at trying to get a design and to form the actual design bases for the control room and subsequent support interface designs. We then write functional requirements, and sit down with the likes of Mr. Remley to talk about hardware and software design, etcetera.

So one of the big things I want to make clear here is

that we're trying very hard to carry the human factors decisionmaking process not only into the control room through the design and control board, but also into the subsequent support areas, like the ERF, the Technical Support Center, and even into the management offices to a degree, and as far down into the details of plant support, as maintenance technicians, etcetera. That's just part of it.

You find that as you begin to look at how all this goes together, the issue of crew decisionmaking becomes one you have to consider above and beyond the question of just individual decisionmaking, and then as the accident increases, you have to talk about how big that crew, in effect, gets, and how --

MR. WARD: Jim, you didn't mention field control stations. Was that --

MR. EASTER: The local control panels are going to get a similar kind of inspection. The question is going to be really, when it comes to the scope, whether those fall into the AE scope, or whether they fall into ours. If they fall into ours, we intend to put them through a process that's like this as well. That, I can't really completely nail down for certain until we have an active setup here, an active agreement. But yes, you're right. That's exactly right.

In fact, in some ways, backfit situations for this kind of thing are a little easier and a little clearer because

then the utility is the only one that you're dealing with. You're not having to worry about the scopes for it for some of these other things.

[Slide.]

MR. EASTER: One of you, over the course of the decade that we've been working at this, have seen this presentation, and that's one of the reasons why I'm rushing through it.

Relative to the idea of what a functional analysis looks like here, we're doing something that I kind of call a qualitative functional structure. In other words, it's not terribly quantitative. What it really tries to look at is how the relationships of the various, I'll say physical laws that govern the actual operation, the phenomena that you're trying to control, are related, and to try to note the links, and, in those links, describe what the sufficiency criteria is, if you will, that guarantees normal operation.

The whole idea is to construct a structure around which a normal operation is defined. So instead of trying to define abnormality here, we're trying to make a model of normality, and then abnormality becomes things that are different from, so the deviations from the normal show up in that sense.

You can do the decomposition at various places, and to show the, in functional terms, the kinds of things that the

plant design ends up using to achieve those particular functions, and you can get it down to the point where, at least from the control room perspective, you can look at the control room's operator's job in a fairly simplistic sense as being pretty much a commodity controller. He worries about, Is there enough temperature, for example, is there enough water, is there enough pressure, etcetera, and he has mechanisms in place that can either raise or lower those kinds of things in certain reservoirs in the plant.

The idea of the operator then is to look at the ends and outs, and where the reservoirs, and what the balances are, and whether levels are sufficient. It's that kind of description that you're trying to describe in this structure.

So you get down to the point where you're now talking about sources, or methods for increasing the commodity, ways of getting it into the reservoir, and the places where the reservoir resides.

[Slide.]

MR. EASTER: If you can create a structure like that, you can then look at a decisionmaking model, and the one we've chosen is the one that everyone is now familiar with by Yens Rasmussen from Denmark.

Basically, that model can be reduced to four kinds of ideas. One is a monger an feedback kind of thing; one is the issues of planning, how do you decide what to do next and what

needs to be done, and the actual issues of control.

You can lay that model -- better still, you can lay the questions that need to be answered by an operator under each of these activities -- against the structure, the functional structure that you've created at each note in that structure.

You can go in in a particular note and ask, Is that goal being satisfied? Is the process working correctly? Can the processor, the sub-processors that are on standby that are meant to be used in addition to or in case one of them fails, are they ready to go?

Relative to the planning issue, this usually gets down to questions of choices about alternatives, things like, What are the alternatives? Should that particular alternative be in place? What are the conditions necessary under which that alternative can be put into place? And then the questions of control are ones of stopping and starting and tuning of the particular pieces of equipment or functions.

[Slide.]

MR. EASTER: In summary, we use a process that looks like that. Adopted Mr. Rasmussen's model that talks about signs and signals and entry points to the alerting function up through the planning issues, the goal achievement issues; down through the control actions and the feedback that is associated with it; a functional structure model of the plan in functional

terms that allows the determination of relationships that must exist in order to have the particular physical phenomena carried out properly and within the design envelope; mapping those two things together in a way that shows now how the data must be organized, and what data is relative to what other data. That is, creating a context for any piece of data that needs to come through to the plant.

Out of the plant design, you get the answers to these questions. You can go through and ask these questions -- how are they answered? What instrumentation needs to be in place to answer that particular question about that particular functional issue -- and begin to create a database that helps you understand what needs to be displayed to the operators. It also begins to help you understand a lot of things about procedural organization, about the training problems that you need to train for. It helps you understand something about what the instrument lists ought to be.

Rather than simply letting an individual system designer determine what particular pieces of instrumentation are necessary, a total functional structure helps you understand where in the plant you need to have instrumentation that is designed specifically to help the operator understand total process questions.

MR. WARD: Jim, let me ask you a question. To what extent, when you're going through a design like this, do you

have to make assumptions about what I'd call the institutional arrangements in a given plant, the way a shift is organized, how a utility is going to use their STA, or something like that.

MR. EASTER: Yes. I'll take a -- I thought someone might ask that question, so let me take a quick look.

[Slide]

MR. EASTER: I didn't include this in the slide, because this belongs to the utility that we're working with. This is a foreign utility, but I think it's fairly representative.

MR. WARD: This does explain it, though. I can see that.

MR. EASTER: Yes, right. That's right, it does, and it brings you to the point where you realize how much coordination you've really got to think about here, and essentially, what we have done here is to try to outline chunks of, I'll say, decisions, and I have represented the labels, usually, with people or with sets of people, and to talk about what happens when you have this set of people, three operators, plus -- this is also a decomposition model, by the way, sets of decisions that can be decomposed.

In this one, it turns out to be a shift supervisor and the equivalent of RSDA. This is emergency management, and wnat you find out is that this kind of information -- the links

try to show something about what data needs to be transferred where. It doesn't say a lot about the timing or the circumstances. It just says what data has to be transferred where, and the point you're making is exactly that one, and that is that if you begin to now do this decomposition, you see that with an accident, the thing starts right here, with these three control-room operators, but then it grows, and people begin to -- you bring in the STA. The STA decides then that he has to -- in this particular utility, they control -- the ERF controls, basically, everything.

So, the STA decides to call in the ERF, in a sense. The ERF then may decide that they need some technical support, so they'll bring in a technical support center, and every time one of these phone calls goes out, you have got another set of people -- it may be one or it may be 15 -- that are now a half-hour, an hour, an hour and a half behind where the event began, and so, they have to be brought up to speed, and now, you're asking how does that go on, and in effect, we're saying now, with the design of these interface systems, that what you design in the control room in the way of a control-board displays, in the way of, I'll say, SPDS -- trying to meet the SPDS criteria, has to be supported by that kind of synchronization problem, so that it's relatively clear and the amount of discussion that has to go on between these people and those people relative to what has happened and can you see

playbacks and can you do this and can you do that has to be considered as part of the human factors managing interface issue. Okay?

So, that coordination thing is a fairly profound set of things, but it's kind of like the common mode failure in some ways.

MR. WARD: Let's just say normal operation, a given utility might have its operator/shift supervisor responsibilities defined a little differently than another utility, but you're trying to design a standard plan.

MR. EASTER: That's right.

MR. WARD: I question whether the design can be optimized for either.

MR. EASTER: There is a point at which, you're right, that you can't do it quite the same way for every utility. One of the big differences I noticed here is that in this country, quite often, this relationship exists. In this one, it does not. In order for these guys to get here, they have to go this way, for example, and that means that the way you design those displays for that kind of an organization matters, and we're trying to include that, at least in that kind of a context.

Now, in terms of the equipment, in terms of the kinds of physical resources that you need, I still think it's fairly similar plant to plant, utility to utility, but you're exactly right. The nature of the context of the display, the details

of the display design, almost have to be tailor-made to a certain degree.

Now, certainly, the process displays for PWRs -- a PWR is a PWR, but when you start thinking about how do I communicate and how do I organize data so that these guys understand what these guys are doing, that gets to be dependent now on how the organization is done. So, there is a point at which it breaks down. You are now dependent upon how the utility does their thing.

[Slide]

MR. EASTER: To talk a little bit about how we use the concepts -- integration, to us, here in this circumstance or this instance, comes at several levels. One level is the idea that you've got all of the pieces of the control room -- the alarm system, the procedures, the training curricula, the displays, the organization of the controls, etc. -- that there is some guiding background or backbone that helps one understand how that organization and those pieces fit together.

The two things that we use are this decisionmaking model that Mr. Rasmussen put together and, secondly, is the functional structure that I've talked about.

In the case of the alarm system and in the case of the displays, the case of the procedures, the case of the controls, to a certain degree, we go back to the decisionmaking process and try to specifically outline exactly which steps in

the decisionmaking process we expect that chunk or that set of resources available to the control room or available to the TSC personnel, whatever it might be, what pieces of that do that job.

So, in our case, we tried to design an alarm system that will work through that kind of set of steps. The idea, in our mind, of the alarm system is that it's the initiating point for the decisionmaking process. Our paradigm essentially is that the control room is fine, straight and level, that the plant is sitting at some nominal power level, and the operators are reasonably happy with the performance. The alarm system is a dark board; it indicates no big problem. But there is an alarm or set of alarms that do come in, and that instigates the initiation of this process.

We expect the alarm system -- yes, Sir?

MR. KERR: Finish what you were saying.

MR. EASTER: Okay. We expect the alarm system, then, to help the operator, first, funnel what that problem area is. So, we're trying to get the alarm system, in an analogous way, to be the index, if you will, or a table of contents to a book, where the displays and the detailed information form the pages of the book. You want the alarm system to, one, help him understand that there is something wrong and begin to focus his attention where in the information he can find more detailed information about it.

MR. KERR: You have a box there called "Identify State", which I interpret to mean try to decide what's going on. Is that in contradiction to the idea of symptom-based activity, where, at least insofar as I understand symptom-based activity, you don't have to understand what is going on, you just have to see what a number of meters are reading?

MR. EASTER: The idea of symptom-based, to me, gets back to this functional idea.

The identification of state here, to us, I think, means that you understand, at least functionally, I have either got too much heating, not enough heat sink, not enough -- too much reactivity, not enough core cooling, that kind of thing, the way the owners group procedures are, in effect, organized, as opposed to the idea that says I know exactly which pump failed and why, or I know which valve failed and why, which is more, in our view, the event-based kind of thing, so that we have got a set of understanding about the plant, about where functionally it sits in that kind of space, and if the planning issues can be thought about in terms of relative to where I am with those functions, what changes do I need to make to get them back within their envelopes?

MR. KERR: Well, it would seem to me that observing what is abnormal would be the symptoms.

MR. EASTER: Yes.

MR. KERR: You go a step beyond observing what is

abnormal, in that diagram, to using, presumably, an observation of what is abnormal to identify a state.

MR. EASTER: Okay. Let me do it in terms of this.

[Slide]

MR. EASTER: What we do when we create the functional structure is to talk about what it is -- for example, in this particular case, I'm looking at water mass inventory in the primary system, and I recognize that I have to have a certain amount of water mass in order to control clad temperature and to control primary pressure. That means that these two functions, if you will, are putting demands on the systems that, in fact, do this job, and I can define a region of acceptance.

In this case, for controlling primary pressure, I know that the water mass has to be above the heaters and pressurizer in order for me to say that I am within the normal bounds of the operational envelope of the plant.

So, I can define a structure where the links and the -- what we call "predicates", the yes or no questions are relatively straightforward and relatively clear-cut, and it's this that I mean by state identification. If I can go through here and say yes, all of these are met, then I know that, in effect, the alarm board ought to be blank and everything's flying in good shape.

If, in fact, I find that this is out of bounds, that

it is abnormal, that it does not meet the criteria, then I have got a different state, in the functional sense, and I have to -- my planning objective, then, is to figure out how do I restore this function within its necessary envelope, and that mean, if I have got an alternative function to help do that, maybe I go to the alternative, because this one is working right or whatever, but it's that kind of functional thinking that we're trying to get instilled into the design, to get -- to be an intrinsic part of the display and thinking process that goes on in the control room.

Does that make any sense? Is that clear?

MR. WARD: Well, I thought maybe the answer, Bill, if you go to the Rasmussen diagram again --

MR. EASTER: Okay.

[Slide]

MR. WARD: When you identify -- you know, observe what's abnormal, then you might take the shortcut over there. That's the functional restoration --

MR. EASTER: Right. In the procedure sense, that's exactly right. What you find is that procedures are able to quantify these shortcuts, are able to make them very specific. So, if you get a state that you recognize what the answer is, what the control action is, you can go quickly to this direction, and to the extent that the function restoration or symptom-based procedures have covered all of this kind of

process here, then they can help you do this.

The thing that we're trying to add, though, is -- ne of our guiding first principles, or ideas, maybe, about what is a good operator was then even though he has a well-done set of procedures and he's got a good training program, the test, if you will, that helps you understand if the operator is in command of his tasks is if he is mentally ahead of what's happening in the plant, so that he has a mental model, if you will, that will help him anticipate, if he executes the procedure that he is told, what will happen and what will happen next in the evolution of the event that he is in.

So, we're trying to prepare a display system that, even though he's got a good set of procedures, will help him be that kind of operator and will help him be confident about the procedures that he's working with, help him to continually be able to match what he thinks ought to go on against what the procedures are telling him he needs to do and what will happen.

MR. KERR: Okay. I have what I think is an associated question, and maybe this is not the time to answer it.

If an operator, a good operator, is faced with a situation and looks up or remembers the appropriate procedure or the procedures that seem to be appropriate, but his gut feeling tells him that, in this situation, they are wrong. what should the operator do? Do what his gut feeling tells him or

follow the procedures? And if you prefer not to answer that, I --

MR. EASTER: From the perspective of what it means to tell the operator right now, I'd probably prefer not to answer it. In the sense of what we're trying to do with the design of these interfaces -- is to get it to the point where he can reconcile and understand why his gut feeling is inconsistent with the procedures and help him understand what those differences are.

MR. KERR: But his gut feeling might be correct.

MR. EASTER: Exactly. That's right. His gut feeling might be correct, and what I am hoping is that the interface I'm working to -- is that the interface will support that, will him understand that, in fact, yes, his gut feeling is right.

MR. KERR: I have asked this question of some utility people, and on at least two occasions, I have gotten the response that we tell the operators to follow the procedures.

MR. EASTER: Yes. That's right. Most utilities that I have talked to, that's exactly what they do. So, the question, then, is where do you put the resultant of the actions? Do you blame the person that wrote the procedures, or do you blame the operator because he didn't follow his gut action?

Here, we're trying to work through -- I'm not guaranteeing you, obviously, that we're going to be 100-percent

successful, but what we're trying to do is improve the interface in such a way that when he gets into those situations, he has got an interface that can help him with that, can help him see what the plant is doing in a clear enough way so that he will recognize that the procedure, maybe, because he has picked the wrong one, he needs to go to another one.

I'm not sure that I really, as a vendor, am in a position to tell the operator straight up that the --

MR. KERR: I was only asking for your opinion. You've obviously thought about this some, and you have studied it more than the average.

MR. EASTER: Yes. My opinion is that if we can design the interface the way I would like to do it, then I would want him to be able to recognize and do what his gut feeling has said and recognize where the procedure-selection process has been, I'll say, waylaid or gone astray and be able to get back in it.

My own personal feeling now is that the procedures we've pretty well put together, the owners group procedures, etcetera, probably do a pretty good job of encompassing the things that can happen to the plant from the systems-based point of view. So, the question of will he get to a situation here that says that the symptom-based procedures, if he is in the right one, if he had chosen the right one, will lead him

astray is probably pretty small.

On the other hand, though, there may be a misinterpretation question relative to what he reads on the control board that helps him or doesn't help him through the issue of selecting the correct procedure. So, what we're trying to do here is to be sure that he has got the capability to make these independent judgments about what the procedure ought to be doing and can help him understand whether or not the response of the plant, when he is working through a procedure, is correct, and thereby, hopefully, help him with the problems that he may get into by mis-selecting or misinterpreting so that he gets into the wrong procedure.

MR. KERR: Thank you.

MR. CARROLL: You are down to 12 minutes.

MR. EASTER: The question, then, is what's the most important things to tell you. I think probably the thing to do is to jump down and show you collectively a set of -- I can talk about a lot of things off of one slide.

[Slide.]

MR. EASTER: I apologize for how dark it is. This is a large board. The image that Gil showed you a moment ago in the discussion of the I&C showed you a full-sized circular control board. That circuit control board is a result of the idea that we still want to have single push buttons for single actions, just like we do now.

Even though they may be multiplexed, the idea of going to a particular place in the control board and finding a particular valve or an auto-manual station and working it in much the same way that current control boards are worked, is still the way the switch board is done.

It's laid out a little bit differently, but it has that basic philosophy of one switch for one control action. However, the rest of it, even though it looks somewhat similar, I think is significantly different. We've gone back once again in trying to understand how the pieces -- the alarm system, the DTL display or information system and the control actions -- how to lay those out is determined by a combination of the decision-making model and the idea of the functional layout that -- the functional structure that tells you about what the plant processes are about.

In the case of the vertical sections of this board, the decision-making model is prevalent. The alarm system, as I talked about a moment ago, review, as the entry point in the decision-making process. In looking at designing a new control board, we went back and looked at a lot of annunciator system designs.

One of the things that is predominantly useful about traditional annunciators is the special dedication idea. Operators have found that putting particular issues in particular spots and leaving them there is very effective. So

we tried to capture that.

The difference is that we have laid it out in a functional sense. So all the alarms about pressure and temperature are captured in specific sections of the board. The sections are then divided into goal achievement versus process. So the operator comes into this alerted that there is a problem, gets some indication about where it is -- it's in the RCS temperature arena.

It's a goal achievement meaning that the temperature is not being controlled within its normal band. There's a process somewhere that has failed and he can get a better idea then of where the display system he needs to go to find additional information.

So the alert, state identification begins with the alarm system. The planning issues, determining what states need to be changed, what components need to be altered, and in what direction is done here. Finally, the detailed control actions are located down here for these functions.

So in the vertical sense, you get now the monitoring, planning, control. The feedback gets almost the reverse. In the details of feedback, you see the components, lights change indicating that hopefully the components did change. You begin to see that the functional measurements of flow and pressure begin to change and you finally begin to see the alarms disappear if things were done correctly.

The radial direction things are laid out functionally the way energy flows. So, in effect, on the lefthand side, you'll start with the reactivity issues, control, and that kind of thing, and move through the energy process until, on the righthand side, you wind up with the steam generators and the steam turbine and finally the generator.

The far wings of the board are the vital electric power and th_ non-vital electric power. The things that are less essential, if you will, to the energy flow process.

So the control board we've looked at is circular for a number of reasons, one of which is that we put a supervisor's work station, if you will, in the center of it.

[Slide.]

MR. EASTER: This is a full-sized plywood mockup. I think some of you on occasion have seen. This central station is set up to handle the shift supervisor or the control room senior reactor operator. He has access to all the plant data. He's got a Reg Guide 197 Plasma that allows him to use those displays that are pertinent to the 197 application, which, in fact, are subsets of the total set of displays, so that the continuity is maintained from normal operation through the various phases of abnormal operation.

There are multiple places where 197 can be picked up around the board for the operators. There is a support panel for the alarm system that allows the operators to query the

alarm system. The alarm system can be looked at as a means for the plant to talk to the operator.

We also provide more of an operator-paced kind of thing where the operator can query the alarm system for set points and for logic, for other things that are -- for other messages that might be related that are in the various alarm system queues, etcetera, and can interrogate the alarm system pretty well from one end to the other.

We find that having it circular like this aids the communication; both visually, this fellow can see everything. He has a minimum amount of error parallax at seeing various alarms, watching what the operators are doing.

Also, from the point of view of verbal communications, this kind of environment is pretty good from the acoustics. The operator standing at the bench board can talk straight into the board and because of the concavity of the board and the circular shape, this fellow has no difficulty hearing them.

In fact, you find that when you go into this room that you can actually hear them better if they're talking into the board rather than turning around and facing this shift supervisor.

MR. WARD: So there are reactivity control stations all the way around here?

MR. EASTER: The control rods are right in this

vicinity. We've put a sit-down section that's primarily a monitoring section, two segments right in the middle for the normal -- when things are just going straight and level.

So the idea of operation is that the operator would be sitting here monitoring the performance. He might get an alarm, figures out what it is he needs to do and comes up and makes the control action and comes back.

There is on each section the functional arrangement. Functionally, each of the control sections has got the controls, the displays and the alarms for those functions that are consistent with each other. So he can do much of the monitoring that he needs to do from a stand-up position if he desires.

So if he gets into some kind of abnormality that requires a lot of attention out here, he can still get all that information. But in a normal, I'll say power operation where it isn't essential that he be standing in front of a particular control bench, we give him a central station that's got telephones and that kind of thing, but no great deal -- set of controls.

Does that answer your question?

MR. WARD: Yes. This is a lot newer than the 1984-85 era design, right?

MR. EASTER: Not really. It's basically, essentially the same.

MR. WARD: Is that right?

MR. EASTER: Yes. The waste heat systems are over here, containment system here, reactivity control, pressure and temperature control, steam generator control, turbine control, etcetera, goes around like that. So we've still got essentially the same split.

We've got a reactor operator on the lefthand side; if you will, a balance-of-plant operator on the righthand side; and, a senior supervisor in the center. The idea, again, is that strategy for this fellow, tactics for these two guys. So the idea here is that this fellow does more of the overall plant health, plant state analysis and setting the direction for various systems and components to be placed in. And these two fellows at the bench board are in charge of trying to get the particular systems or particular components into those states.

The alarm system is kind of the focus point where all fo the members of the control board have then equal visibility to the alarm system and can focus the discussion of their actions about the alarms that are existing and whether -- and what kinds of actions need to be taken to clear them.

Now, again, I've shown you and focused this presentation on the control board and the control room, but the kinds of -- this kind of thinking, this kind of process needs to be put through to the remote shutdown panel, the ERF, the

TSC, the local panels, etcetera. That's the intent of what we've done.

The design that we have, however, is focused also on the control and we haven't necessarily done a lot of detailed design with local panels. We've done some work with the technical support centers, etcetera.

In the interest of time, let me ask if -- it's been very fast and I haven't covered all the slides necessarily, but are there any questions that I can quickly answer and still keep you all on schedule?

MR. CARROLL: I'm looking at the draft SER, the three pages that deal with this subject, four pages, and I guess what I conclude from it is that aside from the staff saying that -- making the very positive statement that the applicant has established a qualified multidisciplinary design team, everything else is sort of couched in language that says we're not going to really get into this at the PDA stage.

MR. DONATELL: That's correct. The finalized design hasn't been submitted. Essentially, all of Chapter 18 is off to FDA stage.

MR. CARROLL: Okay.

MR. WARD: I don't understand. On Page 18-3, it says -- I'm looking at a March 1989 one that says our staff concludes that the preliminary design analysis is acceptable. What point were you making, Jay? What are they holding open?

MR. CARROLL: For example, under three, it was a very large qualifier of this review and its conclusions apply only to the PDA phase. Staff review will continue at such time as --

MR. EASTER: We had a discussion with the staff a couple of years ago. They spent a day with us looking at these designs and talking with us about design process, etcetera.

The thing that we haven't done yet that I think the staff was concerned about is we haven't done a great deal of what I'll all testing with this design. We need to, in effect, get with a utility and to work through some of these ideas about organization and particularly about how operators will actually perform and work out in this design.

My understanding was at the conclusion of that discussion, that's pretty much where the staff was -- the conclusion they were coming to, too. We had pretty well worked through the issues of the post-TMI requirements.

Essentially, in 25 words or less, the requirements are being incorporated in the design process. So I don't have either a stand-alone SPDS or a stand-alone menu of SPDS displays. The approach we've taken is to include the requirements of SPDS in the alarm system and couple that with the display system for, I'll say pre-trip or pre-alarm -- in order to have the requirement for the continuity of the SPDS operational prior to trip or prior to alarms going off so you

can see the excursion transpire.

The coupling between the alarm system and the display system is the way we're approaching the SPDS requirement. Similarly, other systems or other requirements that came after Three Mile Island are being incorporated in the design. 0700, we're putting the design review issues straight into the design of the layout of the board while we do it, rather than going back and doing a separate design review.

The only system that is really still an independent system, and it was ever before Three Mile Island, is the PAMS or Reg Guide 197 and Gil talked a little bit about that in terms of the processing equipment that is used for that.

It has its own display, as I pointed out here, in the control board. The displays that appear on it will be and are subsets of the displays that are used in normal operation. So that, in a capsule, is the way we'd address those.

MR. CARROLL: All right. I guess what I was getting to is what would ACRS say about this particular issue, other than good luck, Westinghouse, and we'll talk some more about it at the FDA stage?

MR. DONATELL: Yes.

MR. KERR: It seems to me that this issue is like what are, to me, a surprising number of other issues that I encountered in the PDA; namely, that we haven't really reached a conclusion yet. I'm beginning to wonder what the purpose of

the PDA is, but maybe I will learn more as we discuss it further.

MR. CARROLL: Okay. I want to thank the staff and Westinghouse for some very good presentations today. I guess we'll see you at the next meeting.

[Whereupon, at 4:04 p.m., the Subcommittee was adjourned.]

REPORTER'S CERTIFICATE

This is to certify that the attached proceedings before the United States Nuclear Regulatory Commission

in the matter of:

NAME OF PROCEEDING: Meeting of the Advanced Pressurized Water Reactor Subcommittee

DOCKET NUMBER:

PLACE OF PROCEEDING: Bethesda, Maryland

were held as herein appears, and that this is the original transcript thereof for the file of the United States Nuclear Regulatory Commission taken by me and thereafter reduced to typewriting by me or under the direction of the court reporting company, and that the transcript is a true and accurate record of the foregoing proceedings.

Marilynn Nations

Marilynn Nations
Official Reporter
Ann Riley & Associates, Ltd.

RESAR SP/90 PDA
REVIEW STATUS

A PRESENTATION TO THE
ACRS SUBCOMMITTEE ON
ADVANCED PRESSURIZED REACTORS

LOREN DONATELL, PROJECT MANAGER

JANUARY 10, 1990

PRELIMINARY DESIGN APPROVAL

- 13 HAVE BEEN ISSUED
  - LAST WAS NOVEMBER 14, 1978

- RESAR SP/90 PDA IS THE FIRST TO INCLUDE SEVERE ACCIDENT POLICY STATEMENT IN REVIEW

- CONSTITUTES A REFERENCE DESIGN
  - CONSTRUCTION PERMIT APPLICATION
  - MANUFACTURING PERMIT APPLICATION

- REQUIRES DESIGN DETAIL EQUIVALENT TO A PSAR
  - DEFINED IN 10CFR50.34

- SUBJECT TO 10CFR50.109

CURRENT REVIEW STATUS

Accomplishments to January 1990

DSER PRA "FRONTEND"	MARCH 1988
ACRS SUBCOMMITTEE	APRIL 1988
DSER - SRP	JUNE 1988
DSER - SRP	MARCH 1989
WESTINGHOUSE RESPONDED TO OPEN ITEMS	JUNE-SEPTEMBER 1989
ACRS SUBCOMMITTEE	SEPTEMBER 1989
WESTINGHOUSE SUBMITTED AMENDED USIs/GSIs	OCTOBER 1989
ACRS SUBCOMMITTEE	NOVEMBER 1989
COMMISSION APPROVED JUNE 1990 COMPLETION OF THE PDA	DECEMBER 1989
ACRS SUBCOMMITTEE	JANUARY 1990

OPEN ITEMS

ACCEPTABLE	50
FDA COMMITTMENT	18
> FDA	2
MINOR	9
UNKNOWN	15
PROBABLE OPEN	13

SCHEDULE TO COMPLETE PDA REVIEW

items to be accomplished

ACRS SUBCOMMITTEE — FEBRUARY 1990

Re: DSER CHAPTERS

NRC ISSUES DRAFT FINAL SER — MARCH 1990

ACRS SUBCOMMITTEE — APRIL 1990

Re: DRAFT FINAL SER

ACRS FULL COMMITTEE — MAY 1990

Re: DRAFT FINAL SER AND REQUEST LETTER

NRC ISSUES FINAL SER, — JUNE 1990

PDA DECISION AND SSER

W ADVANCED PWR

BRIEFING ON

RESAR-SP/90

ACRS SUBCOMMITTEE

ON ADVANCED PWRs

JANUARY 10, 1990

E1:15

W RESAR-SP/90
ACRS SUBCOMMITTEE ON APWRs

PURPOSE

- REVIEW THE STATUS OF THE NRC SAFETY EVALUATION OF RESAR-SP/90 PARTICULARLY WITH RESPECT TO THE STANDARD REVIEW PLAN FOR FSAR CHAPTERS 7, 9, 10, 11, 12, 15, AND 18

- SEVERE ACCIDENT ISSUES AND PRA WERE COVERED IN SEPTEMBER 1989 SUBCOMMITTEE MEETING

- CHAPTERS 3, 4, 5, 6, AND 8 WERE COVERED AT THE NOVEMBER 1989 SUBCOMMITTEE MEETING

- COVERAGE OF CHAPTERS 13, 14, 16, AND 17 IS NOT ANTICIPATED AS PART OF THE ACRS REVIEW FOR THE PDA

W RESAR-SP/90
ACRS SUBCOMMITTEE ON APWRs

LIST OF ACRS/W RESAR-SP/90 MEETINGS

3/23/82 SUBCOMMITTEE ON SAFEGUARDS AND SECURITY (ALBURQUERQUE)

5/5/83 WESTINGHOUSE SUBCOMMITTEE

8/10/83 WESTINGHOUSE SUBCOMMITTEE

9/25/83 WESTINGHOUSE SUBCOMMITTEE

11/6/87 FULL-COMMITTEE
- ACRS 12 RECOMMENDATIONS OF JAN. 15 LETTER

4/6/88 ADVANCED PLANT SUBCOMMITTEE
- REVIEW OF DRAFT SER ON PROBABILISTIC SAFETY STUDY

9/28/89 ACRS SUBCOMMITTEE ON APWRs
- REVIEW OF DRAFT SERs
- SEVERE ACCIDENT ISSUES

11/3/89 ACRS SUBCOMMITTEE ON APWRs
- REVIEW OF DRAFT SER CHAPTERS 3, 4, 5, 6 & 8

1/10/90 ACRS SUBCOMMITTEE ON APWRs
- REVIEW OF DRAFT SER CHAPTERS 7, 9, 10, 11, 12, 15 & 18

*3/x/90 ACRS SUBCOMMITTEE
- COMPLETE OPEN ITEMS

*4/x/90 ACRS FULL COMMITTEE
- REVIEW OF FINAL SER

* NOT SCHEDULED, SUBJECT TO CONFIRMATION BY STAFF & ACRS

W RESAR-SP/90
ACRS SUBCOMMITTEE ON APWRs

DRAFT SAFETY EVALUATIONS REPORTS

		RESPONSE STATUS
PRA FRONT END (MARCH 21, 1988)	o ACRS SUBCOMMITTEE MEETING ON APRIL 6, 1988 o PDA OPEN ISSUE 107	8/31/89
AUXILIARY REVIEW (JUNE 10, 1988)	o 7 OPEN ITEMS	
SYSTEMS REVIEW (MARCH 9, 1989)*	o 40 PDA OPEN ISSUES PLANT/REACTOR/AUXILIARY SYSTEMS	6/9/89
	o 41 PDA OPEN ISSUES STRUCTURAL/MECHANICAL SYSTEMS	6/28/89
	o 26 PDA OPEN ISSUES TRANSIENT ANALYSES/ SINGLE FAILURE	8/31/89
PRA BACK END	NOT RECEIVED	
USIs/GSIs	o USIs & HIGH/MEDIUM GSIs SUBMITTED	5/23/88

*INCLUDES 7 OPEN ISSUES FROM JUNE 1988 DSER

MEETING AGENDA
JANUARY 10, 1990 ACRS SUBCOMMITTEE

RESAR-SP/90 PDA OPEN ISSUES

8:30 - 8:40	ACRS OPENING REMARKS	J.C.CARROLL
8:40 - 8:50	STAFF INTRODUCTION	L.DONATELL
8:50 - 9:00	W INTRODUCTION	E.M.BURNS
9:00 - 9:30	GENERAL PLANT ARRANGEMENT	T.VAN DE VENNE
9:30 - 11:00	CHAPTER 7 - INSTRUMENTATION & CONTROL	G.W.REMLEY
11:00 - 12:00	CHAPTER 18 - CONTROL ROOM & HUMAN FACTORS ENGINEERING	J.R.EASTER
12:00 - 1:00	-- LUNCH BREAK --	
1:00 - 2:00	CHAPTER 9 - AUXILIARY SYSTEMS	T.VAN DE VENNE
2:00 - 2:30	CHAPTER 10 - STEAM AND POWER CONVERSION	T.VAN DE VENNE
2:30 - 3:00	CHAPTER 11 - WASTE MANAGEMENT	T.VAN DE VENNE
3:00 - 3:30	CHAPTER 12 - RADIATION PROTECTION	W.A.HENNINGER
3:30 - 4:30	CHAPTER 15 - ACCIDENT ANALYSIS	E.L.CARLIN

W RESAR - SP/90
ACRS SUBCOMMITTEE ON ADVANCED PWRs

STATUS OF DRAFT SER OPEN ISSUES (PDA)

- 107 INITIAL DSER OPEN ISSUES
- CURRENT STATUS
  - 54 HAVE PRELIMINARY STAFF APPROVAL
  - 33 REQUIRE ADDITONAL EFFORT TO RESOLVE
  - 6 TO BE DEFERRED TO FDA SUBMITTAL
  - 14 NO NRC FEEDBACK
- RESOLUTION TO BE REFLECTED IN FINAL SER

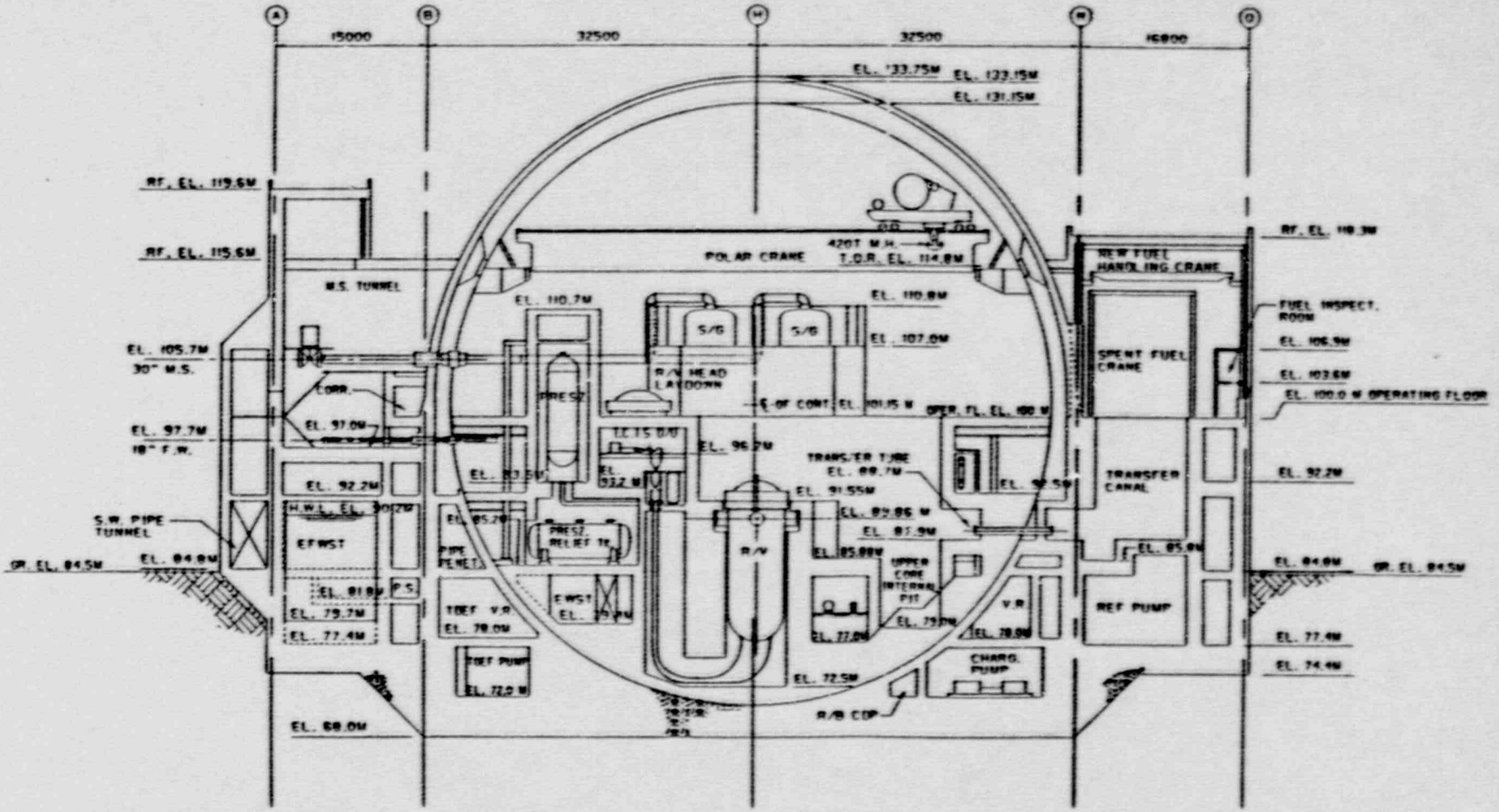
APWR

GENERAL ARRANGEMENT

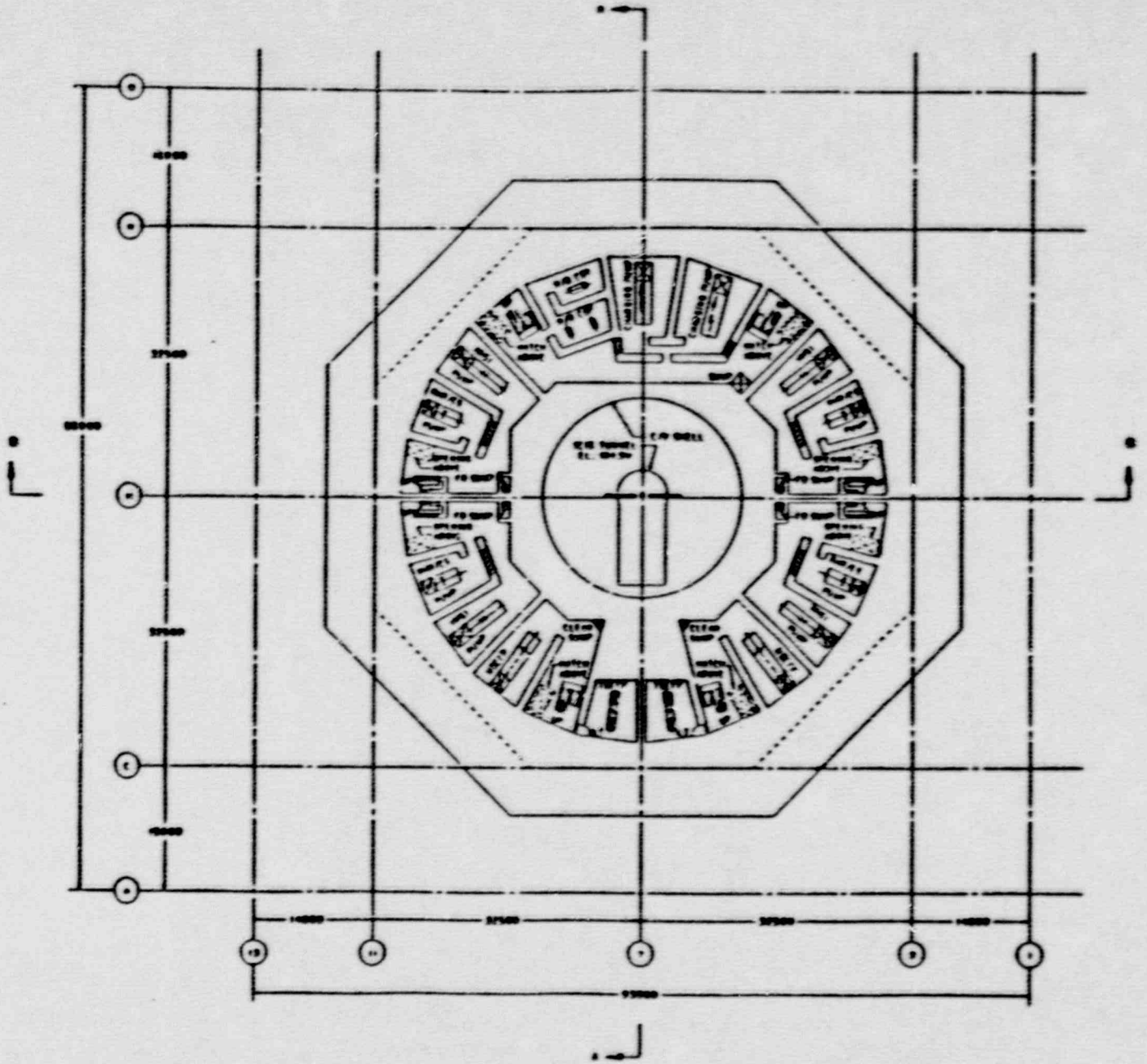
(CHAPTER 1)

APWR REACTOR BUILDING

SECTION

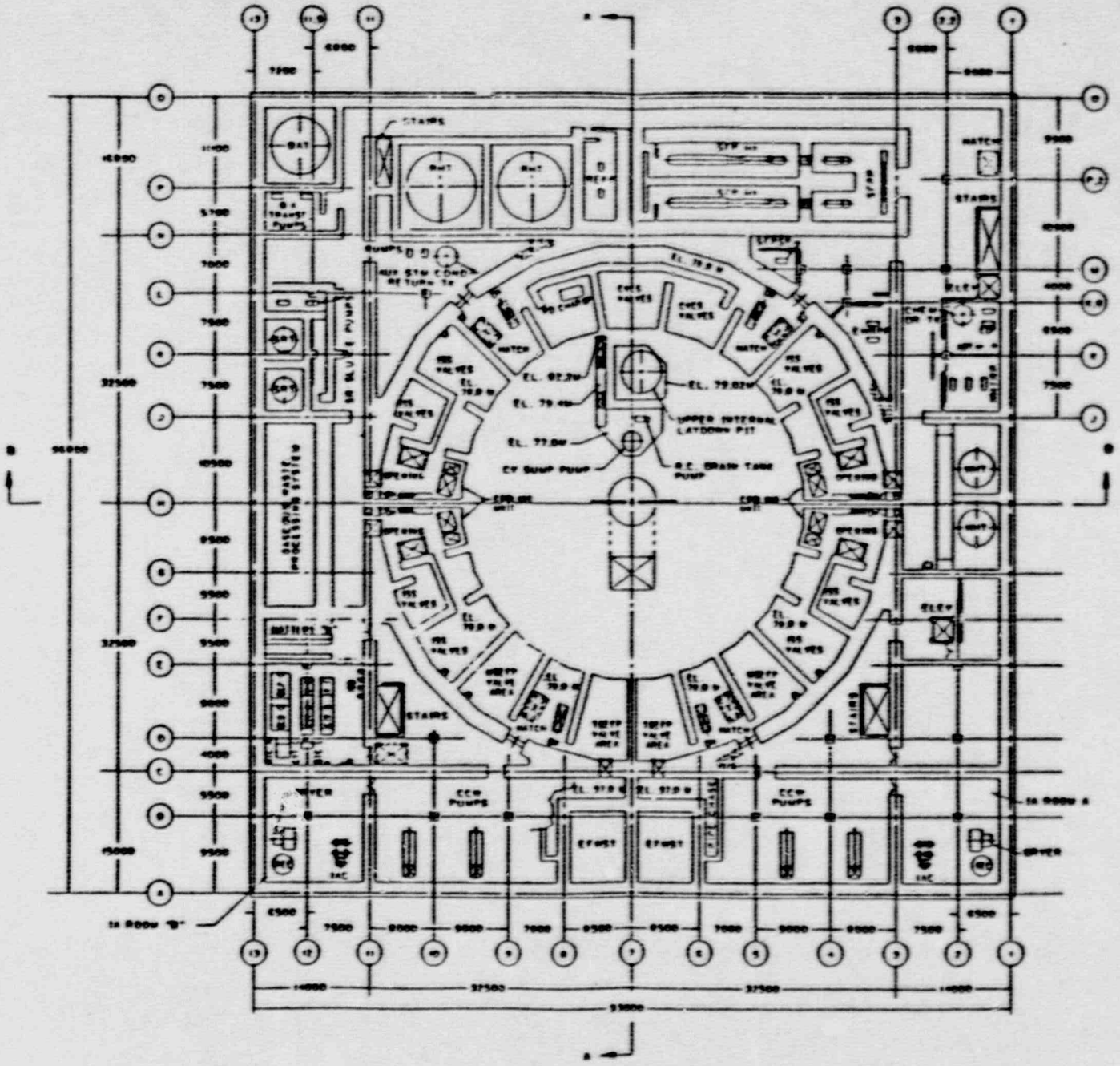


APWR REACTOR BUILDING



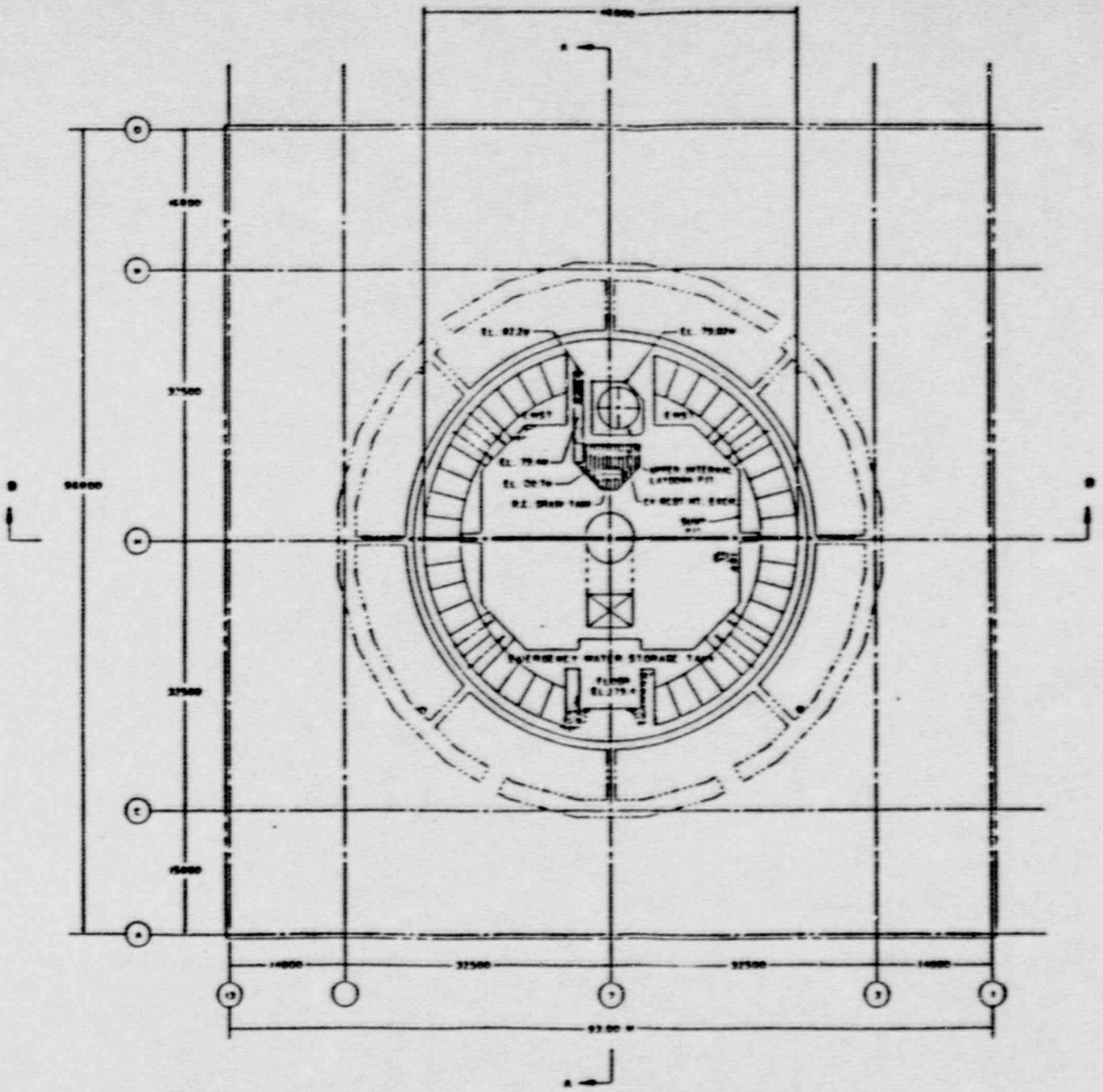
El. 72.0 m

APWR REACTOR BUILDING



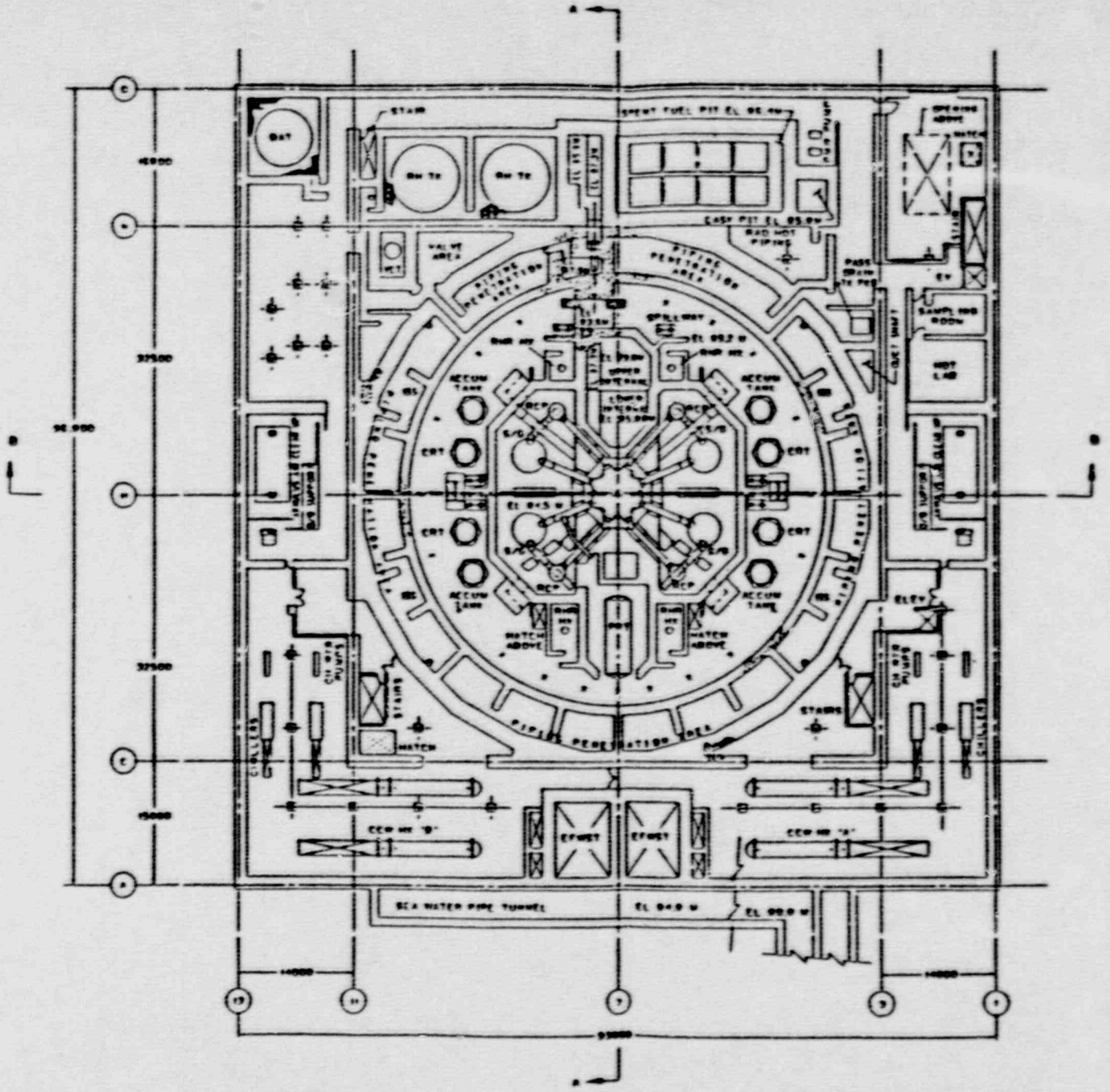
El. 77.4 m

APWR REACTOR BUILDING



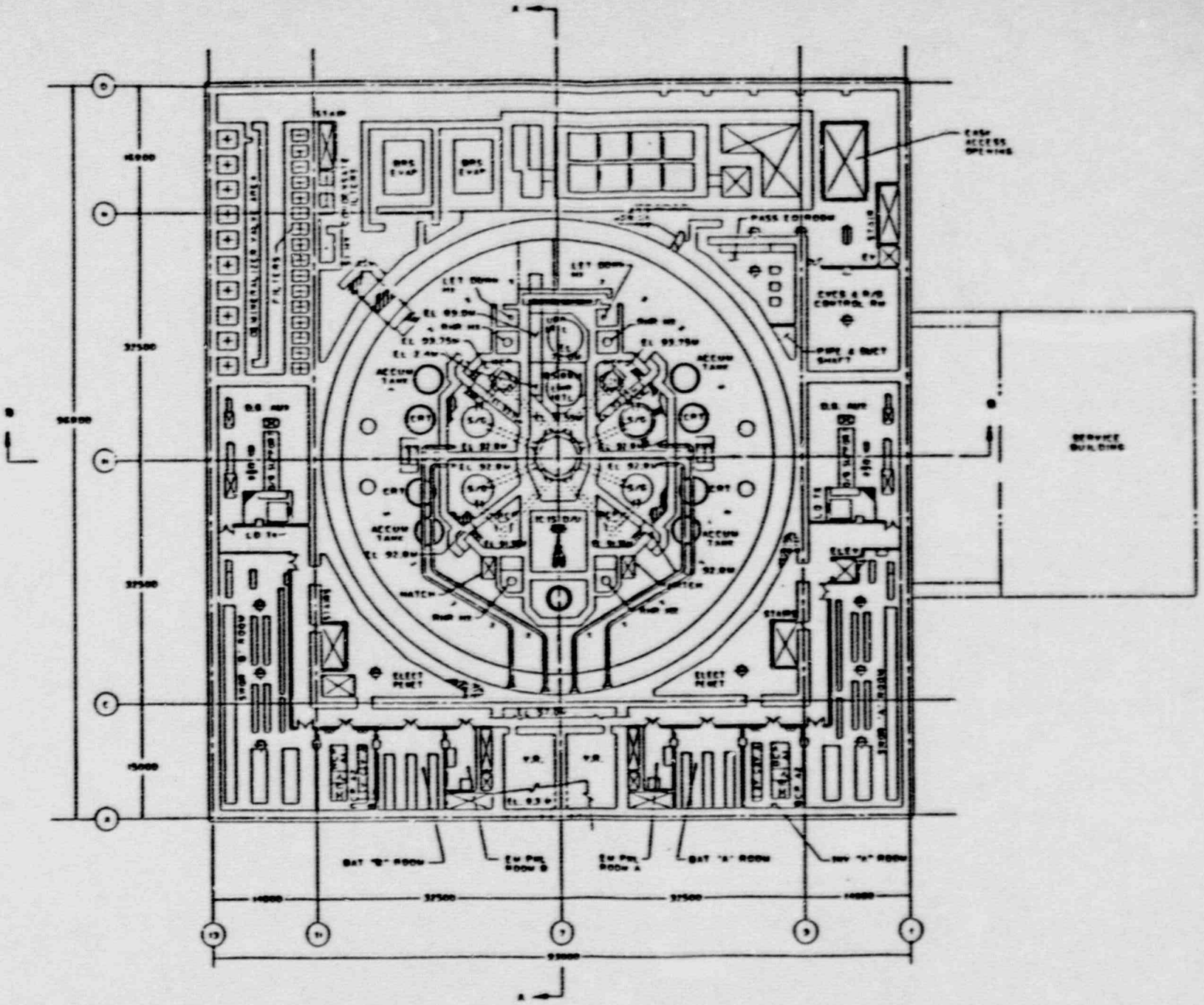
El. 83.2 m

APWR REACTOR BUILDING



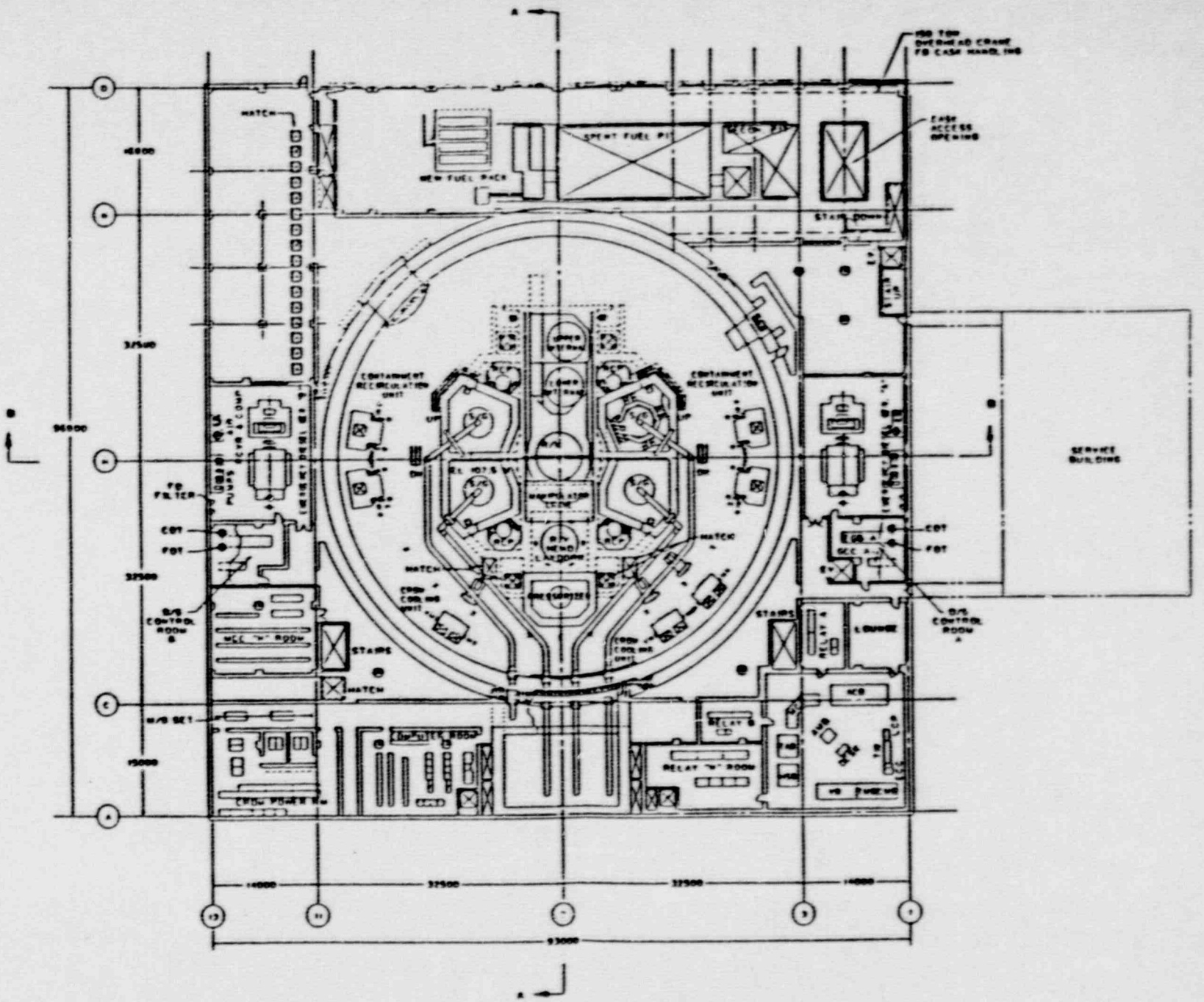
El. 84.8 m

APWR REACTOR BUILDING



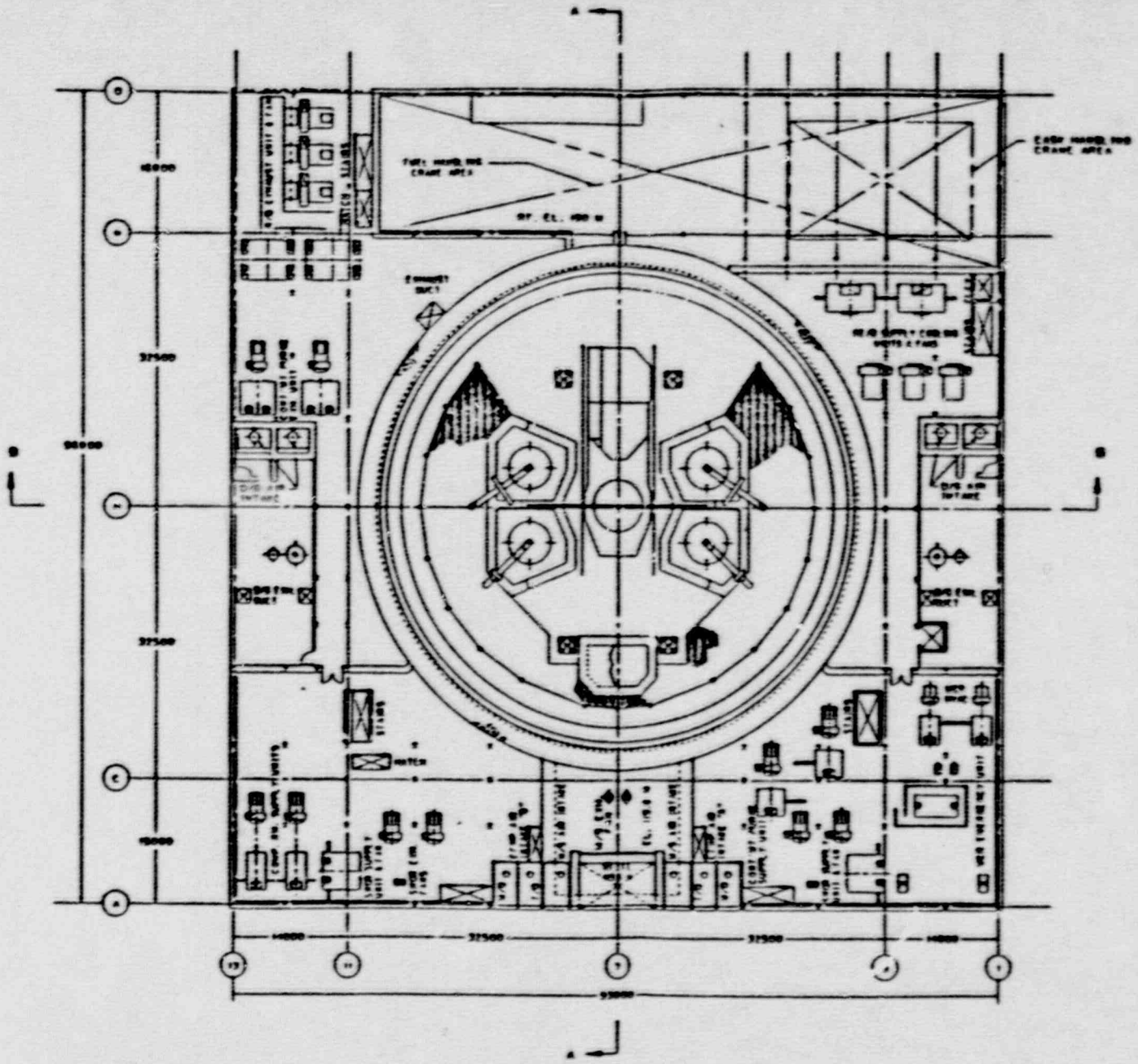
El. 92.2 m

APWR REACTOR BUILDING



El. 100.0 m

APWR REACTOR BUILDING



El. 107.6 m

W ADVANCED PWR

BRIEFING ON

RESAR-SP/90

ACRS SUBCOMMITTEE

ON ADVANCED PWRs

CHAPTER 7

INSTRUMENTATION

AND

CONTROLS

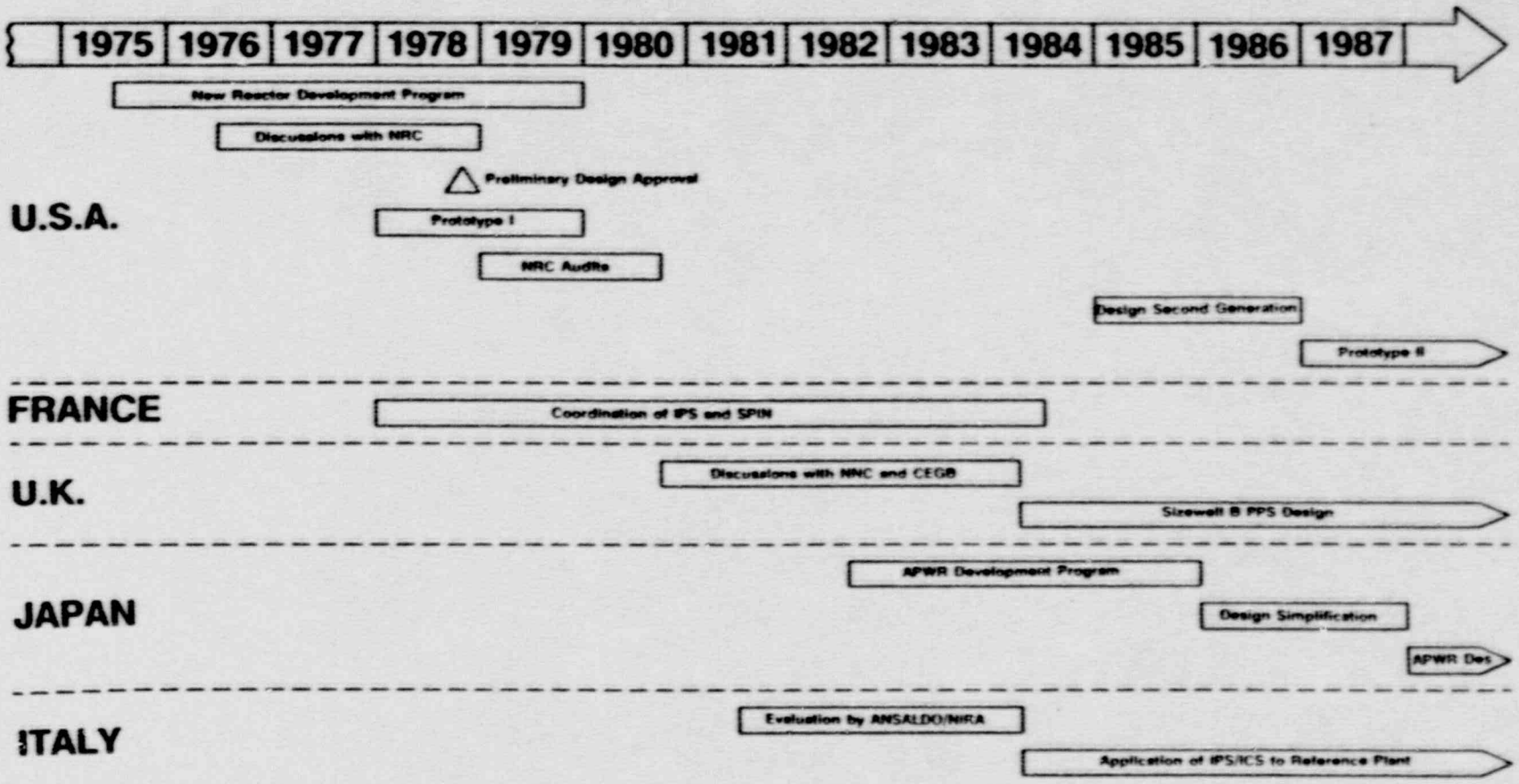
JANUARY 10, 1990

E1:15

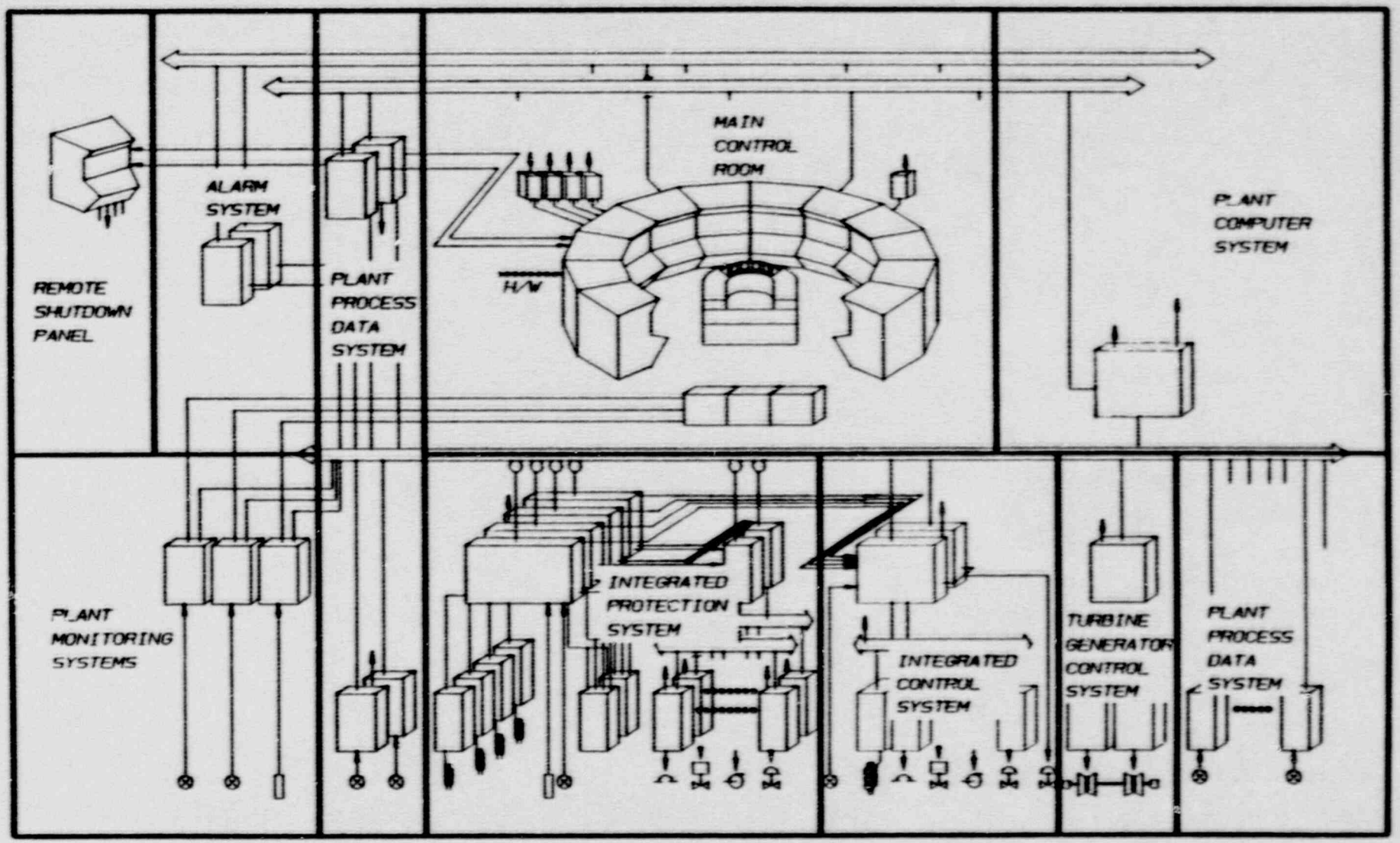
DESIGN EVOLUTION

1080 D19799 001

HISTORY OF WESTINGHOUSE ADVANCED I&C DEVELOPMENT



I&C ARCHITECTURE



INSTRUMENTATION AND CONTROL SYSTEMS

- I&C architecture overview
- Integrated protection system (IPS)
- Integratd control system (ICS)
- Integrated logic system (ILS)
- Main control room (MCR)
- Plant alarm system
- Plant process data system
- Plant computer system
- Plant monitoring system

Instrumentation & Control Systems
OVERVIEW

- Digital technology:
  - 32-bit plant computer system
  - 16-bit microprocessors
  - Distributed digital processing architecture
  - Multiplexed communications
  - Fiber optic cabling
  - Sophisticated control and protection algorithms
  - Fault-tolerant design

Instrumentation & Control Systems
OVERVIEW

Westinghouse objective:

- Use digital electronic technology to provide improvements
  - Availability
  - Operability
  - Maintainability
  - Construction schedule
  - Costs
  - Flexibility for the future
- Integration of total plant instrumentation and control systems

INSTRUMENTATION & CONTROL SYSTEMS OVERVIEW - DESIGN EVOLUTION

Item	Previous		Current
Architecture:	Central Processing	→	Distributed Processing
Communications:	Hardwired	→	Multiplexing, Fiber Optics
Protection and Control Logic:	Solid State, Relays	→	Digital, Microprocessors
Westinghouse Scope:	System Level Actuation	→	Component Level Actuation

1050 D19799 043

INSTRUMENTATION & CONTROL SYSTEMS OVERVIEW - DESIGN EVOLUTION

Item	Previous		Current
Signal Selection:	Manual	→	Automatic
Testing:	Manual	→	Automatic, Functional, Self Diagnostic
Availability:	2/4→1/3 Logic	→	2/4→2/3 Logic
Cabinetry and Hardware:	System Specific Design	→	Standard Modules
Information Displays:	Analog and Some CRT Displays	→	Graphic CRT, Qualified Plasma Displays and Same Analog

1050 D19799 044

INSTRUMENTATION & CONTROL SYSTEMS OVERVIEW - SEPARATION FEATURES

- Distributed digital architecture with layout flexibility
- Fiber optic signal transmission prevents fault propagation
- Clean separation of safety trains and channels
- Clean separation of safety and non-safety equipment

INSTRUMENTATION & CONTROL SYSTEMS OVERVIEW - I&C COMMUNICATIONS NETWORK

- Two types of multiplexed communications:
  - Data links
  - Data highways
- Data links for special requirements
- Hierarchy of data highways
- Serial input/output highways
- Control highways:
  - Protection logic highways A & B (C & D)
  - Control logic highway
  - Process control highway
- Data acquisition and display highways:
  - Monitor highway
- Off-site communications

INSTRUMENTATION & CONTROL SYSTEMS OVERVIEW - DATA LINKS

- Separation requirements:
  - Simplex data links
  - Clean separation between safety channels and trains
  - Clean separation between safety and non-safety equipment
- Redundancy requirements
- Time response requirements
- Subset of HDLC protocol applied to simplex data links:
  - ISO 3309-1979 for frame structure
  - ISO 4335-1979/Add. 1-1979 for data communications
- Transmission medium:
  - Fiber optical
  - Electrical (twisted shielded pair)

INSTRUMENTATION & CONTROL SYSTEMS
OVERVIEW - SERIAL INPUT/OUTPUT HIGHWAYS

- **Serial I/O bus:**
  - Main control board multiplexers
  - Integrated Logic Cabinet (ILC) I/O
  - Integrated Protection System (IPS) analog and digital test buses
- **Based on Intel "BITBUS"**
- **Performance:**
  - Transmission rate of 375 KBPS
  - Through-put of 50 KBPS
  - Average response of 2.5 millisec per message for small messages
- **Twisted shielded pair transmission medium**

INSTRUMENTATION & CONTROL SYSTEMS
OVERVIEW - CONTROL HIGHWAYS

- "Closed" systems developed by Westinghouse:
  - Number of nodes serviced is fixed
  - Masterless brcadcast system
  - Access protocol is a token bus
- Transmission medium:
  - Fiber optical
  - Coaxial
  - Dual medium (mixture of fiber optical and coaxial on same highway)
- Physical specifications:
  - Maximum number of stations is 64
  - Coaxial bus maximum length is 10 KM
  - Fiber optical highway topology radial
  - Fiber optical highway maximum distance between two stations is 2 KM

INSTRUMENTATION & CONTROL SYSTEMS
OVERVIEW - CONTROL HIGHWAYS

(Continued)

- Performance:
  - Transmission rate of 10 MBPS
  - Through-put of 3 MBPS
  - Average response of 1.5 millisec per station
- Error control:
  - CRC used in a cyclic manner
  - System response is transparent to station failure(s)
  - Source internal memory to destination internal memory data checking

INSTRUMENTATION & CONTROL SYSTEMS OVERVIEW - DATA ACQUISITION & DISPLAY HIGHWAYS

- Monitor highway not involved with active plant control
- "Open" system:
  - Interface with various types of equipment
  - Need for addition of equipment
- "Open" system requires use of accepted industry standards:
  - All hardware and software elements available to implement the monitor highway are defined in the ETHERNET Specification IEEE 802.3
  - Westinghouse is studying a monitor highway implementation as defined in the MAP Specification which is a token bus compatible with IEEE 802.4
- Coaxial transmission medium

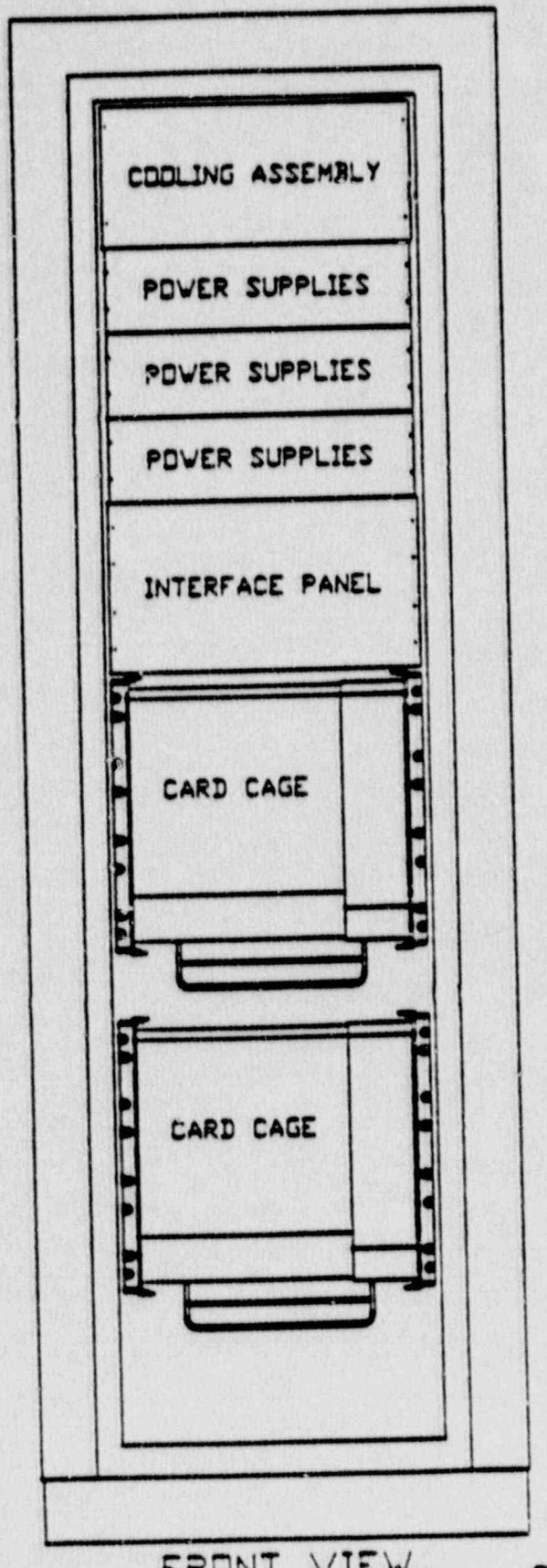
#8

Instrumentation & Control Systems - Overview
Standard Cabinet Design - Elements

- Termination frames
- Microprocessor card chassis
- AC power filter box
- AC power distribution box
- Power supply chassis
- Power supplies
- Blower and fans
- Cables
- Interface panels

1087 D20131.001

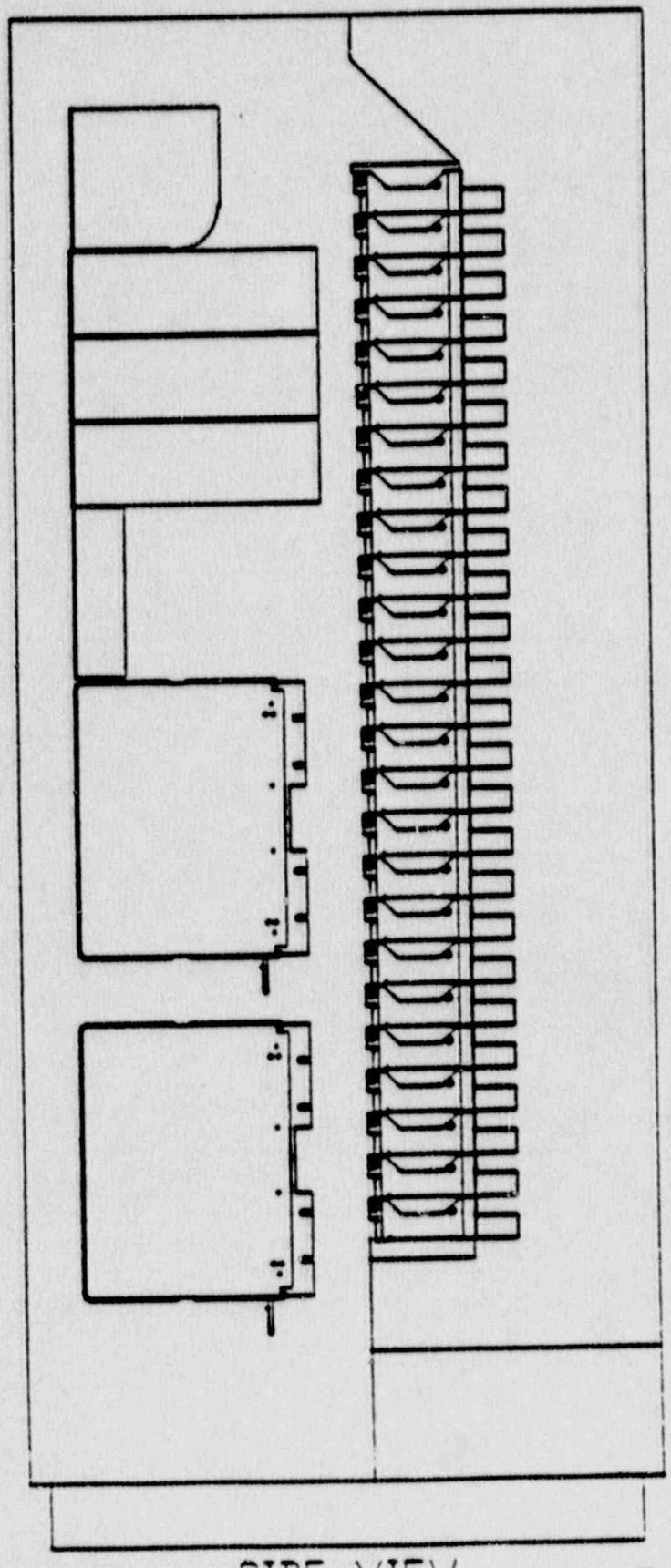
TYPICAL I&C CABINET CONFIGURATION



FRONT VIEW

SKJEH-060385 REV -

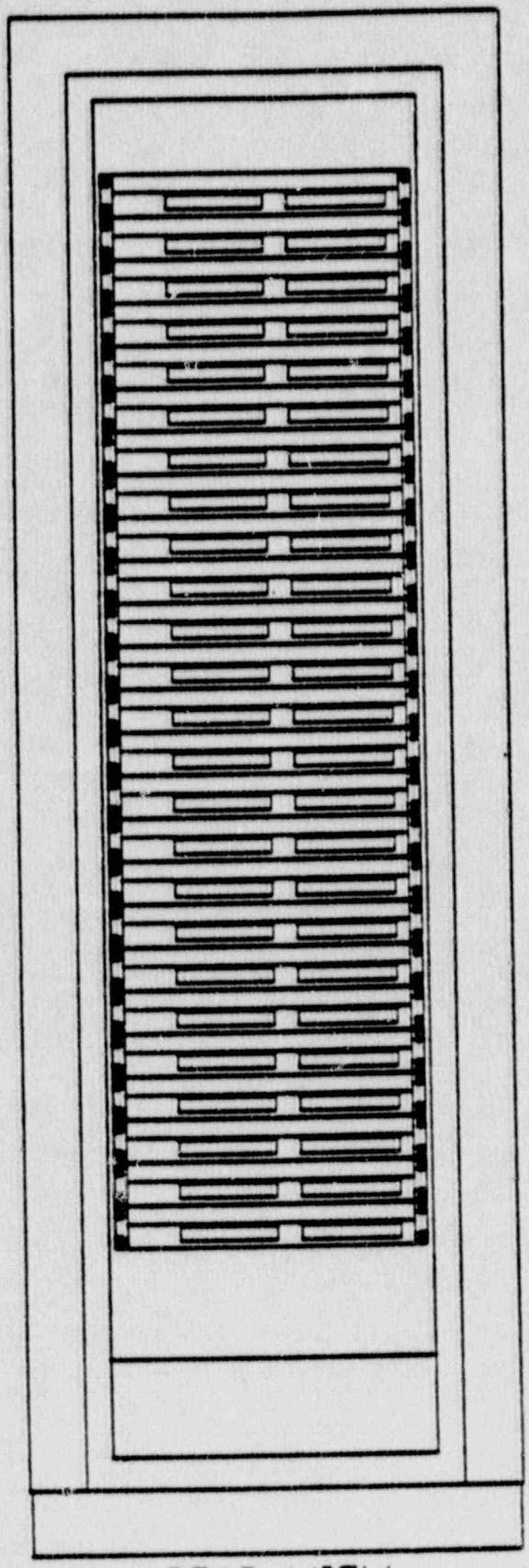
TYPICAL I&C CABINET CONFIGURATION



SIDE VIEW

SKJEH-060385 REV A

TYPICAL I&C CABINET CONFIGURATION



REAR VIEW

SKJEH-060385 REV A

Instrumentation & Control Systems Overview - Standard Cabinet Design - Environment

- Temperature:
  - 60 to 105 degrees F normal range
  - 40 to 120 degrees F abnormal range
- Humidity:
  - 0 to 95 percent (non-condensing)
  - 95 degrees F maximum wet bulb temperature
- Seismic:
  - IEEE 344-1975
- Electromagnetic interference:
  - EMI reduction window glass
  - Screened louvers
  - Cable entrance plates
  - Field wiring shielded from microcomputer wiring
  - Shielded sensor cables
  - Optical isolation

1087 D20131.012

Instrumentation & Control Systems Overview - Standard Cabinet Design - Printed Circuit Boards

- Microcomputer printed circuit cards:
  - Power from modular supplies associated with the microcomputer printed circuit card frame
  - Industrial standard computer bus (IEEE 796)
- Input/output printed circuit cards:
  - Powered from redundant 15.6 VDC supplies
  - Surge withstand capability (IEEE 472-1974)
  - Westinghouse printed circuit card design standard 71.40
  - Mounted in metal wrapper
  - Mechanical keying
  - Analog test bus (test injection and monitoring)
  - Digital test bus (test injection and monitoring)

INSTRUMENTATION & CONTROL SYSTEMS OVERVIEW - MAINTENANCE FEATURES

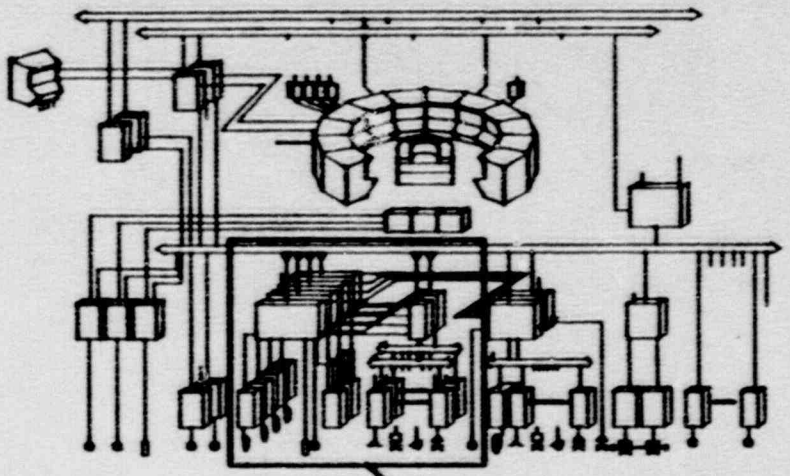
- Automatic testers in each protection cabinet satisfy periodic test requirements
- Self-diagnostics locate faults to the replaceable module within seconds
- Modular repair with standardized components
- Maintenance bypasses to allow on-line repair without error-induced trips
- Remote readout of complete system status
- Built-in troubleshooting equipment
- Total software maintenance capability on site
- Setpoints and constants are entered directly in the engineering units
- Stable, accurate calibration with a significant savings in time
- Calibration constants are maintained in non-volatile memory if power is lost

Instrumentation & Control Systems

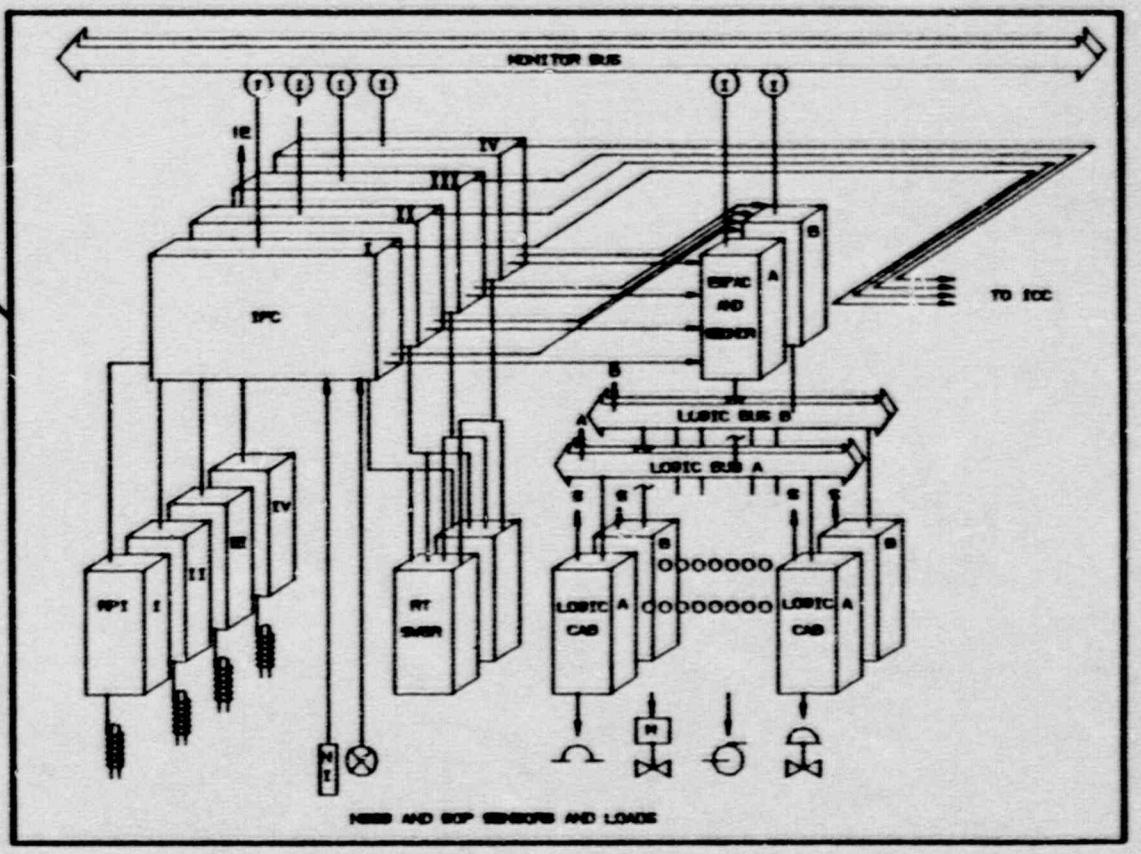
INTEGRATED PROTECTION SYSTEM

1060 D19799.004

INSTRUMENTATION & CONTROL ARCHITECTURE



INTEGRATED
PROTECTION
SYSTEM



Instrumentation & Control Systems
INTEGRATED PROTECTION SYSTEM (IPS)

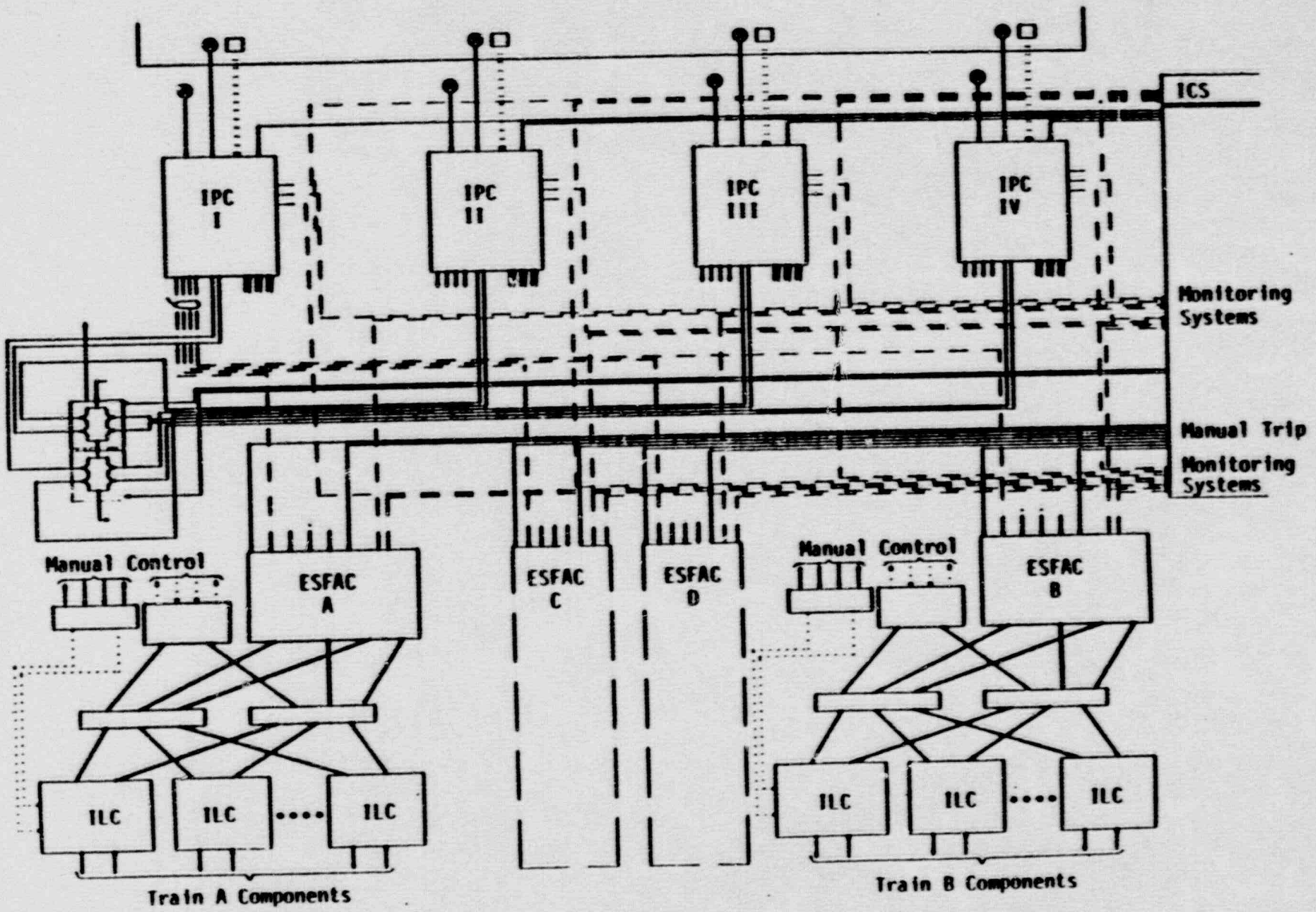
- Performs all automatic reactor safety actuations:
  - Reactor trip (RT) actions
  - Engineered safeguards (ESF) actions
- Provides interface for manual safety actuations
- Complete scope design including:
  - Nuclear instrumentation
  - Rod position measurement
  - Interposing logic for ESF actuations
  - Main control board interface
  - Emergency control board interfaces

Instrumentation & Control Systems
IPS - MAJOR GROUPS OF EQUIPMENT

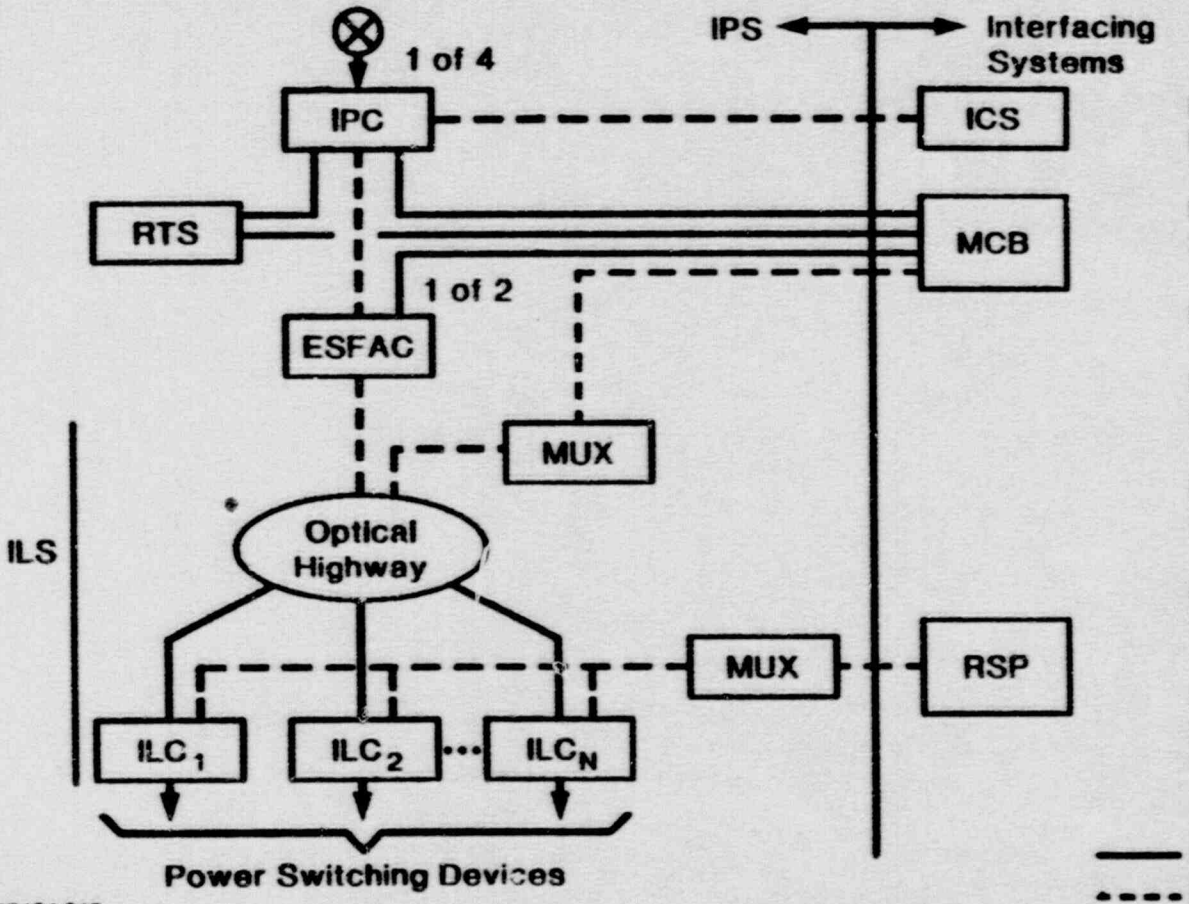
- Rod Position Indication Cabinets (RPI)
- Integrated Protection Cabinets (IPC)
- Engineered Safety Features Actuation Cabinets (ESFAC)
- Reactor Trip Switchgear (RTS)
- Integrated Logic System (ILS):
  - Protection Logic Cabinets (ILC)
  - Logic Bus
  - Control Board Multiplexers

Instrumentation & Control Systems
IPS - MAJOR GROUPS OF EQUIPMENT

- Rod Position Indication Cabinets (RPI)
- Integrated Protection Cabinets (IPC)
- Engineered Safety Features Actuation Cabinets (ESFAC)
- Reactor Trip Switchgear (RTS)
- Integrated Logic System (ILS):
  - Protection Logic Cabinets (PLC)
  - Logic Bus
  - Control Board Multiplexers


ICS
IPC I
IPC II
IPC III
IPC IV
Monitoring Systems
Manual Trip
Monitoring Systems
Manual Control
ESFAC A
ESFAC C
ESFAC D
Manual Control
ESFAC B
ILC
ILC
ILC
ILC
ILC
ILC
Train A Components
Train B Components

Instrumentation & Control Systems
IPS - SYSTEM INTERFACES



IPC: Integrated Protection Cabinet

RTS: Reactor Trip Switchgear

MUX: Multiplexers

ILS: Integrated Logic System

ILC: Integrated Logic Cabinet

ICS: Integrated Control System

MCB: Main Control Board

RSP: Remote Shutdown Panel

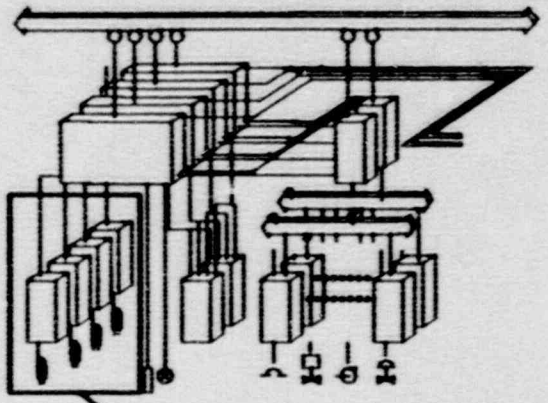
Hardwired

Multiplexed

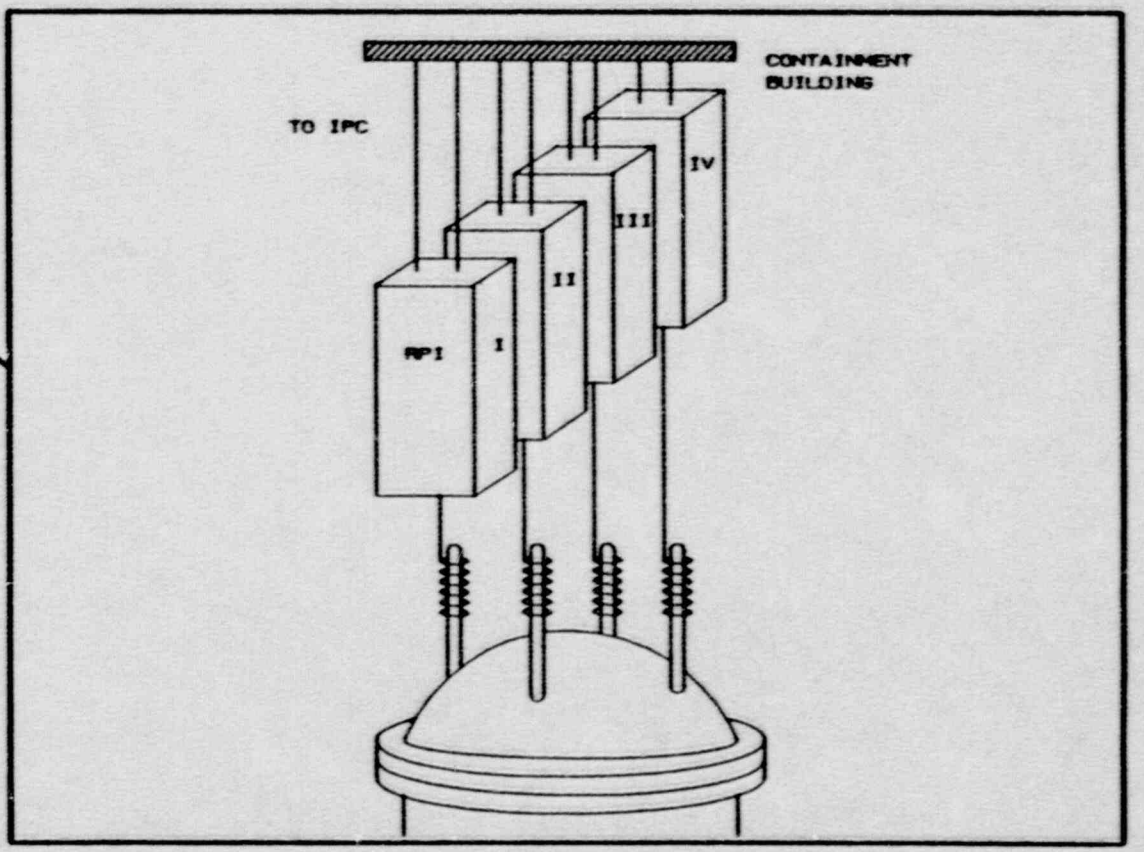
Instrumentation & Control Systems
IPS - IPC Process Inputs

- Transmitter input
- RTD input
- Contact input
- Pulse input:
  - Reactor coolant pump speed
- Nuclear instrumentation (microprocessor-based signal conditioning)
  - Source range (preamp external to IPC)
  - Intermediate range
  - Power range (four section excore detector)
  - N-16 power range

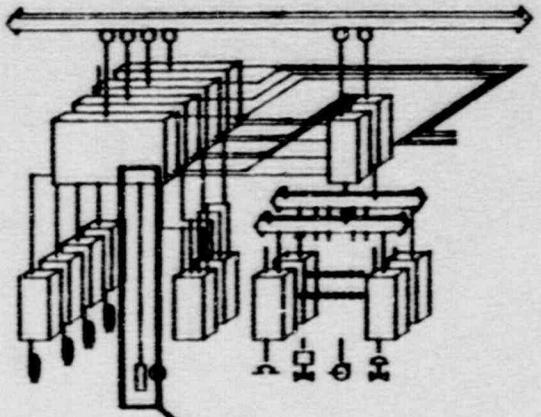
INTEGRATED PROTECTION SYSTEM



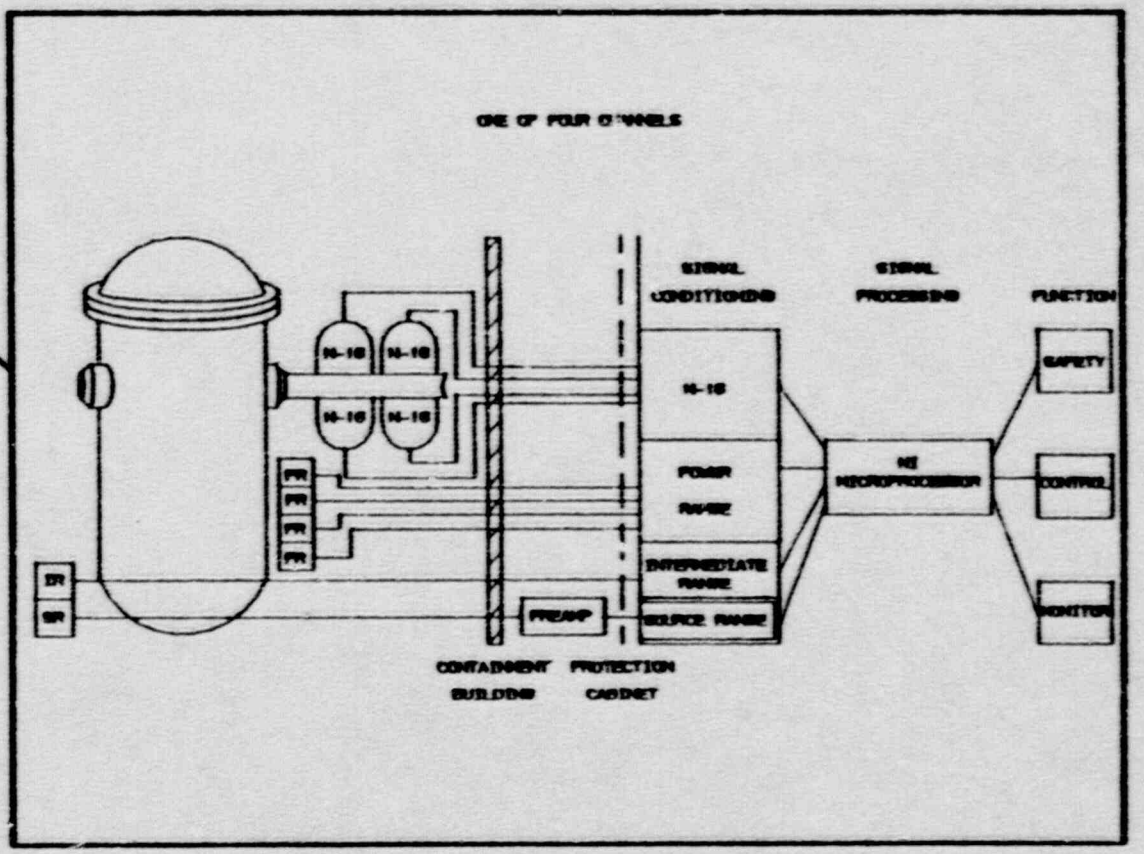
ROD POSITION
INDICATION
CABINETS



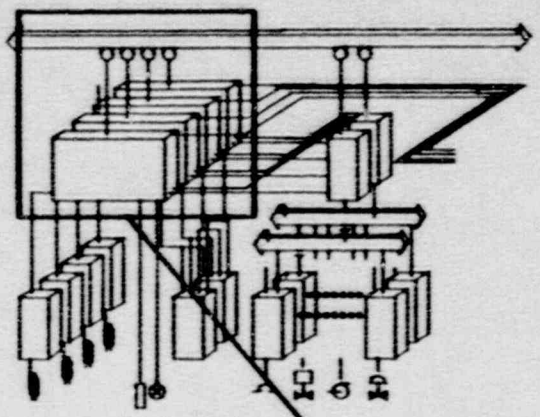
INTEGRATED PROTECTION SYSTEM



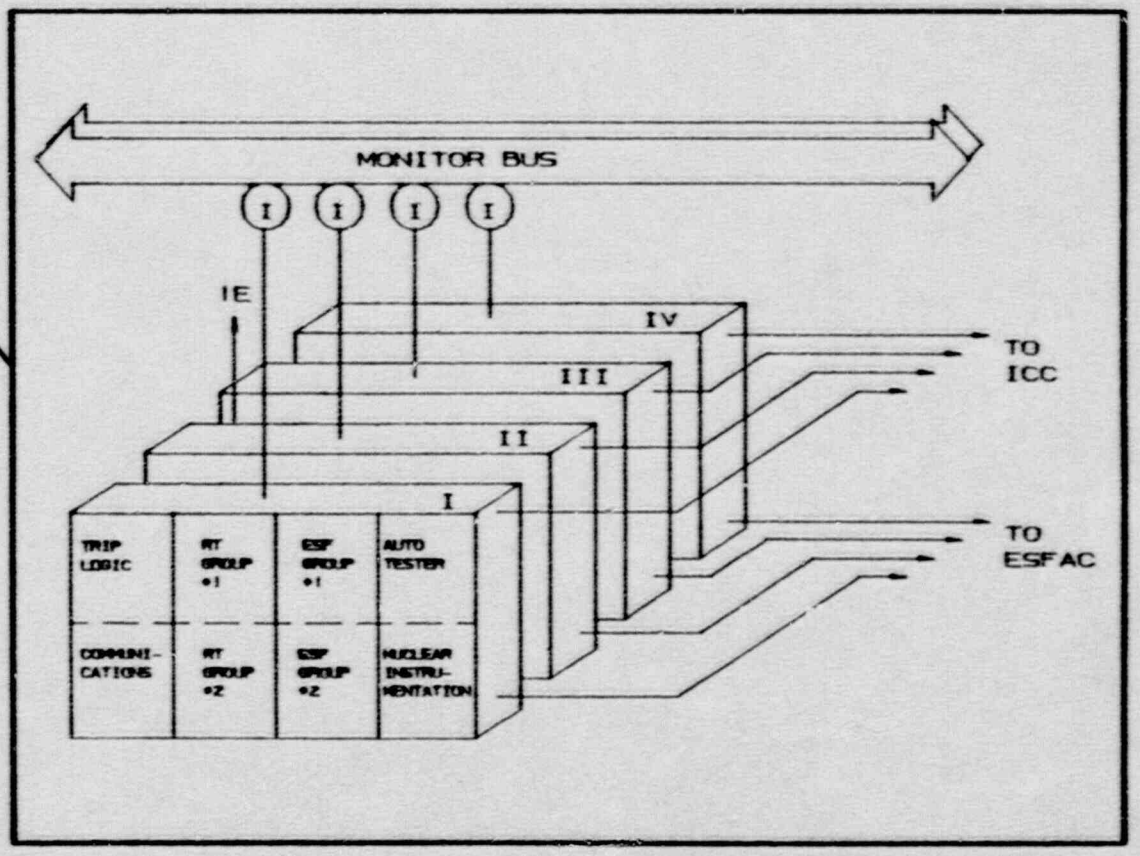
NUCLEAR
INSTRUMENTATION



INTEGRATED PROTECTION SYSTEM



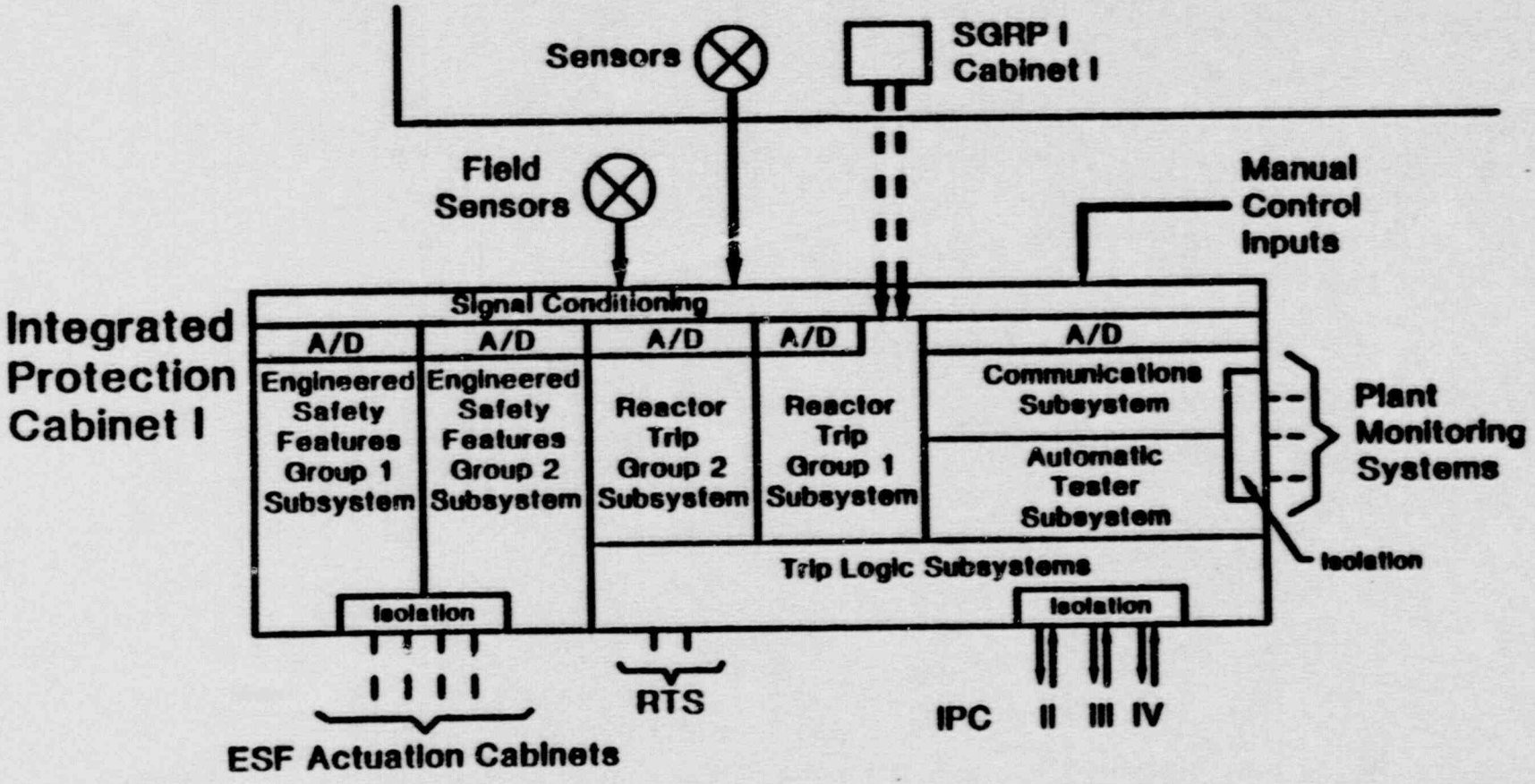
INTEGRATED
PROTECTION
CABINETS



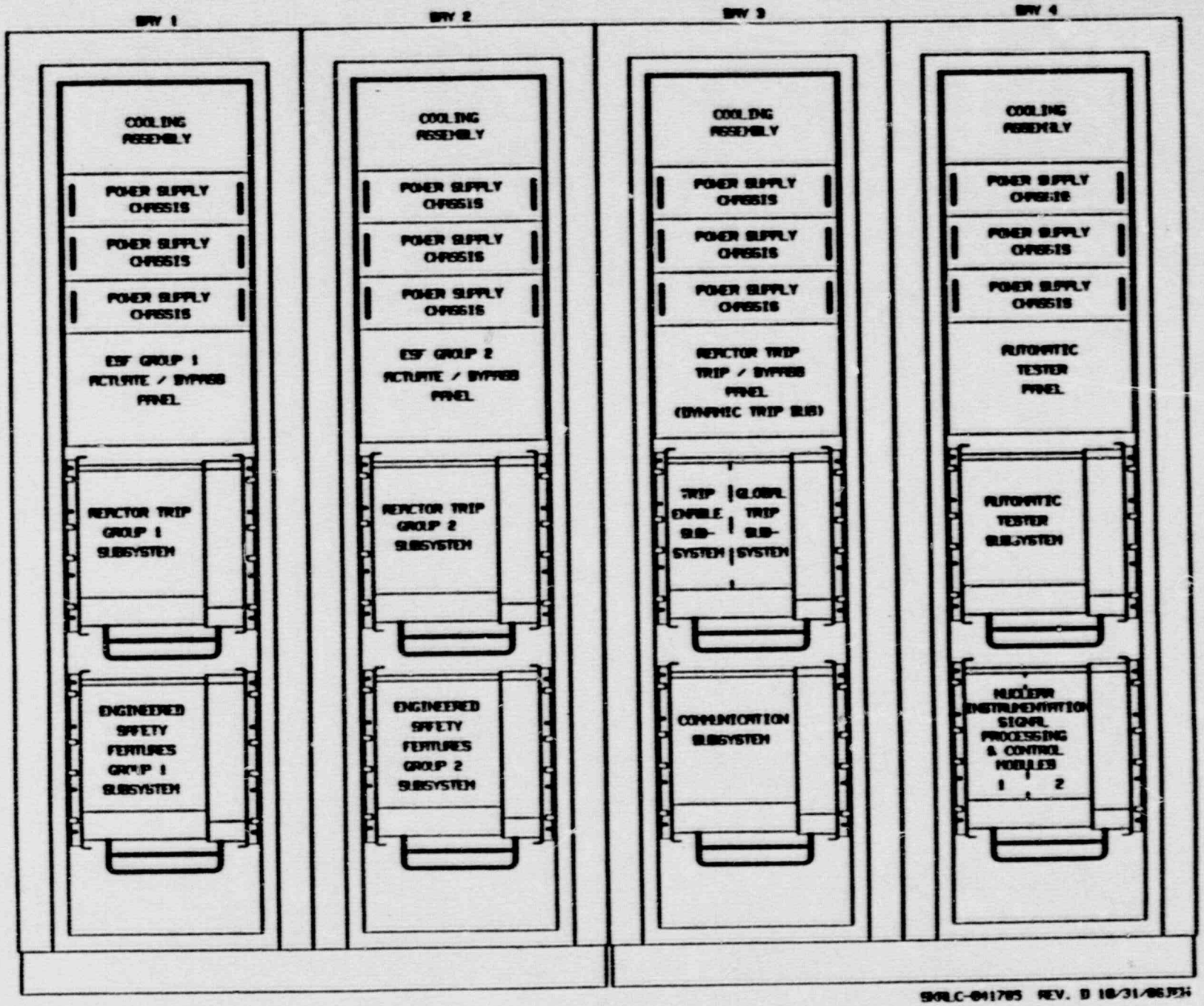
Instrumentation & Control Systems
IPS - Integrated Protection Cabinets (IPC)

- IPCs provide the following functions:
  - Receive and process inputs from plant sensors
  - Receive manual inputs from the Main Control Board
  - Convert input signals to digital logic signals representing reactor trip or ESF actuations
  - Transmit trip logic data to and receive trip logic data from three other IPCs
  - Perform two-out-of-four voting operations on received data
  - Output Reactor Trip (RT) signal to trip breakers
  - Transmit ESF trip and bypass status to ESFAC
  - Transmit process sensor data and calculated data to the Integrated Control System (ICS)
  - Transmit data to external systems (e.g., Plant Process Data System, Plant Alarm System, Plant Computer)

Instrumentation & Control Systems
IPS - INTEGRATED PROTECTION CABINET (IPC)

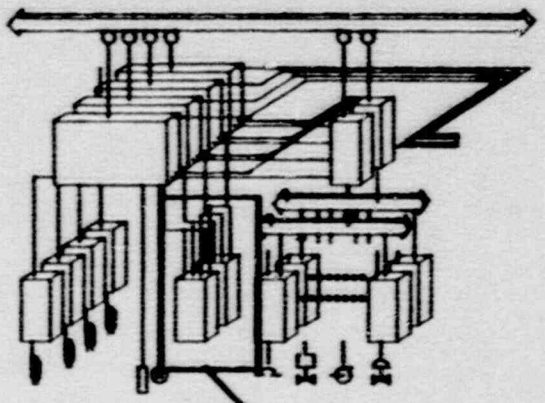


1007 D18779 024

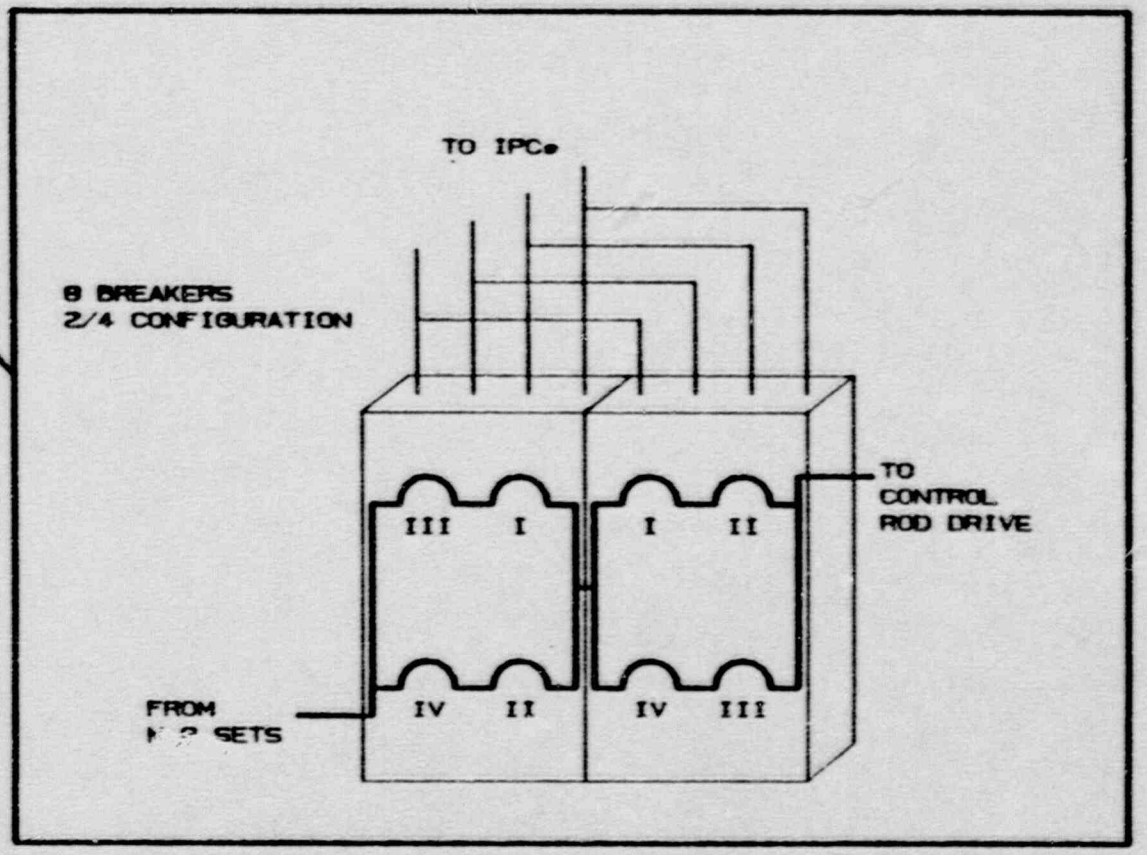


SKALC-041785 REV. D 10/31/86

INTEGRATED PROTECTION SYSTEM



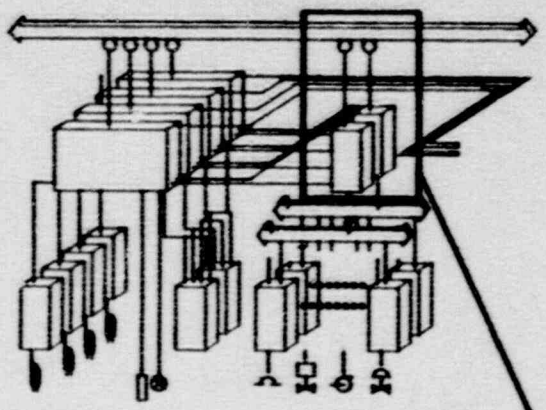
REACTOR
TRIP
SWITCHGEAR



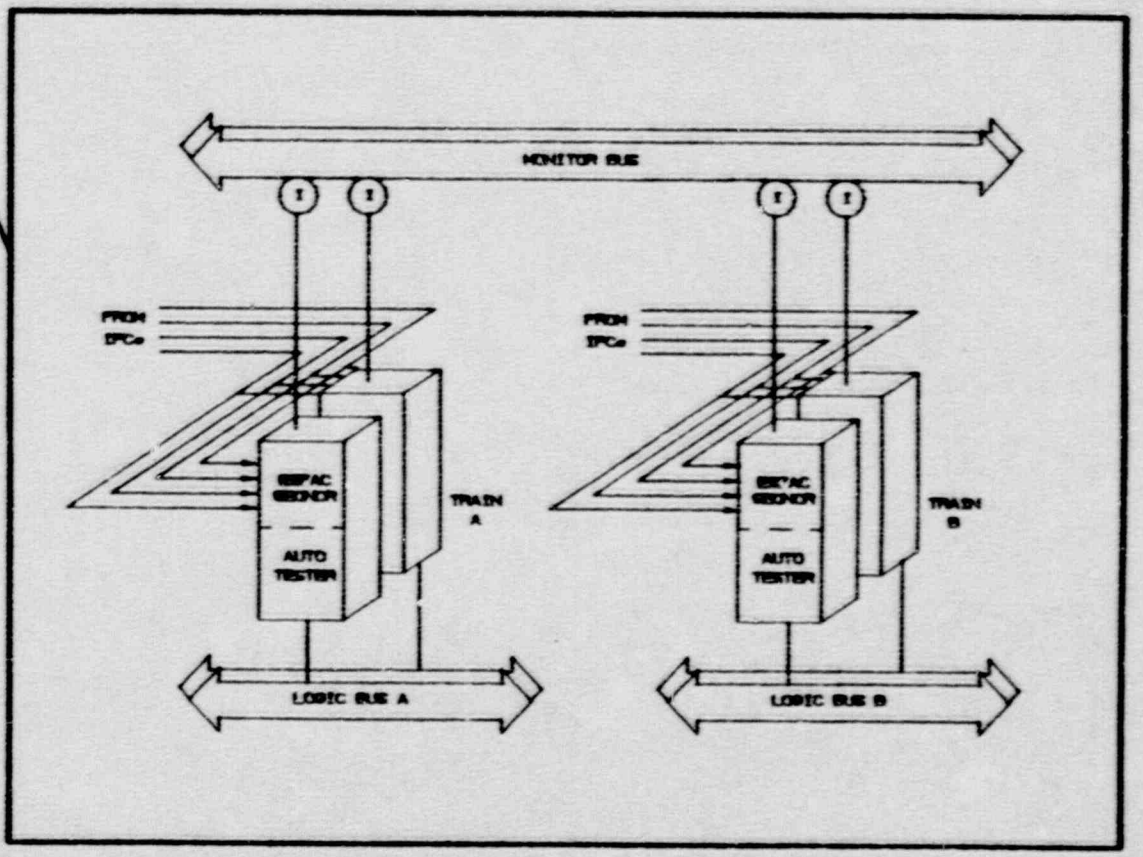
Instrumentation & Control Systems
IPS - Reactor Trip Switchgear (RTS)

- Eight circuit breakers arranged in two-out-of-four configuration
- Automatic trip from IPCs both:
  - Undervoltage trip attachments (UVTA)
  - Shunt trip attachments (STST)

INTEGRATED PROTECTION SYSTEM



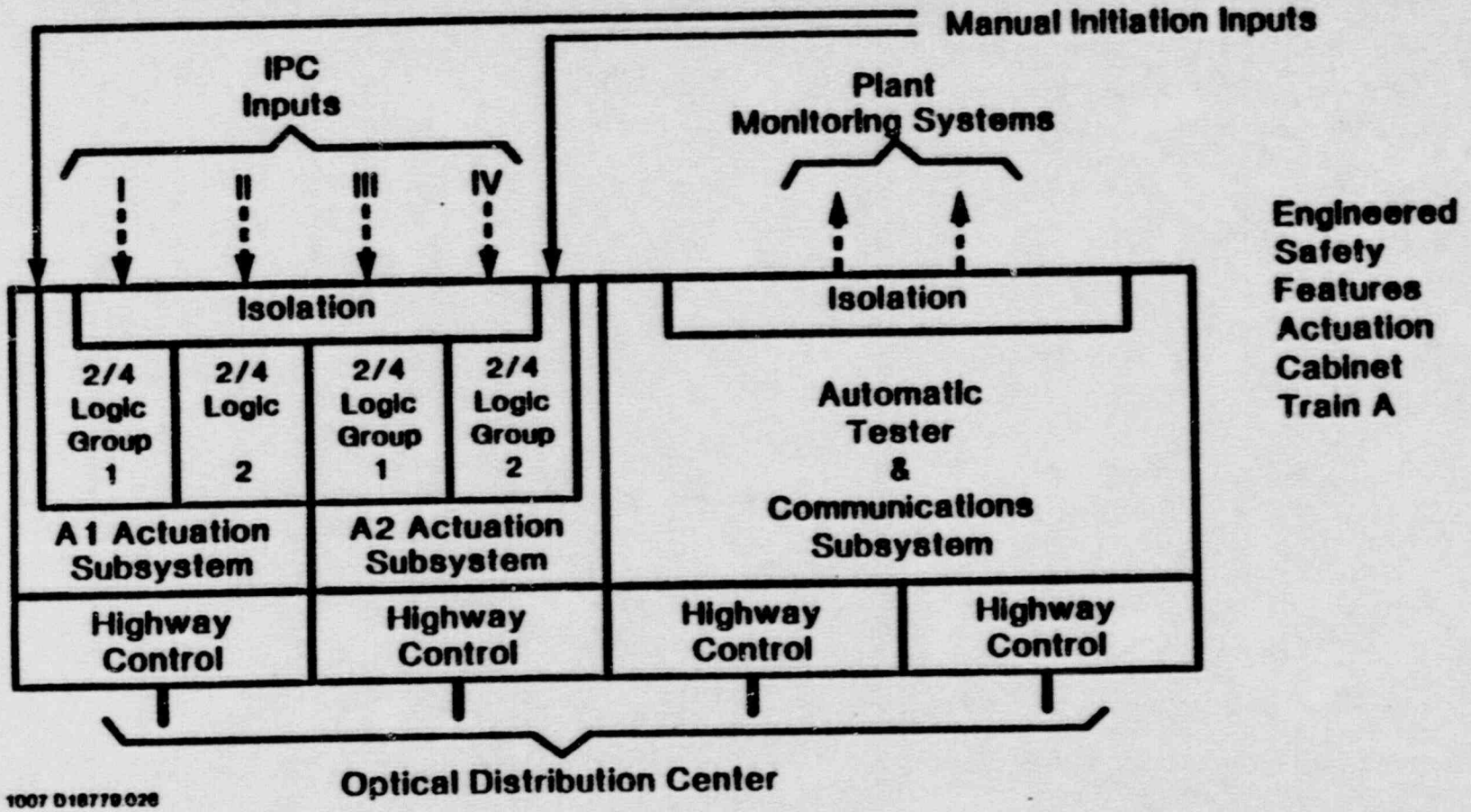
ENGINEERED SAFETY
FEATURES ACTUATION
CABINETS

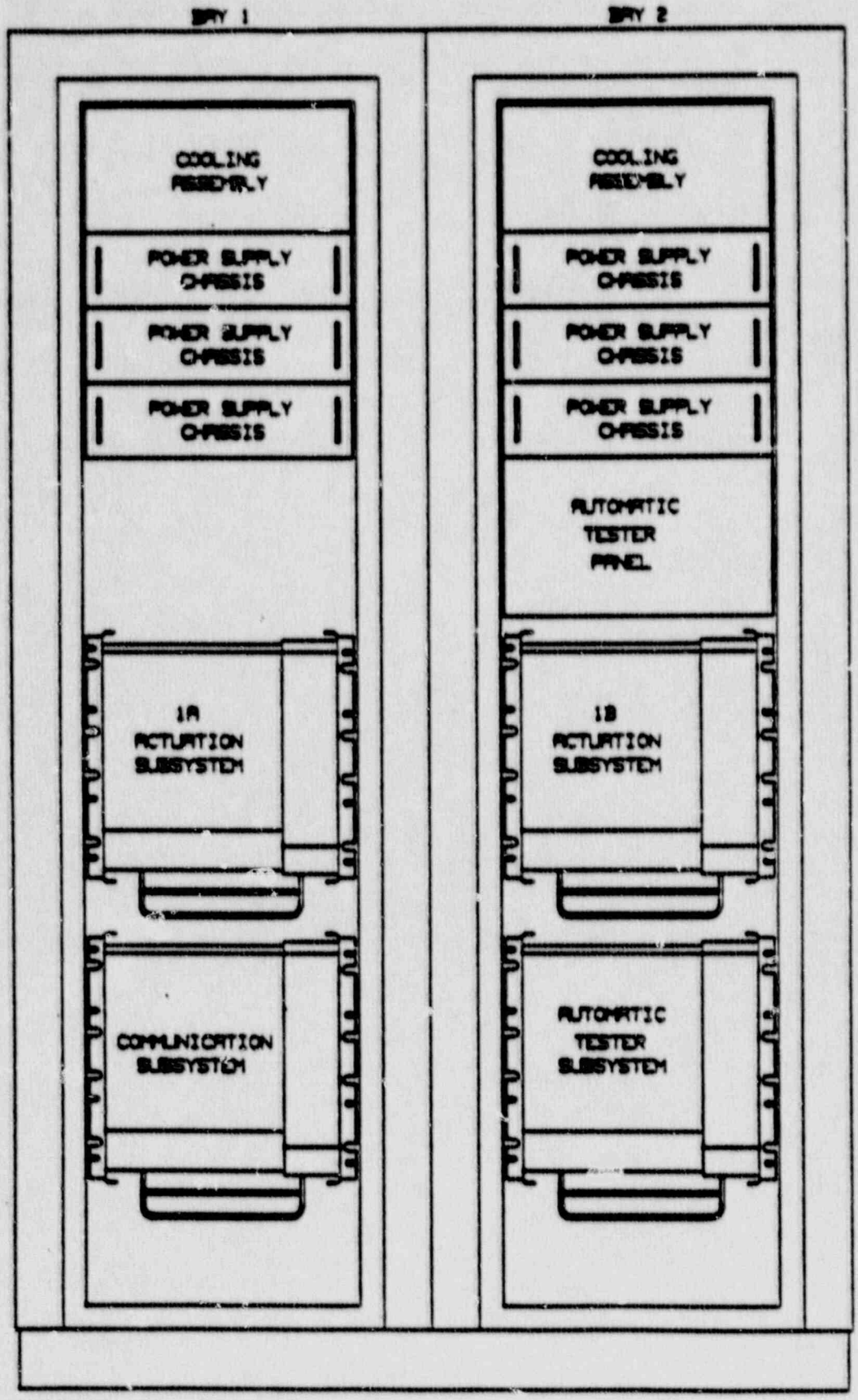


Instrumentation & Control Systems - IPS - Engineered Safety Features Actuation Cabinets (ESFACs)

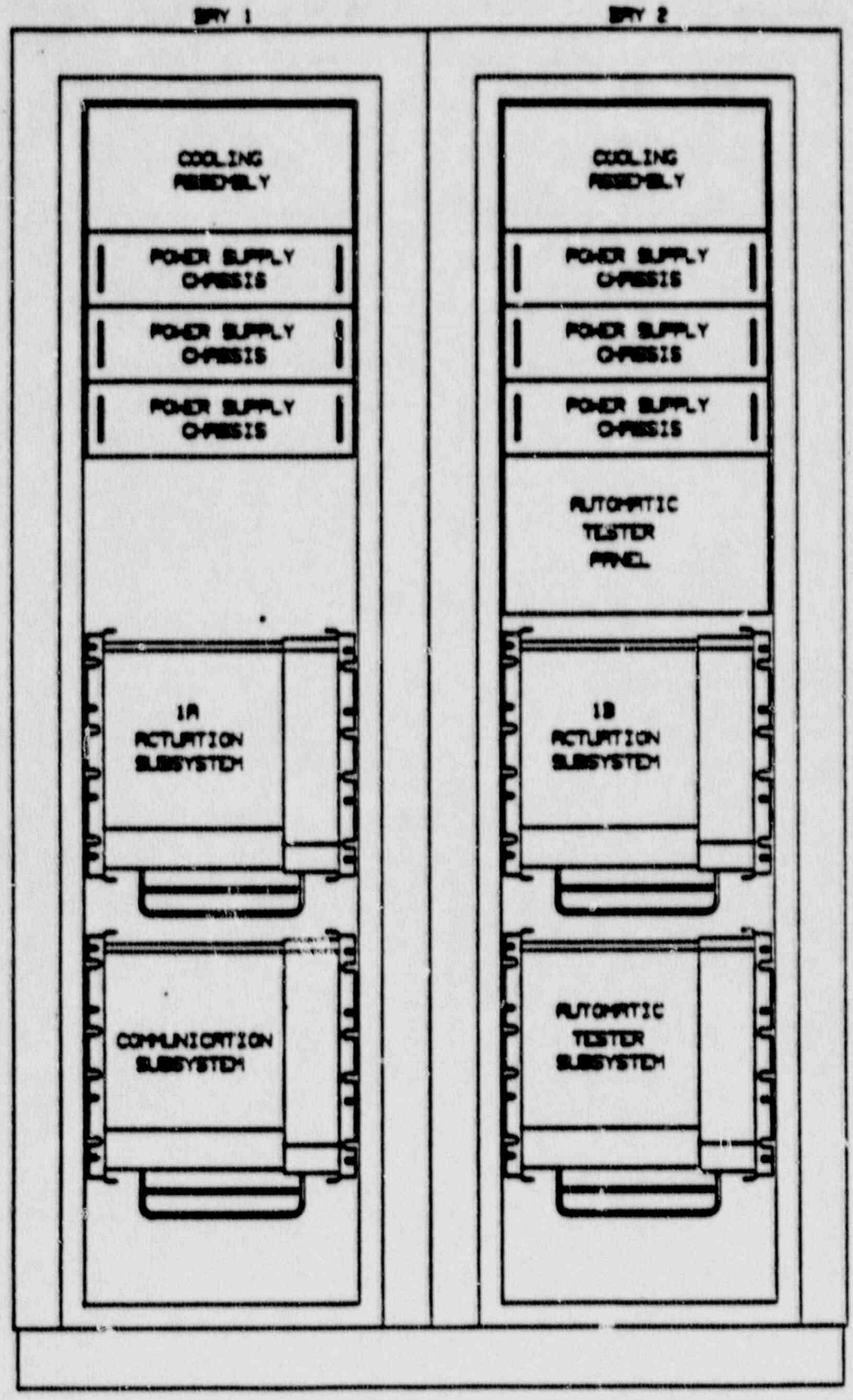
- ESFACs provide the following functions:
  - Receive ESF bistable trip and bypass signals from four IPCs
  - Perform two-out-of-four voting operations on ESF actuations signals received for IPCs
  - Receive manual ESF system level inputs from the Main Control Board
  - Perform system level ESF logic
  - Perform blackout load sequencing
  - Provide system level ESF actuation signals (e.g., S,P,T) to ILCs via logic bus
  - Receive and process safety-related interlock bistable trip and block signals
  - Transmit ESF actuation status to external systems (e.g., Plant Process Data System, Plant Alarm System, Plant Computer)

Instrumentation & Control Systems
IPS-ESF Actuation Cabinet (ESFAC)



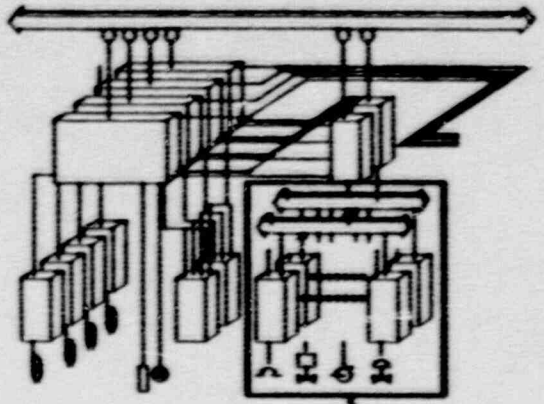


SKJEH-050885 REV.E 10/31/86JEH

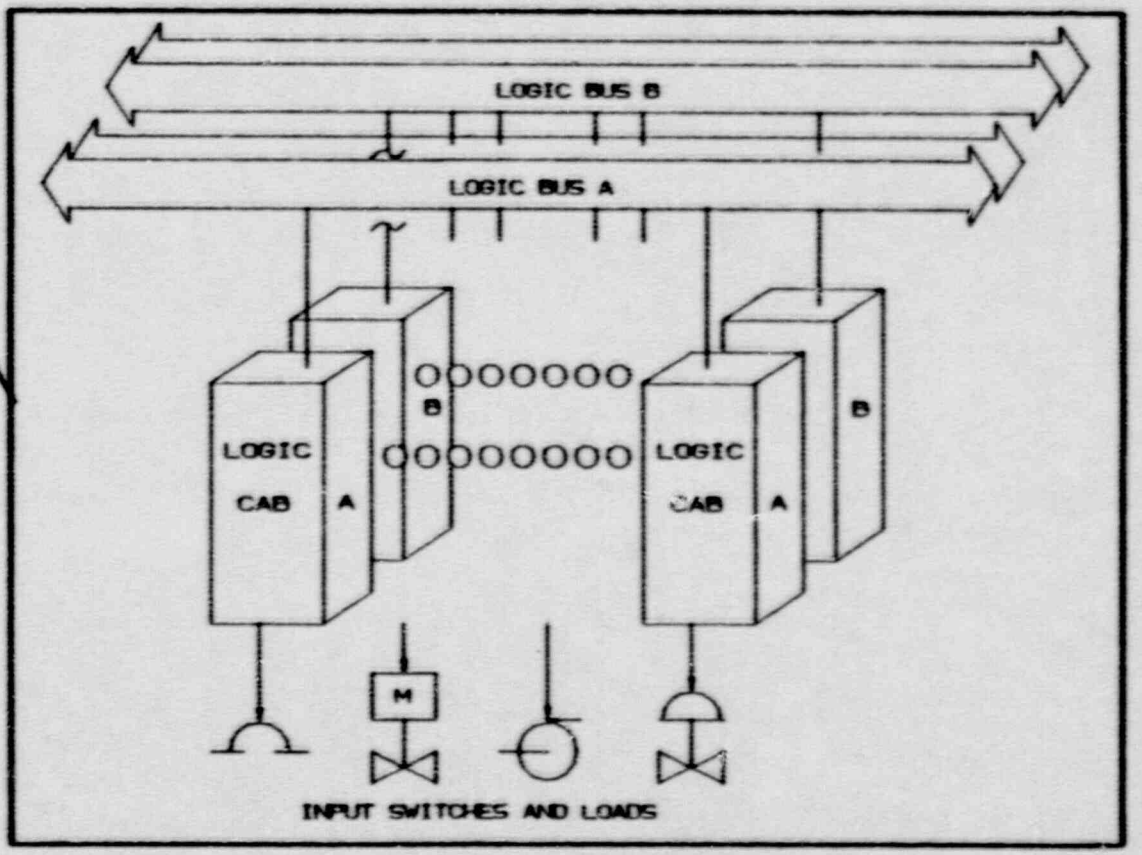


SKJEH-050885 REV.E 10/31/86JEH

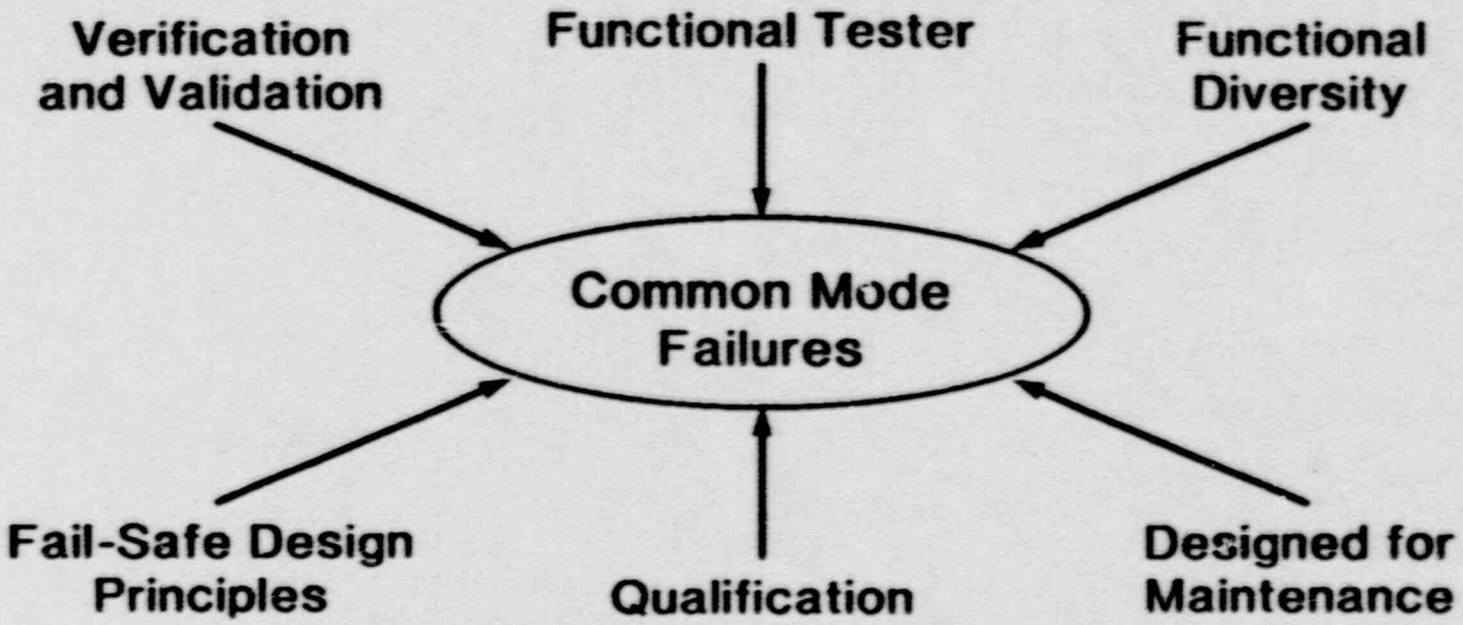
INTEGRATED PROTECTION SYSTEM



INTEGRATED
LOGIC
CABINETS



Instrumentation & Control Systems
IPS - COMMON MODE FAILURES



1067 D20131.016

Instrumentation & Control Systems
IPS - AVAILABILITY FEATURES

- Fault-tolerant design implemented by using redundancy
- Two-out-of-four safety system architecture
- Bypass function for test, maintenance, and sensor failure
- Functional diversity maintained by the system architecture (NUREG 0493):
  - Three-way control system separation:
    a) Control (prevention)
    b) Scram (termination)
    c) Engineered safeguards (mitigation)
  - Safety function groupings:
    a) Independent functions that operate on the same event are separated
    b) Two reactor trip groups per channel set
    c) Two engineered safeguards groups per channel set

Instrumentation & Control Systems
IPC - Designed for Maintenance

- Integrated automatic functional tests locate equipment faults down to replaceable module
- Self-checking algorithms locate equipment faults down to replaceable module
- Remote readout of system status
- Local readout of system status
- Setpoints and constants are entered directly in engineering units
- Stable, accurate calibration that is easily verified

Instrumentation & Control Systems
IPS - Automatic Test Features

- Integrated automatic functional tests (IEEE-279)
- Tests can be run without re-configuring equipment interfaces
- Centralized test panel
- Test results are displayed and hardcopy data is provided
- Failures diagnosed
- Substantially reduced test cycle time

Instrumentation & Control Systems
IPS - Fail-Safe Design Principles

- Dynamic operation
- Self-checking algorithms run continuously
- Watchdog timers
- Perferred failures modes

Instrumentation & Control Systems
IPS - Qualification

- Qualified to meet IEEE 323-1974 and IEEE 344-1975
- Uses methodology of WCAP 8587 which has been approved by the United States Nuclear Regulatory Commission
- Microprocessor-based systems have been successfully qualified using WCAP 8587

Instrumentation & Control Systems
IPS - Verification and Validation

- Analysis and testing done by an independent team
- Assures that the design principles have been followed (WCAP 9153, IEEE/ANS 7-4.3.2, IEC 880)
- Demonstrates that successive steps of the design process satisfy the requirements of the previous steps
- Demonstrates that the integrated system meets the design basis

I&C DEVELOPMENT ENGINEERING DEFINITIONS - V&V

- **VERIFICATION:**

  The process of determining whether or not the product of each stage of the system design process fulfills the requirements imposed by the previous design stage.

- **VALIDATION:**

  The test and evaluation of the integrated system design to ensure compliance with the functional, performance, and interface requirements as specified in the system functional requirements.

I&C DEVELOPMENT ENGINEERING PLAN DETERMINANTS - V&V

Determinants in the configuration of a V&V plan:

- Customer requirements/system design requirements
- Regulatory criteria
- Industrial guidelines and standards
- In-house policies and procedures
- I&CDE System Design/Implementation Process (SYSDIP)
- I&CDE V&V program

I&C DEVELOPMENT ENGINEERING
GUIDELINES, CODES, & STANDARDS - V&V

ANSI/IEEE/ANS STANDARD 7-4.3.2:

Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations

IEC PUBLICATION 880:

Software for Computers in the Safety Systems of Nuclear Power Stations

IEEE STANDARD 729:

Standard Glossary of Software Engineering Terminology

IEEE STANDARD 730:

Standard for Software Quality Assurance Plans

IEEE STANDARD 829:

Standard for Software Test Documentation

IEEE STANDARD 1012:

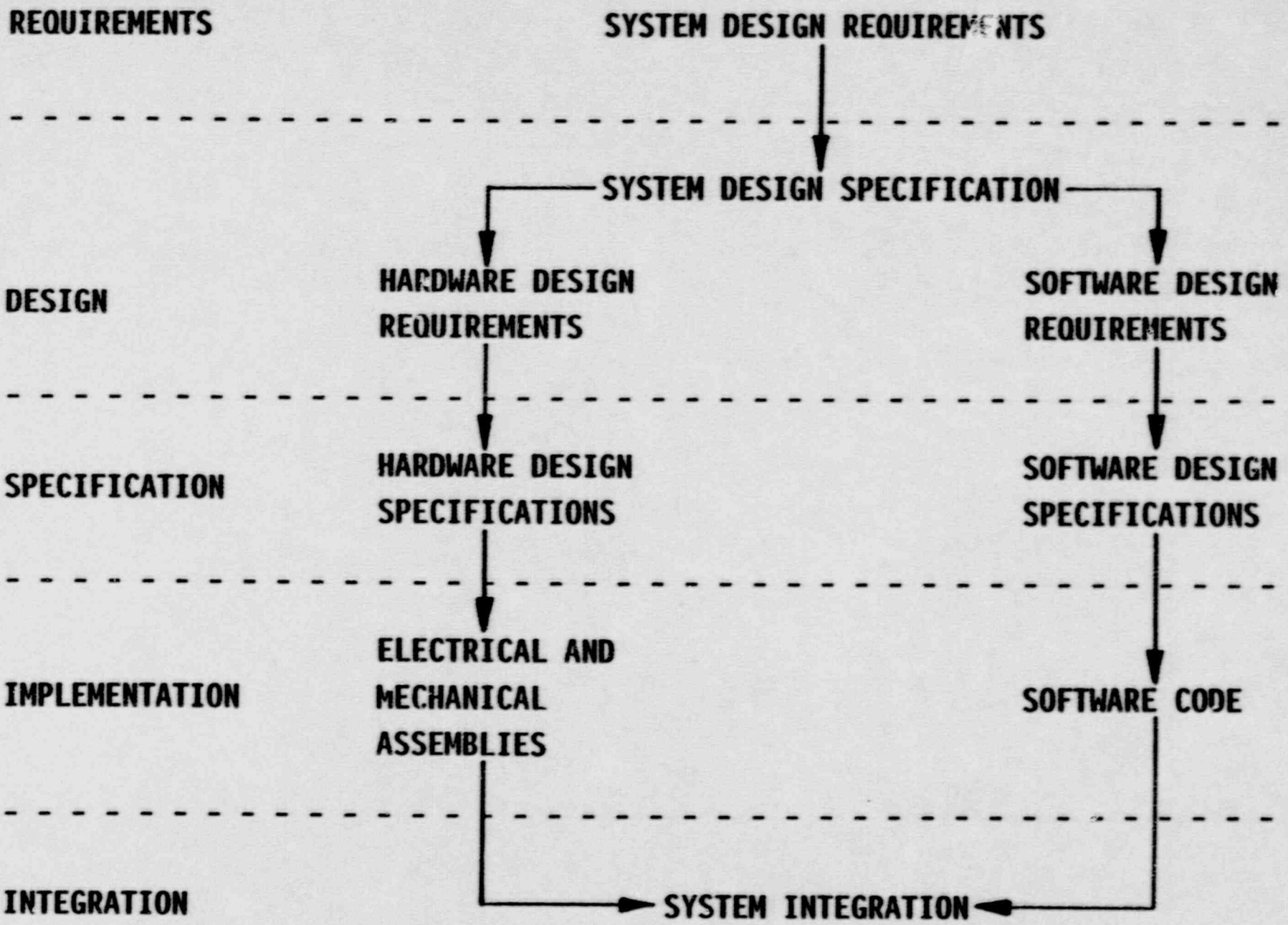
Standard for Software Verification and Validation Plans

I&C DEVELOPMENT ENGINEERING OVERVIEW - V&V (CONTINUED)

- **WHEN IS V&V PERFORMED?**

  V&V parallels the System Development/Implementation Process and serves as a complementary engineering analysis to provide an assessment of the system design, including early detection and resolution.

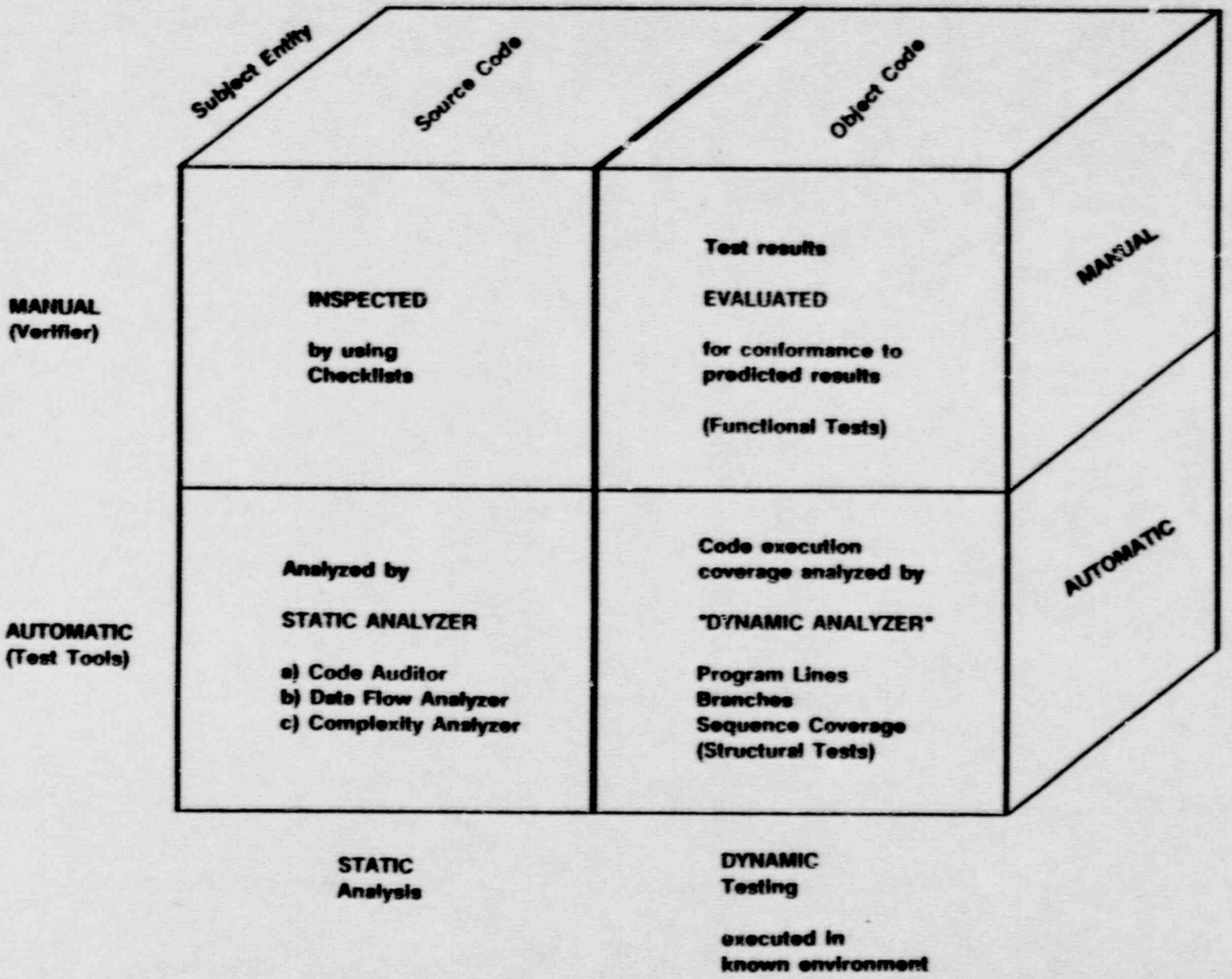
DESIGN PROCESS



I&C DEVELOPMENT ENGINEERING
SIZEWELL B V&V PLAN

- The Sizewell B V&V plan for the PPS will consist of four major constituents:
  - IPS Hardware Verification Plan
  - IPS Software Verification Plan
  - IPS System Verification Plan
  - IPS System Validation Plan

SIS VERIFICATION MODEL



INTEGRATED PROTECTION SYSTEM (IPS) VERIFICATION & VALIDATION

Test tools and techniques:

- Code inspection
- Static analyzer
- Automated tester driver code generation
- Dynamic coverage analyzer
- Test results documenter

Integrated software verification environment:

- Collection of tools to support testing activities

INTEGRATED PROTECTION SYSTEM (IPS) VERIFICATION & VALIDATION

Testing Principles:

- Bottom up testing
- Expected test results are derived from SDS
- Functional testing
- Structural testing based on implementation and assumptions about how program errors occur

INTEGRATED PROTECTION SYSTEM (IPS) VERIFICATION & VALIDATION

Test Methodology: Formalized systematic approach

- Set of guidelines to design test cases and for selection of test data
- Automated tools for static and dynamic analysis
- Various coverage metrics documented
- Use of checklists
- Interactive and menu-driven step-by-step procedures for verifiers to conduct test in a consistent manner

INTEGRATED PROTECTION SYSTEM (IPS) VERIFICATION & VALIDATION

Testing Strategy: Test cases and test data are established to address the following multiple (five) domains of coverage:

1) Function coverage: to cover each and every function performed
2) Input coverage: cover significantly different input subdomains, for example:
   a) valid/invalid inputs
   b) normal/abnormal data
   c) singularities or special values
3) Output coverage: generate all types of outputs at least once

INTEGRATED PROTECTION SYSTEM (IPS) VERIFICATION & VALIDATION

Domains of coverage: (continued)

4) **Functions interaction coverage: affecting another or itself during some later execution, especially at hierarchically higher level modules**

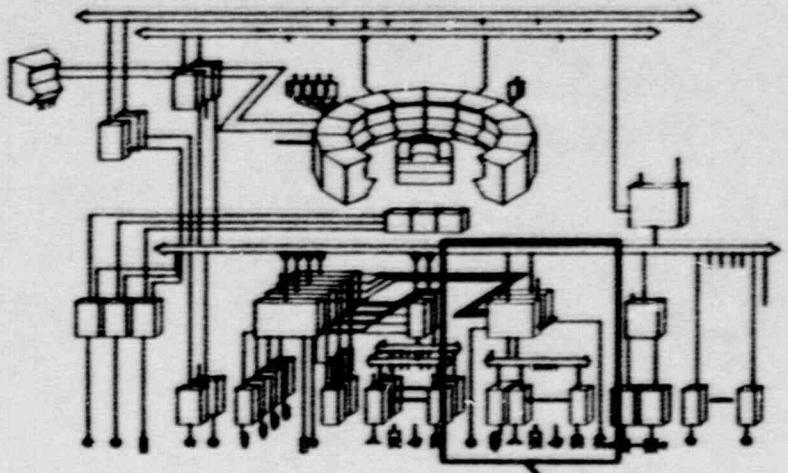
5) **Code execution coverage: to cover each and every line of statement and every predicate outcome.**

Instrumentation & Control Systems

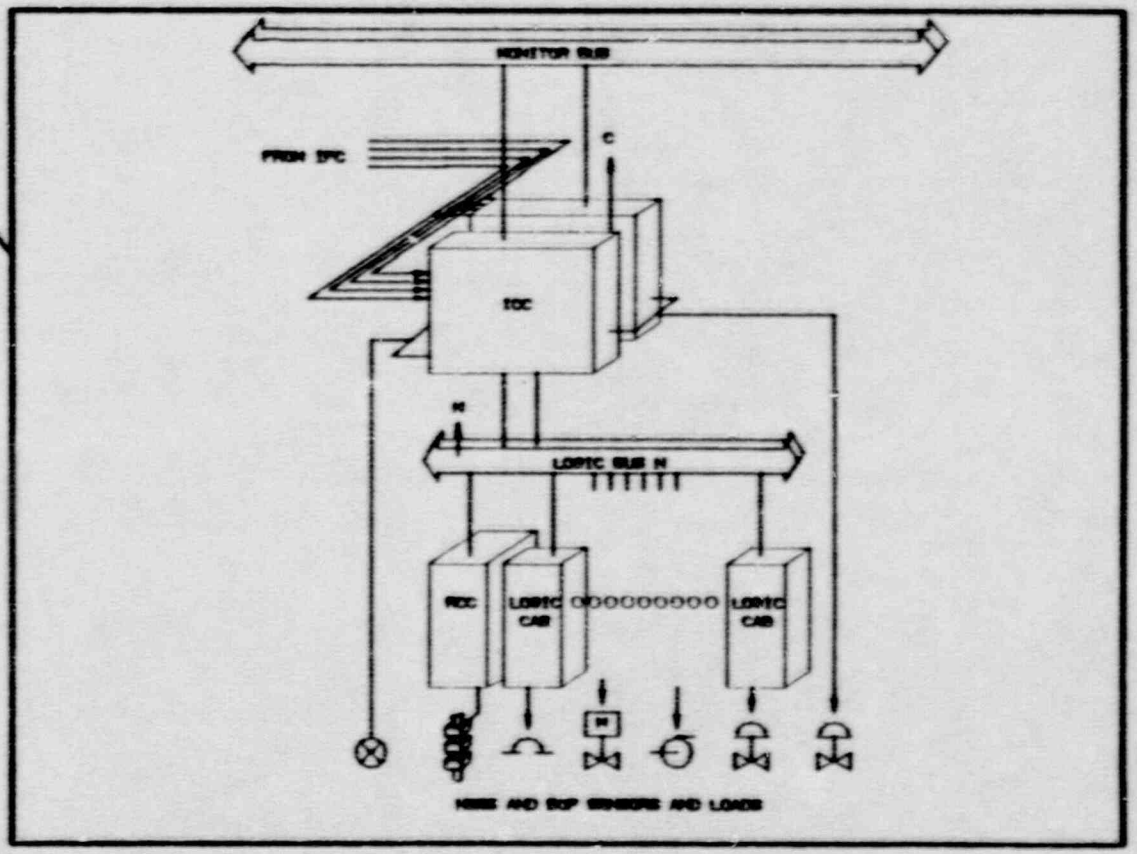
INTEGRATED CONTROL SYSTEM

1050 D19799-006

INSTRUMENTATION & CONTROL ARCHITECTURE



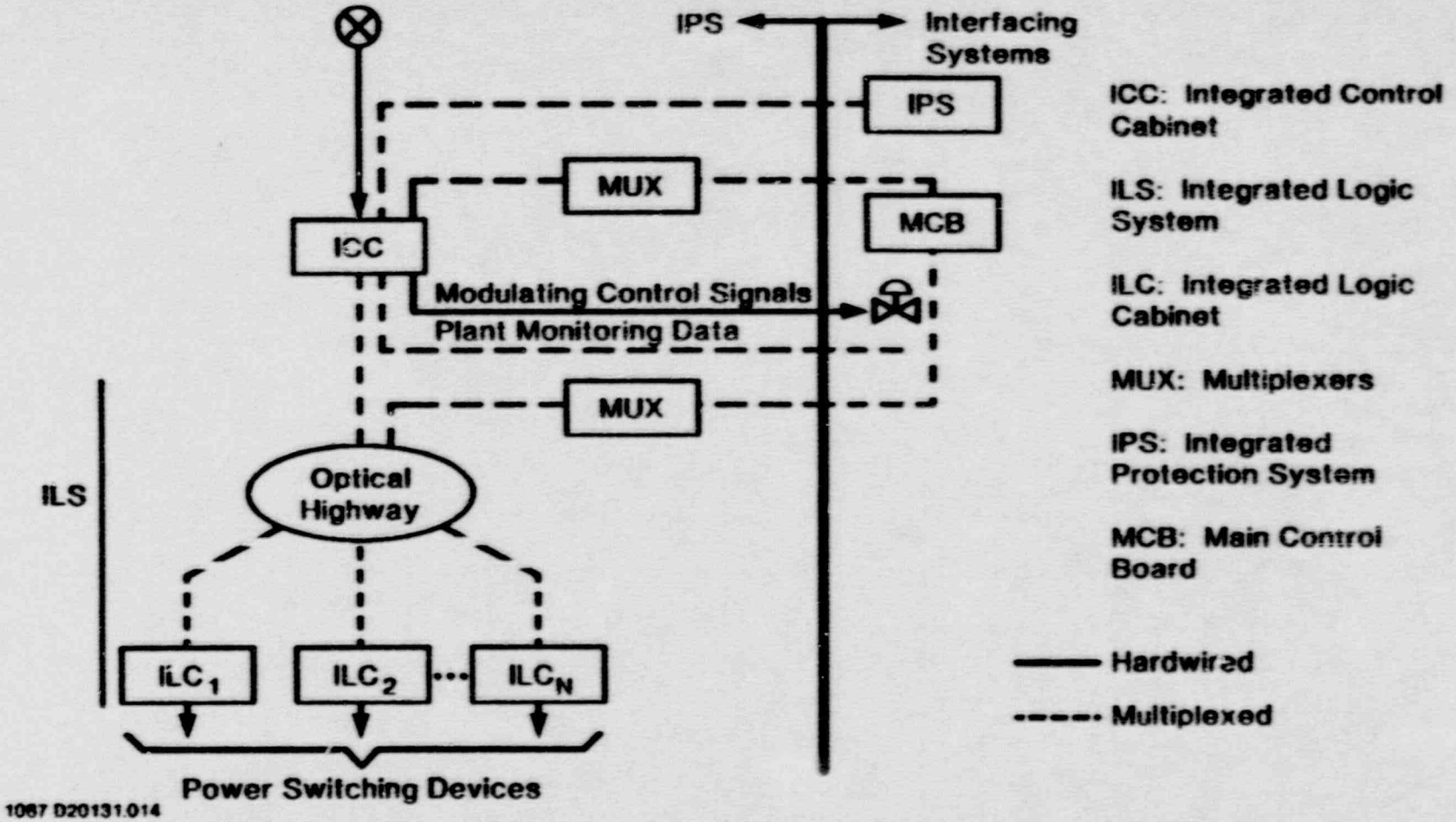
INTEGRATED
CONTROL
SYSTEM



Instrumentation & Control Systems
ICS - MAJOR GROUPS OF EQUIPMENT

- Integrated Control Cabinets (ICC):
  - Signal selector
  - Controllers
  - Process bus
  - Auto/manual control board multiplexer
  - Monitoring interface
- Integrated Logic System (ILS):
  - Control Logic Cabinets (CLC)
  - Logic bus
  - Control board multiplexer

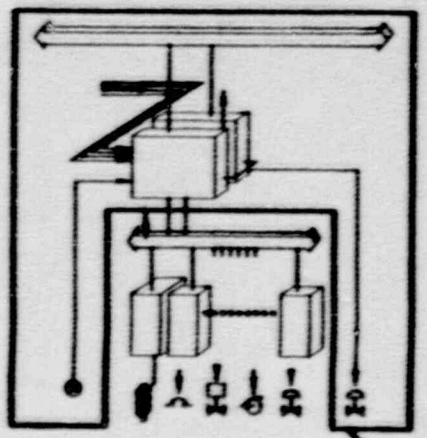
Instrumentation & Control Systems
ICS - SYSTEM INTERFACES



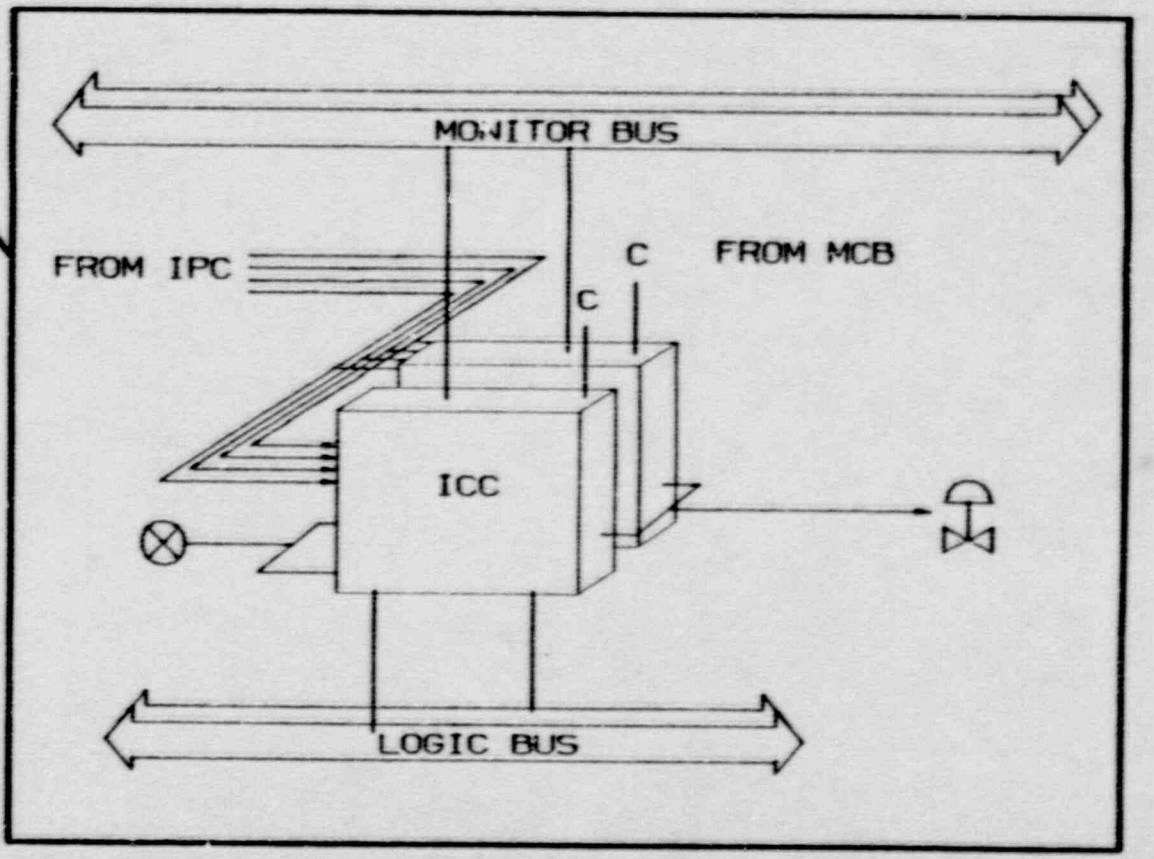
Instrumentation & Control Systems
ICS - COMMUNICATIONS

- Process bus:
  - Redundant
  - Redundant controller receivers connected to the two process buses (partially cross-coupled)
  - System level communications
  - Mostly numeric data with some logic data
  - Modulating control operator interface
- Logic bus:
  - Redundant
  - Optical
  - Component level communications
  - Logic data
  - On/Off control operator interface
  - Similar to IPS logic bus

INTEGRATED CONTROL SYSTEM



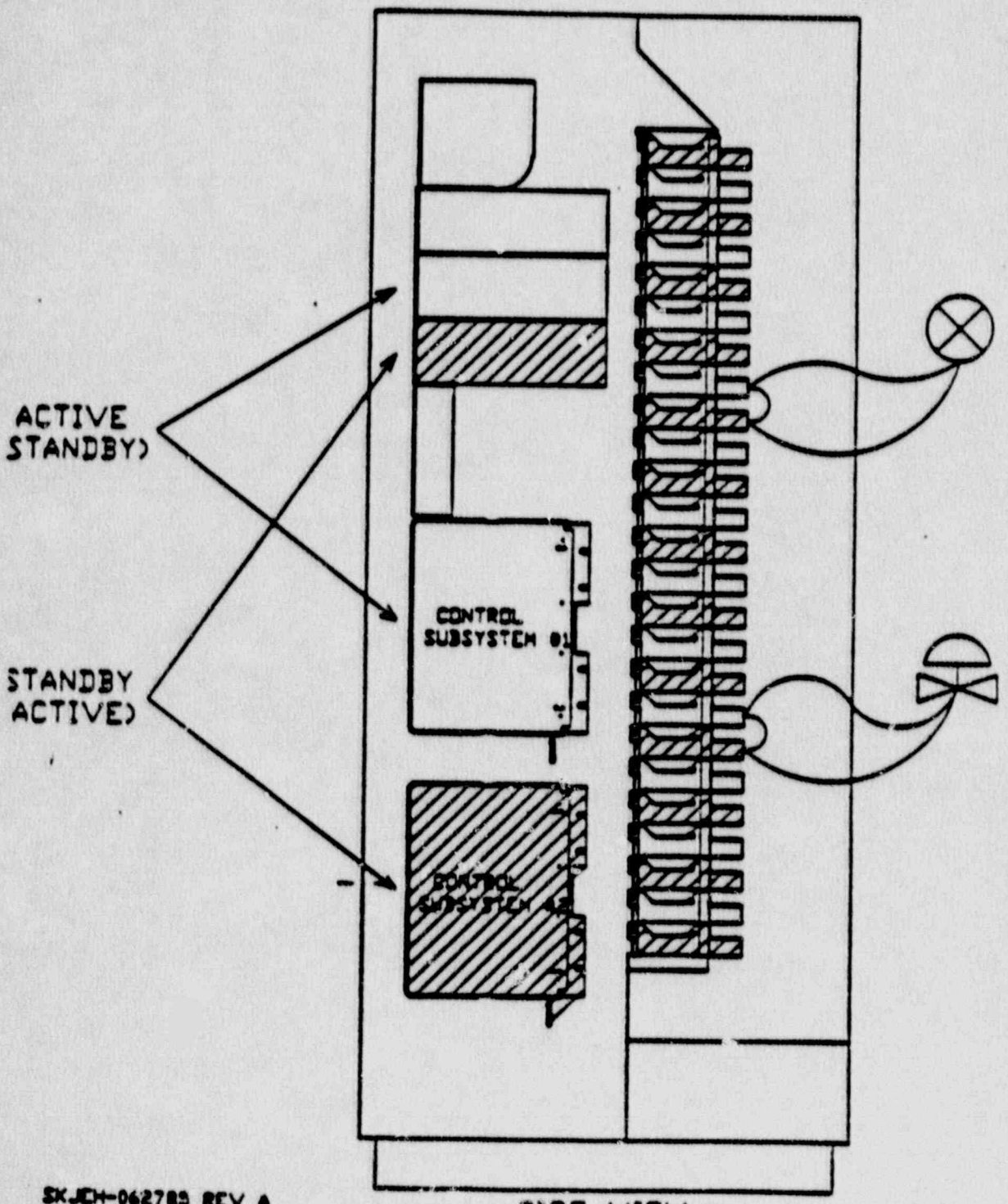
INTEGRATED
CONTROL
CABINETS



Instrumentation & Control Systems
ICC - SIGNAL SELECTOR

- Receives process signals from the four Integrated Protection Cabinets (IPCs)
- Provides correct control information even if one or two sensors measuring the same process variable are incorrect due to failure or testing (IEEE-279)
- Redundant subsystem
- Validated signals are transmitted to controllers via the process bus
- Signal selector tester subsystems similar to IPS tester subsystems (IEEE-279)

INTEGRATED CONTROL CABINET (ICC) REDUNDANCY



SKJEH-062789 REV A

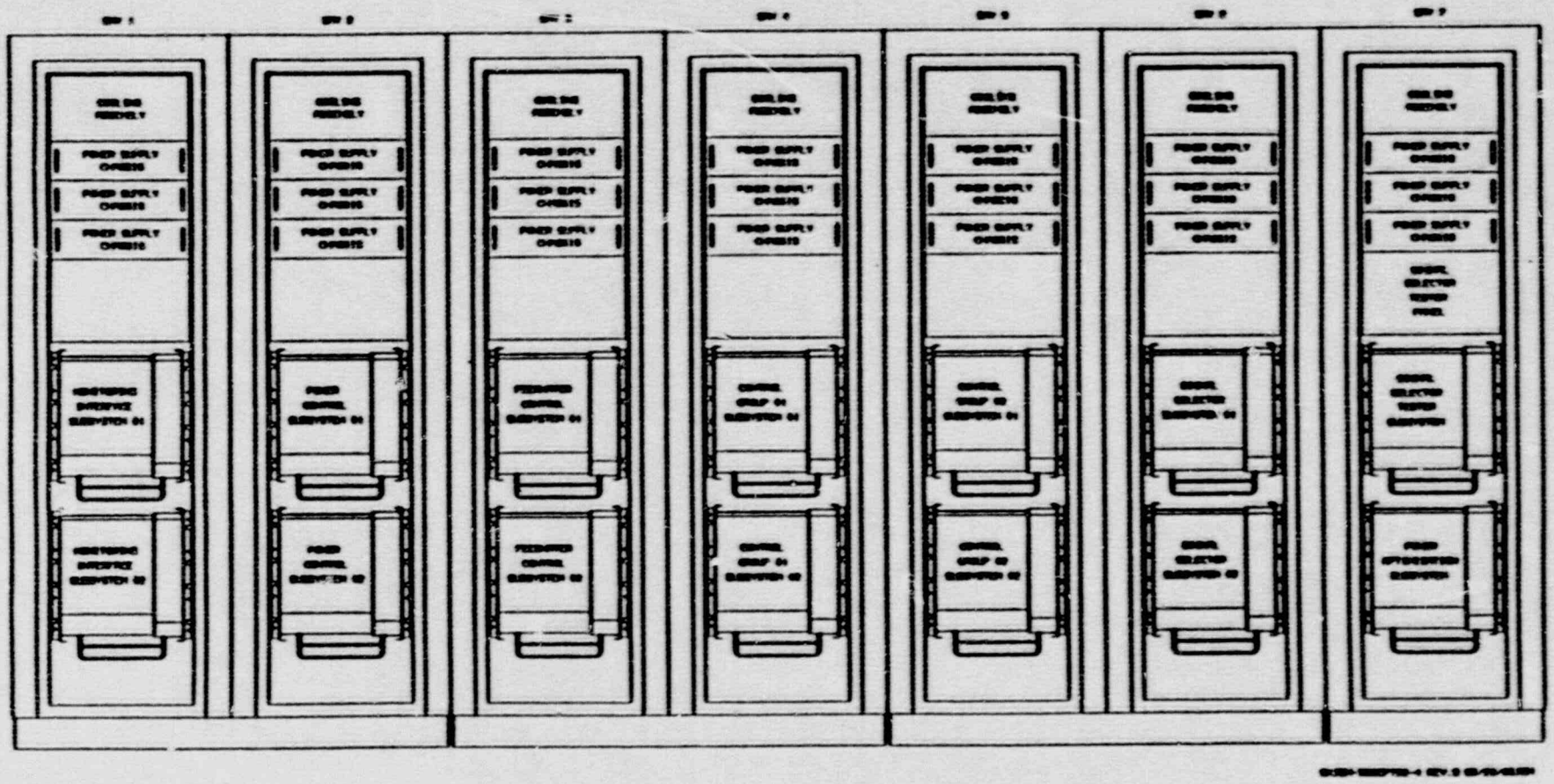
SIDE VIEW

Instrumentation & Control Systems
ICC - REDUNDANT CONTROLLERS

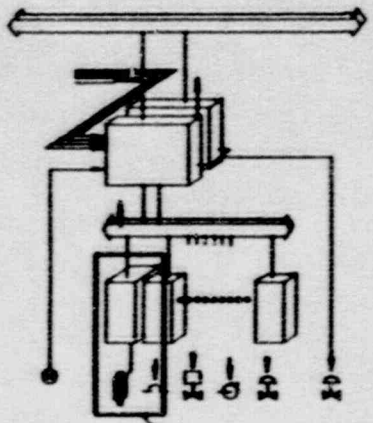
- Architecture:
  - Active controller and standby controller
  - Active and standby roles are interchangeable
  - Redundant controller subsystems have identical hardware and software
  - Upon detection of a failure, control transfer is automatic
  - Control transfer may be manually selected at cabinet
  - Each redundant controller may be powered down separately for maintenance while maintaining both automatic and manual control capability
- Indepedence:
  - Independent microcomputer card frames
  - Independent power supplies
  - Independent input signal conditioning (similar to IPS)
  - Independent output signal conditioning

Instrumentation & Control Systems
ICC - MODULATING CONTROL

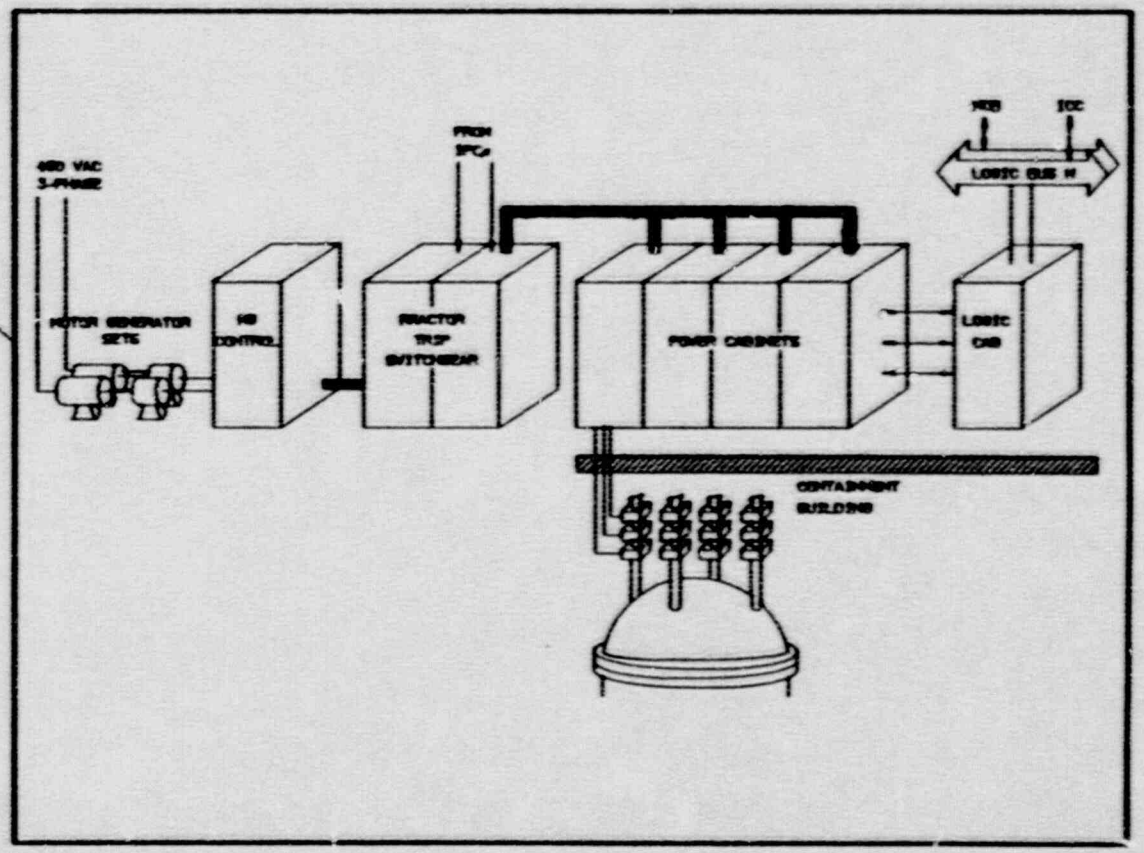
- Both automatic and manual control modes are implemented in digital controllers:
  - Manual control is an operating control mode
  - Backup control for availability is provided by the system redundancy
  - Process feedback displays to the operator are available during manual operation
- Tracking:
  - The standby controller tracks the active controller via information transmitted by the active controller on the process bus
  - Manual to automatic control tracking of demand signal provides bumpless transfer
  - Setpoint tracking is available where desired for control bumpless transfer



INTEGRATED CONTROL SYSTEM



ROD
CONTROL
SYSTEM

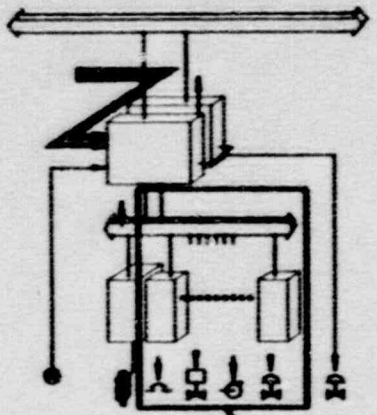


WESTINGHOUSE PROPRIETARY
INSTRUMENTATION & CONTROL SYSTEMS
ROD CONTROL SYSTEM - MAJOR GROUPS OF EQUIPMENT

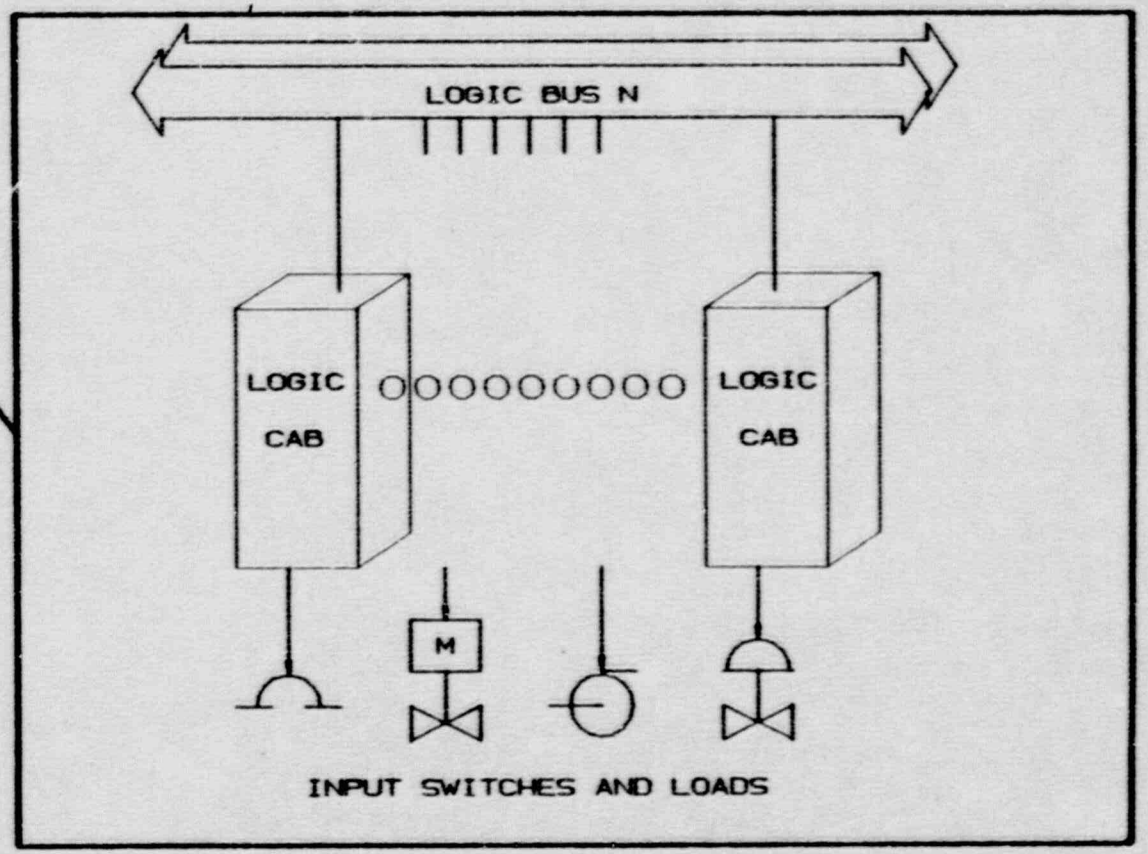
- Logic Cabinets
  - Redundant microprocessor-based logic
  - Receives signals from Integrated Control Cabinets
  - Receives signals from Main Control Board
  - Generates selection and sequencing signals for CRDM motion
  - Performs system diagnostics
- Power Cabinets
  - Receives signals from Logic Cabinets
  - Microprocessor controllers switch and regulate the current to the CRDMs
- Power Supply
  - Two motor generator sets connected in parallel
  - Control cabinets for protection, monitoring, and maintenance

1050 D19799.007

INTEGRATED CONTROL SYSTEM



INTEGRATED
LOGIC
CABINETS



Instrumentation & Control Systems
ICS - AVAILABILITY FEATURES

- Automatic control signal selection
- Redundant controllers
- Error detection and switching
- Improved control algorithms
- Expanded automatic control ranges

Instrumentation & Control Systems
ICS - FEATURES

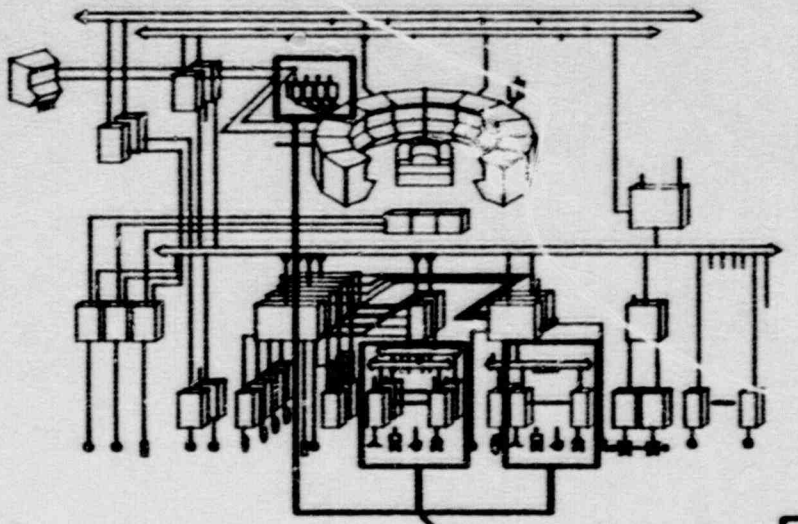
- Coordinates plant control with IPS to maximize core margins and minimize safety system challenges
- Provides input signal validation prior to using signal for plant control
- Automatic testing of signal selector
- Self diagnostics
- On-line calibration capability
- Provides plant and system status information outputs for operator use
- Modular design is expandable to include BOP control functions

Instrumentation & Control Systems

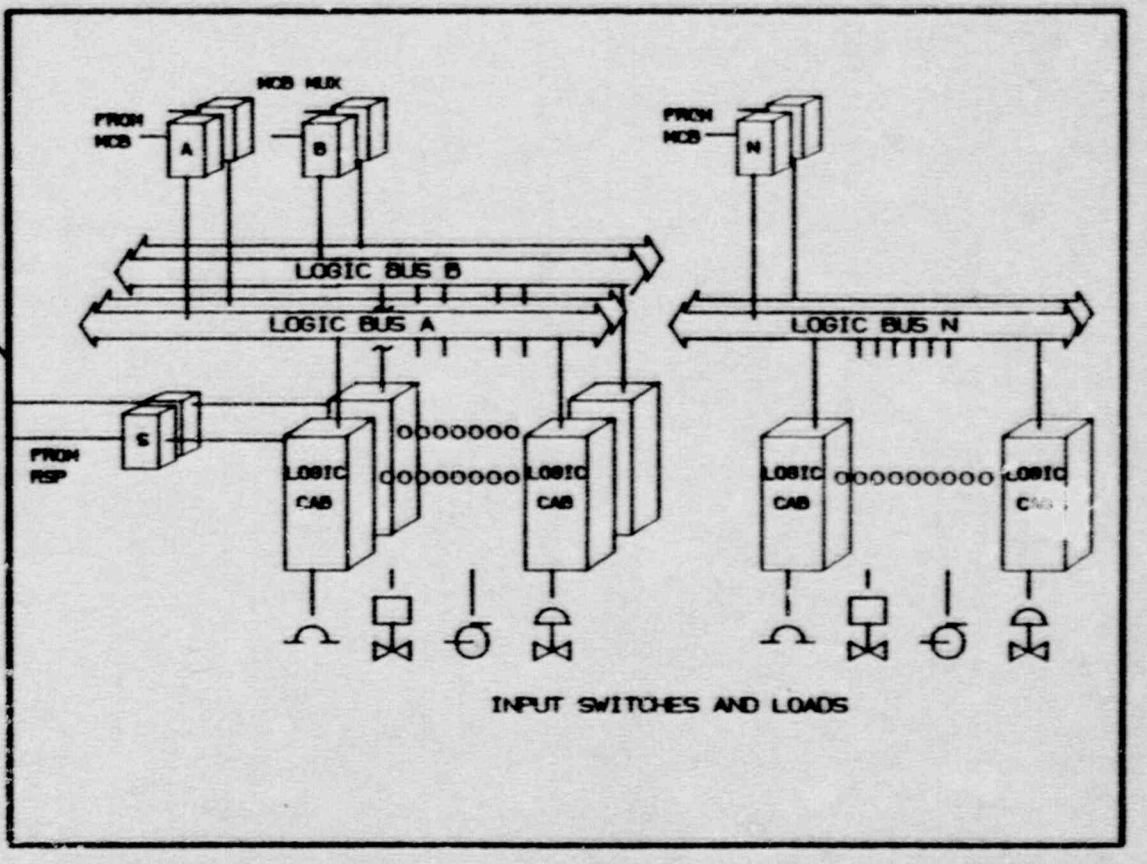
INTEGRATED LOGIC SYSTEM

1060 D19799 010

INSTRUMENTATION & CONTROL ARCHITECTURE



INTEGRATED
LOGIC
SYSTEM

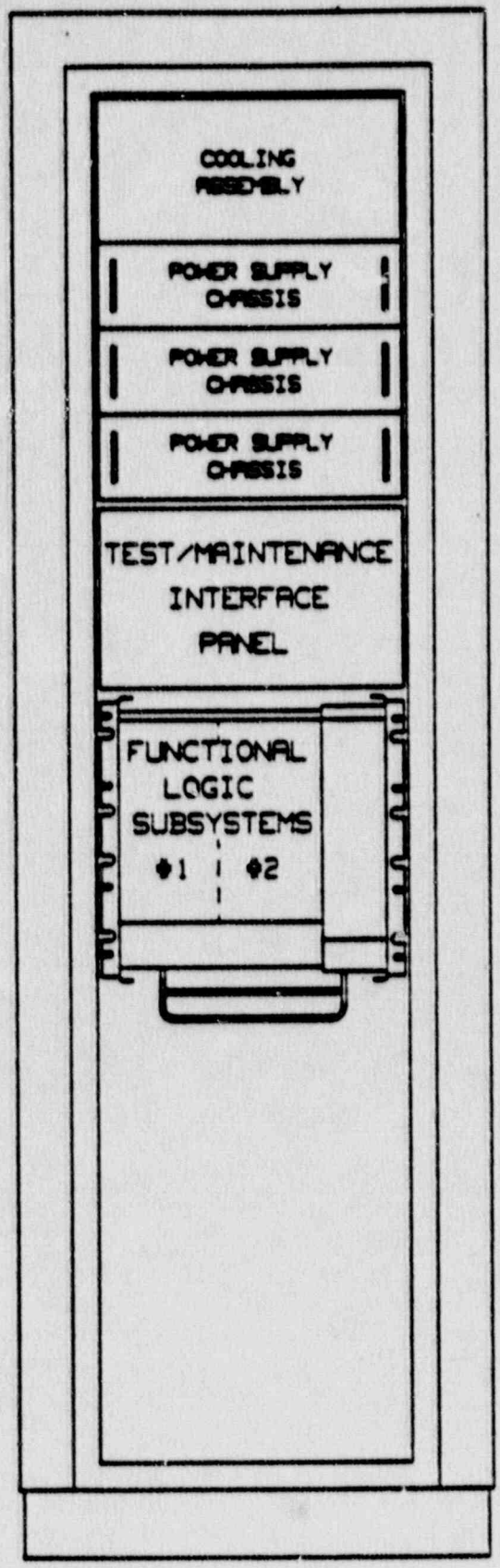


Instrumentation & Control Systems
INTEGRATED LOGIC SYSTEM (ILS)

- Distributed control electronics for ON/Off control of plant components:
  - Automatic control signals from ESFAC and ICC
  - Manual control signals from the main control board and emergency shutdown board
- Performs component specific interlocking logic and provides actuation signals for plant control components
- Transmits plant control component status information to control boards and plant computer

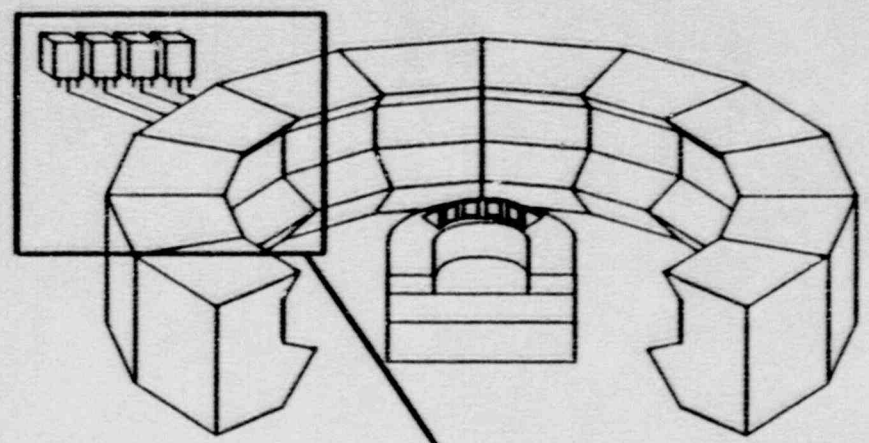
Instrumentation & Control Systems
ILS - MAJOR GROUPS OF EQUIPMENT

- Control board multiplexers
- Logic bus
- Field logic cabinets

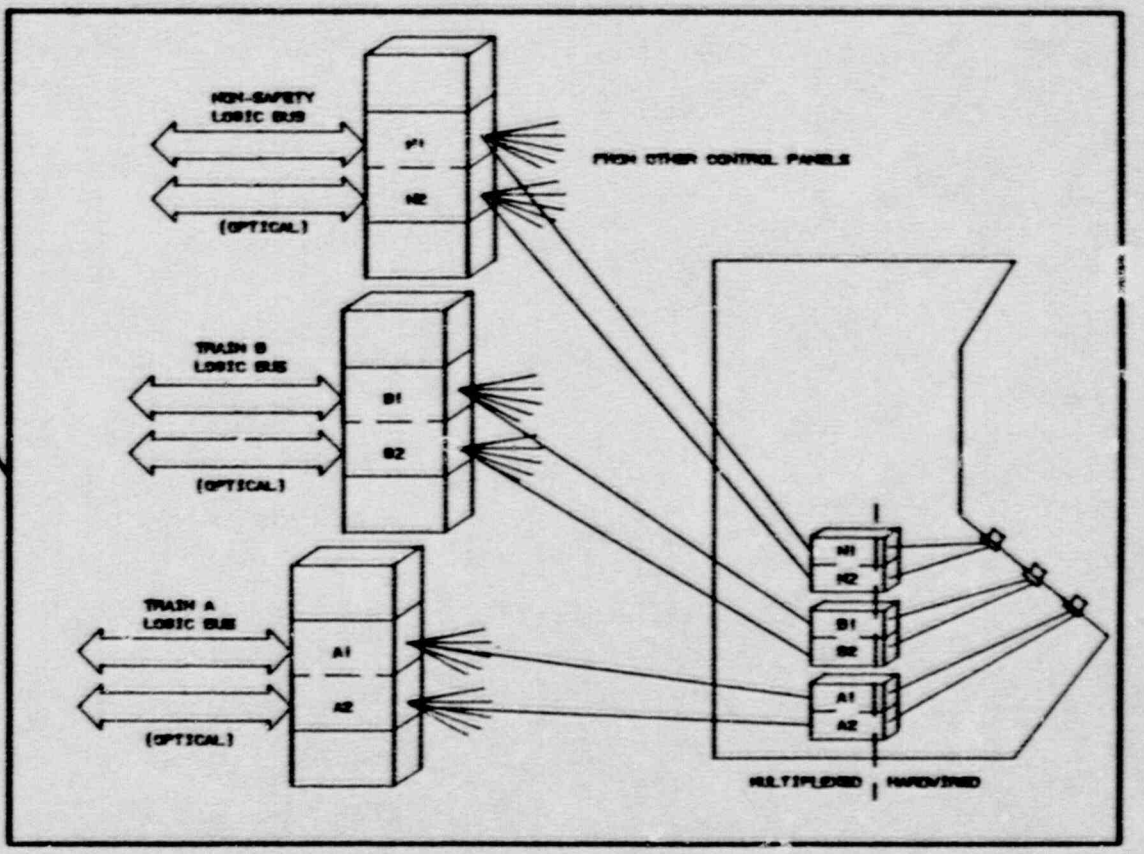


SKJEH-041885 REVA

MAIN CONTROL ROOM



MAIN CONTROL BOARD MULTIPLEXING



Instrumentation & Control Systems
ILS - FEATURES

- Integrated NSSS and BOP functions
- Distributed logic cabinets for layout flexibility
- Distributed logic cabinets with multiplexed interfaces reduces plant cabling
- Reduced plant cabling simplifies separation
- Multiplexed interfaces reduces terminations
- Fiber optic multiplexing provides electrical isolation and noise immunity
- All logic cabinets have a maintenance and local control interface
- Safety logic cabinets have an integrated automatic test subsystem
- Microprocessor-based logic and a symbolic logic compiler simplify logic design and facilitate field logic changes

WESTINGHOUSE PROPRIETARY
INSTRUMENTATION & CONTROL SYSTEMS ARCHITECTURE - COST SAVINGS

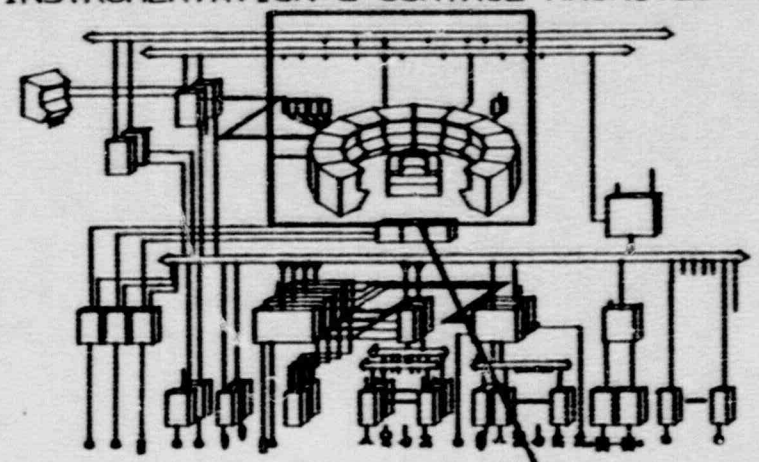
Analysis prepared by Gilbert/Commonwealth (G/C) for Westinghouse:

- Analysis uses V.C. Summer as the reference plant
- Analysis of conventional control versus digital control
  - Ground wire = -3,000 feet
  - Control cable = -1,600,000 feet
  - Fiber optic cable = +19,000 feet
  - Terminations = -40,000
  - Cable tray = -12,000 feet
  - Conduit = -177,000 feet
  - Supports = -7,000
  - Support steel = -18 tons

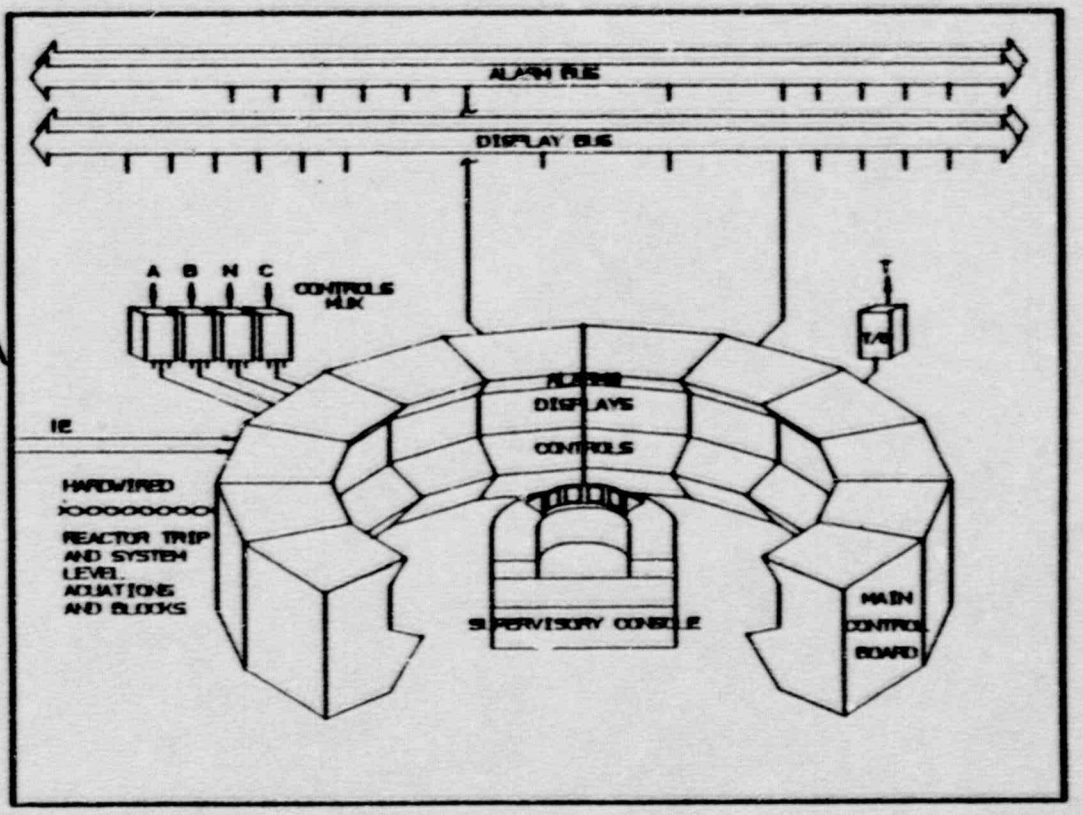
MAIN CONTROL ROOM (MCR)

1069 D19799.019

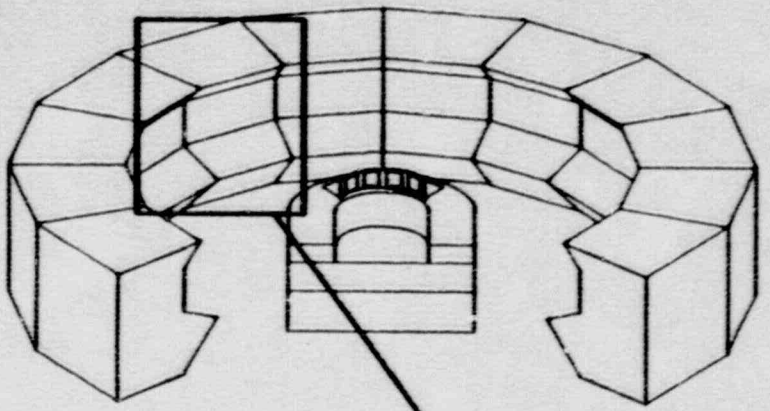
INSTRUMENTATION & CONTROL ARCHITECTURE



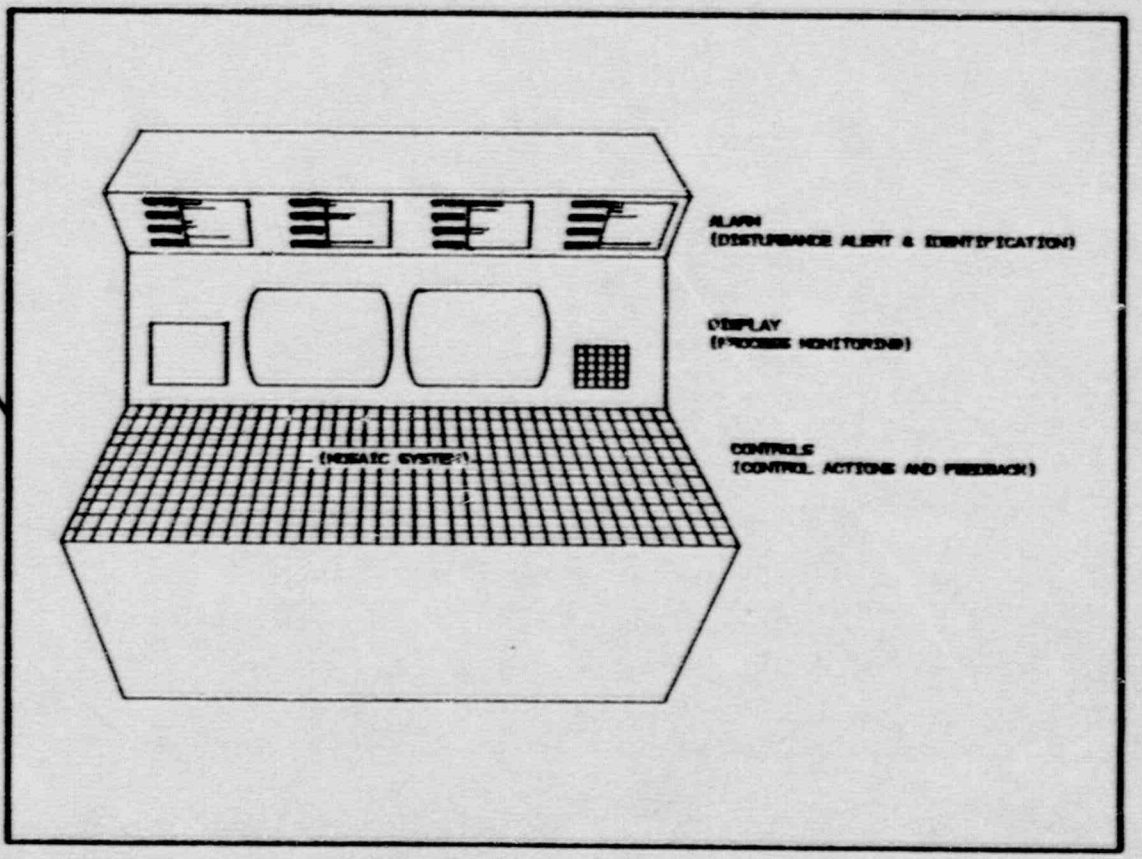
MAIN
CONTROL
ROOM



MAIN CONTROL ROOM



MAIN CONTROL
BOARD



H-30

Instrumentation & Control Systems
MAIN CONTROL ROOM (MCR)

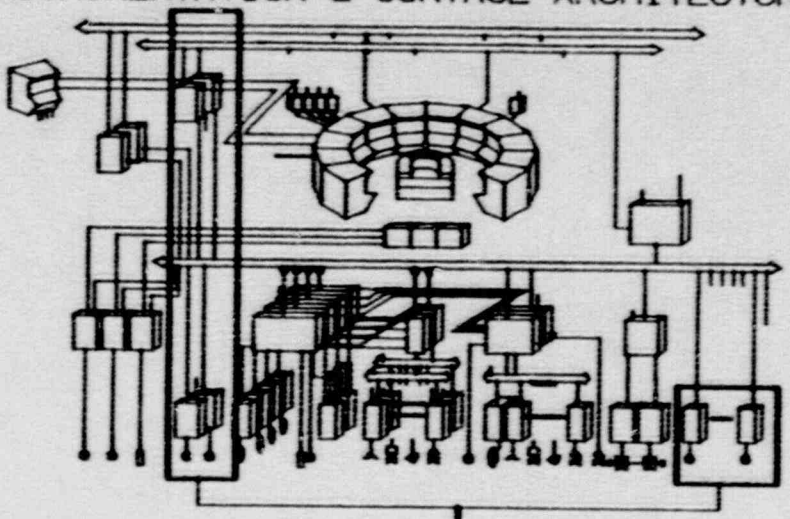
- Dedicated pushbutton controls:
  - Backlighted status indication
  - Multiplexing reduces wiring complexity
- Dedicated indicators:
  - Driven by digital I&C systems
  - Reduced number based on operational needs
- Graphic displays:
  - Qualified for safety related information
  - Operational aids from plant computer
  - Used for plant and systems surveillance
- Alarm system:
  - Driven by digital I&C systems
  - Reduced number based on grouping and prioritization

Instrumentation & Control Systems

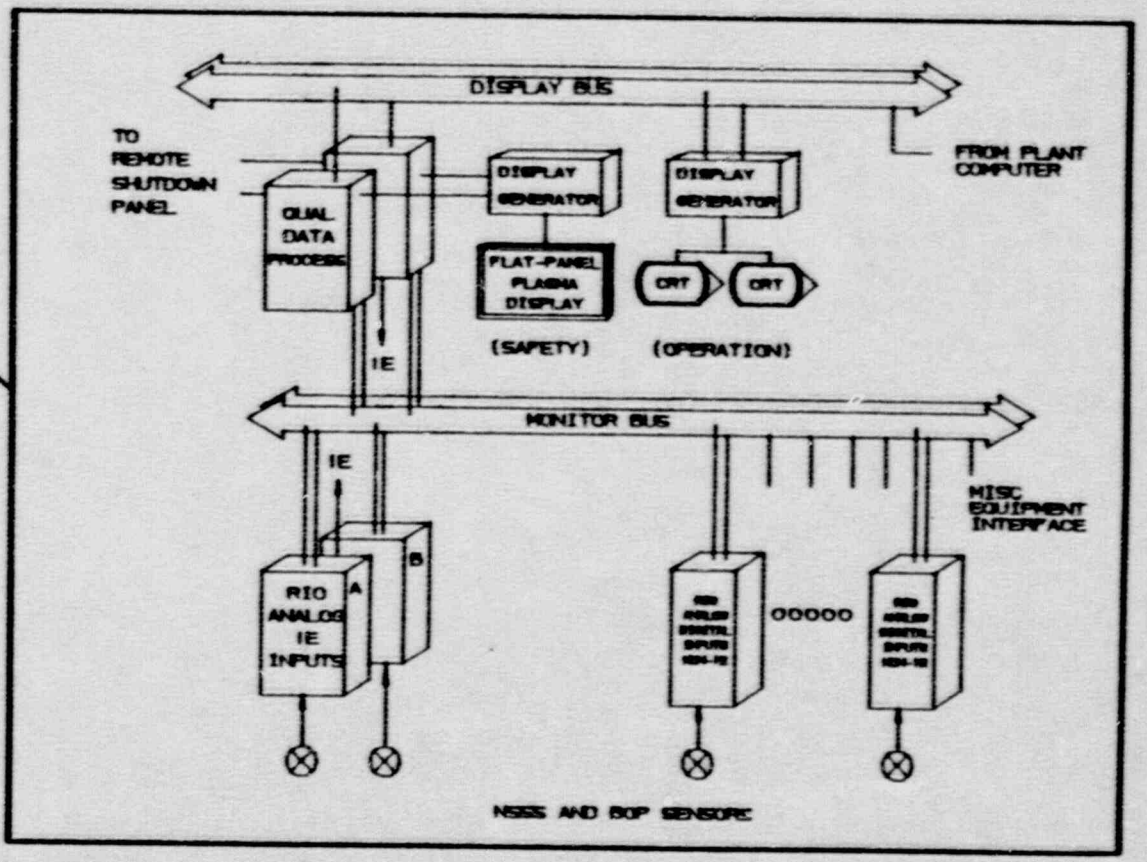
PLANT PROCESS DATA SYSTEM

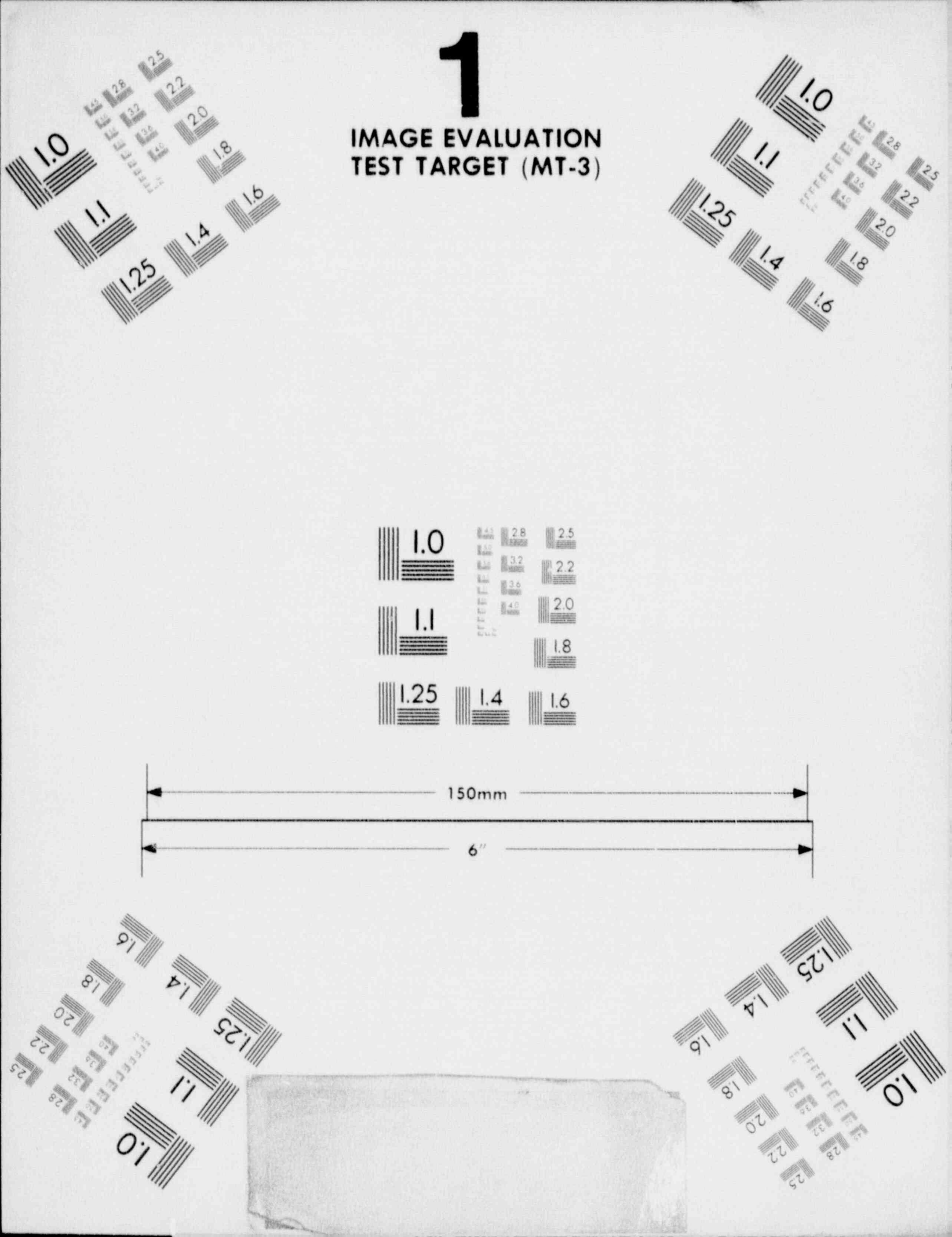
1050 D19799 014

INSTRUMENTATION & CONTROL ARCHITECTURE



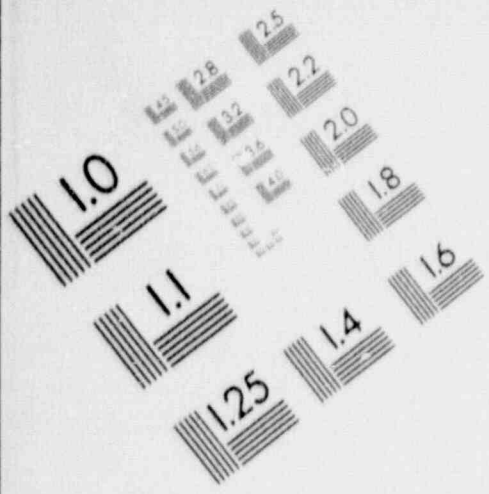
PLANT
PROCESS
DATA SYSTEM

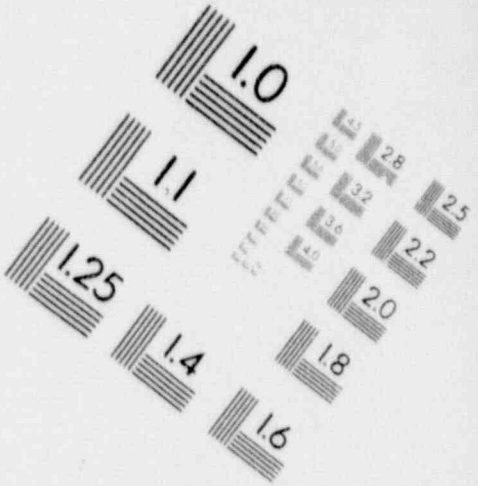


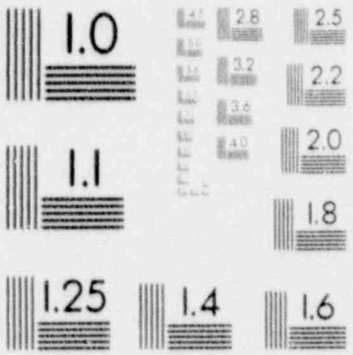

1
IMAGE EVALUATION
TEST TARGET (MT-3)
1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
150mm
6"

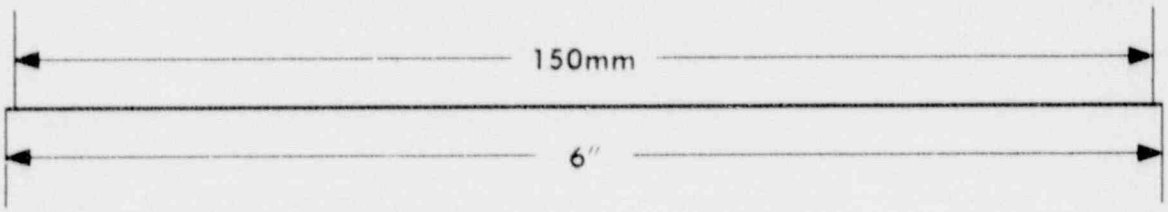
1

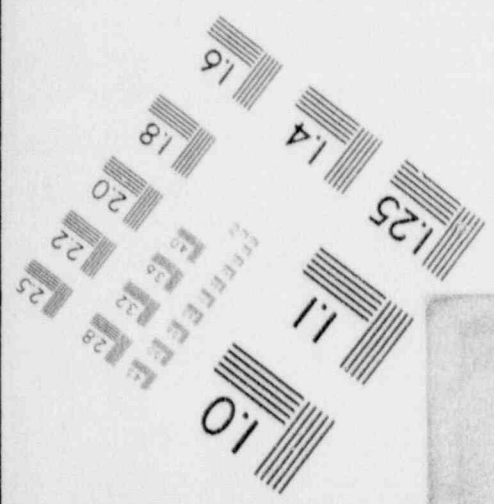
IMAGE EVALUATION TEST TARGET (MT-3)

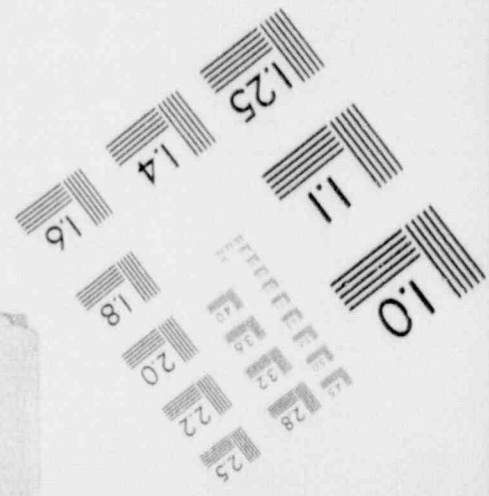






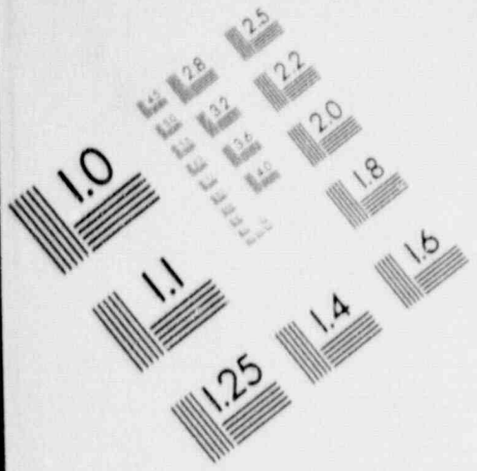


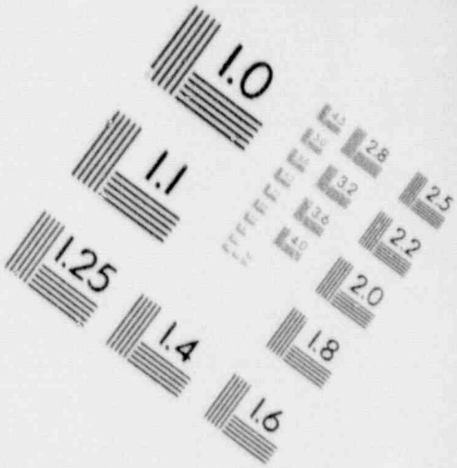


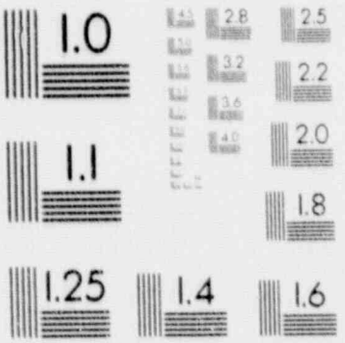


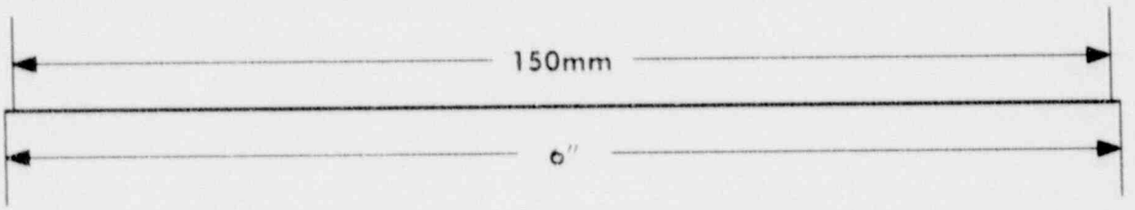
1

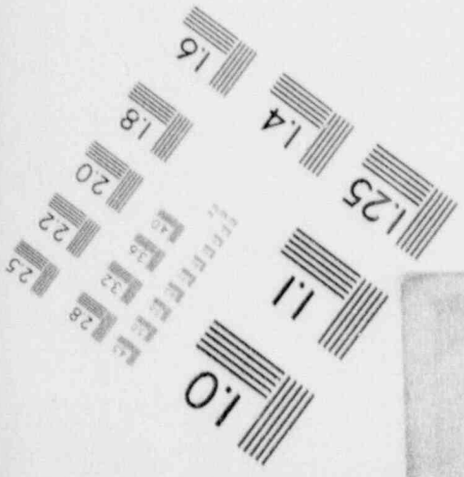
IMAGE EVALUATION TEST TARGET (MT-3)

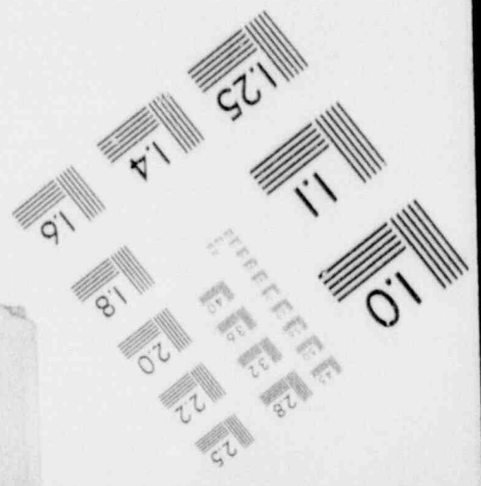


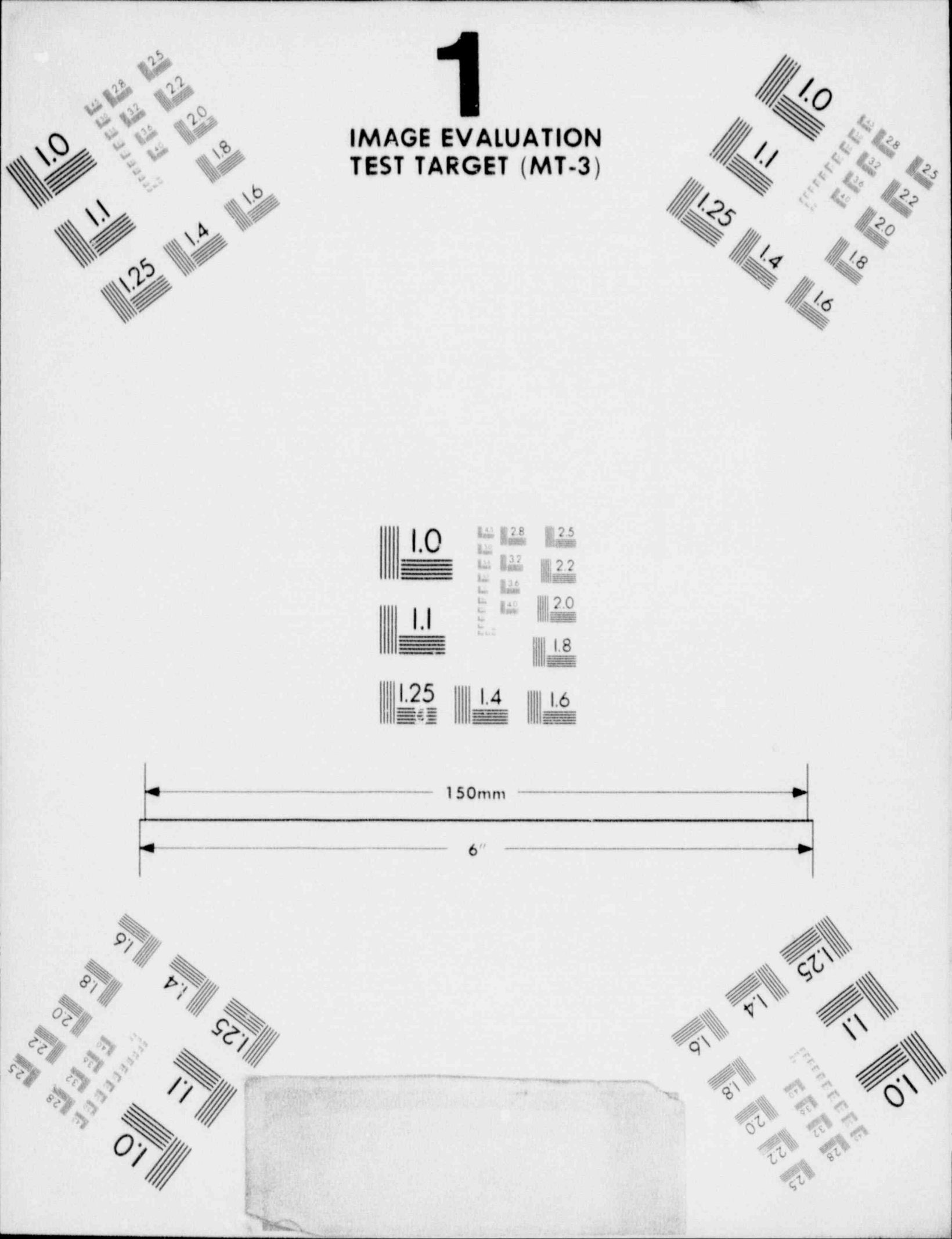








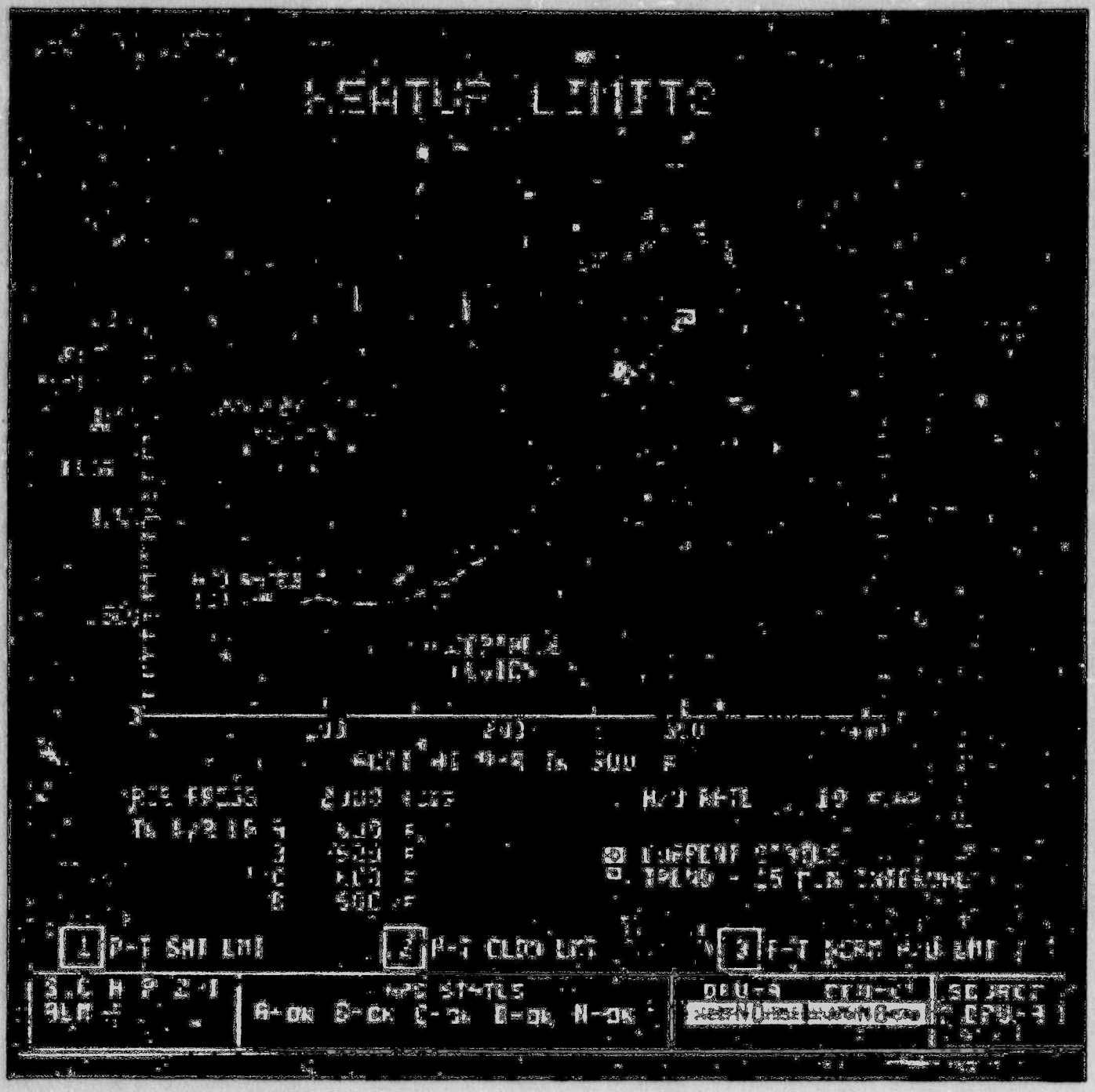


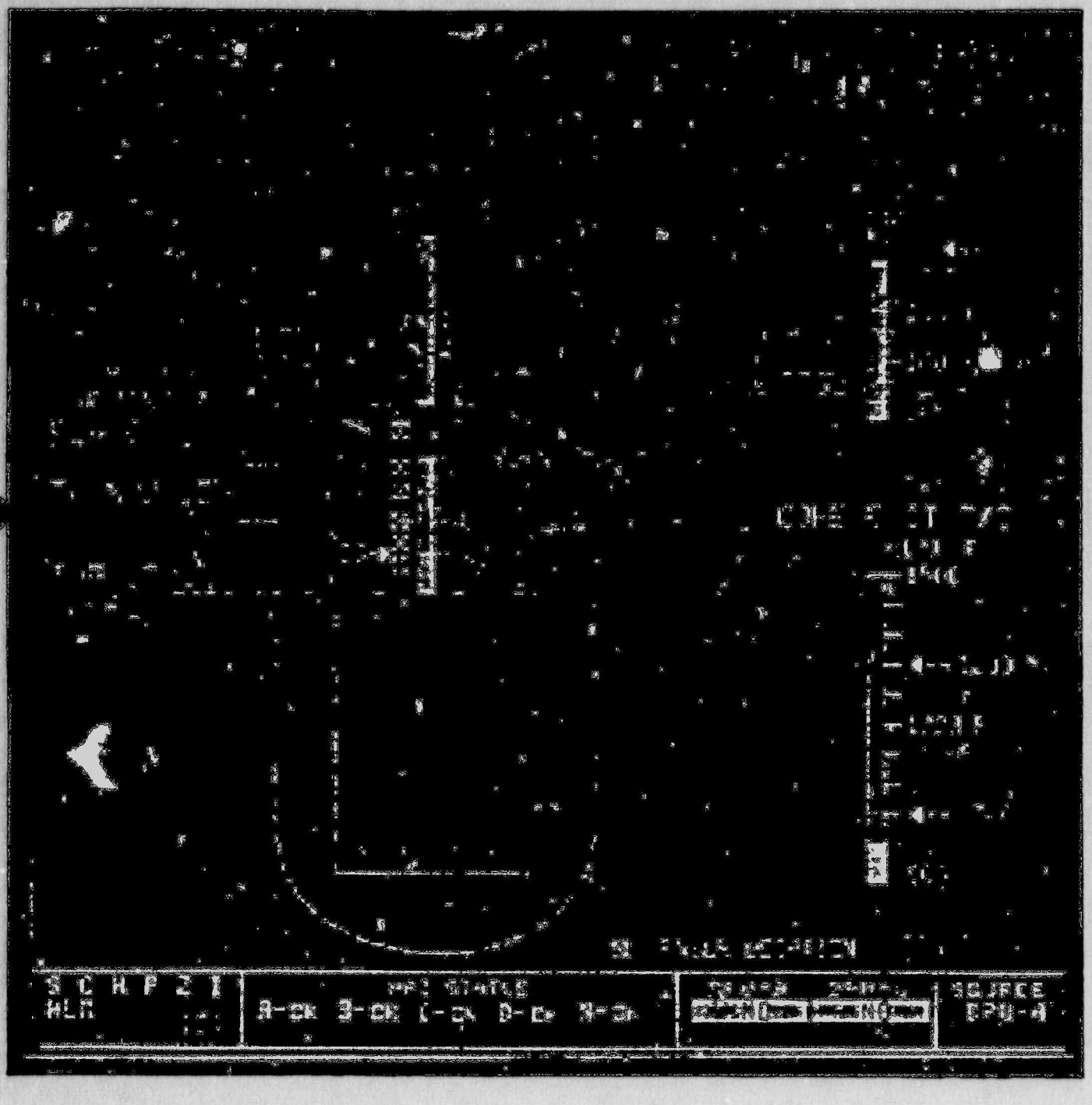

1
IMAGE EVALUATION
TEST TARGET (MT-3)
1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
150mm
6"

Instrumentation & Control Systems
PLANT PROCESS DATA SYSTEM

- Processes data to meet Regulatory Guide 1.97, Version 3, requirements for Category One and Two variables, including:
  - Reactor vessel level monitoring
  - Thermocouple/core cooling monitoring
  - Containment monitoring
- Provides qualified displays for the Regulatory Guide 1.97 variables
- Processes data required for plant operational displays
- Provides the plant operational displays
- Provides data from qualified applications to non-qualifed applications (e.g., plant computer, alarm system)

1007 D18779 044


HEATUP LIMITS
1 P-T SHT LMT
2 P-T COOL LMT
3 P-T LOOP H-U LMT
G-ON G-CK C-ON E-ON N-ON

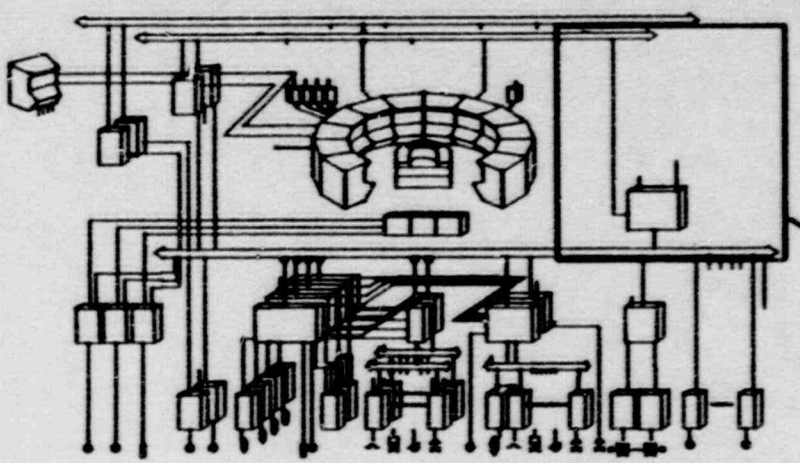


Instrumentation & Control Systems

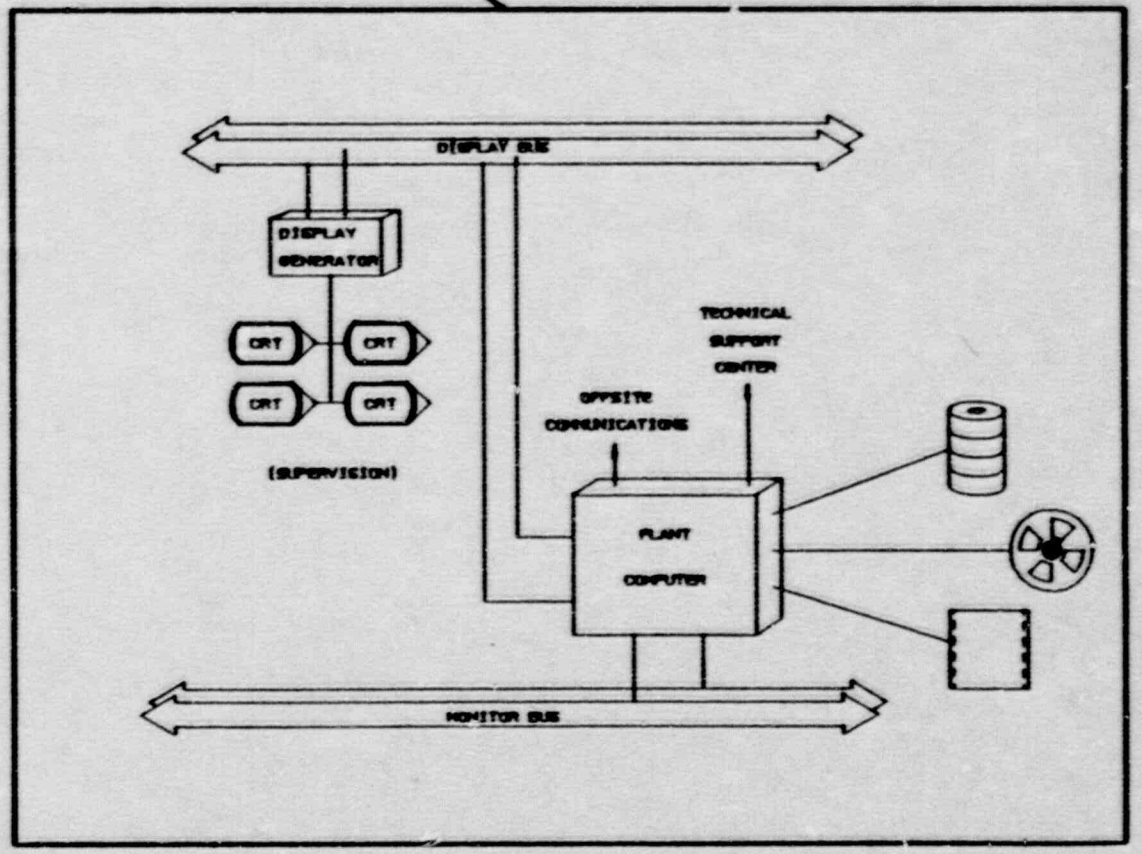
PLANT COMPUTER SYSTEM

1060 D19799.037

INSTRUMENTATION & CONTROL ARCHITECTURE



PLANT
COMPUTER
SYSTEM



Instrumentation & Control Systems
PLANT COMPUTER SYSTEM

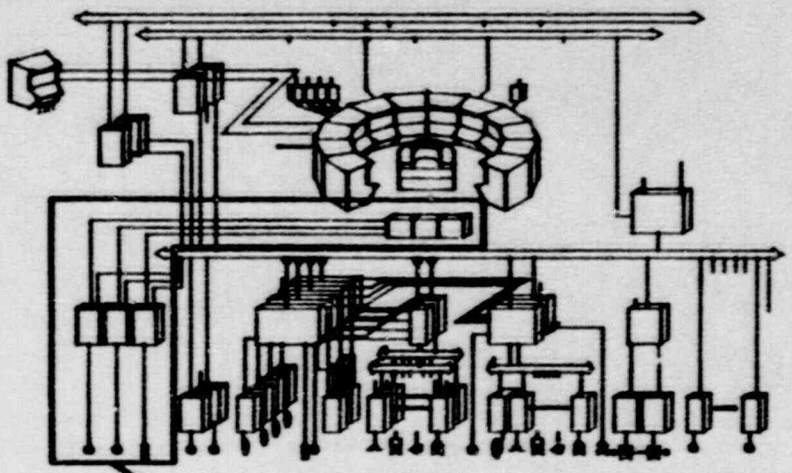
- Integrated communications with the distributed I&C architecture
- Central information management system
  - Historical data storage and retrieval
- Provides the plant function displays:
  - Main control board displays
  - Supervisory console displays
  - Technical Support Center displays
- Executes plant nuclear codes
- Supports the plant emergency response facility:
  - Technical Support Center
  - Off-site communications link

Instrumentation & Control Systems

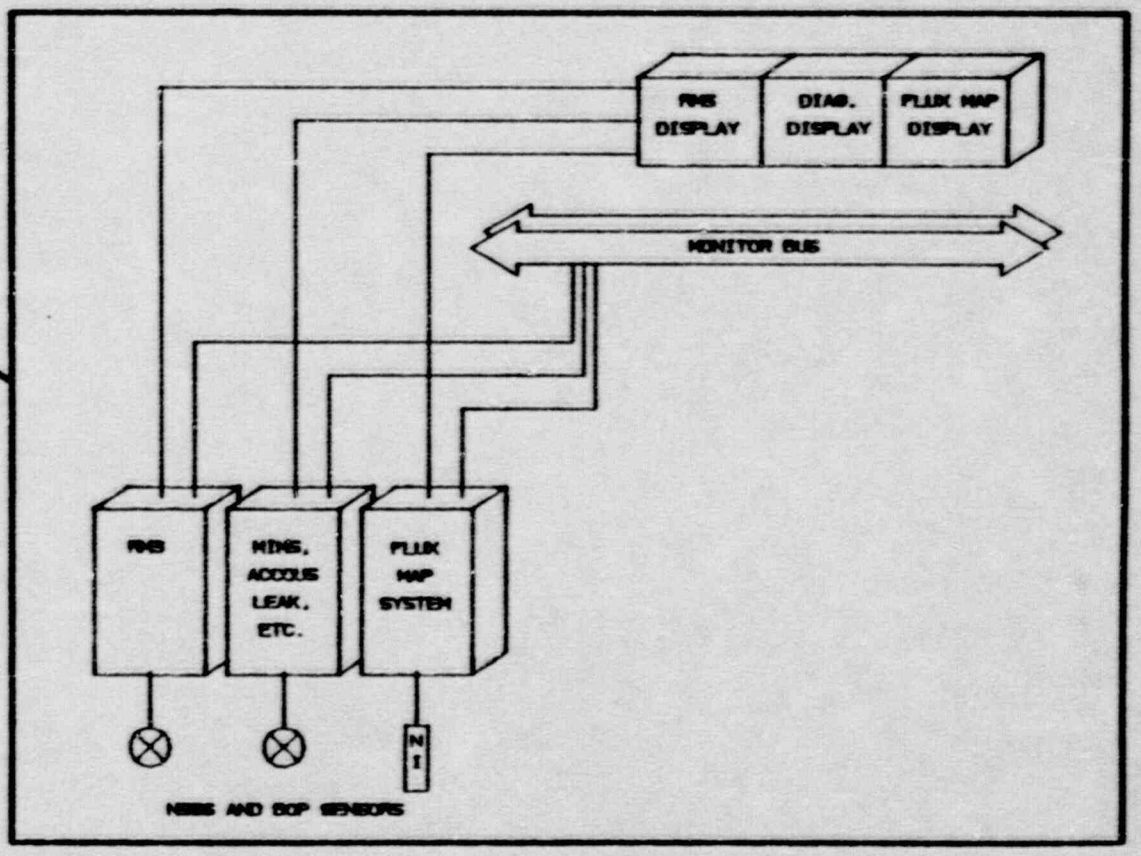
PLANT MONITORING SYSTEM

1050 D19799.015

INSTRUMENTATION & CONTROL ARCHITECTURE



PLANT
MONITORING
SYSTEMS

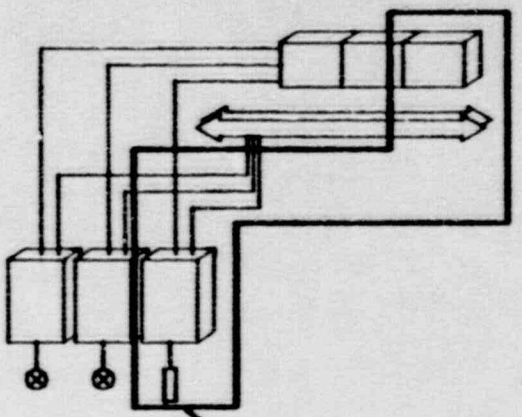


PLANT MONITORING SYSTEMS

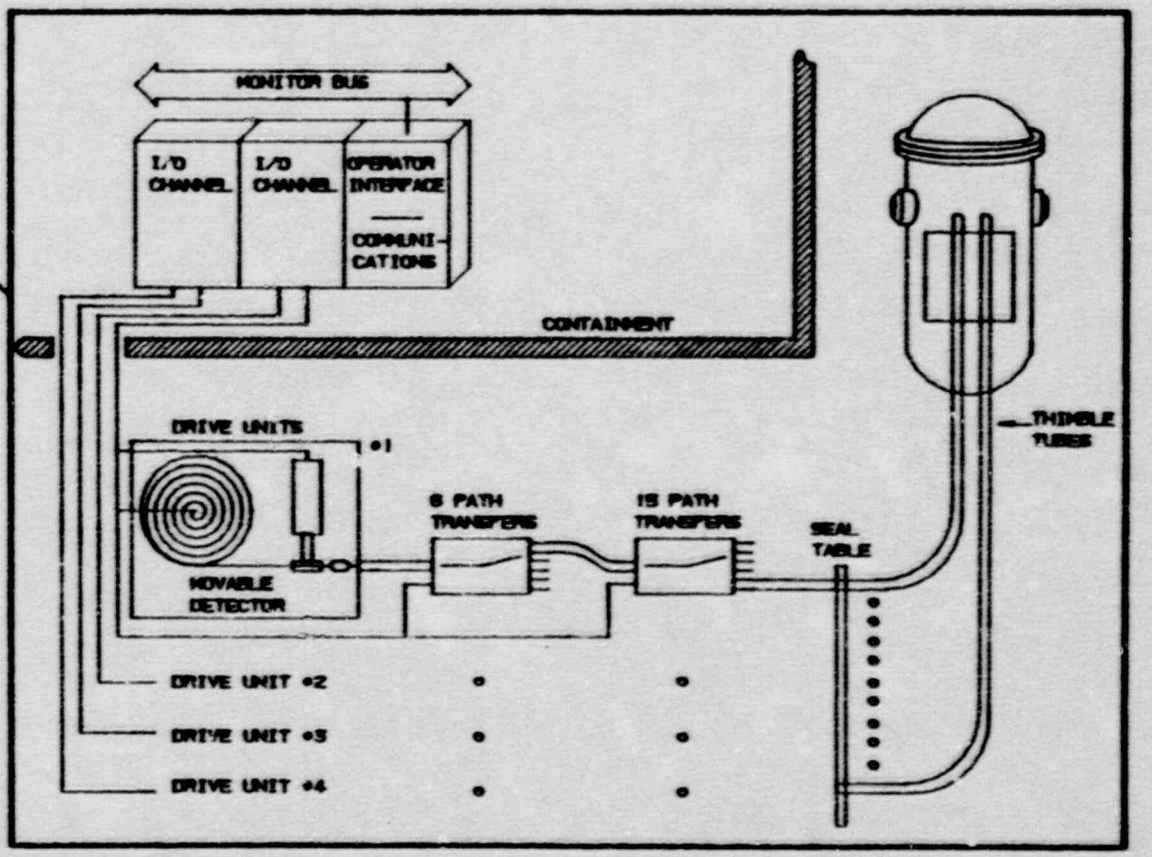
Microprocessor-based Monitoring Systems

- Automatic Flux Mapping System measures incore flux shapes
- Metal Impact Monitoring System detects the presence of loose metallic debris within the reactor coolant system
- Acoustic Leak Monitoring System detects leakage in critical piping systems and provides immediate feedback

PLANT MONITORING SYSTEMS



FLUX MAPPING SYSTEM



APPLICATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGY

Plant-Wide Monitoring and Diagnostic System

- An on-lilne artificial intelligence based component diagnostic system to support plant operations and maintenance tasks
  - Component diagnostic rules - expert rules and criteria about component failures are assembled in a knowledge structure based on component functionality to characterize component health
  - Operator guidance - expert operations knowledge is provided via strategies that would substitute other systems/components for failed components or would minimize usage stress on a specific component
  - Maintenance planning - evaluates the support of critical component failure on plant operations and safety to create a prioritized ranking and provides recommendations for maintenance repair time, alternate fixes, and resources required to repair the failed component

James R. Easter

Man-Machine Design

HUMAN FACTORS ENGINEERING RESEARCH & DEVELOPMENT:

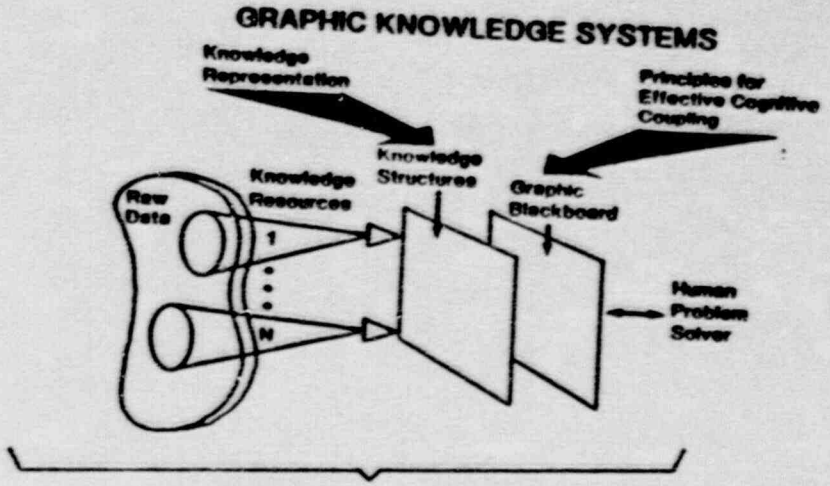
A TOP – DOWN APPROACH

MAN – MACHINE INTERFACE CONCEPT

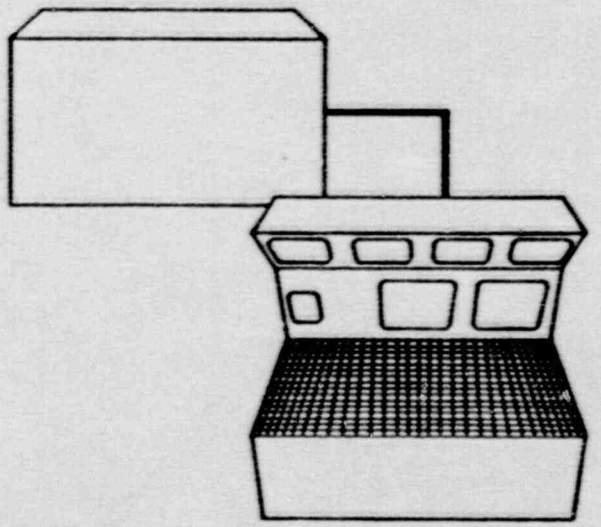
CHANGE IN MMI CONCEPT

IMPROVED TECHNOLOGY

IMPLEMENTATION TECHNOLOGY



INCORPORATE IN DIGITAL COMPUTING SYSTEM



L101686A

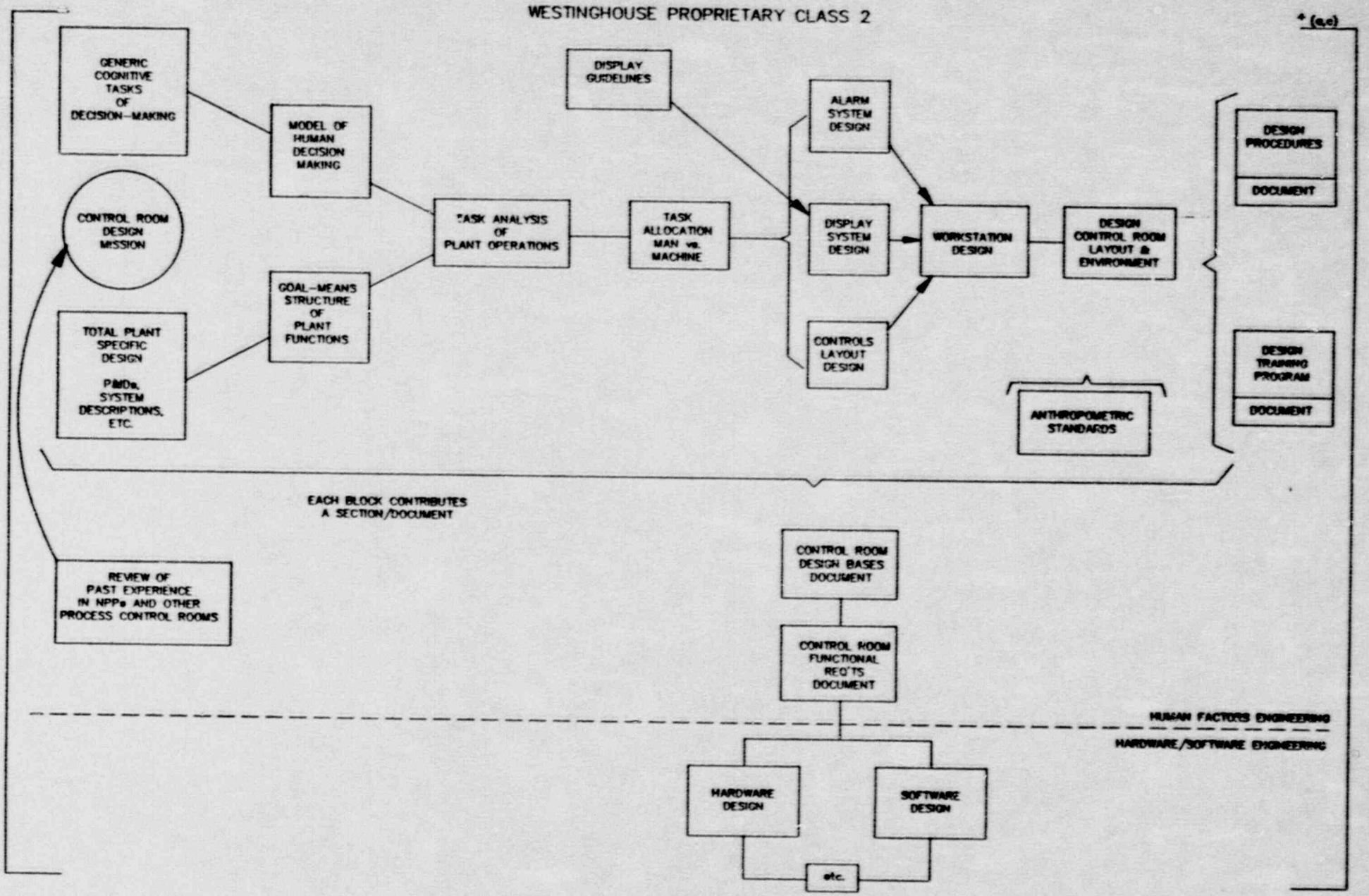
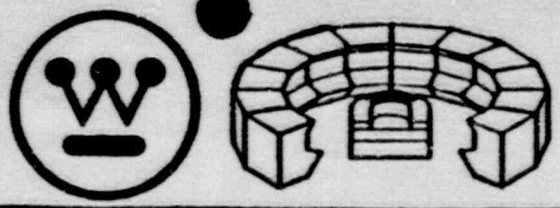


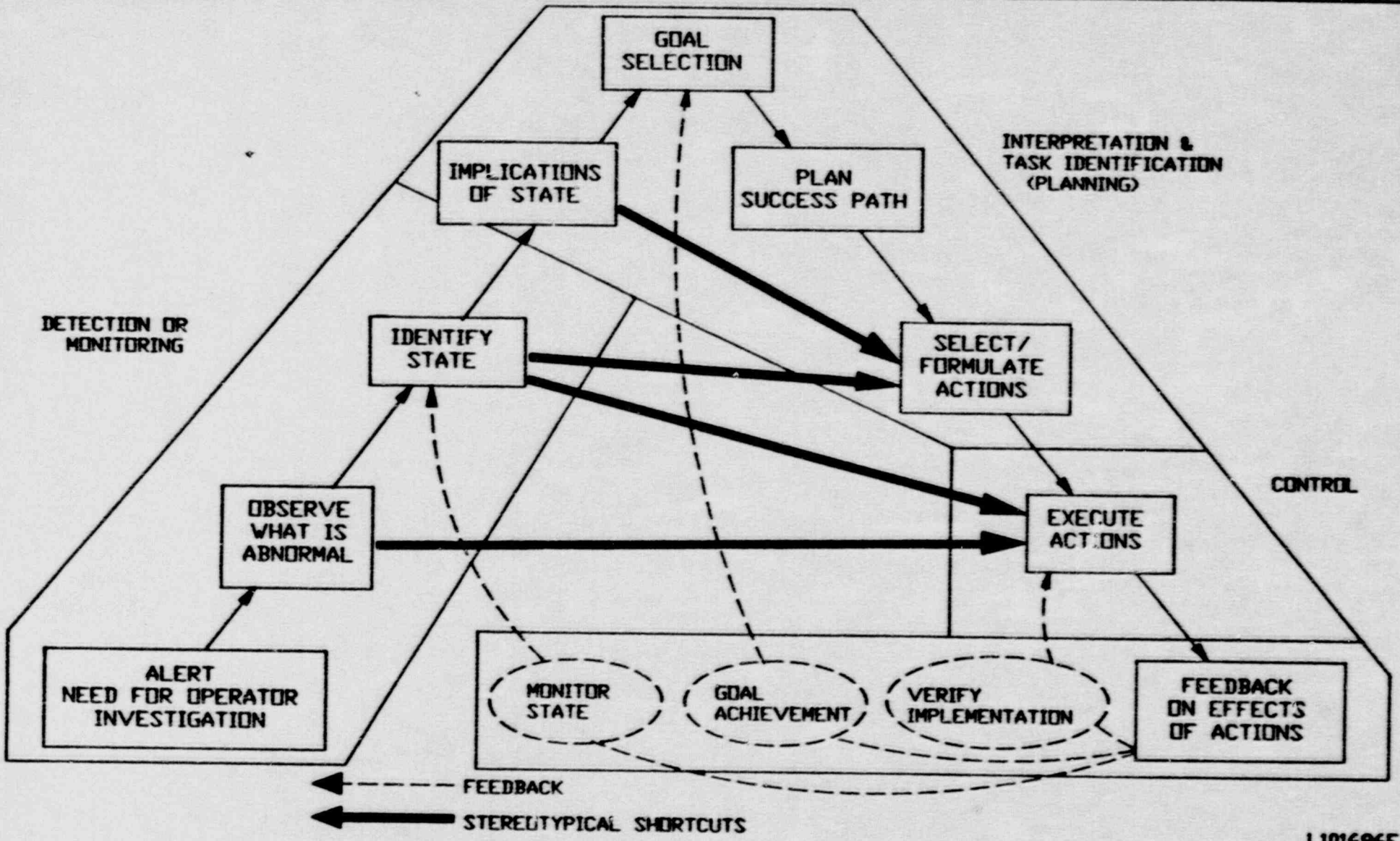
FIGURE 3.2.1.6-1 WESTINGHOUSE CONTROL ROOM DESIGN PROCESS



SIMPLIFIED OPERATOR

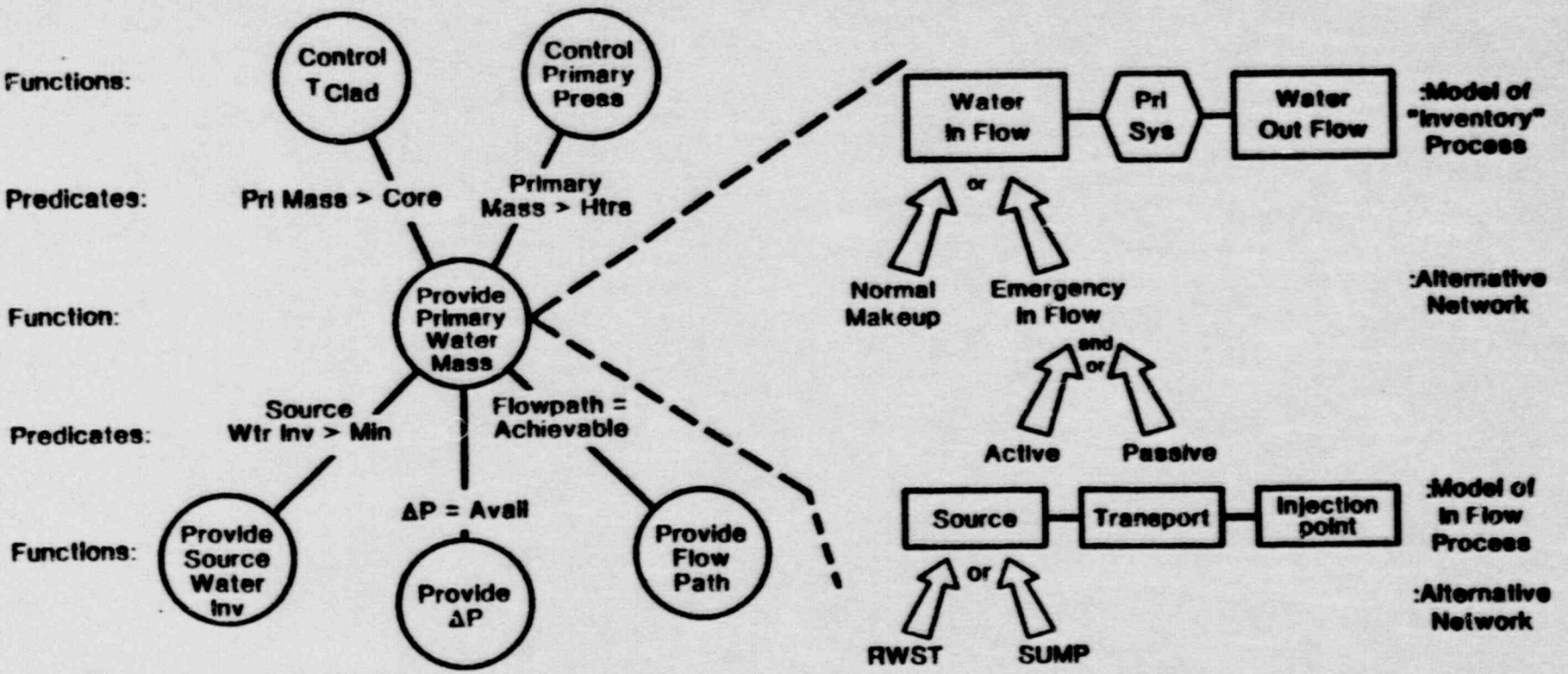
CONTROL ROOM DESIGN: DECISION-MAKING MODEL

(ADAPTED FROM RASMUSSEN)



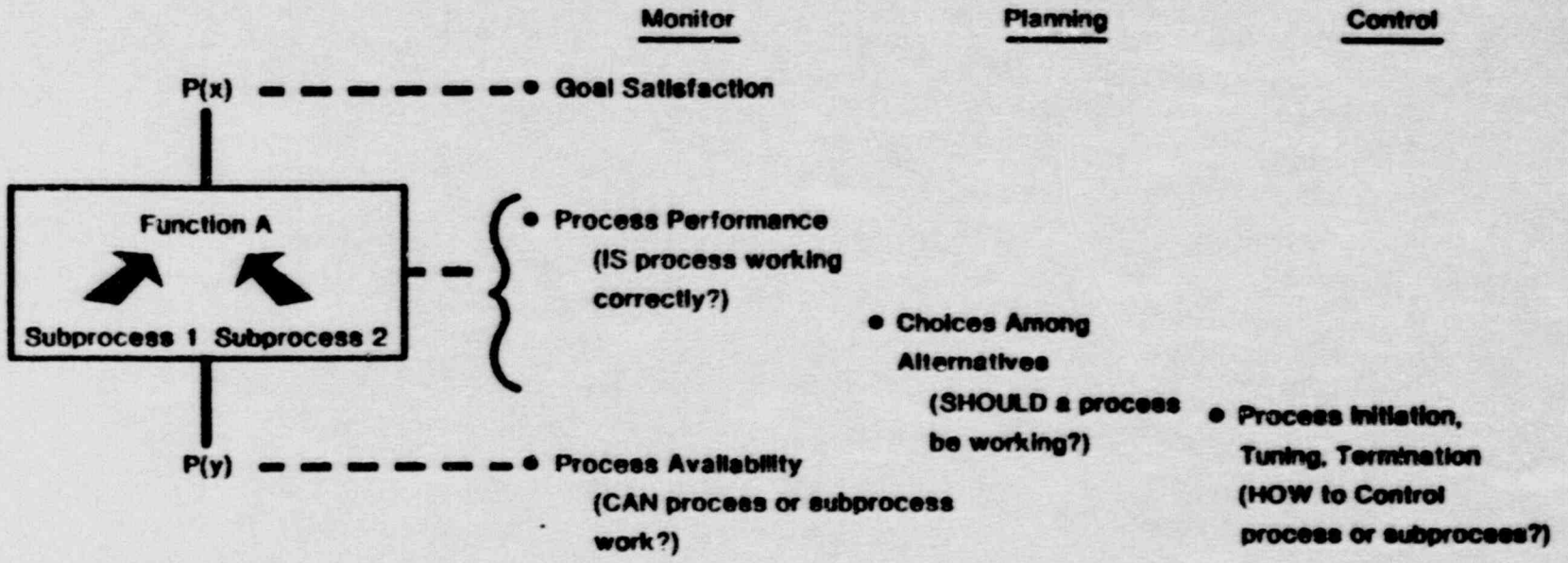
L1016086E

CONTROL ROOM DESIGN PROCESS: FUNCTIONAL MODEL OF PLANT PROCESS, A GOAL–MEANS STRUCTURE



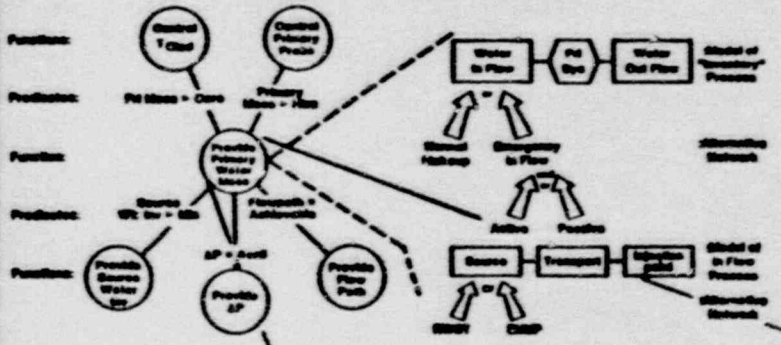
- **Goal/Means Structure**

Tasks

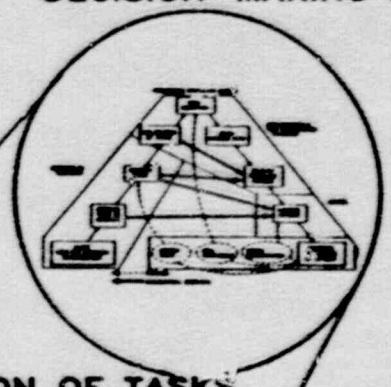


FUNCTION BASED TASK ANALYSIS : SUMMARY COMPONENTS & IMPACTS

FUNCTIONAL DECOMPOSITION OF PLANT PROCESSES

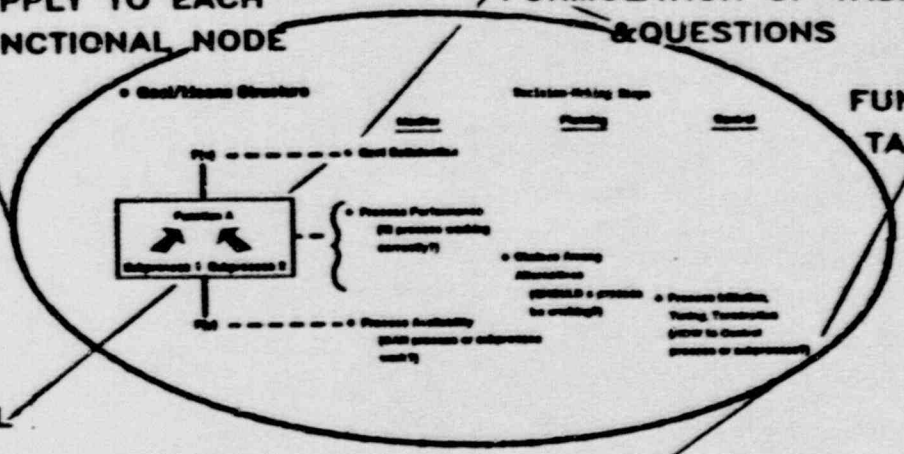


RASMUSSEN'S DECISION–MAKING MODEL



APPLY TO EACH FUNCTIONAL NODE

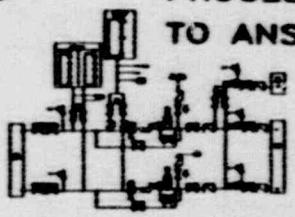
FORMULATION OF TASKS &QUESTIONS



FUNCTION BASED TASK ANALYSIS

PLANT'S PHYSICAL DESCRIPTION

PROCESS DATA NEEDED TO ANSWER QUESTIONS



IMPACTS

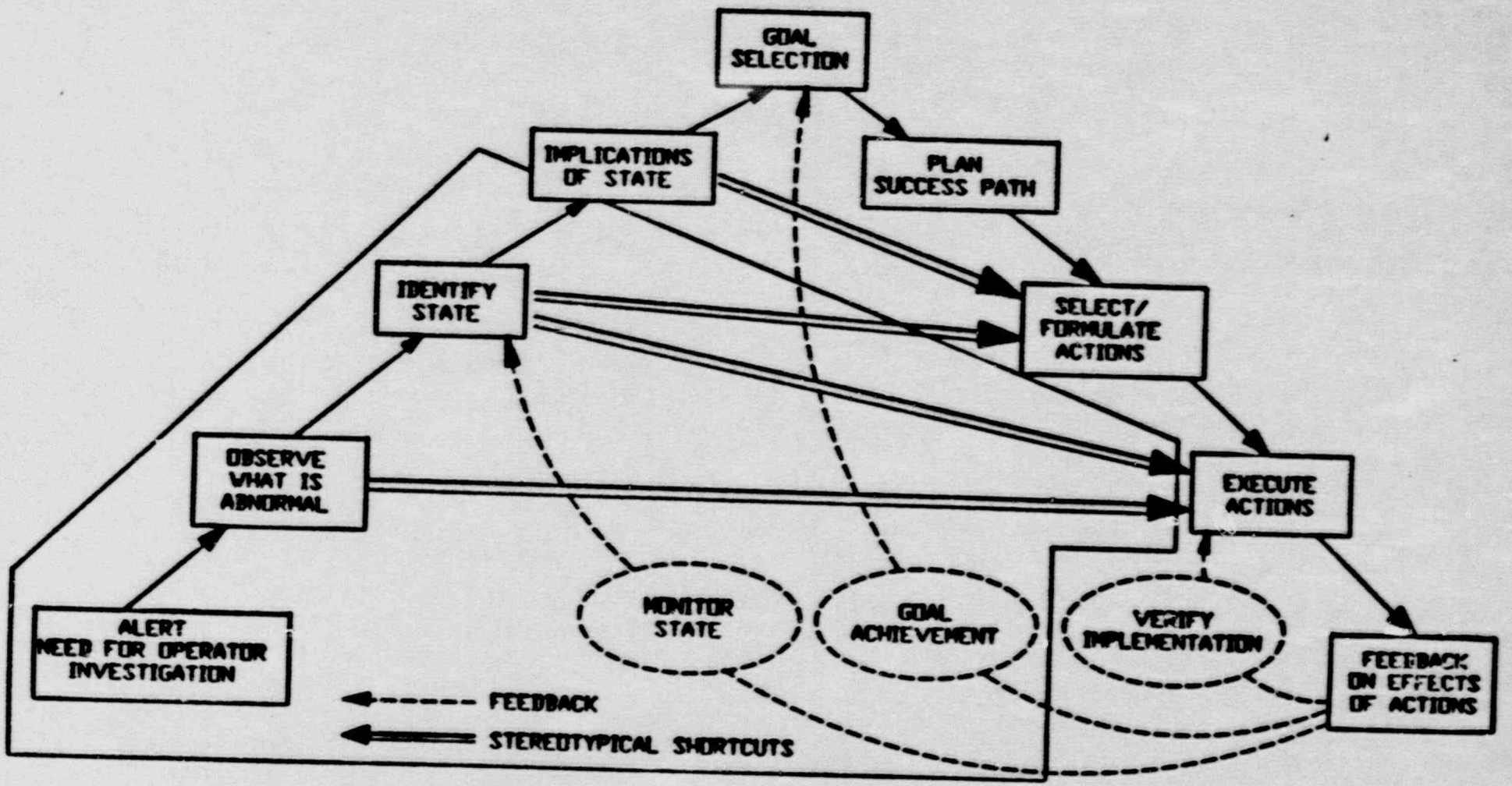
INSTRUMENTATION/CONTROL BOARD DESIGN
- IDENTIFIES REQUIRED INSTRUMENT LIST
- IDENTIFIES REQUIRED ALARMS & THEIR TRIGGERS
- DETERMINES ALARM MESSAGE CONTENT
- DETERMINES ALARM PRIORITIZATION
- ORGANIZES/GROUPS PROCESS DATA FOR DISPLAY
- SUPPORTS SYSTEMS MSR & EQUIPMENT OPERATOR ROLES
- PROVIDES GUIDANCE FOR ROOM & WORKSTATION LAYOUT

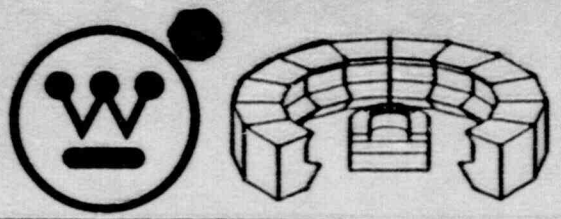
PLANT AUTOMATION
- IDENTIFIES CONTROLLER OBJECTIVES
- IDENTIFIES CONTROLLER INPUTS
- SHOWS FUNCTIONAL RELATIONSHIPS BETWEEN CONTROLLERS
- HELPS IDENTIFY ESSENTIAL CONTROL ACTIONS

PROCEDURES
- CONTENT & GENERAL ORGANIZATION OF PROCEDURES

TRAINING
- ORGANIZES OPERATOR TASKS
- FORMS BASIS FOR PROPER MENTAL MODELS OF PLANT PROCESS — SETS TRAINING OBJECTIVES
- PROVIDES BASIS FOR ASSESSING PERFORMANCE OF OPERATOR TRAINING

ALARM SYSTEM: DECISION MAKING MODEL

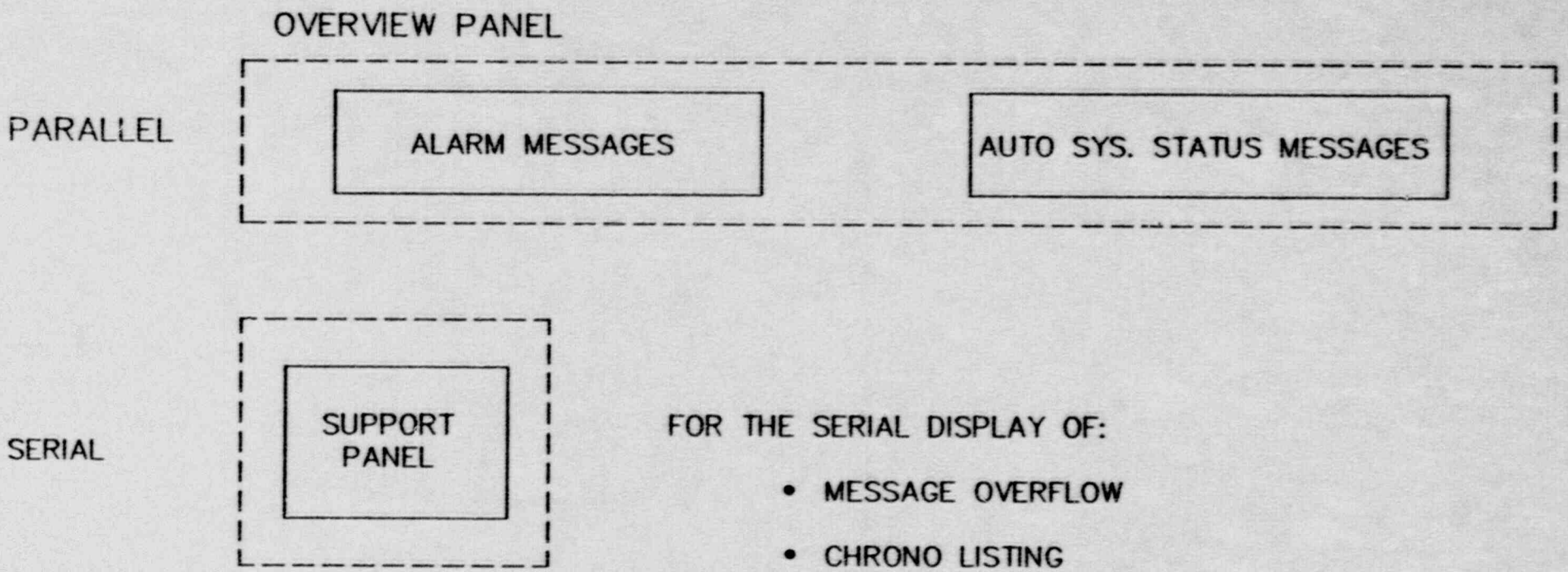




ALARM SYSTEM: TYPES OF MEASSAGES IN THE ALARM SYSTEM

- ALARM OVERVIEW MESSAGES – DISPLAY ABNORMALITY
- ALARM SUPPORT MESSAGES – PROVIDE MEANS FOR OPERATOR TO QUERY THE ALARM SYSTEM
- AUTO SYSTEMS ACTIONS MESSAGES – MESSAGES TELLING THE OPERATOR WHAT THE AUTOMATIC CONTROL SYSTEMS ARE DOING
- EMERGENCY SAFEGUARDS STATUS MESSAGES – CONTINUOUS INDICATION OF THE BINARY STATE OF THE ESF

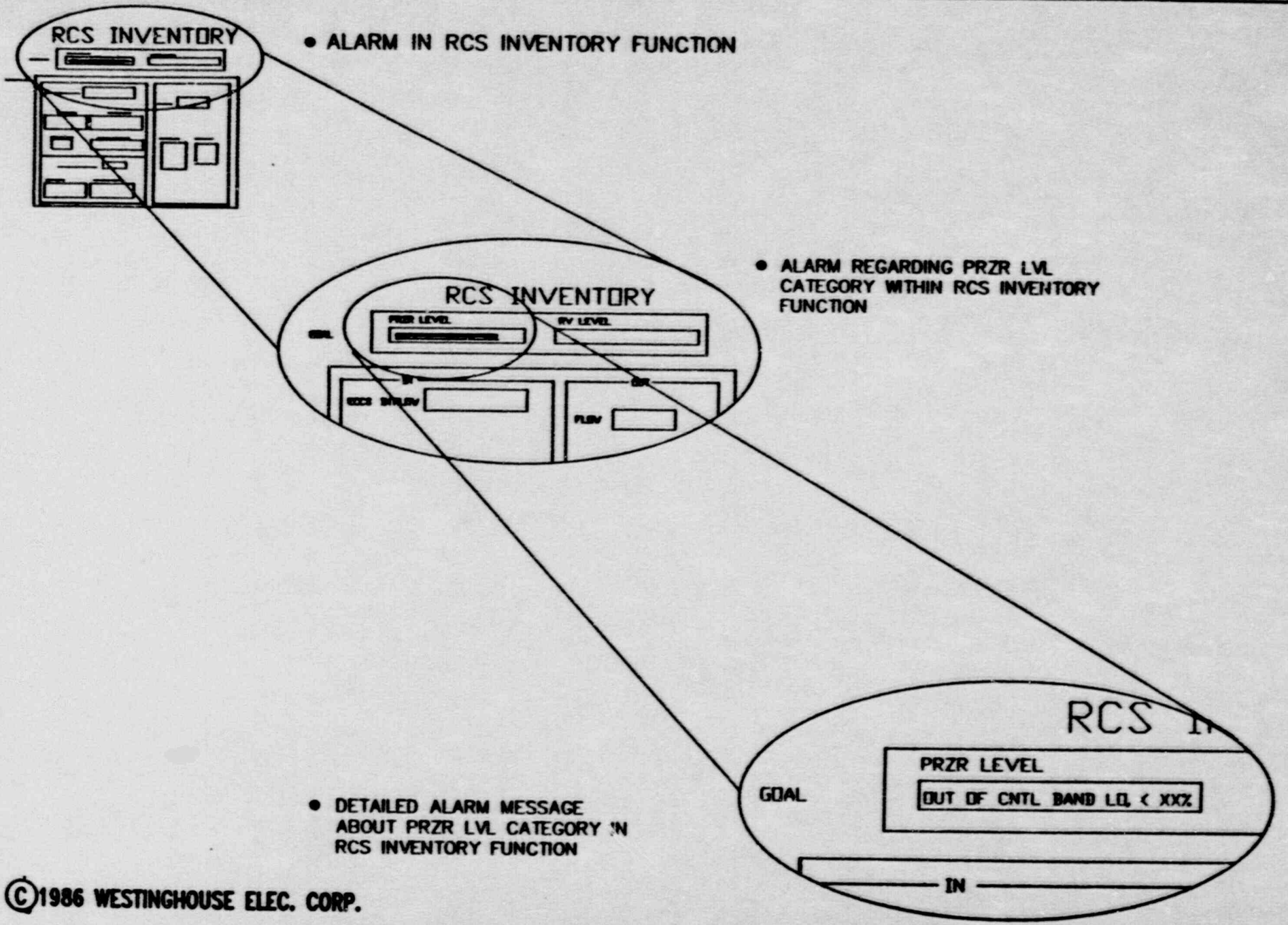
ALARM SYSTEM: HYBRID, PARALLEL/SERIAL DISPLAY



FOR THE SERIAL DISPLAY OF:

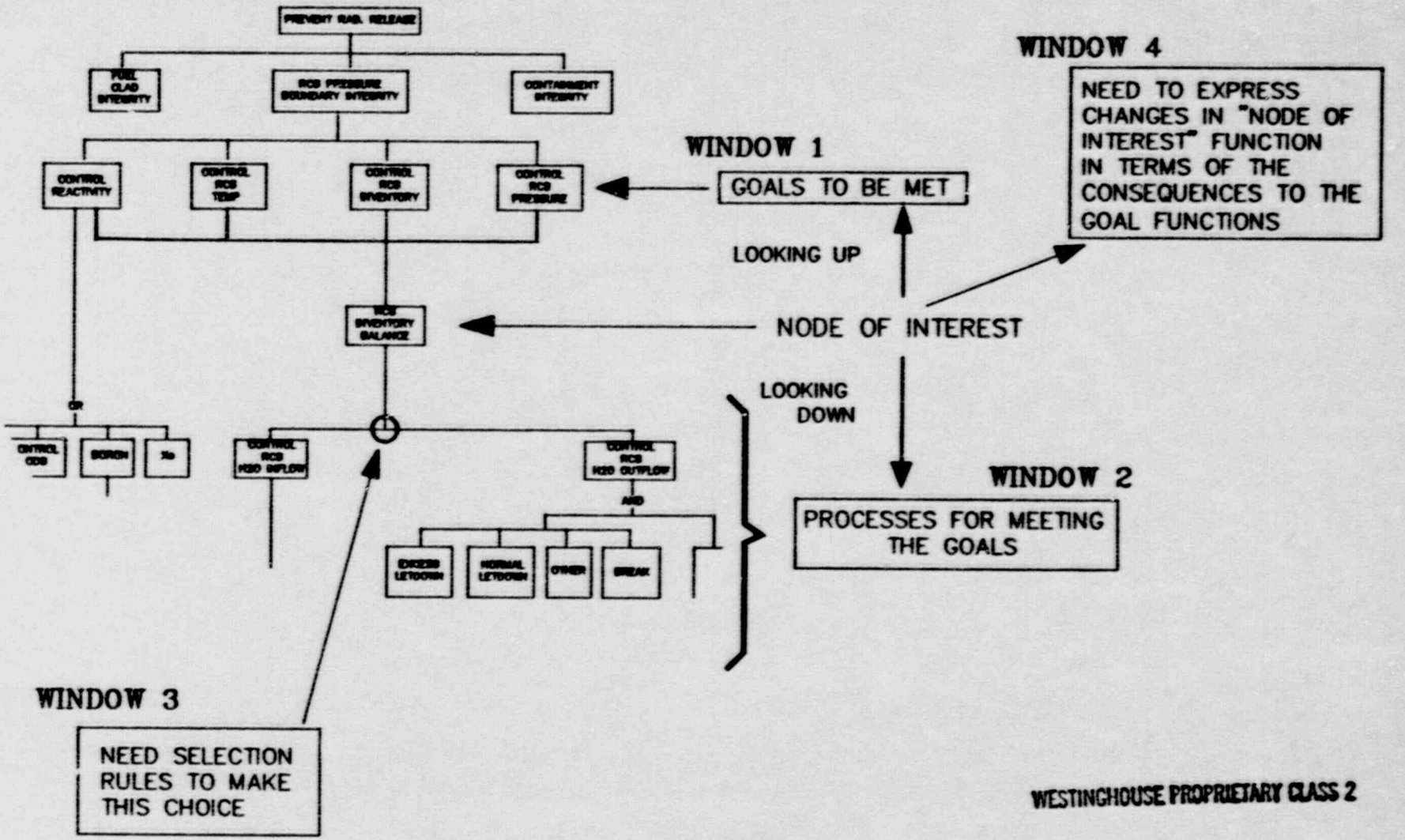
- MESSAGE OVERFLOW
- CHRONO LISTING
- SET POINTS/LOGIC
- PROCEDURES
- ETC.

OVERVIEW PANELS: MULTI–LEVEL MESSAGE ORGANIZATION



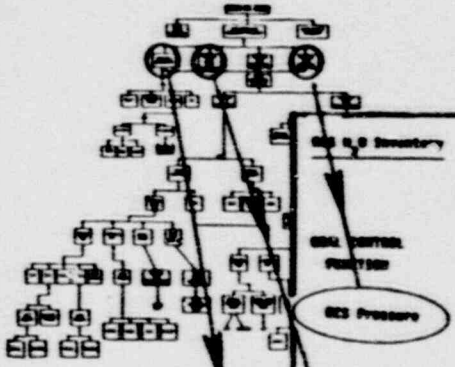
FUNCTIONAL STRUCTURE AND DISPLAY WINDOWS:

ORIGIN OF DISPLAY WINDOW TOPICS

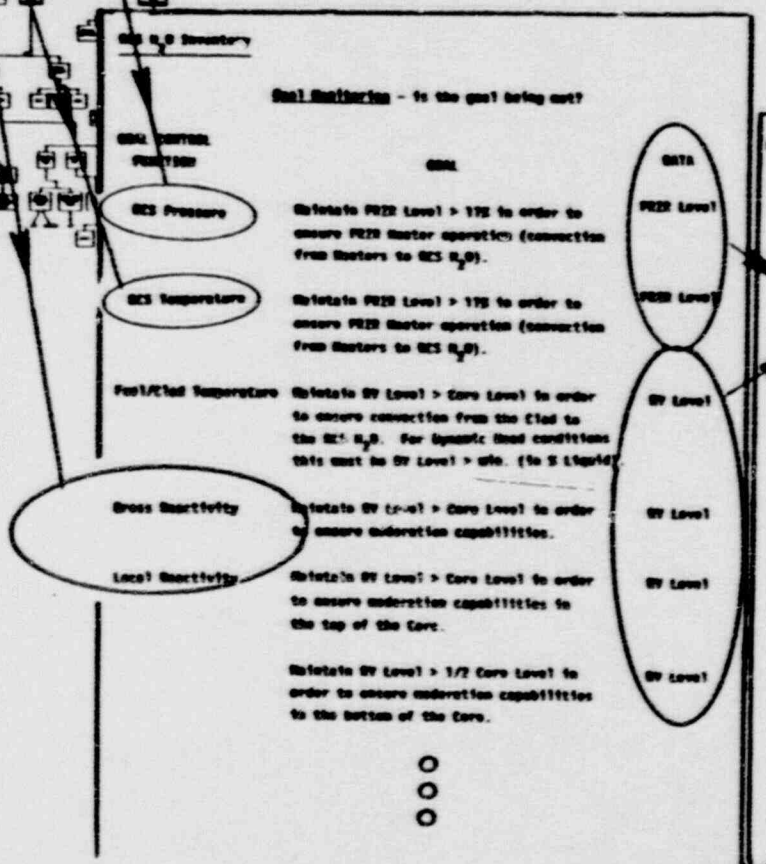


TASK ANALYSIS & DISPLAY DESIGN : FROM FUNCTIONAL STRUCTURE TO DISPLAY WINDOW

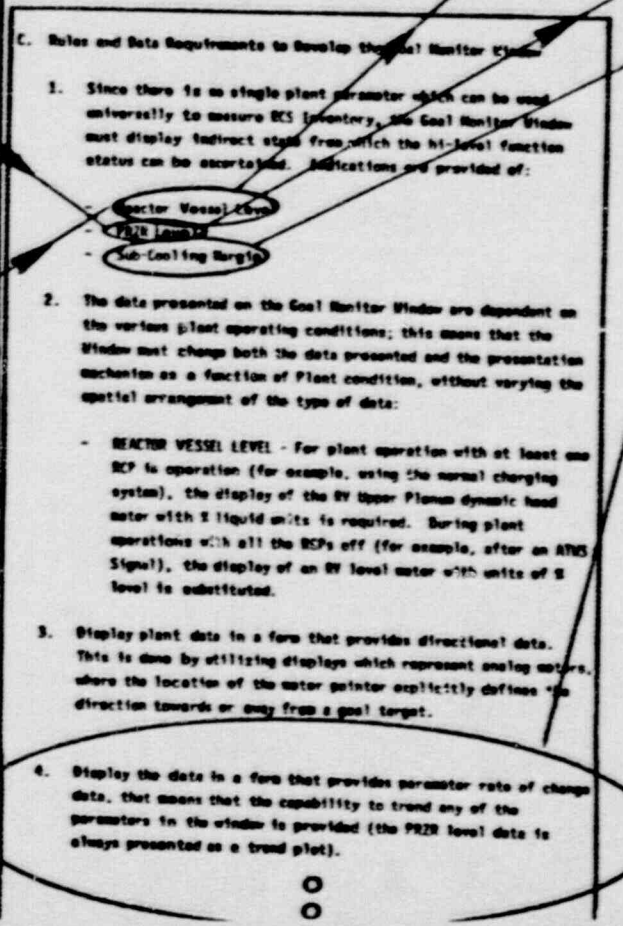
FUNCTIONAL STRUCTURE



TASK ANALYSIS



DISPLAY TASK DESCRIPTION



DISPLAY (GOAL) WINDOW

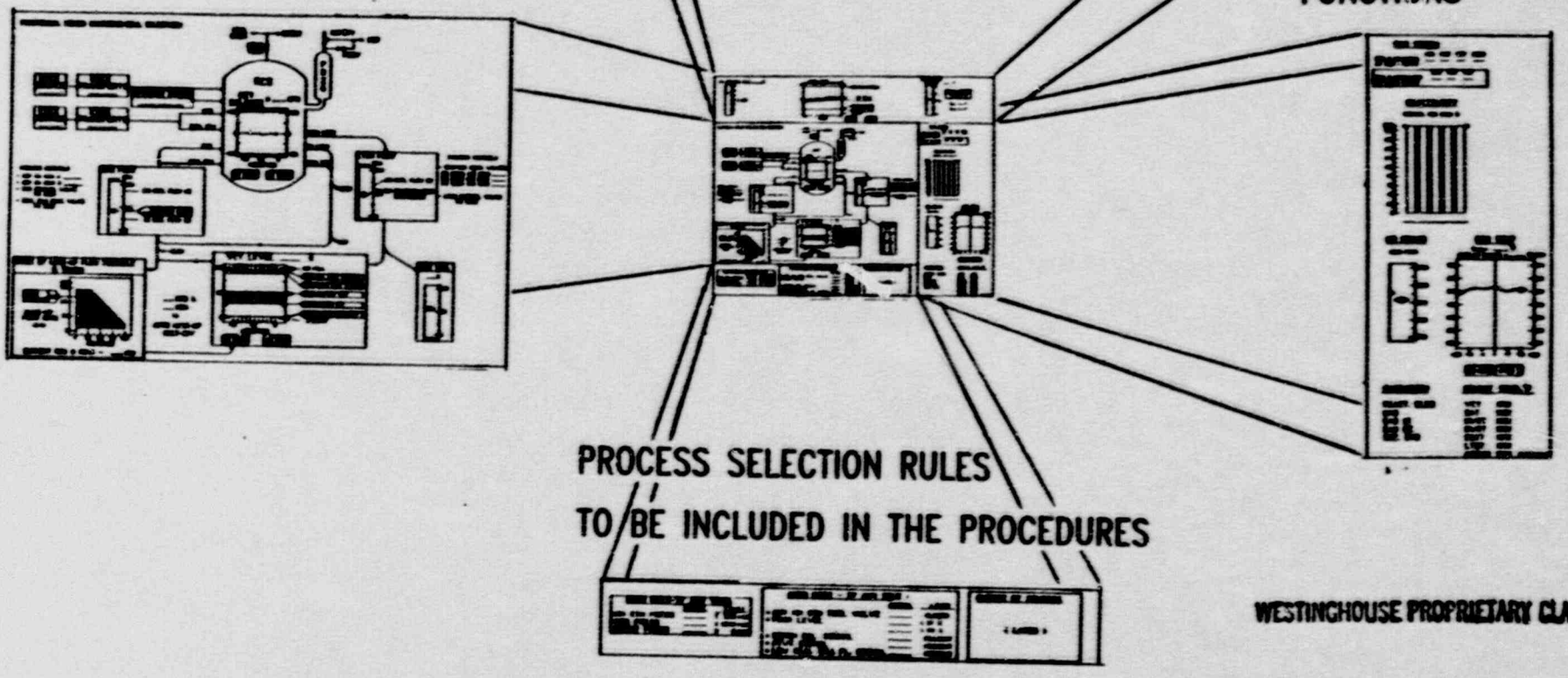
DISPLAY OF FUNCTIONAL DATA :

DISPLAY WINDOWS

MEASURES OF GOAL ACHIEVEMENT

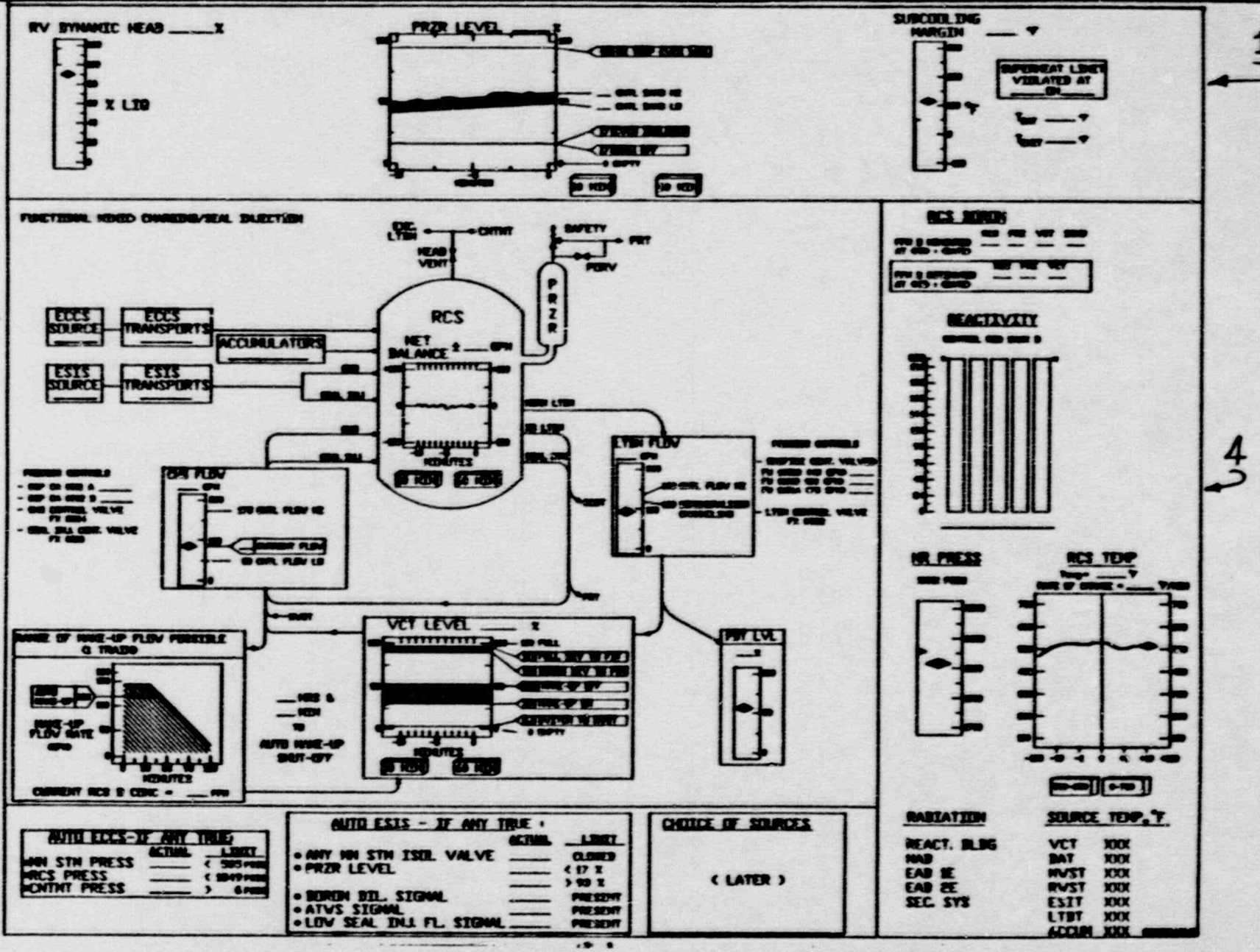
PROCESSES AVAILABLE
TO SATISFY THE GOAL FROM
A FUNCTIONAL (PURPOSE) PERSPECTIVE

EFFECTS ON OTHER
FUNCTIONS



PROCESS SELECTION RULES
TO BE INCLUDED IN THE PROCEDURES

FUNCTIONAL DISPLAYS : A TYPICAL EXAMPLE

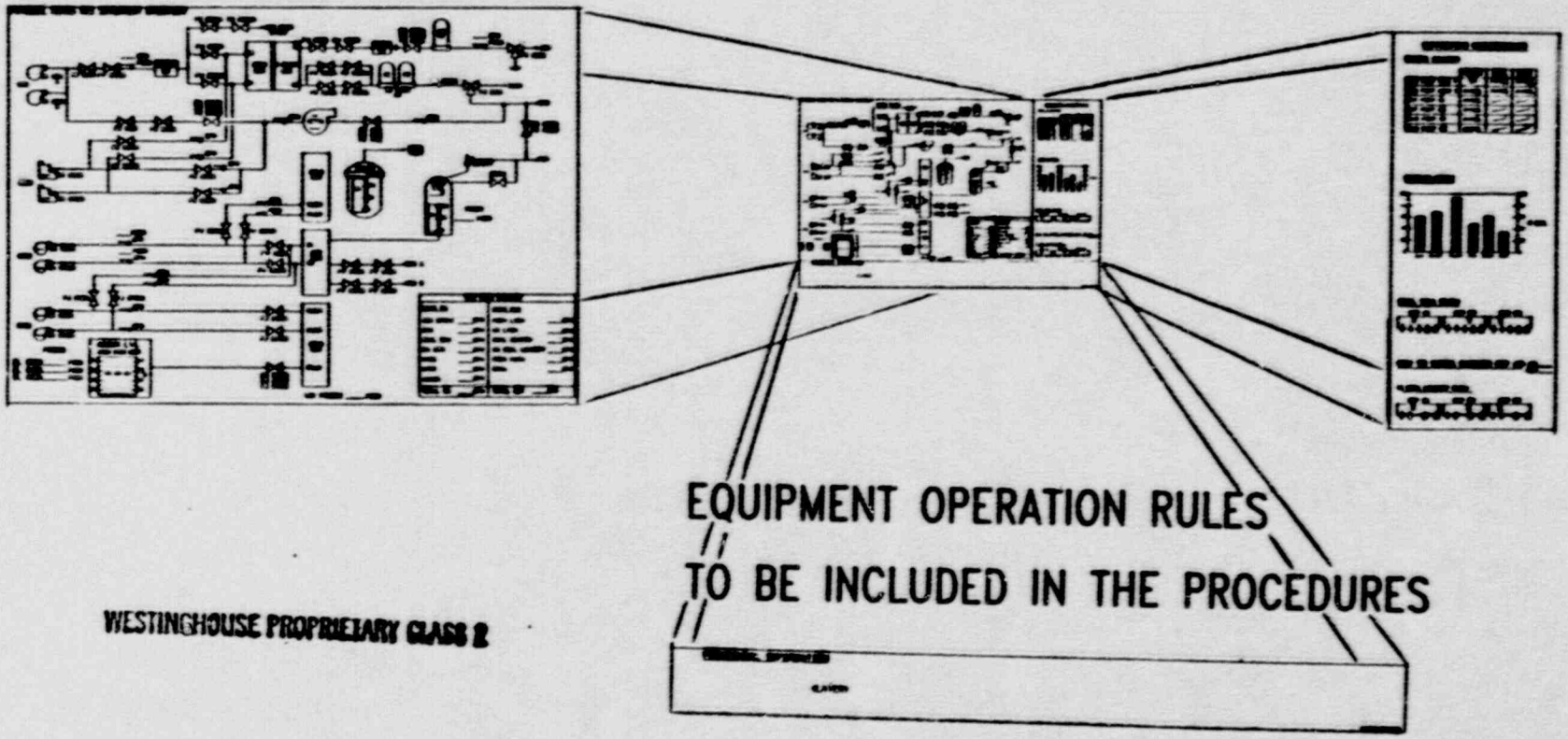


DISPLAY OF PHYSICAL DATA :

DISPLAY WINDOWS

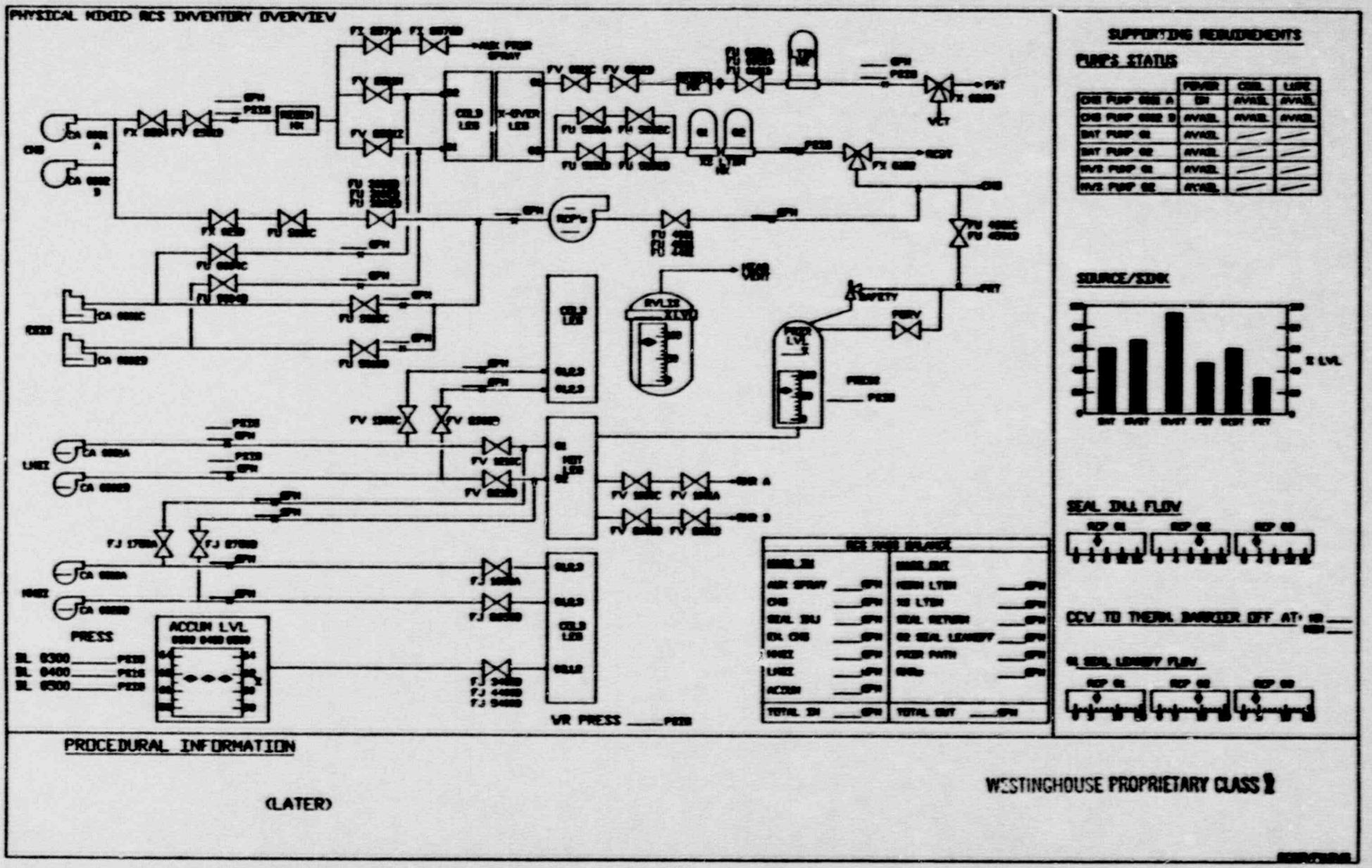
EQUIPMENT DESIGNED TO ACHIEVE THE FUNCTIONAL GOAL

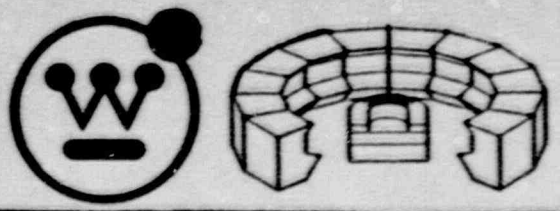
SUPPORTING REQUIREMENTS FOR EQUIPMENT OPERATION



EQUIPMENT OPERATION RULES TO BE INCLUDED IN THE PROCEDURES

PHYSICAL DISPLAYS : A TYPICAL EXAMPLE



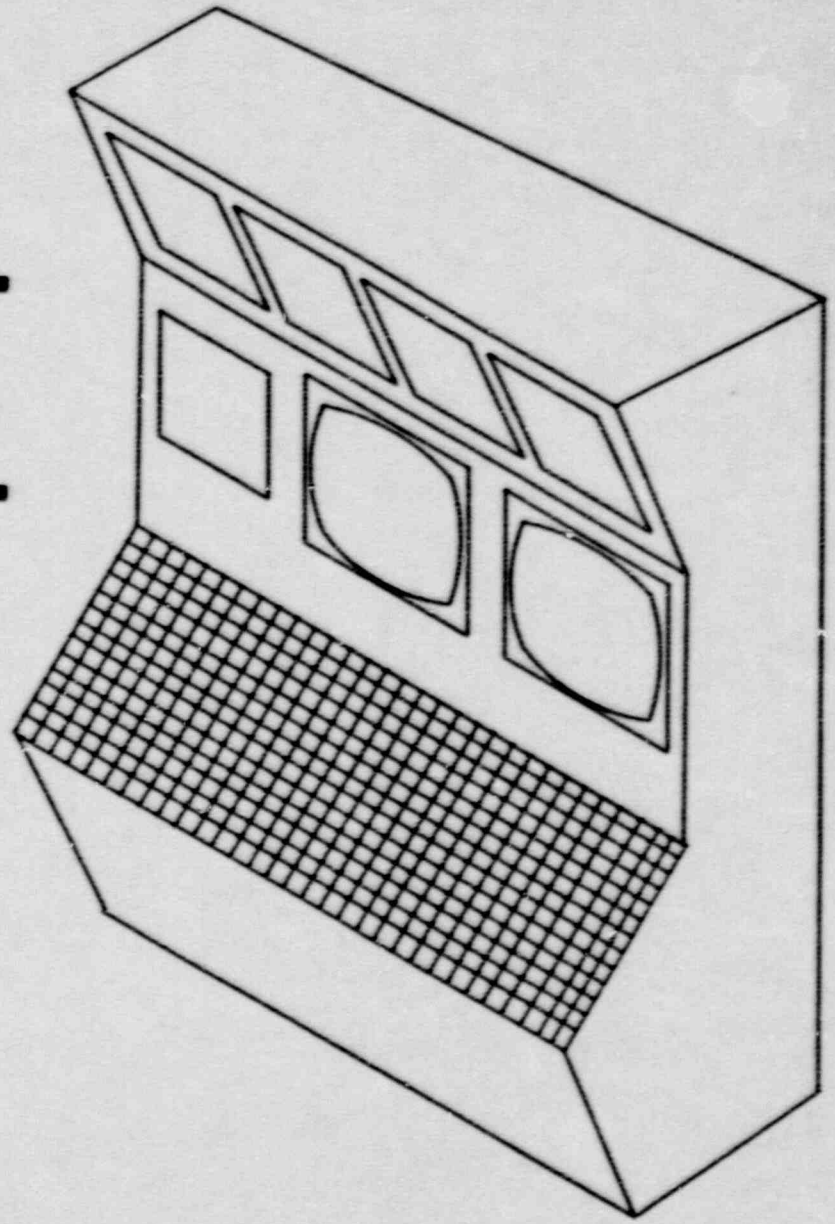


THE DISPLAY SYSTEM: SUMMARY

- DISPLAYS ARE STRUCTURED TO MATCH THE FUNCTIONAL ORGANIZATION OF THE PLANT IN ORDER TO SUPPORT THE DECISION MAKING ACTIVITIES OF PLANT OPERATION. ALSO, THIS FUNCTIONAL ORGANIZATION CONTINUALLY REINFORCES THE OPERATOR'S UNDERSTANDING OF THE PLANT DESIGN.
- THE PHYSICAL DEPICTION OF THE PLANT SUPPORTS THE PLANNING OF DETAILED CONTROL ACTIONS AND FEEDBACK ON THOSE ACTIONS.
- GRAPHIC DATA UTILIZES THE OPERATOR'S PERCEPTUAL ABILITIES TO PORTRAY COMPLEX "DATA BEHAVIOR" WHILE DATA ON GRAPHICS SUPPORTS PLANNING ACTIVITIES BY ORGANIZING PLANT DATA AND CONVEYING ITS SIGNIFICANCE.
- CALCULATED DATA IS INCLUDED IN DISPLAYS AND UPDATED REGULARLY.

CONTROL BOARD SEGMENT ORGANIZATION

ALARMS	DISTURBANCE ALERT & IDENTIFICATION
DATA DISPLAYS	PROCESS MONITORING OPERATIONAL PLANNING
CONTROLS	CONTROL ACTIONS & FEEDBACK



CONTROL ROOM LAYOUT: BENEFITS OF THE CIRCULAR DESIGN

- EASY VISUAL COMUNICATION WITH OTHER WORKSTATIONS FROM
  - SUPERVISORY CONSOLE
  - INDIVIDUAL MCB STATIONS

  SUBSTANTIATED BY FULL-SCALE MOCK-UP

- EASY VERBAL COMMUNICATION WITH OTHER WORKSTATIONS
  - SOUND IS REFLECTED EFFECTIVELY

  SUBSTANTIATED BY FULL-SCALE MOCK-UP

- REDUCES EXTRANEOUS TRAFFIC AND VISITORS TO THE CONTROL ROOM

CONTROL ROOM LAYOUT: SUPERVISORY WORK STATION (CONSOLE)