ACRST-1831

ORIGINAL

OFFICIAL TRANSCRIPT OF PROCEEDINGS

Agency: Nuclear Regulatory Commission
Advisory Committee on Reactor Safeguards

Title: Subcommittee on Reliability Assurance

Docket No.

LOCATION: Bethesda, Maryland

DATE: Tuesday, February 5, 1991 PAGES: 1 - 146

TR04 (ACRS)
RETURN ORIGINAL TO
B.J.WHITE, ACRS-P-315

THANKS! BARBARA JO

#27288

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: February 5, 1991

The contents of this transcript of the proceedings of the United States Nuclear Regulatory Commission's Advisory Committee on Reactor Safeguards, (date) February 5, 1991, 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

Subcommittee on Reliability Assurance

* * *

Nuclear Regulatory Commission
7920 Norfolk Avenue
Bethesda, Maryland

Tuesday, February 5, 1991

The above-entitled proceedings commenced at 8:30 a.m., pursuant to notice, Charles Wylie, Subcommittee Chairman, presiding.

PRESENT FOR THE SUBCOMMITTEE:

C. Wylie
J. Carroll
C. Michelson

ALSO PRESENT:

E. Igne, Cognizant ACRS Staff Member

P R O C E E D I N G S

[8:30 a.m.]

MR. WYLIE: The meeting will come to order. This is a meeting of the Advisory Committee on Reactor Safeguards Subcommittee on Reliability Assurance.

I am Charles Wylie, Subcommittee Chairman.

The ACRS Members in attendance are James Carroll, to my left, and we are expecting Mr. Carlyle Michelson shortly.

The purpose of this meeting is to discuss the reliability and behavior of safety-related solid state devices used in nuclear power plants, especially in proposed advanced reactor designs.

E. Igne 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 January 23, 1991.

Portions of this meeting will be closed due to discussions of company proprietary information.

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.

I want to make a few comments. I probably sound like I am preaching to the choir. The purpose of the meeting is to gather information regarding reliability of safety-related instrumentation and control systems which are being offered for the advanced nuclear power plant designs which are being proposed.

These instrumentation and control systems utilize solid state electronics and utilize solid state logic, digital computers, multiplexing, data gathering, fiber optics transmission and other techniques of an advanced nature. Our concern is the reliability of the components and systems to perform the safety functions when subjected to the environmental conditions which they may experience throughout their life.

I have read over a number of documents and I have been following the LERs for the last umpteen years. Experience has shown that solid state components act strangely under certain environmental conditions such as elevated temperatures, voltage spikes, humidity and other things. They have performed in unexpected ways. They cause plant transients, spurious alarms, equipment outages, erroneous indications, and failure of protection systems.

Some of the questions that we would like answered when considering design techniques being employed where you put these systems together and the environmental conditions from the sensor throughout the systems to the final actuating devices:

Is the necessary separation and redundancy preserved?

Are the systems immune from common mode failures?

To what extent has the reliability of the design techniques and components and systems been demonstrated in the environmental service conditions which they may experience?

If the reliability has not been demonstrated by actual experience, what methods have been used and to what extent has prototypical testing been performed?

Those are some of the questions that I will throw out at the beginning. Now I will call on our Members to see if they have anything they would like to add before we get started.

MR. MICHELSON: I have nothing.

MR. CARROLL: Nothing now.

MR. WYLIE: I know we are interested in what the Staff and EPRI and the nuclear steam suppliers have to tell us today. So let's go ahead and proceed with our agenda. I believe the Staff lead-off is Mr. Matt Chiramal.

MR. CHIRAMAL: Good morning. My name is Matt Chiramal. I am with the Instrumentation and Control Systems Branch of NRR. During this presentation with me are Jim Stewart of the same branch, and Paul Eshleman, who is one of our contractors from Engineering and Science Associates.

In our review of I&C systems, the qualitative aspects of assessing the reliability of equipment and components are really the application of both collective and individual judgments and engineering knowledge in the areas of design, manufacturer, installation, testing and operation of components, equipments and systems.

The collective knowledge is in the form of applicable criteria, design criteria, regulatory guides, nation and international standards, engineering specifications used by manufacturers and designers, design practices, and ultimately, of course, it's the reviewers own experience and knowledge and judgments that makes up the final overview of the systems that we look at.

MR. CARROLL: Just on that point of the staff's experience, tell us about your background.

MR. CHIRAMAL: I used to be an operator in a foreign BWR for seven to eight years. Then I came to the United States and worked with Bechtel as a designer for both electrical instrumentation and control systems at PWRs.

Then I joined the NRC back in 1977, and I've been with the Division of Operating Reactors, initially in the Plant Systems Branch, which worked with both instrumentation and control systems and electrical systems, and then I joined the AEOD as the lead electrical engineer. Recently, I came in and joined as the section chief in the ICS Branch.

MR. CARROLL: And you actually were what in the United States would be considered a licensed operator?

MR. CHIRAMAL: Yes.

MR. CARROLL: What, in Taraport?

MR. CHIRAMAL: Right.

MR. MICHELSON: Matt, as long as you've been interrupted for a moment, let me ask you a question. This term "reliability assurance" always somewhat bothers me because I thought it kind of dealt with the likelihood of a component performing a desired function. But part of what we're concerned with in this sense is a component producing an undesired function. Is that a part of reliability assurance or some other science?

MR. CHIRAMAL: Well, I use [illegible] title "reliability assurance" mainly because that's the title --

MR. MICHELSON: No, I just wondered, is that also within what you consider to be reliability assurance --

MR. CHIRAMAL: Yes. Definitely.

MR. MICHELSON: -- the inability of a component to perform the function desired, but its ability to produce some unwanted function. That's a part of your spectrum?

MR. CHIRAMAL: Yes.

MR. MICHELSON: Okay. Thank you. From a system basis?

MR. CHIRAMAL: From the system point of view, right.

Both Jim and Paul will run us through how we do the review for existing design reviews, operative plan modification views, and, of course, the advanced lightwater reactor reviews.

As you know, the whole process of our review is an evolutionary process. We learn from our experience. Hopefully, when Jim and Paul go through one of these presentations, you can see that evolutionary process being done.

MR. CARROLL: Why don't you start out, Jim, by telling us a little bit about yourself.

MR. STEWART: Okay. My name is Jim Stewart. I'm with the Instrumentation and Control Systems Branch. My background. My bachelor's degree is in electrical engineering. I've worked for six years with Bechtel as a designer in the instrumentation and control area.

I've been with the NRC for six years, both with I&E and then in the reorganization with NRR.

MR. CARROLL: When you were with I&E, were you out in the plants?

MR. STEWART: I was in the headquarters. I did participate in some plant audits, IDIs, plant inspections. I'm currently on the working group for the IEEE 7432 rewrite, which involves a lot of the software and hardware questions now for the equipment that you have concerns for this meeting.

What we wan to show with this slide is that what our review is, like Matt mentioned, is a continuing process. The early plant licensing reviews -- most of the plants that are licensed now were reviewed against a standard review plan which had all the what I would call traditional criteria. Probably one of the more important ones is the IEEE 279, which gets into your question on redundancy and separation.

Some of our more recent reviews, say in the last ten years, through CPC and retrofits and modifications, we have taken advantage of additional review guidance. Now, there's a fair amount of review guidance out there that's available, IEEE standards, IEC standards, various standards, foreign standards, that we use in our reviews as guidance. We'll talk a little bit more about those.

We feel that they are very important and useful. We'd like to get the standard review plan revised to include more of these. That process has started now, but there's a length of time involved in getting that done, and in the mean time, we're going to continue to use them.

I split up into two areas: software and hardware. We're going to be down here tomorrow to talk specifically about software with Mr. Lewis --

MR. CARROLL: So are we.

MR. STEWART: Okay. I didn't know how many of you were going to be on the same committee. I'd like to try and defer an extensive software investigation until tomorrow. So we're going to focus pretty much on the hardware side of it and your environmental concerns.

Just as an aside, we do have requests in to Research. They're going to have a little bit of discussion. But for places where we don't have hard and fast criteria established or where we feel we need additional regulatory guidance, we do ask Research to help us on that.

Just so that we're referring to the same thing, we believe these are the plants that you're interested in for this meeting. We're in various stages of review on these, probably not as far along as some of the plants would have liked.

The first few here are in active review and fairly extensive review at this time. Down through the passive plants, or I believe you used the revolutionary term where we only have a conceptual understanding of what the vendors are proposing.

I have retrofits and upgrades on here because a lot of the questions that you're interested in will apply to the retrofits and upgrades that are being put into currently operating plants.

MR. CARROLL: How extensive is that effort on the older plants?

MR. STEWART: Okay. We have some examples we'll talk about. It's everything from very small non safety pieces of equipment to complete reactor protection system upgrade. So it varies from plant to plant. As the plants get older, I expect we'll see a lot more of it.

MR. CARROLL: How many of those that are of big scale have you got on your plate right now?

MR. STEWART: We've pretty much finished the ones that have come in. I'd say within the last three years, we've done a dozen major retrofit reviews involving computer applications.

I put this slide up because I think this is going to be a topic for conversation today. One point we wanted to make was that the equipment that's being put in is not state of the art in terms of unproven equipment that doesn't have previous experience. Most of the equipment that the vendors are talking about putting in is very similar to what's already existing in the industrial world.

EPRI uses the term in their requirements document "proven technology," and that's why I used it here. They have it in there as a requirement to use it. Now, they have various reasons for doing it. You know, EPRI can talk about that. But in our review, what we'll be looking at is the operational history of this type of equipment, why the different vendors believe that it's suitable for use in a power plant. We'll look at the testing and analysis and similarity to previous designs.

There is no set criteria in Reg Guides or 10 CFR on how proven proven technology has to be. Right now, it's an engineering judgment call. We have a lot of questions to the vendors in the area of how they're going to demonstrate these various aspects.

MR. WYLIE: Well, are you looking at it from an overall system basis?

MR. STEWART: We're looking at it a couple of different ways, starting from the components up through the total system.

MR. WYLIE: But I'm talking about are you looking at it from the actual location of the sensors in the plant where they are, how far they are apart, what the environmental effects could be on those?

MR. STEWART: Yes. We're looking at like as far as the separation and redundancy questions, how separate is separate. The vendors we've talked to for where we have some details are committing to meet all of the current regulations. For example, Reg Guide 175 as far as the physical separation, the 279 requirements for redundancy.

MR. MICHELSON: I can see how you can do that for present-day plants -- in other words, know the physical loca'ions -- but do you have that level of knowledge, say on the ABWR?

MR. STEWART: I don't have a slide on it, but there's a general question on what level of detail is necessary --

MR. MICHELSON. No, that isn't my question. My question is do you know so far where these various components, such as the local transmitters for multiplexing, are going to be located?

MR. STEWART: No.

MR. MICHELSON: I didn't think so, but I thought maybe you were way ahead of what I was aware of.

MR. STEWART: No. What we have is --

MR. MICHELSON: So only on present-day plants do you really know where the components are?

MR. STEWART: Correct.

MR. MICHELSON: And their surroundings?

MR. STEWART: Correct.

MR. MICHELSON: Yes. Okay. Thank you.

MR. STEWART: What we'll have to look at is the vendors. For example, ABWR has committed to meet those requirements, and we'll have to work out a method of verifying that they have, in fact, done that.

MR. WYLIE: Well, that should be a logical question and something they should answer, isn't it? I would think.

MR. STEWART: Part of the problem is this level of detail needed for design certification. How much do you have to have now? How much do you need later?

MR. WYLIE: Maybe the Commission will resolve that for us shortly and we'll be able to talk about it.

MR. STEWART: Right. We are awaiting Commission direction.

MR. MICHELSON: But until you know where the components are located, and therefore know the surroundings, I don't know how you can determine whether the environmental qualification of the component is adequate or not except by some general overlying set of rules that says -- and if certification means rules and not details, that's kind of a new wrinkle on certification.

MR. CARROLL: Well, except that it could mean rules or certification followed by verification that the rules have been complied with.

MR. MICHELSON: That's what I call two-step licensing.

MR. STEWART: Probably my best answer for that is we are awaiting Commission direction. That's probably my safest answer.

MR. MICHELSON: You gave the right answer.

MR. STEWART: It's a good question. Right now, we have the commitments to meet the regulations, but I do not have the tools to verify that they have, in fact, met them.

MR. CARROLL: Now, you say they've committed to meet the regulations, but earlier, you or the previous speaker talked about the need to upgrade and update the standard review plan. There must be a gap in there that you need to be worried about.

MR. STEWART: Yes. I have a slide coming up of what I would call open review issues that we will have to resolve as far as what the criterion and the standards would have to be.

MR. CARROLL: Ultimately, that will be a part of an upgraded standard review plan.

MR. STEWART: Yes. Actually, this is a good example of it right here. The passive plants as a group have more or less said and documented in the early conceptual designs that we've seen that in the I&C area, that they will be very similar to the evolutionary plants. Therefore, currently, we have our existing criteria in regulations and our additional review guidance in areas that we've been reviewing.

We believe that there will have to be new criteria established. There are some areas in here, for example, a single-train RHR system -- we do not have criteria as far as what the acceptable level of redundancy and diversity for the I&C system should be given that you only have a single-fluid train.

The answer may be that the levels of redundancy that are in 279 should still apply. We don't have that answer. That's an area where we will have to come up with what the appropriate criteria should be.

One area that we know is going to be a problem, and we put it up here because it was of interest to the environmental temperature effects, is that the current plans are that there will be no safety grade AC back-up power diesels.

Our concern in the I&C area is primarily in that we're not sure how they are going to demonstrate that they can keep the electronics cool.

All the vendors are aware of the question. We've heard a couple different answers. One answer that we've heard is that they will use a passive HVAC system, and there's been some discussion of how they will do that.

One of the other answers is that they'll go to hardened electronics that can withstand the temperature, which would be fairly, at least in my mind, probably fairly expensive military hardware.

It's an open issue. They will have to resolve it. Which method they end up using, we wait to see.

MR. CARROLL: Just speaking generally, when you talk about hardened components or temperature-rated components, how far can you go if money is not an object?

MR. STEWART: If money's no object, you'd go into satellite hardware.

MR. CARROLL: What kind of temperatures?

MR. STEWART: I'd have to get back to you on that. I can't quote a number off hand. In extremes of what we'd see in containment

MR. CARROLL: Okay.

MR. STEWART: Some of the review issues that we'll be looking at in this area. We'll talk about software in detail tomorrow, but it is definitely a concern. I wanted to give an example of where our existing criteria is applicable. We recently looked at a retrofit, a gammametrics thermomargin monitor for Palisades, and the device was tested. Gammametrics took their nice little box and tested it for the temperature profile that they wanted and demonstrated it was suitable. We looked at the tests, and everything looked fine.

We went to Palisades, and what they had done is they tested the module standing by itself. When they installed it, they stacked a rack of them up together and put sheet metal in between them and cut off all the natural circulation, and --

MR. CARROLL: That's probably the first time that's ever happened, isn't it?

MR. STEWART: Probably the first time. So we asked them, and they had one of their people run through the calculations, and they, in fact, had a problem. They had to install forced ventilation for it.

It's an area where the installation was just simply never checked against what was tested. Nothing tremendously new or innovative about the computer technology had anything to do with it, but in this case it happened to be a computer.

One of the areas that we're --

MR. CARROLL: What's a thermal margins monitor?

MR. STEWART: In this case, it was a replacement for the analogue measurements that they had. Palisades was having problem with steam generator tube plugging and they installed a digital system to replace the analogue system so that they could run closer to the margins on the flows. Quick answer. We can provide details, if you are interested.

Okay. One area that we're looking at is failure modes. With the multiplexers and the digital systems, it's possible to have different failure modes than the traditional "off" or "on" modes. It's not necessary to always fail to a completely off state. You may fail to a mid-loop state. You know, there is much more possibilities and capabilities with the digital equipment, and so we're looking at that in a little bit more detail probably then we would have to with a traditional analogue system.

MR. MICHELSON: It may also be desirable to know whether or not the failure mode of the component is consistent or not. In other words, on elevated temperature, does it always fail the same way? The answer perhaps is no. That creates further confusion in how to analyze unless you analyze all possibilities.

MR. STEWART: We agree with the comment. I think one of the gentlemen I talked with on the IEEE working group uses the word "deterministic," that you design the equipment to the best of your ability so that the failure mode with whatever you use -- watchdog timers, power supply failures, a variety of methods -- that it will fail to a known state, a predetermined known state.

MR. MICHELSON: You mean they can design to fail in a predetermined state, say for elevated temperature?

MR. STEWART: To the extent that they can.

MR. MICHELSON: Well, that doesn't help me much.

MR. STEWART: I know.

MR. MICHELSON: Maybe they can't do it much.

MR. STEWART: A large portion of that goes back to the proven technology of using equipment that's been used in industrial applications, where the environments usually are much worse than what we see in the power plants.

MR. MICHELSON: Well, that depends on whether you're talking about normal operating environments or post-accident operating environments.

MR. STEWART: Most of the digital equipment that we're going to see, the computers are going to be in --

MR. MICHELSON: Well, let's go to the multiplexers, which I understand from lightwater reactors will be all over the building and clearly not all in very well controlled environments.

MR. STEWART: And they will have to demonstrate by testing that that equipment is suitable for that environment.

MR. MICHELSON: Right. And a number of things like converters and so forth are not always necessarily situated where it's a mild -- I can go on and on. The mild environment is not a good answer.

MR. STEWART: Well, we do still have the 10 CFR 50.49 rule that they do have to demonstrate by test that the equipment is qualified for that environment.

MR. MICHELSON: Yes. And part of the demonstration either is show that it's qualified -- I keep getting an answer from the staff that says, "No, we don't have to show that piece of equipment is qualified for environment; we have to show that we can still achieve the safety function of that equipment, be it from another redundant counterpart," that the individual piece is not protected because, in many cases, it's obvious it's not easy to protect it against water spray or whatever. They say, "Well, the function is protected, not the piece of equipment."

So the staff ought to get together on whether they're protecting functions or protecting individual pieces of equipment. If you indeed protect the individual piece of equipment against all the known environments that it might see, then that answers it, that takes care of it. But if you come back and tell me about the function and I have to ask about the unwanted actions from the piece of equipment that is unprotected -- does the staff have a position on whether you're protecting functions or equipment?

MR. CHIRAMAL: Equipment.

MR. MICHELSON: You are protecting the equipment? I will make a little note, and next time, I will tell them to see you when I ask about it and they say, "No, it's the function." We just got done going through fire protection a short time ago, and it's the function they're protecting with fire protection, not the piece of equipment.

MR. CHIRAMAL: That's part of the qualification testing. That is, the equipment itself has to got to meet the environmental conditions --

MR. MICHELSON: So you're protecting this against inadvertent actuation of water from sprays and sprinklers and all that sort of thing, the individual piece of equipment?

MR. CHIRAMAL: Yes.

MR. MICHELSON: If that's true, that's great. I haven't seen that spray qualification yet on a lot of these electrical ports tha\ [illegible] have electrical sprays in the vicinity, but we'll see.

MR.WYLIE: Going back to the earlier question, and it relates to what we're talking about here, regarding the review for the ABWR, for example, and a question regarding the location of transmitters and what have you in all of these plants, whether it be multiplexing or whatever it is, inside containment, how can you do a review if you don't know the location of that equipment and you don't have access to how they're going to handle their grounding, for example?

MR. STEWART: You've asked a very difficult question. This has been one of my major concerns for the last couple of years since we started these reviews. We cannot presently review how Combustion or GE or Westinghouse are grounding their equipment.

MR. WYLIE: Why not?

MR. STEWART: The design certification submittals that we have do not specify a particular equipment.

MR.WYLIE: Then it's not adequate.

MR. STEWART: Therefore, you cannot review the specific grounding. Again, I would have to go back to my answer being we are awaiting Commission direction on what design --

MR.WYLIE: So this falls into that third category of information for audit?

MR. STEWART: I'm not sure how it's going to be resolved.

MR. WYLIE: Yes, I know, but I mean that would be the intent of the staff's recommendation, I would assume.

MR. STEWART: My personal recommendation would be that somewhere before that plant gets turned on, we look at it.

MR. WYLIE: It ought to be up front.

MR. STEWART: Whether it's before design certification, part of the ITAC program, or part of some yet to be named audit procedure, it'll be looked at. Whether it falls in the licensing process, I'll have to wait and see what the Commission wants us to do.

MR. MICHELSON: Are there any harsh environments outside of containment as a review issue, because you labelled this one mild and I wondered what happened to harsh.

MR. STEWART: Harsh? Well, that's what I wanted to -- okay. We'll go ahead and get into that. Typically, when most of us say "harsh environment," or at least in my branch, we're talking in containment traditional temperature, humidity, radiation problems, okay? And the 10 CFR 50.49 rule would apply and that equipment would have to be shown to either function or do its safety function, depending on the definition.

One of the areas that we're looking at is what I call mild environment in that the equipment -- most of the equipment will not be subjected to the high temperatures, humidity and radiation associated with an accident environment. But we're looking at the electrical environment, in particular, electromagnetic interference, static, surge withstanding.

MR. MICHELSON: Well, I guess my question can be stated differently and maybe more explicitly. That is, do you look at the post-accident environment outside of containment for all postulated accidents?

MR. STEWART: Yes.

MR. MICHELSON: Okay. Because some of the postulated accidents are pipe breaks out of containment and things of this sort.

MR. STEWART: Right. Helva breaks, anything like that.

MR. MICHELSON: And for those postulated events, you do look at he environment that all of this equipment is exposed to?

MR. STEWART: The design basis, environment, whatever --

MR. MICHELSON: Okay. Thank you.

MR. STEWART: Whatever it's listed as.

MR. MICHELSON: In some cases, it's not exactly mild after the event.

MR. STEWART: I agree. I agree. And I believe most of the vendors are going to efforts to keep the equipment away from those kinds of environments.

The last issue we had that we wanted to talk about was electromagnetic interference and the associated issues, static, surge withstanding capabilities, RFI, and all those kinds of issues. We brought Paul Eshleman, who is a contractor, with us. He's been on both the retrofit audits with me, he's been helping us with he ALWR reviews, and -- Paul?

MR. MICHELSON: Let me -- oh, he's going to speak next?

MR. STEWART: He's going to speak next specifically on EMI issues.

MR. MICHELSON: Okay.

MR. STEWART: If you have any other issues now, I can try to answer it.

MR. MICHELSON: I had only one other question. You did list fire protection and fire suppression there under mild environment. What did you have in mind?

MR. STEWART: What I had in mind there specifically was your concern about sprays, cardox systems.

MR. STEWART: Are you looking at the heat and smoke and so forth as an environmental influence?

MR. STEWART: The heat as a result of a fire we don't really try and analyze. We pretty much assume that if there's a fire in that area, that that equipment is gone.

MR. MICHELSON: Yes, but not all equipment is in that area, but it may be in the same room, but not in that so-called area. There's a 20-foot separation between one train and the other train which is allowable under Appendix R, and the 20 feet of separation doesn't prevent temperatures in that area from elevating perhaps well beyond what the electronics is capable of.

MR. STEWART: I'm not really an Appendix R person.

My understanding is that if you have a fire in that zone, that any equipment in that zone is --

MR. MICHELSON: No, but then you turned around and said, Well, we'll allow some exceptions. "If you provide 20 feet with no combustibles and a spray system, we'll let 20 feet be the wall," and now you have to prove that that doesn't get too warm or doesn't get to smoky or water doesn't get over on the other side because if it does, then the bets are off again. You do have to look at it, whether you think it should be or not.

MR. STEWART: I'd have to refer back to an Appendix R person for what their exceptions are.

MR. MICHELSON: I hope they are also an electronics person, then.

MR. STEWART: We're available.

MR. MICHELSON: They do deal with combustion, and that's what they tell me: "Oh, it doesn't get above 746 degrees," or whatever. Well, that doesn't help me much on electronics. It doesn't burn, no, but it malfunctions.

MR. CARROLL: Yes. You said you assume it's gone if there's a fire in the zone. What does "gone" mean in terms of the variety of failure modes?

MR. STEWART: Total failure of that equipment and any train equipment that's controlling, either failure to operate or inadvertent actuation. We'll consider both possibilities, or some midpoint failure.

MR. MICHELSON: You will analyze all possible failures of that equipment that's exposed to the adverse environment. Is that what you're saying?

MR. STEWART: We will look at what we believe the failure modes can be for the design basis environment. I don't know what the exceptions to the Appendix R situations could be, so I can't really speak to that. It's definitely going to be on our list now.

MR. MICHELSON: Well, part of a coherence problem, perhaps.

MR. STEWART: Okay. Paul?

MR. CARROLL: I'd like to continue with my survey, Paul, of trying to find out something about the background of the people that are doing these kind of reviews.

MR. ESHLEMAN: Fine. Thank you. My name is Paul Eshleman. I'm working as a consultant to the NRC. I'm an electrical engineer. I worked for about 15 years doing analogue and digital designs for specialized scientific projects for many small projects and also EG&G.

I'm head of Design Group. I worked for ten years for NUS analyzing nuclear power plant safety systems, and I've worked for the past six years serving as a consultant to the NRC and other clients.

The discussion presented here is based on the results of several reviews recently conducted for plant modifications involving the addition of digital based hardware systems as replacements for existing analogue safety systems in currently operating plants. These plants include Palisades, Haddam Neck, Beaver Valley, and also a GE NUMAC instrumentation review.

MR. MICHELSON: Just because I am at least a novice in all of this and I'd like to make sure that when you talk about a digital replacement, you mean going all the way from the sensor at the pipe, for instance, all the way through when you do that replacement?

MR. ESHLEMAN: No.

MR. MICHELSON: Are you using analogue partway and digital at the end or something?

MR. ESHLEMAN: In the situations we looked at here, the sensors were the same sensors using the analogue system, and the digital systems replaced the analogue hardware.

MR. MICHELSON: And where did digital pick up, so to speak? At what point?

MR. ESHLEMAN: Outside of containment.

MR. MICHELSON: Yes, outside of containment, but in the auxiliary buildings and in the reactor buildings, places like that, or did you pick up in the instrument room?

MR. ESHLEMAN: We've seen just about every combination.

MR. MICHELSON: Okay. So it's a possibility that you're using the digital equipment all the way out almost to the sensor. Is that correct?

MR. ESHLEMAN: Of the examples he has up there, no.

MR. MICHELSON: Well, where in these examples did it pick up, then?

MR. ESHLEMAN: At Palisades, it picked up in the control room. At Haddam Neck, it picked up in the auxiliary equipment racks. At --

MR. MICHELSON: Now, wait a minute. Auxiliary equipment instrument room or at the rack?

MR. ESHLEMAN: The instrument rooms.

MR. MICHELSON: Okay. In the instrument room. Okay.

MR. ESHLEMAN: At Beaver Valley, it picked up just outside the cable spreading room. The General Electric NUMAC is not an installed piece of equipment. That was a topical review. With the NUMAC equipment, that would be pretty much a complete digital system from just outside the detectors to the control room.

MR. MICHELSON: Okay. But for most cases so far, they have been confined to the places where you can more readily control the environment to begin with?

MR. ESHLEMAN: Yes, that's true.

MR. MICHELSON: Thank you.

MR. ESHLEMAN: The application of these digital circuits represents a technology upgrade, and they introduce a set of problems not reviewed in the standard review plan. We anticipate that nearly all reactor protection systems could be upgraded or replaced with digital systems in the future.

The concerned evidence in these reviews is that the addition of new technology equipment into an existing electrical equipment does not -- which was designed for analogue equipment technology could cause common mode vulnerabilities which could affect the availability of multiple safety trains.

One of the environmental concerns addressed here is that of conducted noise on the power line circuits. No evidence was presented during the audits of licensee reviews to control or identify the noise present on a safety power supply source.

MR. MICHELSON: Now, in looking at the vulnerability to electromagnetic radiation, particularly from power systems, did you look at the faulting of power systems and what kind -- you know, electrical arcing and whatever and what it might do?

This is a possible failure mode. When you release moisture and things get wet and they start arcing, they start creating quite a bit of local electromagnetic interference. Did you look at that kind of interference or just the kind you see from normal operation?

MR. ESHLEMAN: We asked the licensee to address whatever kinds of faults they could identify --

MR. MICHELSON: Well, let me ask you, did any of them address other than normal operating conditions? Did they address, for instance, electrical arcing?

MR. STEWART: Yes.

MR. MICHELSON: And what did they find? Are you going to tell us?

MR. STEWART: Okay. One example is like a showering arc test, which is pretty close to simulating an arc welder in the area. General Electric -- and we've done some testing ourselves of some equipment for that.

Probably now is a good -- we can talk about what we did with Haddam Neck is probably a good example. Haddam Neck replaced the RPS system with Foxboro modules, which is a -- and they used a Spec 200 micro, which is a microprocessor-based system.

When we saw the original licensee safety evaluation, the only area that they addressed in EMI was a walkie-talkie test, an RFI test, and we felt that that was not adequate.

We went up to Foxboro, and fortunately Foxboro had done extensive testing. They used the C-62/63 series, they used MIL Spec Standards 461, 462, they used IEC standards --

MR. MICHELSON: Maybe you can tell us roughly what kind of test they did. I don't know all the numbers.

MR. STEWART: Okay. What they did is they had an EMI room, a controlled environment, and they placed their equipment in the room, ran it through all the software cycles, and subjected it to a series of tests, and they established an envelope similar to what we would think in a typical EQ.

MR. MICHELSON: Now, the tests they submitted to, these were where they produced various types of -- various levels of electromagnetic variation in the room?

MR. STEWART: Various levels and types of noise.

MR. MICHELSON: And they did the full spectrum of frequencies?

MR. STEWART: Both conducted and radiated --

MR. MICHELSON: And then they saw how their equipment responded to these?

MR. STEWART: Correct.

MR. MICHELSON: And the equipment was in operating order at the time?

MR. STEWART: The equipment was in operating order at the time. So they had a fairly extensive envelope. Our next obvious question was how the licensee knew that their installed condition was within that envelope. They had not done anything, and we had them -- we requested them and they agreed to do it, to go out and measure for a period of time, not a one-time measurement, but for a period of time to try and catch a reasonable sample of transients.

MR. MICHELSON: Well, now these are normal operating transients you're now referring to, though.

MR. STEWART: They are normal operating transients.

MR. MICHELSON: I'm not talking about normal operating transients --

MR. STEWART: But --

MR. MICHELSON: I hope it withstands those.

MR. STEWART: It's similar to the EQ. We can test in the controlled environment. It's difficult to test accident conditions in the operating plant.

MR. MICHELSON: Well, how do you know, for instance -- we have many non-seismically qualified pieces of electrical equipment in a plant, and we have non-seismic insulators and so forth. In the case of a seismic event, you're going to get some amount of electrical arcing from failed pieces of equipment before the arcs clear, whatever.

How do you know how your solid state devices respond to that since they're very susceptible to microvolt levels of signals and you have to be very careful with shielding every bit of it. But how do you know that you've adequately shielded against that kind of electromagnetic interference, or do you?

MR. STEWART: I don't think we have an absolute answer that that can be shown.

MR. MICHELSON: But do you need to worry about that? The same thing is true with fire. Fires also have a habit of creating electrical arcs and so forth.

MR. STEWART: I believe the answer to that is that we rely on the testing to show a high level of qualification.

MR. MICHELSON: But you didn't tell me you tested for any levels of interference of that magnitude. You tested for system transients, which generally are nowhere near that troublesome.

MR. STEWART: And the controlled testing that the vendors do.

MR. MICHELSON: Whatever they might have done. I was just trying to search you out to find out what levels --

MR. STEWART: I don't have an answer.

MR. MICHELSON: -- how good a test did they even do.

MR. STEWART: Well, I can describe the test they did and the test the licensee -- the test the vendor did in the controlled environment and the testing that the licensee did.

MR. MI[illegible]LSON: But isn't environmental -- I thought the whole approach to environmental qualification was you tried to identify some kind of a boundary on your equipment, some kind of a condition that you postulate would be the worst exposure that equipment would get.

MR. STEWART: Right.

MR. MICHELSON: Now, what is the worst exposure this equipment will get? Well, apparently, you haven't really defined it yet because -- until you define that, you can't define the test requirements.

MR. STEWART: I do not believe we have a criteria that has definitively outlined what the worst case electrical environment would be.

MR. MICHELSON: And until you do, it's hard for you to tell me that the equipment is qualified.

MR. STEWART: Until we do, we are using the best review guidance that we have available, which are the military standards and the IEEE standards on testing the equipment.

MR. MICHELSON: Maybe those are quite adequate if you knew what your maximum exposure might be.

MR. STEWART: Well, we are trying by measuring at the plants or the licensee measuring at the plants to get a large enough envelope to have a pretty good feeling that the bulk of the possible situations are covered.

MR. MICHELSON: Of course, what we're talking about isn't experienced at the plants, absolutely. This is an accident, an earthquake, or whatever, a fire -- it hasn't had the experience.

MR. STEWART: We have lightning strikes --

MR. MICHELSON: Oh, yes, and it does interesting things when it's hit.

MR. STEWART: We have transformer fires.

MR. MICHELSON: Yes.

MR. STEWART: We have fairly extensive experience with this equipment in industrial applications where it's seen some pretty bad electrical environments. I don't believe we have a set criteria where we can say this is the worst EMI voltage level that a plant could ever see.

MR. MICHELSON: Well, a design basis one.

MR. STEWART: Right.

MR. MICHELSON: I'm not going to ask you to give me the worst it would ever see because now you're talking about severe accidents. I'm just talking about a design basis EMI. Is there a desi. basis EMI for equipment?

MR. STEWART: No.

MR. MICHELSON: Without that, of course, then you can't tell me you've qualified it for your design basis because you don't know what you're qualifying for yet.

MR. STEWART: We do not have a set criteria for that.

MR. MICHELSON: Okay.

MR. STEWART: It's engineering judgment case by case at this point, yes.

MR. MICHELSON: Okay. Thank you.

MR. ESHLEMAN: The previous analogue equipment designs were not sensitive to a lot of the noise and spikes and what not that are in a plant because the typical calibration procedures tend to mask these, and that they were folded into the data. So we found that plants were really not aware of some of the conditions that might exist on their signal lines and power lines.

MR. MICHELSON: It took a much longer time pulse to do anything to electromagnetic relaying than it does to a solid state transducer.

MR. ESHLEMAN: That's right.

MR. MICHELSON: You're talking microseconds on transducers, and you're talking mini milliseconds on electromagnetic things like relays. Some very fast relays will operate almost but not quite microsecond. For the kind we're talking about that's in the plant today, these are slow stuff. They filter out everything, so that doesn't show up until you replace it with digital.

MR. ESHLEMAN: They have a certain robustness that allow them to survive.

The upgrades we observed to date represent systems which are much more complex than the systems which they are replacing though they perform identical functions, employ the same logic sequences, etcetera.

Now, the complexity results from increased capabilities, such as automatic testing, automatic calibration, and fault location of failed equipment.

MR. MICHELSON: Have you done, then, the analysis, the cost benefit so to speak, keeping in mind what are the real benefits of replacing all this analogue equipment with the digital? There are some testing advantages and so forth, but does it outweigh the safety disadvantages, which you could start naming a lot of safety disadvantages to digital equipment.

MR. STEWART: The staff has not done a cost benefit analysis on replacing or, with the new plants, putting on complete digital systems instead of analogue. I don't want to imply by what we're saying here that we believe that the digital systems are less safe than the analogue systems.

We have some concerns in the area, and obviously we're trying to highlight these concerns here, but the digital systems with the self-diagnostic capabilities that they have, with the ease of maintenance, improvements in that area, with the accuracy -- we're eliminating a lot of the problems we've had with electronic drift. There are improvements to be made. I expect maybe the different vendors will talk about some of the trade-offs in that.

We believe that if --

MR. MICHELSON: But ultimately, don't you have to show that the replacement is at least equally safe to what was already there?

MR. STEWART: Yes.

MR. MICHELSON: And might even be more safe, but certainly not less safe. You do enough of an analysis to always convince yourself that what they're doing is not less safe irrespective of economics.

MR. STEWART: My criteria is specifically that.

MR. MICHELSON: Must be equally safe?

MR. STEWART: Equally or better, yes.

MR. MICHELSON: Okay.

MR. ESHLEMAN: Due to these additional capabilities, it's projected that the systems would have a higher availability because of the automatic calibrations and the vault locations.

Given these conditions, the audits attempted to find what engineering design control was being applied to prevent electrical transients resulting from lightning phenomena and switching of the circuits.

We know from history that instrument failures, particularly digital computers, are not very tolerant of transients on power and signal cables.

In order to protect the various safety grade equipment from these undefined but potentially disabling ploys, the reviews look for design concepts which would implement pulse or noise diverting devices to bypass the unwanted spikes or noise away from the interconnected equipment.

We feel there currently exists applicable criteria for these design tasks, and we reference IEEE 518, 1050 EMC 6312. By that, we don't mean that these are prescriptive; rather, they offer an engineering approach of how to identify pulses, noise, and what techniques are available to try to install these bypasses.

These standards were used based upon the theme mentioned earlier by Mr. Stewart that additional criteria beyond the standard review plant references are required for these high technology applications.

These documents that I've mentioned here provide the working basis for the identification and control of the EMC pulses and noise which we found on all our safety equipment that we reviewed.

Another concern we looked at in the operating plant environment was radiant electrical energy into both the cables and the equipment. The most frequent source of large electrical transients we feel is generated by the opening or closing of disconnect switches to deenergize or energize buses.

All of these events either have high frequency signal sources or have sharp wave fronts that cause high frequency oscillations. There are also some intentional RF sources in the plant, such as radios.

MR. MICHELSON: When thinking about the problem of, for instance, breaker arcing as it opens, did you look at the probability that there's going to be 15, 20 or so breakers opening at about the same time when having to deal with the problem?

In the accident case, when you're clearing boards to get ready for diesels and so forth, a lot of breakers are moving. I mean, the magnitude of the radiation is going to be, you know, much greater than it was for a single breaker opening. Is that taken into account or thought about?

MR. STEWART: He's pointing to me. We thought about it but did not come up with a criteria --

MR. MICHELSON: But is it a significant increase in levels of radiation? Clearly, you could calculate. If you got good data from one breaker at various distances, you can certainly integrate that calculation into 20 breakers at a particular point and see what the other contributions are.

MR. STEWART: I think that's an example where actual operating experience and industrial experience gives us a pretty good level of confidence that that situation is covered.

Normal breaker arcing, especially since most of the equipment that's most susceptible to it isn't right there, that's a pretty typical industrial situation where a lot of breakers are opening and closing at the same time.

MR. CARROLL: Why do you say that?

MR. STEWART: Because when you turn large systems on and off, many of the breakers will operate at one time. Loss of off-site power, a lot of the breakers will trip at one time. I think those are situations that we probably have seen.

MR. CARROLL: You probably have seen them?

MR. STEWART: That's true.

MR. CARROLL: Or have you seen them.

MR. STEWART: I would have to say we probably have seen them.

MR. CARROLL: Were you doing monitoring --

MR. STEWART: We have probably seen them because we have not been monitoring in the plants all the time, no.

MR. MICHELSON: Yes, now, of course, the problem is that most of today's plants don't have all this sensitive digital equipment in that vicinity. The new proposals may have it in that vicinity. So having never seen it doesn't mean it isn't there; it just means you haven't produced a vulnerability to it yet. The next plant may or may be converting to a particular system and a particular plant may introduce that vulnerability. You just never know. But I just wondered if you had any good data on whether it's something to think about or not.

MR. STEWART: I don't think we have good measured data. There has been some effort. General Electric did a survey where they went around and surveyed a lot of plants to try and get a basis for what they were testing, for example. We don't believe that it's a 100 percent envelope of all the possible situations.

MR. WYLIE: There's a lot of buffer, I'll call it buffer between where these things are happening and down to these sensors. It's not as bad as I think it's being painted.

MR. CARROLL: The other one that will get you in trouble is if somebody leaves a cabinet door open. I've seen this sometimes with security guys going around and using their walkie-talkies, "No problem," "No problem," "No problem." Some days, a technician is down in the area with the door open, and the guy operates his walkie-talkie, and boom.

MR. WYLIE: Don't open more than one channel at a time.

MR. CARROLL: Yes.

MR. WYLIE: Please proceed.

MR. ESHLEMAN: The technology upgrades noted in the reviews utilize higher frequencies through the solid state devices. The signal levels are typically lower, and the densities of the circuits are much higher.

This identified another problem because the typical grounding concerns now are shifting from single point grounding, which as traditionally been utilized by plants for equipment operating below 100 hertz to equipment with signals ranging into the megahertz frequencies. So now we have to look at some sort of multipoint type grounding.

We looked at this and say that the shielding and ground paths should be evaluated for this equipment and asked the licensee to do that. We don't feel it's an easy task, incidentally, particularly in an existing plant where it's very, very difficult to establish what the true grounding paths may be.

Again, we feel that standards and criteria for grounding are available from some of these references, that there is an approach that's available out there. It's a matter of applying this approach for each problem.

Another effect we looked at was the surge withstand capabilities of the new equipment. Here, the existing equipment requirements and tests were typically identified to be provided as a component test prior to installation, and the required system specification or operating system testing was not provided to the licensee.

What we were looking for here is for the licensee to apply a standard like C6245 or something to identify what kind of environment the equipment could operate in so we at least had some sort of a baseline.

MR. MICHELSON: Is all this wiring inside of conduit or digital circuits? It's shielded cable, but is it inside of a conduit as well or is it just shielded cable in a tray, for instance, or may it be?

MR. STEWART: Are you talking about examples that we've seen in the retrofits?

MR. MICHELSON: I'm thinking now the replacement shell, and then I was going to ask, well, how about improved lightwater reactors? Are they required to be in conduit then?

MR. STEWART: It depends on the specific piece that you're talking about. A fair amount of it will be fiber optics.

MR. MICHELSON: Well, yes, but not all the way necessarily.

MR. STEWART: Not all the way necessarily, sure.

MR. MICHELSON: And where it is hard wiring, is it shielded? Is it allowed to be in cable trays with at least instrument level stuff in it or what are the restrictions?

MR. STEWART: Wiring is allowed to be in cable trays.

MR. ESHLEMAN: It varies from plant to plant.

MR. MICHELSON: Oh, yes, I realize that. But now improved lightwater reactors, is there a requirement that it be in conduit or is it going to still be in cable trays?

MR. STEWART: There is no requirement that it has to be in conduit.

MR. MICHELSON: Okay.

MR.WYLIE: But it's shielded?

MR. MICHELSON: I would hope.

MR. WYLIE: Shielded cable.

MR. STEWART: I would hope.

MR. WYLIE: Of course, it could be interlock armored shielded cable, too.

MR. MICHELSON: That would help a little more if they had good grounding on it.

MR. ESHLEMAN: What we found during these audits was that each site tends to be configured differently as far as the electrical environment is concerned. Types of interference signals are different and the coupling mechanisms vary. This requires analysis to identify the possible effects.

The testing of these configurations also presents a dynamic situation that I guess we've talked about since the safety equipment is req ired during times in which the plant operating configurations may be quite different than the normal plant testing conditions.

Results of the reviews of the safety system upgrades to date indicate that system replacements are occurring on a system by system basis.

In general, the designs are constrained to the application of the criteria used to the original equipment. The application of criteria was found to exist based on previous supplier experience. In other words, the person supplying the equipment was tending to identify a much more stringent requirement than the plant had identified for the equipment.

The example that Jim talked about before was Haddam Neck. In this case, there were some Foxboro equipment which had been identified. It turned out that that equipment was a repeat order from a Swedish plant, and the Swedish plant had identified a number of IEC standards. So the equipment had been qualified to what we reviewed to be adequate criteria, but it was based upon a previous kind of application rather than the plant identifying the requirements.

Also, we noted that the original cables for both signal and power can be used in place or new cables are typically routed in the same manner as the old. The plant configurations and the partial replacement of equipment mean that each application of any given system is a unique application and has to be looked at in an engineering sense.

MR. MICHELSON: On cabling used for digital equipment, is there a requirement that it be able to withstand wetting and so forth? The reason I ask the question is that in looking at rubber and various other kinds of insulated power-jacketing, we said, Gee, we don't worry about spray on it. That was just a given.

Do we have to worry about water spray on this digital cabling? Is it that good that water -- see, on power cabling, we've said it was that good. Only in the case of immersion did we have to qualify the power cable, to my recollection.

How about this cabling? Do you have to start worrying about actuating fire protection sprays on the cable trays and getting into this cabling? We said it wouldn't hurt the power cabling, but I'm not sure about this.

MR. ESHLEMAN: Jim, do you have an answer? I can say that we looked for qualified cable.

MR. MICHELSON: Was that one of the qualifications, to be able to withstand wetting and operate properly?

MR. ESHLEMAN: My answer to that would be no, that we looked at qualified cable, but I do not explicitly remember looking for wetting.

MR. MICHELSON: That's something you might want to look into, then, because I think, as I recollect, the -- we said power cabling was a non-problem if we just turned the --

MR. STEWART: Yes. The cabling that we expect to see is not going to be substantially different than what's in the existing plants. Research has an active issue now to revisit cable qualification, and specifically water.

MR. MICHELSON: I thought it would be a somewhat different kind of cabling. But it may not be. You may be right. If it isn't significantly different, fine.

MR. STEWART: The only kind of cabling that's going to be significantly different will be the fiber optics, the quantity of fiber optics.

MR. MICHELSON: Yes, but all the electrical will be shielded, jacketed, well protected against moisture?

MR. STEWART: Coax with different kinds of jackets, sure. I don't think it's going to be substantially --

MR. MICHELSON: And qualified junctions if there are any?

MR. STEWART: yes.

MR. WYLIE: Most of that stuff's polyethylene, PVC, or something of that nature, and it's moisture resistant material.

MR. MICHELSON: Well, water spray, then, should be a non-problem, you're saying?

MR. STEWART: I don't think water spray is going to be a particular problem unless you get elevated temperatures or some kind of solvent or something in it.

MR. MICHELSON: Yes.

MR. STEWART: Research is looking at it, and if they believe new criteria is needed, we'll apply that.

MR. MICHELSON: Okay.

MR. FARMER: After we did some LOCA tests on cables out at Sandia, we did an immersion test, and this was both coax and power and controlled cables. The majority of the cables, even after going through a LOCA degradation, survived the immersion test very well. We'll be publishing that report as a NUREG within probably the next 90 days.

MR. MICHELSON: And that would be typical of the kind of cabling that's being used on the digital systems as well?

MR. FARMER: Well, to the extent Jim's remark that they're using standard cable is true, yes.

MR. MICHELSON: Well, standard cables of the variety you have tested?

MR. FARMER: Yes.

MR. MICHELSON: Qualified cables, right.

MR. CARROLL: How about connectors?

MR. FARMER: We didn't test connectors. The cables were themselves immersed, but the leads are taken out above the water.

MR. CARROLL: You can get water going down a cable and get to the connector.

MR. FARMER: Connectors are scheduled to be tested, but that will be probably this summer.

MR. ESHLEMAN: To summarize, then, the goal of these reviews was to identify the equipment qualification and then determine as best we could the environment that the equipment was to be installed in and try to look and see that there was an adequate engineering review performed to ensure that this was compatible between the two.

Moving on to some ALWR design reviews, these reviews were conducted to determine the ability of the proposed digital systems to provide the required safety system capabilities to execute the safety functions in the presence of EMI and surges.

In all these cases, the RPS and SVAS system designs have been identified as to be performed by digital circuitry. Now, these designs propose the multiple use of a limited number of circuit types which really reflects the cost advantage of digital circuitry. The problems with this approach is that the common mode failures from some outside events, such as EMI, could encompass multiple safety trains and redundant safety capabilities.

Briefly, the EPRI requirements for ALWR indicated a generic design goal, but there are no specific protection requirements for EMI EMC or surge withstand effects.

Reviews of the GE ABWR indicated an instrumentation design functioning much as their previous analogue BWR design, with widespread multiplexing of data, which is isolated by fiber optic links to train base process systems.

The CE system 80+ utilizes multiplexers again, fiber optic isolating systems. It's a little more complex and utilizes segmentation of signals and redundant processors.

MR. CARROLL: What does that mean?

MR. ESHLEMAN: They've broken the signals down into functions, so they have split the process up in pieces, and a lot of these pieces have redundant back-up processors available for them for that particular function.

MR. MICHELSON: But that's all within the same unit, though. Isn't it exposed to the same environment?

MR. ESHLEMAN: It's exposed to the same

environment.

MR. MICHELSON: So if the environment got one, it might also be getting the back-ups at the same time.

MR. ESHLEMAN: That's a common mode problem. That's right.

So, to summarize, the design approach is observed for the ALWR range and the use of a distributed process system, such as the ABWR to the multiple process systems we just talked about for 80+. All of the designs depend upon multiplexers, cable volume reduction, and fiber optics for isolation.

It should be noted that all the designs propose the use of automatic testing calibration and fault location on this basis indicated in an approved system of availability.

MR. MICHELSON: Now, the equipment that does the fault detecting is also in the same packaging as experiencing the potential fault and exposed to the same environment?

MR. ESHLEMAN: That's true.

MR. MICHELSON: The fault tester is perhaps no better off than equipment being monitored. It's got to be independent of the environment to be a fault tester of that equipment. This is a routine fault tester is all it amounts to.

MR. ESHLEMAN: Yes.

MR. MICHELSON: Okay.

MR. ESHLEMAN: No specific limitations on circuitry technology, such as impedance levels, voltage levels or complement densities were identified in any of th e submittals.

Protection from EMI EMC typically was left as a component requirement with little or no system criteria, standards or approach identified.

The GE ABWR uses the NUMAC in-house criteria for each subsystem, and they have generated a series of testing and operational criteria for that. Again, it is postulated back on a component basis rather than an overall system basis. CE indicates the criteria for their core protection calculator units will be applied to the hardware. So they have some experience there as to what has survived in existing plant environments.

MR. MICHELSON: Now, your comments are relative to electromagnetic interference only?

MR. ESHLEMAN: That's right. That's correct.

MR. MICHELSON: Thank you.

MR. ESHLEMAN: So we see each supplier with their own criteria really based upon experience, but the application of this criteria is typically applied at the component level.

MR. MICHELSON: Now, part of what you looked at was lightning. Is that correct?

MR. ESHLEMAN: That's a concern, yes sir.

MR. MICHELSON: Yes. And what did you conclude concerning lightning?

MR. ESHLEMAN: Pardon?

MR. MICHELSON: What did you conclude concerning lightning vulnerability?

MR. ESHLEMAN: There were no requirements identified in the design submittals for protection from lightning other than a generic protect against EMI transient.

MR. MICHELSON: And presumably, lightning falls within the spectrum of the EMI that you're presumably protected against? Is that the assumption?

MR. ESHLEMAN: I think that's true. It always has been.

MR. MICHELSON: Is that a good assumption?

MR. STEWART: Lightning is definitely one of our concerns, yes.

MR. MICHELSON: No, no, no. Is lightning within the envelope of the EMI that the vendor is using in qualifying his equipment?

MR. STEWART: No.

MR. MICHELSON: It's a separate issue?

MR. STEWART: If the lightning gets to the microprocessors that these vendors are going to use, that microprocessor will probably be destroyed.

MR. MICHELSON: Yes. Very likely.

Now, EMI also produces, in addition to direct electromagnetic radiation, it ionizes air and so forth in the process. If it's arcing, for instance, it could be ionizing air. Now, that ionized air is also a potential adverse environment if the electronic equipment starts drawing that ionized air into it for cooling. Is that a problem at all?

MR. ESHLEMAN: That's something I did not look at. I'll have to divert to Jim on that.

MR. MICHELSON: Certainly, ionizing the area around the equipment --

MR. STEWART: Yes, right where the sparks would be.

MR. MICHELSON: I just don't know how far it travels before it discharges itself and so forth.

MR. STEWART: I can't answer your question.

MR. MICHELSON: It's in the dust particles and whatever.

MR. STEWART: We have not considered that.

MR. MICHELSON: But, you know, this stuff doesn't like little charged particles to sit down on it.

MR. STEWART: The spacial separation requirements, back to IEEE 279, would still be maintained. So you'd have to have -- I'm trying to think of a postulated event that would do that --

MR. MICHELSON: Well, we do allow both trains of equipment in the same room, in the same air space.

MR. STEWART: Yes.

MR. MICHELSON: It has to be physically separated, but in the same air space.

MR. STEWART: Yes.

MR. MICHELSON: There are plenty of auxiliary instrument rooms that have Train A and Train B in them

MR. STEWART: Right. We have not considered ionized air as a concern.

MR. WYLIE: As long as it's shielded.

MR. MICHELSON: I don't know whether there's enough -- well, no, the cards aren't shielded at all.

MR. WYLIE: Sure. They're in a cabinet.

MR. MICHELSON: Yes, but the air is being drawn right into the cabinet.

MR. WYLIE: If it's grounded and it's shielded, it won't get very far.

MR. MICHELSON: Yes.

MR. STEWART: If you're aware of some guidance that we should be following or looking at --

MR. MICHELSON: No, I'm not. I'm just asking whether you even considered it or not.

MR. STEWART: No, we have not considered it.

MR. MICHELSON: Now, two things. First of all, do you have a substantial source nearby, and in many cases, perhaps there is no credible source of ionized -- for ionizing the air, but if there is, then you have to decide how big that source is and then see whether or not it dissipates before it gets to the cards because if it gets into the cards, I think that's an uncertainty then as to whether the cards continue to function.

MR. STEWART: Okay.

MR. MICHELSON: You're well aware of all the clean room problems and so forth with charged particles.

MR. STEWART: We'll add ionized air to our list.

MR. MICHELSON: Yes. Just think about it and see if it's credible.

MR. STEWART: We'll have to look and see whether there's any guidance available.

MR. MICHELSON: See, this has gotten into the same problem with electric welding and so forth. They've had trouble in the past with cabinets, solid state cabinets, when people have come in and started welding nearby and there was always the argument, Was it the electromagnetic radiation from the welding or was it the charging up of the air particles and drawing them into the cabinets? I don't know. That's something you ought to think about.

MR. CARROLL: Along the same lines, you obviously are trying to ventilate these cabinets. What happens to solid state gear when sooty smoke is put to the equipment?

MR. STEWART: Sooty smoke from a fire in the cabinet, for example?

MR. CARROLL: Or an adjacent cabinet.

MR. STEWART: Well, the worse case would be that the temperatures would be so high --

MR. CARROLL: No, I'm not talking about the effects of temperature, I'm just talking about the effect of carbon.

MR. STEWART: Of just the smoke itself and the carbon?

MR. MICHELSON: This is where you get a lot of charged particles, too, by the way. Soot's got a lot of charged particles.

MR. STEWART: We haven't specifically tried to analyze what possible circuit pads could be deposited on the card or anything like that. The only criteria I know we have for looking at that would be an Appendix R type review of whatever is causing the fire.

MR. CARROLL: Yes, but see the fire protection guys don't understand the subtleties of solid state instrumentation.

MR. ESHLEMAN: Some of the circuit cards now come with coding which could protect against this, but I can't say that that is a requirement.

MR. MICHELSON: Yes. Unfortunately, they can't coat the contacts, though. It is the contact areas, then, you start worrying about. Yes, they usually are coated.

MR. CHIRAMAL: This is an area we can have Research look at.

MR. MICHELSON: But the way this soot gets into the room also is by a ventilation system if it happens to be coming from an area where there is a fire.

MR. CARROLL: You do have filters. I don't know how effective they are.

MR. CHIRAMAL: This is something we have to look at.

MR. MICHELSON: Some have filters, some don't.

MR. STEWART: Well, if it's safety grade equipment, it'll have redundant HVAC systems, safety grade HVAC systems, too. So, you know, if you have one that's a problem --

MR. MICHELSON: Yes, but what you often find is that there's a so-called normal ventilation system and an emergency ventilation system, and you use the normal when you can and the emergency when you have to, and the normal brought the smoke in.

MR. STEWART: We agree that it's a possibility for smoke to get to the equipment. We'll have to look at it.

MR. MICHELSON: If I believed what you said earlier, and I don't, but you said earlier that each piece of equipment was protected against the environment that it saw; therefore, each piece of equipment, indeed, has to be protected and you don't worry about redundancy of equipment, you worry about that piece of equipment and whether it's protected.

MR. ESHLEMAN: In summary, then, I'd like to say that what we have observed, we think there are other systems that have comparable complexity that utilize digital circuitry, and they are typically found in military applications where they also employ high technology.

There, it's clear by MIL Spec requirements that a plan and a documented approach from the start of the system design is a requirement. I kind of feel like there should be an overall plan laid out right from the beginning.

MR. MICHELSON: Is it your view that the vendors are following that approach?

MR. ESHLEMAN: I have seen no evidence that that is the approach taken. What I'm saying is I think that's a way of identifying EMI EMC surge kind of problems, identifying, I d say, a standard or a criteria, some sort of level that you think the system might be designed to.

As these systems occur over a period of time, the technology is going to continue to change, and so the problem is not one that you can stop at one time; it's something you have to live with on a continuing basis.

MR. WYLIE: What is your recommendation?

MR. ESHLEMAN: That the same kind of approach be followed that they utilize for military platform applications where they actually form -- that becomes a part of the requirement and it is identified early on in the design, not after. Most of the EMI problems that I am familiar with are only addressed after the fact as opposed to before.

MR. MICHELSON: Does the military identify a design basis level of EMI that the equipment must withstand?

MR. ESHLEMAN: Well, in similar kind of applications, they form a committee, and then every other equipment supplier has to meet the requirements identified by the committee.

MR. MICHELSON: Okay. There is a MIL spec for it.

MR. ESHLEMAN: There's a MIL spec for it.

MR. MICHELSON: Does that MIL spec prescribe the level of EMI, it's frequency distribution and magnitude that it has to withstand?

MR. ESHLEMAN: No, it doesn't get prescriptive.

MR. MICHELSON: It just says, You shall withstand something?

MR. ESHLEMAN: No, it says that everybody will sit down together and identify what each one can stand so all the systems can work together.

MR. MICHELSON: For a partic lar system of some sort?

MR. ESHLEMAN: Yes. It typically is geared --

MR. MICHELSON: Like an aircraft.

MR. ESHLEMAN: An airplane or a boat or something like that.

MR. MICHELSON: And if it's got to be near an atomic bomb, that's one thing; if it has to be --

MR. ESHLEMAN: It depends on what kind of problem. That's right, if it has to survive that.

MR. MICHELSON: So it's done on a ad hoc basis, you're saying?

MR. ESHLEMAN: But it's done from the beginning of the design.

MR. MICHELSON: For that particular aircraft.

MR. ESHLEMAN: Right.

MR. MICHELSON: Yes.

MR. ESHLEMAN: This concludes my presentation.

MR. CARROLL: Your view is that GE and Westinghouse --

MR. ESHLEMAN: I have not looked at the Westinghouse design. The other designs I have not seen it addressed at this level.

MR. CARROLL: Okay. Thank you. I'm sure they're going to give us a response to that criticism.

MR. WYLIE: Does this complete the staff's?

MR. STEWART: Yes.

MR. WYLIE: I think at this time, we ought to take a break. We have to clear the room for the closed session. We're behind time a little bit. Let's take a ten-minute break.

[Whereupon, the subcommittee recessed for lunch, to reconvene at 1:00 p.m., this same day.]

AFTERNOON SESSION

[1:00 p.m.]

MR. WYLIE: We will resume. I call on Mr. Ken Scarola of Combustion Engineering to begin this afternoon's session.

MR. SCAROLA: Good afternoon, gentlemen. Thank you very much. I am from ABB/Combustion Engineering, Ken Scarola. I'm the Manager of Advanced Control Complex Engineering at CE. I will be talking about the NUPLEX 80-Plus advanced control complex which is the I&C system used for System 80-Plus. I'll be addressing it this afternoon from a hardware reliability point of view, and then I'll be addressing software reliability later tomorrow.

First of all, by way of introduction, what I will be doing is going through all of these items which I believe are the major contributors to the reliability program that we have at CE. At the end, what I will do is I've made a list through this morning of what I thought were the major questions. I will hope to address most of those through my presentation, but I'd like to go back at the end and see if there may be some that I may have missed, and then I'll recap them and see if I can offer answers on those, as well.

These are the major contributors to the reliability aspects of NUPLEX 80-Plus. I'll just run down the list. Field-proven products; that we use equipment qualification on top of that; we have an internal quality assurance program which includes extensive configuration of controls; the designs themselves are fault-tolerant, and I'll explain what that means.

Because of the software-based technology, we are now doing extensive automatic testing. Standardization in the design, the use of minimum number of components is a major contribut r as well to reliability. Lastly, I will talk about the availability analysis techniques that we're now using to put numbers on the availability of these systems for those folks that like numbers.

First of all, proven products. NUPLEX 80-Plus is somewhat unique from what you may have seen from the other suppliers in that the entire design is composed almost entirely of off-the-shelf available products. We are not designing things unique for the nuclear industry application.

There are some exceptions to that, and those exceptions exist in the sensor area where some of the in-containment sensors are, indeed, nuclear-specific items. The other area is in the rod drive control system area where the power supplies for the mag jacks are, in fact, nuclear-specific items. But in terms of the protection system, control systems, monitoring systems, these are all made up of entirely commercially-available products.

I've listed here the range of those products. It goes from programmable logic controllers. We use a number of IBM PC AT computers, not all of them from IBM, but that family of computers. There are many computers, CRT workstations. We have electro-luminescent display workstations, and we use both conventional cooper as well as fiber optic communication networks.

Most of these are also in use in nuclear applications, including safety-related applications, Class 1-E applications. Certainly the majority of the application is in the fossil area, the industrial area, but there are some nuclear applications, as well. With all of these off-the-shelf products, we then need to integrate them, and CE integrates those using industry standard interface techniques.

For things like data communication, CE is using industry standards, and even for things like back planes within the systems themselves. So all of these systems are made up of products that we buy off-the-shelf and then we integrate them in a manner that is within their experience base, essentially using industry standards.

The important point is that the NUPLEX 80-Plus technology will not be debugged by the nuclear industry. We're not prototyping this equipment for the nuclear industry. It's in thousands of applications already.

From an off-the-shelf product, we then have to look at how do we qualify that for the specific nuclear requirement that it's going into. So we do analysis and/or testing to verify that the off-the-shelf product performance meets the nuclear requirements in the following areas. We address seismic in accordance witn IEEE-344, the environmental considerations, temperature, humidity, radiation, that's in accordance with IEEE-323.

MR. MICHELSON: The first thing you have to do, of course, is decide what your environment and so forth is before you worry about the testing program. How do you go about deciding what your various environments are and what the maximum temperatures in a room might be when the equipment has to function and so forth?

MR. SCAROLA: The environments we are designing to is in about the third slide after this.

MR. MICHELSON: It will come later.

MR. SCAROLA: I can tell you how we go about that, and that's basically based on experience in the industry, discussions with the architect, the architect engineers that CE is essentially designing with, and we go ask the individual end users what is a reasonable environment for this equipment. So we establish the envelopes based on basically a reasonability of an experience level.

Let me give you just some background. This slide that I'm going to show is not in your package, it's in the software package that I'm going to show tomorrow. In hindsight, I think I needed it here and it will give some help in understanding the physical locations of the NUPLEX 80-Plus equipment.

What all these boxes show are the physical separation locations for the I&C equipment in the System 80-Plus design. What we're showing is basically that there are four independent Class 1-E separation equipment rooms. So it's not like in the older plants where we had four channels of equipment inside one equipment room. We now have separate equipment rooms for all four channels.

MR. MICHELSON: Each channel has its own room, is that what you're saying?

MR. SCAROLA: Each channel has its own room.

MR. MICHELSON: Thank you.

MR. SCAROLA: It has its own electrical distribution inside that room. It has its own HVAC for that room.

MR. MICHELSON: That's a dedicated HVAC?

MR. SCAROLA: It's a dedicated HVAC. Let me go back a second and say that the A and C share the HVAC system at some point back in the design because we do not have full four-train HVAC.

MR. MICHELSON: How many trains of HVAC --

MR. SCAROLA: We've really only got two-train
HVAC. Two-train.

MR. MICHELSON: Clearly with two trains you've got to do a lot of sharing.

MR. SCAROLA: What I'm saying is that the A and the C share one train and the B and D share an independent train. Now, within the equipment room itself, the HVAC is unique to that room, but if you go back to the service water system, you will find that eventually there is commonality.

MR. MICHELSON: You're using chilled water and local air handling units in each room.

MR. SCAROLA: I don't want to speak specifically about the HVAC design in this meeting.

MR. MICHELSON: But that's how you control the environment. I thought you were trying to make a point of how well the environment was controlled, so I needed to know a little about how you do it.

MR. SCAROLA: What I'm trying to indicate is that the environments in the rooms are, in essence, single failure independent, yes.

MR. MICHELSON: So you're using two trains of chilled water in the Channel A room, for instance, is that right?

MR. SCAROLA: No. In the A room, there is one train of chilled water, but that's independent from the B train of chilled water.

MR. MICHELSON: But not of the C train.

MR. SCAROLA: So failures that would exist in the A train would not propagate to the B train.

MR. MICHELSON: All right. So you've got two-train chilled water, also.

MR. SCAROLA: Yes. Similarly, there's a non-safety equipment room. The main control room is independent from the remote shutdown room and, in fact, these man-machine interface areas are completely separate from the I&C equipment rooms.

This is what we call the control complex. Now, once we go outside into the plant, we also locate multiplexers out in the plant. The multiplexers are not shown in this drawing, but I can say that in the System 80-Plus design, we maintain four quadrants in the auxiliary buildings and the reactor building such that the same four-channel independence that we have here is maintained through the four quadrants that basically circumference the circular containment for the spherical containment.

MR. MICHELSON: But the multiplexers are not in -- are they in areas where there is potential for an adverse environment or are they located in rooms with just a modest amount of other equipment?

MR. SCAROLA: No. There is the potential on failure for adverse environments, but the potential for the adverse environment to be in the A area and the B area at the same time is not there.

MR. MICHELSON: But you haven't attempted to separate it out.

MR. SCAROLA: Right. So that will give you an idea as to how we separate equipment. So from the environmental standpoint, we basically look at 323 criteria. From an EMI standpoint, we're using Mil Standard 461 as the guidance, and I will discuss the EMI a little bit further. Surge withstand is in accordance with IEEE-472 and fault isolation in accordance with 384, as augmented by 175.

We use manufacturers' experience and manufacturers' internal verification testing where we can justify it. In other places, we do supplemental verification testing. In addition to all of these criteria, we then do a further evaluation of the products for any of the age-related failure mechanisms. Again, that is in accordance with IEEE-323.

So that's basically the --

MR. CARROLL: How about my sooty smoke, how do you evaluate that?

MR. SCAROLA: Sooty smoke, I would not attempt to evaluate the actual effects of sooty smoke. The way I would handle that is that the smoke that exists in the A equipment room will not exist in the B equipment room and that the sooty smoke may produce a failure that is now covered by the failure modes and effects analysis. But it will be confined to a single division.

MR. MICHELSON: You do your failure modes and effect analysis looking for unwanted responses from the equipment, as well as desired responses?

MR. SCAROLA: Certainly the failure modes and effects look at situations where the equipment fails in what we call a safe state and it fails in the non-safe state, as well.

MR. MICHELSON: You do that for each and every function performed by that multiplexing equipment or whatever is being looked at?

MR. SCAROLA: We, in essence, bound the failure modes and effects analysis to the hardware/software boundary interface. In other words, where a microprocessor now produces a hardware output, a contact output, an analog output, whatever, that's where we do our failure modes and effects analysis. We don't go inside the box --

MR. MICHELSON: When you do that, there are various ways of doing that. One way is to look at them one at a time. Another way is to look at multiple failures of equipment. Since the equipment is all getting hot at about the same time, there's a possibility of multiple unwanted actions all being produced somewhat simultaneously.

How do you sort it out? The old FEMA was always one at a time, but this is a new situation. This is where a number of equipments or devices are failing together and not one at a time.

MR. SCAROLA: But the most limiting effects of all of those failures are combined to a single channel or a single division.

MR. MICHELSON: That's right.

MR. SCAROLA: So we can take the worst case effect of a division and say that division either fails to actuate or it spuriously actuates.

MR. CARROLL: There are other possibilities, aren't there?

MR. SCAROLA: With regard to safety systems, there really aren't many other possibilities. The safety system is either going to actuate or it's not going to actuate. There are not systems that normally would assume any types of intermediate states.

MR. MICHELSON: But some of these outputs are decision logic. They're not always just telling something tc open or close or to start or stop. Some of them are in decisionmaking logic trains, which now it introduces a spurious signal into that train and you have to chase it down to make sure it's okay.

MR. SCAROLA: So I would agree, but that decision logic is only the input into what eventually becomes a final actuation. The final actuation is the effect on the plant, and I think that's all we're really concerned about; will the pump spuriously start independent of all of the paths that may have resulted in that spurious start of that pump.

We make an assumption in our failure modes and effects analysis that there is some scenario, we don't know how we get there, but there is a scenario that results in that pump spuriously starting.

MR. MICHELSON: That scenario is in conjunction with whatever caused this to begin with, such as perhaps a fire or a pipe break. You have to add that into the scenario, obviously. This is not a random failure of equipment. Now, this is a fire that's doing other things, including affecting this multiplexer and you have to approach it from that viewpoint.

MR. SCAROLA: Right. But I would --

MR. MICHELSON: Now you have to make sure the fire and its other effects is not reaching other boundaries already or whatever.

MR. SCAROLA: I think the important criteria is that the effects of the fire, regardless of how severe the fire is, are limited to within a single division or a single channel.

MR. MICHELSON: Hopefully that's the case, as long as you don't use common ventilation ducts and things of this sort.

MR. SCAROLA: There are situations where that's not the case, For example, inside the main control room. So we know inside the main control room that a fire will have an impact on multiple channels. That is all four safety channels and non-safety into the main control room.

MR. MICHELSON: Did your FEMA analysis pertain only to safety-related equipment?

MR. SCAROLA: To the extent that we documented it in the SAR, yes.

MR. MICHELSON: You don't look for non-safety equipment and what effect its malfunctioning may have on the safety-related functions?

MR. SCAROLA: We do to the extent that we take credit for the proper operation of those control systems in the safety analysis. For example, Chapter 15 analysis makes certain control system assumptions. These are the types of things that led to the segmentation requirements that --

MR. MICHELSON: Don't forget that what we're really worried about is not Chapter 15 analyses. Those are the main steam and feedwater and pipe breaks inside of containment. I'm worried about the pipe breaks outside of containment, fires outside of containment, other kinds of accidents of that sort. Those aren't part of Chapter 15.

MR. SCAROLA: Then I would say that they're not analyzed.

MR. MICHELSON: That's what we're concerned about here. For fire outside of containment, that multiplexer becoming involved in the heat of the fire creating a problem that we didn't even foresee. That's the purpose of the qualification.

MR. SCAROLA: Certainly I would have to say that if the multiplexer is exposed to a fire, the multiplexer is going to fail. We have to assume that before we detect the failure and we shut the multiplexer down that the multiplexer has an opportunity to spit out erroneous data. That is, in fact, part of our analysis on a single division.

MR. MICHELSON: You do that as a part of analyzing -- assuming a fire in that location, as well.

MR. SCAROLA: Yes, we do.

MR. MICHELSON: So if I look at a FEMA, I'll find that.

MR. SCAROLA: What you will see in the FEMA is not the cause of the failure, but the failure. In other words, we will assume in the FEMA that a multiplexer puts out erroneous data.

MR. MICHELSON: I've looked at a lot of FEMAs and that's exactly what they do and that doesn't address the problem of these incidents outside of containment and how they might ultimately effect the safety of the plant. They address the one problem of when a multiplexer misbehaves, what kind of end actions it has and you show them to be acceptable or unacceptable.

But they don't bring in the fact that in the meantime there's a fire going on in an area or a pipe is broken and water is running around or whatever. Generally, I can't find it in the FEMAs. FEMA is very much a piece of equipment oriented on what it's output might do. But it doesn't bring in what other things are going on at the same time. That's the problem with the FEMAs, at least I've seen. But I'm going to look at yours and see if it's more comprehensive.

MR. SCAROLA: I'd like to think about that a little bit and maybe respond at the end. In your package, there is a sheet that identifies the environment that we are putting the I&C equipment into. There are three environments that we define. One is the main control room environment. One is the I&C equipment room environment which includes the remote shutdown facility. Then we have the field locations where we would locate multiplexers.

What we designed for is a normal environment which is basically what we based the MTVFs of these systems on; their normal exposure to ambient conditions. Then we have what we call the abnormal environment which would be the maximum situation, the maximum design envelope.

Now, certainly we can exceed the maximum design envelope in any one of these areas, but that would be considered a failure in that area that would result in a failure of a single division or a single channel. In the cases where we have multiple safety channels in the same location, such as in the main control room, then an environment that would exceed the abnormal is the result of multiple failures, and that is not part of our design envelope.

MR. MICHELSON: What is an equipment room?

MR. SCAROLA: If I go back to this picture here, the five rooms on the bottom are of the I&C equipment rooms. This is where we locate all of the microprocessors for the protection system, control systems, etcetera. In NUPLEX 80-Plus, the main control room is a passive device. There is no decisionmaking taking place by the electronics inside the control room.

In essence, you can sever this line and have no impact on the performance of the control systems or the protection system.

MR. MICHELSON: In your equipment rooms, what else is in there besides the cabinets containing the solid-state control equipment, anything else?

MR. SCAROLA: I'm trying to think. In some of the rooms, we may have inverters and in some of the rooms we may have circuit breakers or motor starters.

MR. MICHELSON: Some rather energetic equipment, then.

MR. SCAROLA: Very much so.

MR. MICHELSON: So the environment there is certainly subject to possible breaker disintegration, things of that sort.

MR. SCAROLA: Certainly the environment is subject to --

MR. MICHELSON: Such as electrical fires.

MR. SCAROLA: Subject to fires, but, as I said, fires within a single channel. It's subject to EMI, it's subject to surges, but, again, we confine those to within a single channel and we combine them by the design envelope.

MR. MICHELSON: What is the qualification of the individual components on a given solid-state card? What kind of specs are you using?

MR. SCAROLA. We are using what we call industrial grade devices, which are 70 degrees C devices. The equipment in most situations has manufacturers' guarantees or operating specifications of 60 degrees C.

MR. MICHELSON: What's the difference between the 60 and the 70?

MR. SCAROLA: I'm sorry?

MR. MICHELSON: What is the difference between the 60 degree number you just quoted and the 70 degree you gave me a little earlier?

MR. SCAROLA: Seventy degrees C is the component integrated circuit specifications and the design spec of the equipment. Sixty degrees C is manufacturers' warranties.

MR. MICHELSON: On the individual components.

MR. SCAROLA: On subassemblies or systems that we're using.

MR. MICHELSON: The other refers to a full card.

MR. SCAROLA: Right. One is the component specification and one is the manufacturer's willingness to guarantee his equipment. So there is a margin in there.

MR. MICHELSON: I'm just surprised why the card is rated for 70 and the components rated for 60, if I understood it correctly.

MR. SCAROLA: No. I think it's the other way around. I'm saying that the component, the integrated circuits, the resistors, transistors on the card are 70 degrees C devices, but the subassembly is 60 degrees.

MR. MICHELSON: Somehow after you put them on a card they'll stand a higher temperature?

MR. SCAROLA: No. It's just manufacturers' willingness to stand behind their products.

MR. MICHELSON: All right. Strange.

MR. SCAROLA: As you can see, we designed for an ever lower temperature, so there's even more margin in there, as well.

MR. MICHELSON: That temperature you've got at the bottom, you didn't quote me ambient in the room. Those are ambient in the room.

MR. SCAROLA: Right. These are the ambient temperatures --

MR. MICHELSON: The number of 70 degrees C wasn't ambient in the room. That was ambient at the particular location in the cabinet where that component is, which is way above because of the heating effects in the cabinet.

MR. SCAROLA: We are designing for these environments with natural convection cooling. There is no forced air. What we're seeing in most situations is less than 15-degree heat rise inside the cabinets.

MR. MICHELSON: Fahrenheit?

MR. SCAROLA: Fahrenheit, yes. Excuse me. Now, we anticipate that there may be some selected environments that actually have a higher normal temperature and then possibly a slightly higher abnormal temperature. In those situations, we intend to put forced ventilation, but those have not yet been identified for this plant.

MR. MICHELSON: In situations like loss of off-site -- station blackout -- you somehow assure that none of these rooms get over 104, keeping in mind there is no longer any cooling to any of the rooms.

MR. SCAROLA: I don't know if we have addressed station blackout.

MR. MICHELSON: But you will address it eventually and whatever the duration of station blackout, you've got to make sure the rooms don't heat up, because a lot of these are powered by batteries. So the heat generation rate remains fixed, but the cooling rate goes to zero. Some have got kilowatts of heat in those rooms, depending on the size of these cabinets and how many are in there and what else is in there.

MR. SCAROLA: I don't really know the complete answer to the station blackout question, but I do know that we are taking some credit for the diversity between the diesel generators and the alternate AC source, which is a gas turbine, such that I'm not sure that we assume complete loss of all HVAC.

MR. MICHELSON: Unless they put these big chillers on that gas turbine, which is possible, but not likely.

MR. SCAROLA: We will certainly take that as a question to --

MR. MICHELSON: The humidity that you're quoting here, you're not indicating any droplet formation. It's really 90 percent is maximum.

MR. SCAROLA: Actually, this is a summary. In the details, we do talk about non-condensing humidity.

MR. MICHELSON: You specify non-condensing.

MR. SCAROLA: Yes.

MR. MICHELSON: Now, in reality, out in the field locations, if you bust even a hot water pipe, you're going to get condensing atmosphere. First of all, the equipment is cold and the steam and water coming out are much hotter. Is any of this qualified at all for condensing or water formation, water droplets from --

MR. SCAROLA: From water right on the equipment?

MR. MICHELSON: Yes.

MR. SCAROLA: Not right on the equipment. What we do is we design the cabinet enclosures such that they would avoid condensation.

MR. MICHELSON: But you're not enclosing the cabinets because you've got to cool them. You said it was all natural circulation. So I've got to take the air out of the room and that means I'd take the steam and whatever with it. It isn't filtered out.

So you're going to have a condensing atmosphere in the cabinets for those kinds of situations. You're just not designing for water spray at all.

MR. SCAROLA: If that's the case, that we have a condensing atmosphere where the ambient is, in fact, condensing, then we would have to address that. I don't know that that's the case. I would agree that if that is the case, it's got to be addressed.

I'd like to go on to EMI qualification, if I could. What I included is a page out of our qualification program document and this is basically the summary that identifies that for all of the equipment, we establish an EMI baseline. That's in accordance with Mil 461 where we expose the equipment to EMI in various tests and we determine the susceptibility of that equipment, that forms the baseline.

Then we take and we perform site characteristic evaluations to verify that the equipment is not operating inside its baseline. This is the same approach we have taken since the first installation of the CPCs at Arkansas, where we put the CPCs through this type of test, and then we did a site survey on EMI to verify that the CPC was not going to see an EMI exposure that it was susceptible to.

MR. MICHELSON: This is for normal operation.

MR. SCAROLA: This is for all operation.

MR. MICHELSON: How do you simulate all the possible accident conditions that might exist and so forth in terms of EMI effects?

MR. SCAROLA: What we take credit for in the new designs is the physical geographic separation of the equipment into the separate rooms and that if we do see an EMI situation that's beyond the envelope, then that's now considered a single failure.

So we're handling this the same way we handle environmental temperature, fire, or anything else.

MR. MICHELSON: When you say single failure, you mean single failure of the whole cabinet somehow or one component in the cabinet?

MR. SCAROLA: We assume that if the equipment is exposed to an environment, including an EMI environment that's beyond its design bases envelope, that that results in a failure of that division --

MR. MICHELSON: But failure means no unwanted actions or do you include an unwanted action analysis now?

MR. SCAROLA: That's what I was trying to get at before. When we do our failure modes and effects analysis, we assume the equipment fails. We don't normally worry about what caused it to fail. It might be a fire, it might be EMI, it might be water spray, it could be dust.

We don't know what led to the failure, but we do assume that the equipment fails adversely in both directions; either failure to trip, spurious trip, wrong decisions.

MR. MICHELSON: Do you assume all the

possibilities to occur simultaneously from that particular EMI and impinging upon that particular cabinet? I don't think it will, by the way, but, on the other hand, I don't think only one thing will happen either.

MR. SCAROLA: We do assume all subsequent related effects of that failure.

MR. MICHELSON: Concurrently?

MR. SCAROLA: Yes. Concurrently. We do not attempt to speculate on the unrelated events that may be occurring concurrently.

As I said before, this is the program that CE has used for the core protection calculators in all of our plants. Now, as far as forming an acceptable baseline; in other words, what is the envelope for an ALWR; we can speculate on what a reasonable envelope might be, but we don't do that.

What we do is we test the equipment either until it fails or until the top end of what the Mil Standard says. So we basically get as much data on that equipment as we possibly can. I don't know that a baseline is something that we can establish at this point as to what is a minimal acceptable EMI baseline.

MR. CARROLL: How relevant is the Mil Standard to what goes on in a nuclear power plant?

MR. SCAROLA: Parts of it are relevant, parts of it are not. There are parts of the Mil Standard that talk about conducted interference, which I think are much more relevant to what's inside a nuclear power plant.

I think the most applicable criteria for what happens in a nuclear power plant is more the IEEE-472 surge withstand criteria, which is basically surges on lines that do produce radiated interference and they are at the 3,000 volt level and they are much more characteristic of circuit breakers opening and closing.

I think more importantly than any of these tests in the CE design is that we're using industrially-hardened manufactured equipment that has thousands of units in operation in environments that are much, much worse than nuclear power plant environments. The programmable logic controllers we use are used on the factory floor at General Motors and Ford right next to the arc welders.

They're used in steel mills right next to the blast furnaces. So I really think that the industrial experience, in my opinion, even though it doesn't have the paperwork to back it up, per se, I believe it's much more valuable than the actual testing that we run.

Next I'd like to talk about quality assurance configuration control. Certainly ABB/CE maintains an industry-approved quality assurance/quality control program. We are using commercial suppliers for a lot of our equipment. So we must do an internal audit of those suppliers to verify that they have configuration controls, that they have the ability and the mechanisms in place for reporting deficiencies, and also to take corrective actions.

We hold the dedication responsibility for the application of commercial products into the nuclear industry, and this is something that has been ongoing in the nuclear industry for some time now, that we are dedicating commercial products to safety systems and safety applications.

So CE holds the responsibility for failure modes and effects evaluations when the vendors identify deficiencies in their product. We hold the responsibility for 10 CFR 21 reportability. That is an important part of our reliability program.

MR. MICHELSON: Are any of your multiplexers located inside of containment?

MR. SCAROLA: Not in the System 80-Plus design, but I will say that NUPLEX 80-Plus is also the I&C complex for the heavy water reactor NPR. In that design, we will be putting multiplexers inside the containment and they are being designed now. They may have to be special products, not commercial products.

MR. MICHELSON: Do you do your analog-to-digital conversion for System 80 at the multiplexer cabinet or back at the sensing device?

MR. SCAROLA: The A-to-D conversion is done within the multiplexer. We send serial data, serial bit form data over the datalinks.

MR. WYLIE: Where do your fiber optics originate?

MR. SCAROLA: Most of our fiber optics -- I'm hesitant to say all, but the answer might be all -- exist inside the I&C complex, the instrumentation and control complex. We're not using fiber optics for remote multiplexing. We're using fiber optics where we require independence between safety channels or between non-safety and safety.

If we stay within a division, inside a channel, we are using copper. We're not using fiber.

MR. MICHELSON: Is there a reason for that?

MR. SCAROLA: Mostly cost. To go to fiber is more expensive and we can achieve the required noise immunity with copper. We don't have to go to fiber to get the required noise immunity.

MR. MICHELSON: There are a number of arguments about the vulnerability of copper to noise pickup during, say, a fire in a cable tray or things of this sort as opposed to fiber optics which fail much more graciously, at least that's some people's --

MR. SCAROLA: If you look at it harder, you'll see that the weak link in any fiber optic interface are the electronic receivers and transmitters. To say that the fiber immune, yes, that's very true.

MR. MICHELSON: The point is, though, the fire is out in a cable tray, not back at the transmitter or receiver. For fires in cable trays, the fiber optic is thought to be less susceptible to producing unwanted actions than would be a copper transmission.

MR. SCAROLA: I won't argue. I can't say one way or another.

MR. CARROLL: Although you haven't mentioned it, QA brings up a topic we've discussed with others; namely, this EPRI requirement that these systems be looked at by an independent group as the design evolves. How are you doing that?

MR. SCAROLA: If you wouldn't mind, I'd like to leave the discussion of V&V until tomorrow.

MR. CARROLL: I think it's broader than V&V, though.

MR. SCAROLA: We apply V&V from the requirements all the way through the end product. I've heard that some people apply verification and validation to the software. Our V&V program starts at the requirements because we believe the requirements are the biggest source of error, and I will talk about that tomorrow.

MR. MICHELSON: A bigger V&V than we might have thought of.

MR. CARROLL: It also includes looking at the hardware?

MR. SCAROLA: Yes.

MR. CARROLL: Independently.

MR. SCAROLA: We verify the hardware -- I go back to the beginning. We start the verification process at the functional requirements. The functional requirements then become allocated to hardware and software. So we then take two paths, a hardware path and a software path.

Those get verification and validation both. Then we bring the hardware and software back together through an integration path, and then we do verification and validation at that point, as well. The most common source of error in any systems, I don't care if they're software systems or hardware systems, occur at the functional requirements level. They don't occur in the implementation phase.

We have evidence to prove that in our CPC program, and I will talk about those tomorrow.

MR. MICHELSON: Do you put your multiplexer copper inside of conduit going back to the control room or wherever it terminates?

MR. SCAROLA: No, not necessarily. No.

MR. MICHELSON: They could be just laying in cable trays.

MR. SCAROLA: Absolutely. The only place we will use conduit is where it's more economical than a cable tray or if we are going to credit that conduit for some sort of barrier protection. In many places, since we are using multiplexing, there may only be that multiplexer in that region, then it will be economical to use conduit --

MR. MICHELSON: What voltage levels are you restricting the cable tray to when you lay the conduit or the coax on the cable tray?

MR. SCAROLA: We separate instrumentation and control cabling from power cabling.

MR. MICHELSON: But what voltage level do you prescribe as maximum for instrumentation? Cutting if off at 110 or cutting it off at 400 or 600? Where do you cut it off at?

MR. SCAROLA: I don't have Chapter 18 in front of me, but I believe that anything up to 120 volts is considered instrumentation and control, and anything above that is considered power. But I would like to refer to Chapter 18 before that.

MR. WYLIE: All the cables are shielded, though.

MR. SCAROLA: Excuse me?

MR. WYLIE: All the cables are shielded.

MR. SCAROLA: All of the cables have shielding, right. That is right. And all the multiplexing, we do error detection. If there are no more questions on that, I'd like to go to the next slide. I'd like to talk about fault tolerant designs, because that's another important aspect of the reliability program.

Fault tol:.ance is used very much I think ambiguously in this industry. Fault tolerance means different things to different people and we apply it differently among our systems. Fault tolerance can be achieved through redundancy in all the multiple independent channels, as we do in our safety systems. In the plant protection system, the engineered safety feature actuation area, and the discreet indication and alarm system, we actually have independent channels.

So we're fault tolerant in that we can take single failures in one channel and that will not propagate to the other channel.

MR. CARROLL: You said discreet indication and alarm. What does the modifier discreet mean?

MR. SCAROLA: The discreet indication and alarm system is the name of a system in the NUPLEX 80-Plus design. What it refers to is we have solid-state devices, computer-driven displays on the main control panel that look like conventional analog displays.

So instead of having a lot of information on one

CRT, we have individual pieces of information that we refer to as discreet information.

Another means of fault tolerance is fail-safe design. A plant protection system fails safe in that on a failure we initiate a reactor trip or we initiate engineered safety features. So that's another means of fault tolerance in this design.

MR. MICHELSON: How do you assure that you fail safe with solid-state components?

MR. SCAROLA: To the best of our ability, and we don't take credit for it.

MR. MICHELSON: Then you don't really have a fail-safe design. It's an intention to have one, but you're not taking credit as having accomplished that intention. Is that it?

MR. SCAROLA: I would say that's a correct assessment.

MR. MICHELSON: So it's a little oversell, then.

MR. SCAROLA: We have never in this industry, whether it was hardware systems or software systems, been able to credit fail safe as a means of meeting the single failure criteria. So this is just something over and above the single failure criteria.

There is also fault tolerance through dual CPUs and also dual communication links and we do that essentially in non-safety systems. In our control systems and in our data processing system, which is the CRT-based information system, we have what we call primary processors and standby processors, primary datalinks and standby datalinks.

So there is a level of fault tolerance through that redundancy arrangement. That is used in control systems to enhance the availability or reliability of that control system. We are not essentially taking any credit for that in our safety analysis. It's an enhancement to availability.

There is also part partitioning through segmentation. This morning, I think you heard Ed Rumble talk about segmentation as imposed by EPRI and that we segment the various parts of the control systems such that when a control system fails, you can find that failure to the boundaries of that functional aspect of that system and it doesn't propagate such that you have unmanageable transients in the plant.

We do the same thing in the CE control systems, but we also take segmentation and we impose it on the protection systems, as well.

MR. MICHELSON: In earlier designs, a certain amount of cross-talk was required even between safety channels in order to make certain kinds of decisions. These were designed such that in the failure of the cross-talk, you always made the safe decision. Do you still have any need for cross-talking between your various channels in making your logic decisions and how do you handle the failure modes in those cross-talks?

MR. SCAROLA: We have the exact same need and we handle it the exact same way.

MR. MICHELSON: How do you assure, though, fail safe in the cross-talk since we're now dealing with solid-state devices that are cross-talking?

MR. SCAROLA: You cannot assure fail safe. You can --

MR. MICHELSON: How do you answer the problem, then? I thought in the old days we could assure ourselves that it did fail safe because there were relays and whatever and certain ways they could call up.

MR. SCAROLA: You assume that communication between safety channels is a source of single failure. So when the A channel talks to the B channel and the B channel tries to do a two-out-of-four logic on the data from the A channel, you must assume in your failure modes and effects analysis that the B channel can't get the data from the A channel.

You design it such that the most likely failure mode is fail safe, meaning if the B channel can't get any data, it assumes that the data has gone into a trip state and it then handles it as if it did.

Mh MICHELSON: What does it do if it gets incorrect data and doesn't know it's incorrect?

MR. SCAROLA: That's why you do two-out-of-four logic inside that channel.

MR. MICHELSON: But only two of them are required to complete the logic.

MR. SCAROLA: But there are four of them available.

MR. MICHELSON: One of them is faulted and one of them is trying to cross-talk and it's getting misinformation, and so it decides not to do anything because it thought it got some correct information and the decision was don't trip.

MR. SCAROLA: Okay. Then we assume that that entire channel doesn't work and we have an A channel, a C channel and a D channel.

MR. MICHELSON: In the case of reactor protection, I think you're all right. You've got four trains. But in some of these other logics, you don't have four-train, do you?

MR. SCAROLA: We have four-channel initiation of reactor trip and all the engineered safety features.

MR. MICHELSON: But the two-train decisionmaking --

MR. SCAROLA: Four-train decisionmaking. But when it comes down to the execution, the instrumentation and control divisions match the division in the mechanical system. So in System 80-Plus, we do have four divisions of emergency core cooling. We do have four divisions of emergency feedwater.

MR. MICHELSON: Why do they need to cross-talk at all?

MR. SCAROLA: To make the appropriate decision on whether or not to initiate that --

MR. MICHELSON: Generally, it's to hold back on the initiation, isn't it?

MR. SCAROLA: That's why we go to four channels. We go to two channels --

MR. MICHELSON: So the assumption is that one of those two made an incorrect decision but the other two are totally independent of that decision and they make a correct one.

MR. SCAROLA: Right.

MR. MICHELSON: So everything is four-train.

MR. SCAROLA: No. Not everything is four-train. What I said --

MR. MICHELSON: Electric power.

MR. SCAROLA: -- was the four divisional actuation matches the four mechanical divisions where we have four.

There are -- we do have engineered safety features in System 80-Plus that are only two division. Containment spray, for example, is only two divisions.

MR. MICHELSON: Auxiliary feedwater.

MR. SCAROLA: No. The auxiliary feedwater is four divisions. There are others that are only two, and my mind is drawing a blank at the moment.

MR. WYLIE: Mr. Scarola, I apologize, but I'd like to end at 2:00, five minutes.

MR. SCAROLA: You'd like to end in five minutes?

MR. WYLIE: Yes.

MR. SCAROLA: Let me just talk about segmentation in the safety systems and just show you that we analyze all of the design bases, accidents in the plant, and we ensure that we've got at least two reactor trip and engineered safety feature paths that are running on separate microprocessors inside each of the channels.

I'll speak more about segmentation when we talk about software tomorrow. Another part of the reliability contributors is automatic testing. All of the systems in NUPLEX 80-Plus employ self-diagnostics, meaning that they will do memory checks, they will do communication error detection, they're a watchdog, timers, and we look at things like A-to-D accuracy.

The safety systems also include memory checks of the program memory, meaning that the machine continuously looks at its memory to make sure nothing has been altered. It reports that memory, the final memory checksum, off to another system that has inside it what the memory checksum ought to be.

We do that basically to detect program memory faults, as well as to enhance sabotage protection, and we'll talk about that more tomorrow. The final level of testing inside the plant protection system is automatic functional testing, where we actually force the software to run through the reactor trip algorithms, the engineered safety feature algorithms on a continuous basis.

So all of these tests are, in essence, hardware tests, but inside the protection system, we also do a functional test on a continuous basis. Standardization is another important part of reliability. All I can say here is that we don't have much standardization in existing plants, and that's resulted in very difficult personnel training, spare parts problems, and also repair time problems.

That's basically because we use so many different I&C components from so many different manufacturers. So in NUPLEX 80-Plus, we maximize standardization. We have not, however, forgotten that we need defense-in-depth. So we do maintain a minimum level of system diversity and I will talk about that when we talk about software tomorrow because that's an importanc part of our software program.

Lastly, I'll talk about the availability analysis techniques. I think the most important point on this slide is right here, that the analysis that we do now considers the meantime, the MTBF, meantime between failure of components, the meantime for repair of those components, and the failure modes and effects.

We do realize that there are more contributors to reliability and possibly unreliability and we are still developing methods of handling these. These are things like software reliability, human error, and the benefits of self-diagnostics and automatic testing. We don't -- and I might make it a little broader -- the industry doesn't have very well accepted methods of handling these types of things and we are working on that.

So right now the basis of our availability numbers really exists up in this area. With that, I will close. Thank you very much.

MR. WYLIE: Thank you very much, Mr. Scarola. I'm sorry we had to hurry you up. We have another meeting following this one. Mr. Brian Reid, Westinghouse.

MR. REID: My name is Brian Reid. I work in the Plant Instrumentation and Control Group at Westinghouse in our Advanced Technology Division. What I'm going to cover today is really kind of a mixture of things, in that we talked earlier about promises and reality in terms of requirements.

Today I'm working on the AP-600 program which, I guess, by your definition, is promises since we aren't at the stage of building anything yet. Some of the equipment we are going to be talking about here today is, in fact, reality in the sense that it is applied to the Sizewell B system in the U.K. and we've already built prototype equipment and are now building production equipment in the U.K.

As we go through the presentation, there may be some confusion in terms of whether we're talking past or future. I'll try to be clear in the discussion when I answer questions as to whether or not we're talking about the things that will be or the things that already are.

I think it's important to establish a reference point here in terms of where the industry has gone; in particular, where Westinghouse has gone in the past with respect to solid-state technologies. I won't spend much time on this chart, but what you can see is that there are classes of applications that we typically got involved in; controls, information processing, and within those groups, you could break things down into analog and microprocessors and full-blown mainframe computers and so forth.

Across this axis here, I've indicated some of the applications of those technologies and how they've changed. For instance, when I first joined Westinghouse back in 1968, we were just coming out of the mag amp age and had started a new set of transistorized controls. I've been with it as we've gone through the eight-bit design which the original Westinghouse integrated protection system that part of RESAR-414 was based on.

I went away for a while and when I came back the guys were working on 16-bit microprocessor based technologies with some 32-bit implementation for some of the graphics workstations. So things are moving very quickly. The other thing that I think is important is that we're beginning to see a convergence that, in the past, if you were doing data processing, you used a computer. If you were doing control, you went out and bought a controller.

We're seeing now that the product lines are beginning to come together, which gives us some real benefits in terms of a broader applic[illegible] for the technologies and also a more cost-effective way to do the engineering and to make sure that when you do the engineering you've got a good solid base of applications you could sell it to.

I'm going to skip through a couple of slides here because I can see I've got more viewgraphs than we have time. One of the things we did at the beginning of our program for the new I&C systems I'm going to describe was to set out a number of primary design objectives. These were very high-level goals. They were based on things we learned from previous applications and also things that our customers had told us they wanted.

Many of those types of requirements are now institutionalized in the Chapter 10 requirements and in some of the other requirements of the EPRI document. So it's very gratifying to see that we are coming together on this. First of all, I guess I would say that we use modern technology not because it's there, but because it solves a problem.

I did go through one or two iterations in the early days when we did use it because it was there and we quickly concluded that that wasn't the right way to go.

MR. MICHELSON: In the slide which you left out, but there's no mention of whether or not we use this technology because it's safer. Do you make any claim at all that this is a safer way to do it? You don't need to go back to mag amps.

MR. REID: That's a tough call in that, first of all, I don't know any real good way to measure safety in the sense that we could use a yardstick or a meter.

MR. MICHELSON: Well, you know the things you think are intuitively less safe with this, you know the things that are intuitively more safe.

MR. REID: If you look at the places we've had problems in the past, testing has been a big problem, manual intervention during testing, cables, fires in cable spreading rooms have been a big problem in the past. The ability to maintain accurate calibration of your instruments has been a big problem. Those are all kinds of problems or some of the kinds of problems, let's say, that we have addressed.

MR. MICHELSON: I thought you weren't changing out the instruments, you're just going to a digital conversion somewhere downstream in the instrument.

MR. REID: That's true, but --

MR. MICHELSON: Then that doesn't effect the instrument.

MR. REID: If you would look at the accuracy analysis that we have to do on the old analog-based products, about half of the error in the accuracy analysis was allocated to the analog processing. We have essentially wiped that out now. So we've improved the accuracy significantly, which gives us more margin in the rest of the plant.

Similarly, by the use of multiplexing, we've managed to essentially -- well, on new Westinghouse designs, there's no cable spreading room anymore. So that tremendous volume that was full of cables is now no longer there.

MR. MICHELSON: That's certainly a plus.

MR. REID: There are a number of other issues. Our objective was to look at problems that had to be solved and then find ways to do a sensible design that would address those problems.

MR. MICHELSON: And you try to maintain the same level of safety that you thougnt you already had?

MR. REID: Yes, sir, we do. I think we've improved on it in many cases because of that. Let me very briefly. One of the issues was how could we simplify cost and schedule on plants. Now, that, in itself, may not seem like a safety issue, but one of the problems that you get into in building these plants is typically the installation of the instrumentation control equipment is at the tail end of the job and there are probably thousands of people running around trying to pull cables at the last possible minute when the rest of the plant is finally at a state where it can be taken care of.

By the use of the multiplexing and some of the other techniques, we've reduced the amount of cabling that needs to be pulled tremendously. And through some other applications which involve separating the functional design from the physical design, we're at the point where we can give the information that's needed to pull cables earlier, which gets the peak much lower and it spreads it out in time.

So you've got a much better chance of doing a sensible job and being able to get the equipment installed. The simplified plant layout using standard size cabinets and modular system configuration. That was very important to us. To provide an interface that could be use by plant application or processing engineers for configuring the equipment.

Our objective is not to design systems that -- at least those parts which are field configurable, that require software people to do the design. Our objective is to allow the well-educated utility personnel or people from our applications group to do configuration.

MR. MICHELSON: You're not talking about the improved light water reactor in that regard, are you?

MR. REID: The AP-600, yes. That has these characteristics. Now, there are two kinds of software typically we get involved with.

MR. MICHELSON: I'm thinking of the APWR.

MR. REID: APWR has virtually the same equipment on it. The places where you see different --

MR. MICHELSON: I thought you were doing the total design.

MR. REID: I'm sorry.

MR. MICHELSON: I thought you were doing all the design on the APWR or will do it.

MR. REID: Yes. We are.

MR. MICHELSON: You're at the PSAR stage now.

MR. REID: I'm not sure I understand.

MR. MICHELSON: What does it have to do then with the statement about the utility?

MR. REID: We recognize that after we ship a plant, in spite of best efforts, things change.

MR. MICHELSON: If it's a certified design, I would sincerely hope not. That's what we're dealing with here.

MR. REID: I agree.

MR. MICHELSON: Certified designs only and I was surprised at the statement.

MR. REID: I think even in a certified design we have to make provisions for changes to take place over time. Components may no longer be available. I don't disagree that there has to be some mechanism to deal with it.

MR. CARROLL: It depends what --

MR. MICHELSON: Configuration control is a very important thing and that's what he's dealing with here.

MR. CARROLL: You can make changes under 50.59 if they're --

MR. MICHELSON: And then the NRC elects whether they want to review it or not. It doesn't mean it's automatically accepted.

MR. REID: Continuing, we wanted a design in which we could reduce the impact of hardware failures on the plant operation, and we saw that we could do this by increasing the use of redundancy in certain areas and by designing systems in ways that were more fault tolerant in the event that they did fail.

We wanted to improve the reliability of the system by making, first of all, things that would fail less often, but, even more importantly, I think, when they do fail, as they must, to be able to detect that failure quickly and effect repairs quickly. From a maintenance perspective, and this is a place where a lot of problems have occurred in the older plant designs, we wanted to make the actual repair easy. Our way of addressing that is through the use of modular component technologies.

The intent is that for most failures, the solution will be to replace a circuit board with one that's already in stock and then restore the system. We wanted to improve on the ability to do the periodic functional testing by the inclusion of an integrated tecter.

Now, on the older Westinghouse designs, there is a manual test panel provided. The operator has to go in there, reconfigure the system with switches that are built into the panel, run his test, and that takes about eight hours a channel set, which means to do four channel sets, you've essentially used four shifts or four days, however, the utility chooses to do that.

First of all, we wanted to get the man out of that test and then we wanted to be able to speed it up, which we have been able to do. Some of the characteristics of the, if you will, tools we have to work with and the kinds of things that ended up in our architecture are things like modular design.

We've made very large use of what I call reusable building block modules. These are modules that you can put together in different ways to create different kinds of systems, both new systems and backfits. Obviously there's a lot of digital technology. We have the ability to use high-performance microprocessors, if we need to. We have a graduated approach where we've used the kinds of processors that are required to do the job.

We've used distributed processing in many cases. Now sometimes it's physically distributed, sometimes it's only functionally distributed. But in virtually all cases we have replaced the big mainframe computers, for instance, with small distributed microprocessor applications.

You'll see a lot of data highways and datalink communications in the system. This is the other result of having a distributed system. You have to put the information back together again. Data highways and datalinks do that. It's an hierarchical architecture that allows us to communicate amongst devices that need communication strictly amongst themselves and keep that traffic out of the way of the plant level communications that are gradually flowing upwards.

We use fiber optic cabling where it makes sense to do so in the design. We have a fault tolerant design which I wasn't going to get into, but I can to the extent it makes sense.

MR. MICHELSON: Is there some reason why you use fiber optic cabling?

MR. REID: Yes, a couple of reasons. One reason, very specifically, is to provide Class 1-E isolation between the four physically independent and redundant trains. We also use fiber optic cabling for other communications in a data highway that's part of our system. We chose it because it seemed right, although technically one could argue that copper would do the same job. Some of the discussions we had with the previous speaker were of interest there.

MR. MICHELSON: The second reason you cited, so you could use it for other information at the same time, that can be done with copper, can't it?

MR. REID: Yes. In fact --

MR. MICHELSON: The real plus is the total electrical independence of a fiber --

MR. REID: Well, we have different applications. Even within trains, we use fiber optic cables in some cases, even though there's no need for Class 1-E type separation, because it just makes us feel better.

MR. CARROLL: If you've got a lot of information coming out --

MR. REID: As it turns out, in the Westinghouse design, we use the same data rates for both copper and the fiber optics in the application I'm thinking about right now. But in looking ahead, we see that for, if you will, the plant-wide data highways, where you're getting very large volumes of data having to be moved around, there fiber optics seems to be the answer. The fiber distributed digital interface is a big very high speed ring bus that handles a hundred megabits per second, which you probably wouldn't be able to do with copper.

MR. MICHELSON: Do you put the cabling in a tray or do you require it be in conduit?

MR. REID: How can I answer this. There are several categories. The fiber optic cabling we say you can put anywhere you want because it has no physical coupling into the system. We like to keep it away from cable trays that have big huge cables because these things are like a quarter-of-an-inch in diameter and you don't want them to get physically damaged when they're laying with other cables.

But we really don't have any specific requirements, other than just to treat it carefully when you lay it, as you would any other instrumentation cable. One of the things the fiber optic does for us is give us clean separation between the safety equipment. In our previous designs, and it was a question to Ken earlier about are we still communicating back and forth between the four redundant channel sets, the answer is yes, we still are.

One of our objectives in this new design was to find ways to communicate more effectively. In the past, we used to send two wires over for every analog variable that had to be compared. In the new system, we use multiplexed fiber optic -- well, we use fiber optic cables with multiplexed data.

That reduces the number of cables running back and forth between the four physically separated sets to a relatively small number. It, in effect, gives us a very clean separation. There are small penetrations between the fire barriers now with essentially non-combustible cables going through them.

MR. MICHELSON: How do you do your FEMA analysis for, say, local damaging of the multiplexer or whatever?

MR. REID: Very much the same way that Ken has identified. We try to anticipate what are the kinds of failures that we will have to deal with and then take their effect.

MR. MICHELSON: But do you take all the possible failures simultaneously, at least simultaneously to the extent of a particular cabinet heating up or a particular multiplexer cabinet heating up? Do you consider all the possibilities of failure simultaneously for that cabinet?

MR. REID: There's two kinds of failures you have to consider. The failures that cause the system to give you good answers; in other words, safe answers --

MR. MICHELSON: Can you pre-predict safe --

MR. REID: No, you can't. It's the other kind that are the tough ones and I don't think we have any good way of handling that either. We assume that the information that comes from another channel is bad and we then deal with the fact of it being bad. In the case of being bad and recognized as bad, it's simple. We simply ignore it or force the system into a lower level of redundancy. If it's bad and we don't know it's bad, then we have to assume at that point that it's the only cabinet that's bad or the only source that's bad and we are still safe because we've got three other good channels.

MR. MICHELSON: We have a lot of inputs from a given cabinet, a given multiplexer, and we don't know which ones are bad and which ones aren't. We don't even have a sensor that tells us that because it's involved in the same temperature excursion. So how do you treat it? Do you assume all of them are bad?

MR. REID: You basically have to say that a whole channel set is now wrong. I'm getting bad information.

MR. MICHELSON: And look at the worst consequence of all of those being wrong and being interpreted by the other one that's still valid.

MR. REID: With the system I'm describing, there will be no consequences simply because it's a two-out-of-four system. I can lose two of the four channel sets and still be able --

MR. MICHELSON: Are all of your systems set up on four-channel, all the control systems?

MR. REID: Well, this is a viewgraph that's not in your package. I'll have to get you a copy afterwards. It's a very busy viewgraph. Across the bottom here is the protection and safety monitoring system. It has two functions. One is to trip the reactor through opening the reactor trip switch gear, and that takes place at a four-way redundant set of equipment.

Now, depending on the plant application, the engineered safety features, very much as was described earlier, are governed by the mechanical or fluid system trains. An AP-600 plant, for instance, the passive plant, in general, has four-train --

MR. MICHELSON: We'd like t talk about the improved light water first, though, since that is our most immediate concern.

MR. REID: Let's talk about then in the case of advanced light water reactor. That system, I think, is a two-train system, two fluid trains. In that situation, this set of cabinets would still be four-way redundant because that's not governed by the number of mechanical trains.

MR. MICHELSON: Are they in four different rooms?

MR. REID: Yes. Completely separate rooms. These cabinets are governed by the number of fluid system trains. This picture was AP-600, so there's four of them. If this were the APWR, there would be two, one per train. These cabinets then interface to field cabinets that actually start and stop the pumps, open and close the valves. Those are also matching the redundancy of the fluid system trains.

This drawing shows four of them in a current design --

MR. MICHELSON: You don't even loop through the control room at all. You go directly from the --

MR. REID: That's right.

MR. MICHELSON: -- control cabinet right back to the field device.

MR. REID: That's right. This is an example of the fiber optic data highway that exists within a protection set, and the fiber optics there are used not for Class 1-E separation or isolation, but simply because it seems like a good communications path that solves some design engineering type problems.

I won't spend hardly any time on this since it looks more like a marketing slide than a technical slide. What I tried to do here was to identify in a general sense how the different kinds of features that are available to us or capabilities that are available to us these days using the modern technology and some of the newer architectural features, how they address areas of the plant that are important, some more important than others.

It's there more just to give you something to think about. We have endless arguments over where to put X's and where not to put X's. But I think it's a good way to think about those things. The Westinghouse design process as it relates to equipment and system design is perhaps a little different from what you've heard before.

We start with a set of core digital electronic equipment. The characteristics of that kind of equipment are listed here, and they're fairly obvious if you think about that these are basically m.c-ocomputer type products. The technology is moving quickly. There's always a new and better widget out there. They cost a lot of money to develop.

So people who are going to build 30 or 40 of them probably aren't going to design too many. Other industry set the standards and they typically are very complex. Now, our design approach to deal with those is to not design them, but to purchase them from vendors. Typically Intel products are those which we use on the system, Intel multi-bus fc.m factor.

We select board level modules and we rely initially on a broad-based experience, a broad experience base as the starting point for saying those are sensible and reasonable to use on our products. They are, however, part of our full-fledged verification and validation program. So we go well beyond what the vendor 's and will be able to tell us.

The important thing here is that's the standard interface for the next layer. That's the IEEE-796 bus or the multi-bus. This allows us to buy products that can be mixed and matched and plugged in and updated over time. Now, in the nuclear industry, one of the big drivers that we see is the I/O modules because they typically are special in a nuclear application.

They tend to be more along the lines of established technology; A-to-D converters, digital analog converters, things like that don't change nearly as fast as the microprocessors themselves. We use them in large numbers. As I said earlier, they are typically very specialized requirements, like surge withstand, like noise immunity, the ability to do testing and so forth.

Our design approach here is that we design them ourselves. We have a line of circuit boards which have been designed specifically for interfacing to microprocessors for nuclear applications. This integrates the diagnostics into the board and makes it part of the system design. We design these boards along with the -- these boards are designed and verified along with the rest of the system.

From a reliability point of view, one of the major items in nuclear applications is packaging. One of the things that makes nuclear applications so different is seismic requirements. So seismic integrity is very important and the packaging; namely, the containers in which you put the boards has to be able to meet those requirements. It's important to provide protection from interference, EMI, RFI, and something a lot of people don't think about is you would like to control access.

What that means is, at least from our perspective, we design our systems so that you limit access to the insides of the cabinets only to people who need to be inside the cabinets. The boards themselves, the I/O cables can be run to the back of the cabinet where there's no access to the electronics.

So by controlling access to the equipment, you reduce the likelihood that there will be problems caused by busy fingers. The Westinghouse approach here is to use a cabinet that has been designed by Westinghouse and qualified by Westinghouse, and that is, in fact, used now for about five years. We've got cabinets out there in backfit applications.

Those cabinets are designed with EMI-RFI shielding in mind right from the beginning. Within the cabinets, the other hardware is based on modular replaceable units. I talked about interfaces given a distributed system. There's a need to be able to put the system back together again in a functional sense.

Interfaces are interesting in that we have to deal with multiple vendor interfaces as a system evolves. Not everything that is provided comes from Westinghouse. So we have to deal with that. Once you begin tying systems together, there's obviously a potential for interaction. So it's very important to consider that in the design. And whether we like it or not, often requirements are vague.

At the time systems are being configured, certain protocols may not yet have been developed and standardized. So our approach to deal with those kinds of questions is to, first of all, stick very heavily with international standards. Go with standard that are already out there that people are using that will make the conveyance of that knowledge and information easier.

Use fiber optic datalinks; this reduces the potential for interaction very significantly. Relative to the requirements, our intent here is to keep the data format flexible. When you're talking between two systems, almost nobody ends up with the same protocol at the other end when you get down far enough into the system design.

So we've designed our systems to be flexible in the sense that we can provide the ability to do a translation, where we need to, to enable that communication to take place.

Finally, and this is a little bit off the sequence, but I think it's an important one. Maintenance is a topic or a subject that, I guess very much like reliability, it needs to be designed into the system at the beginning. You can only go so far at the end by going back and trying to figure out how to maintain something.

MR. CARROLL: When did Westinghouse make this discovery?

MR. REID: I personally made it about 20 years ago. I know, I was getting zinged. The characteristics, though, of maintenance in a nuclear plant is that we typically have relatively complicated systems.

They may not be complicated as a rocket launch, but the systems are relatively large. Often the symptoms are rather vague. Because of the nature of the system, you can't always tell this is what's wrong. Maintenance is clearly a key to reliability. Once something starts to malfunction, you've got to get in there and fix it.

So our design approach to deal with that was to start with the intent to have a fully automatic tester that would localize faults down to the circuit board level, replaceable module level, typically. We would build in comprehensive diagnostics which would be running all the time. The automatic tester runs once a month or whenever the utility feels it's appropriate, and to use plug-in modules as a basic mechanism to be able to get in there and out of there quickly once you've determined which is, in fact, the faulted system or the faulted module.

As far as the design process goes, I think Ken made a very good point earlier about the fact that most of the errors in systems occur at the beginning of the process. We do a very good job of building the wrong thing exactly right and that's been proven time and again.

One of the parts or portions of our design process that supports the whole concept of reliability and availability is to start with a structured process to begin with. That structured process starts with the system design requirements; Ken called them function requirements, but you can see the same split he described. An increasing level of detail as you go through, until finally you come up with the final individual products and you stick them back together at the bottom.

Now, the next viewgraph, which you won't be able to read with the lights out in your package because it's a C or a D size drawing reduced to A size, so I'm going to talk about it with respect to the shapes rather than the details. This is called our system design and implementation process. This is the implementation of that previous sketch.

What it shows is coming into the process a set of design requirements, the system design, a design verification that takes place at that level. The dotted lines represent verification steps, the solid lines represent design steps, the breakdown of the system into modules and subsystems and the types of documents and so forth that are provided at each level.

What you can see is that there is a set of internal verification steps that take place along the way. Then finally there is a big loop that goes all the way around to the front of the design and that's what we call validation. That is the point where you really find out if what you thought you were doing meets the input requirements.

We are very well along the way in this process, specifically for the Sizewell program, and what that means is that many parts of this process will not have to be repeated for other jobs. As you follow this process down, you're getting into the design of the individual circuit boards, the software modules.

It's our intention that those modules will be reusable. So that the next time we do a job, the system-type activities will have to be redone at some level. But once we get down here into where we would do module and subsystem design, most of that work is already done now. In terms of our process, we will sort of skip to the design implementation integration stage and the validation would then take place around that.

Now, there will be typically new things required in new applications. So this process is important because we will have to revisit it occasionally. If a new circuit board is designed, we'll have to make sure it all fits in and that the verification and validation program has been applied appropriately to that design.

MR. CARROLL: Where does the independent look come into this?

MR. REID: The independent look is basically the dotted lines here. At Westinghouse we have a separate verification and validation team that is defined. This team is responsible for a complete verification of both hardware and software. I was manager of that team at one point in time. They needed somebody who did not report in to the same reporting structure that the designers were in. It turned out I had been involved in this program back about ten years prior to that. So I had enough knowledge to be dangerous and to be able to ask good questions.

I had reporting to me about three or four hardware designers and about, at one time, I guess as many as six to ten software verifiers. I shouldn't have said designers, but verifiers. Their job was to take every piece of code that was part of the system, every circuit board that was part of the system, and go through these steps where the dotted lines are indicated.

MR. CARROLL: How about the requirements part of it, who was helping you then? Hopefully not the software guys.

MR. REID: There's really three. We haven't got to the third part yet. I'd forgotten that. There's a validation function as part of the verification and validation program. The validation group is responsible for looking at the input functional requirements, translating those essentially into a set of test specifications and test requirements that they can then apply on the final product over here in the systems validation phase.

So we close the loop essentially twice. We close the loop actually more than twice, but internally during a set of small steps we close the loop with verification activities. Then there's one big step at the very end where we go back to the fundamental requirements and use those as a basis to test the final product.

That program is virtually complete for Sizewell. They're doing some cleanup work, but the program is virtually done. So we've been through this once. It's tough. It takes a lot of people to verify a job properly, but it works.

MR. CARROLL: How do you know?

MR. REID: Because we found mistakes. We didn't find many, which makes me think that our input --

MR. CARROLL: How do you know they found them all?

MR. REID: I don't know. In fact, I know I didn't find them all. What I do know, though, is that one of the characteristics of this process is you don't just depend on one technique to look for problems. You come at it from a number of different ways. You inspect the code. The first thing my guys do is inspect the documents. That's the very first thing they do, is read the requirements and make sure that they think they're complete and that they think they understand them.

Then they read the code, the source code and check for -- I'm stealing Bill Rumbly's thunder from tomorrow -- but basically we check to make sure that the code designers use good programming practices. This is before you ever look at the code to see what it does, but is it the right kind of code. Then they do tests with mechanized equipment that counts numbers of lines and looks for structures that are incorrect.

Finally we get around to running it in a test environment. Ultimately it's run in the final product as a subsystem, and then finally as a complete system. So, no, I won't say we'll catch every one, but I think the process we've got will give us a very good probability of catching most of them simply because they may be able to hide from one technique, but there's a good chance that one of the other ones will cause it to pop up.

MR. WYLIE: How long have you been using this process?

MR. REID: Sizewell job started about five years ago, I guess. I'd say about five years, maybe a little longer than that. In terms of design features to support maintenance, this chart basically ties together the kinds of things that we think are important in maintenance;

preventive maintenance, corrective maintenance, and adaptive maintenance; and the kinds of design features that are implemented or can be implemented in these kinds of systems to address those issues.

Preventive maintenance in the sense of calibration means you're looking for did the calibration disappear, did it go out of whack. The automatic tester can help you find that and often self-diagnostics will do that. You can see that the different kinds of problems can be addressed by different features in the system.

MR. CARROLL: I guess adaptive maintenance is new terminology to me.

MR. REID: It was to me, too.

MR. CARROLL: Tell me what it means.

MR. REID: What it means really is things change in a plant and it may turn out that you're getting bad results not because the system is wrong, but because somebody has reconfigured some other part of the plant and now your flows are different.

So being able to change calibration or maybe a new sensor was put in and it behaves a little differently. I would have chosen a different word than adaptive, I think.

The next viewgraph is simply in words a little bit more about what each of those points are. Unless you have specific questions on those, I'll skip by that.

MR. CARROLL: How close is the hardware we're talking about to something I am familiar with, namely Eagle 21.

MR. REID: That's a very good question. Remember I mentioned earlier about modular building blocks. Eagle 21 is an example of a modular building block, where we took the basic fundamental design, we took the same card cage, the same power supplies, the same circuit boards, with a few exceptions, and we figured out how we would stick them into a different cabinet.

Sticking them into the different cabinet was what caused the exceptions because the old Amco racks, the 19-inch Foxboro style racks are not the same dimensions as the racks we use now. But much of the code is similar. There are very special requirements on the older plants because of the form fit and functional replacement constraints. But that is an example of using the equipment.

There are other products similar to that; the digital position indication system that was just put in at Rochester. I say "just." It seems like it was three or four years ago now. It's an example of the same kind of thing where we're able to take a set of tinker toy type building blocks and plug them together. It's not as easy as it sounds, but it's a lot easier than starting from scratch.

MR. CARROLL: The DRPI you're talking about, though, went into a lot of earlier plants originally.

MR. REID: No. Well, we're in our third, maybe even fourth generation of digital RPI. The original one was an analog implementation. They used sort of LVDT type detections.

MR. CARROLL: Right.

MR. REID: We went to a -- I forget the exact name for it -- digital RPI, which was based on digital technology, but not microprocessor technology. We just recently put a system into Rochester which is an upgrade to the DRPI using microprocessor technology. That same system is now in Sizewell and would be in our new plants when we build them.

As far as environmental design is concerned, we have in our design process requirements to speciiy -- excuse me -- we have specified requirements for EMI, RFI, and the IEEE surge withstand. The British were very adamant. They helped us quite a lot, I guess, because I think we got further under the direction than we might have gone otherwise.

But they gave us very specific requirements about the kinds of system characteristics that we would have to have. One of those characteristics was to be very stoutly designed, I guess to use a British term, against EMI and RFI. The cabinets that we have manufactured look like this.

These are filters -- well, they're both air filters and they are EMI-RFI filters on the door.

You can't quite make it out here, but there's a special gasket that goes all the way around the door and there's a mating metal surface inside the door jamb. So when the cabinet doors are closed, there is no pathway in for EMI or RFI interference.

MR. MICHELSON: Is that because the filters are metal filters and grounded? Is that how you prevent it from --

MR. REID: No. There's actually two filters. There's the EMI filter, which is a metallic filter that has dimensions that are appropriate to --

MR. MICHELSON: And it's well grounded.

MR. REID: Yes. Also, though, there's an air filter just to --

MR. MICHELSON: Is it fiberglass air filter?

MR. REID: I don't think it is. I think it's some kind of a porous foam type filter.

MR. MICHELSON: Do you know what micron size it's designed for?

MR. REID: I don't know. I can certainly find out.

MR. MICHELSON: No. It's not that important.

MR. REID: Its main intent is to keep chunks out, not to keep microns out, though.

MR. MICHELSON: Okay.

MR. REID: It's a dust filter primarily.

MR. MICHELSON: It won't keep charged particles out, although that screen might keep charged particles out.

MR. REID: The screen might help. Some of the cabinets have a requirement for a panel in the door so that the status can be observed on test panels inside. For those we had to come up with a special glass that has a film embedded in it that's conductive. So even though you can see through it, it provides an appropriate barrier.

MR. CARROLL: What happens when the security guard walks by the open cabinet that the instrument tech is working on and calls the CAS or the SAS?

MR. REID: There's two answers to that. First of all, the right answer is nothing should happen. My answer right now is we don't know. We've done some testing with the microprocessor equipment and our initial findings were that, strange as it may seem, they seemed to be less susceptible to radio frequencies than the analog equipment because their impedance is internal or much lower.

If you look at the structure here, the cards are sort of back inside here. My guess is if he's not real close, nothing will happen. But obviously if you put in any kind of a barrier, as soon as you violate that barrier, you're wiped out. If you're doing automatic testing, for instance, you're periodic testing, there's a couple of things I think are important.

First of all, it can operate completely unattended. So you don't even need to have the door open once you've launched the automatic tester. You can come back after it's done. If the light tells you it's okay, it's okay, and you could then plug in your printer and get a record.

What that means is you can close the door while the test is going on. The other thing is you should only be testing one system at a time anyway, one train. So even in that case, the results shouldn't be too horrible. But the fact is whatever barriers you put in to protect against EMI and RFI must be violated when you do maintenance, so during that period of time, you are at some risk.

MR. CARROLL: Is that a forced ventilation cabinet?

MR. REID: Yes, sir.

MR. CARROLL: How many fans?

MR. REID: There are two fans here. There are two fans inside the circuit --

MR. CARROLL: What's the circulating pathway through there?

MR. REID: The air comes in the bottom and runs up in parallel through the microprocessor boards and across I/O boards which are at the back of the cabinet pointing toward the door on the other side.

MR. CARROLL: Where does it discharge?

MR. REID: Right out the top here. It's hard to tell here, but the --

MR. CARROLL: That's a discharge?

MR. REID: This makes a big plenum when the door is closed. This whole area is the exit.

MR. CARROLL: It has a metailic mesh filter on it also to keep the EMI out?

MR. REID: That's right. Now, we haven't done the testing yet, but the plan is to ship a bunch of these cabinets -- I shouldn't say a bunch -- several up to a test facility that will expose them to the fields that the customer specification --

MR. CARROLL: Those are redundant fans, each one of which alone would do an adequate job of cooling?

MR. REID: Right. Well, the interesting thing is on the AP-600, which is a passive plant, you remember this morning Ed mentioned about the desire to have passive cooling. One of the ways that you help passive cooling along is you keep your room very cool to begin with.

So when you lose your air conditioning, you've got more time to react before the temperature rises to unacceptable values. The design basis for the room in which these cabinets will be on the AP-600 plant, at least for the safety cabinets, is about 65 degrees.

We've concluded that if you keep the air at 65 degrees, you don't need fans. We do get enough natural circulation in here.

MR. CARROLL: Even through that filter arrangement.

MR. REID: Yes. We're still having to make some internal decisions; do we want to keep the fans running; do we want to put a thermostat on them and add more complications.

MR. CARROLL: They're powered off the same power -- they're powered off the essential power bus.

MR. REID: That's right. In fact, one of our objectives to get rid of the fans is those fans have to run on the same batteries that have to provide power for 72 hours during a loss of all off-site power. So that's just another load on the battery.

MR. CARROLL: But the problem is that the room isn't being cooled during that 72 hours.

MR. REID: That's right. The room temperature will rise, by spec, 20 degrees in 72 hours.

MR. CARROLL: That means there's not many power sources in the room.

MR. REID: Just these cabinets basically.

MR. CARROLL: That's the only thing.

MR. REID: Yes.

MR. CARROLL: How much power?

MR. REID: A single bay like this is about 800 to 1,000 watts.

MR. CARROLL: You're talking about a kilowatt in each one and how many bays do you have in a room?

MR. REID: It's probably eight to ten.

MR. CARROLL: You're talking about a lot of power and you're talking about a 20-degree rise in an eight-hour period.

MR. REID: There are a few more things that --

MR. CARROLL: Yes. There's a few more things that are adding to it. You're talking about 20-30 kilowatts of power into the room.

MR. REID: We have a few more tricks, though, going for us. Not all of this equipment is needed after a station blackout. For instance, all the reactor trip equipment has no value after blackout because --

MR. CARROLL: So you're supposed to go and deenergize these circuits.

MR. REID: So we're looking at ways to cut back on the amount of power that's generated.

MR. CARROLL: This 20-degree rise isn't very much from 65 degrees, I assume.

MR. REID: No, it's not. It's a tough challenge for the --

MR. CARROLL: You're talking about keeping it down below 85 degrees at the end of eight hours with 15-20 kilowatts of heat, more or less. I don't know how much less. That's quite a trick.

MR. REID: Many of the Westinghouse products were designed for industrial applications. For that reason, the IEEE surge withstand has been one of the criteria we've designed to essentially, I would say, for the last ten years or so. So all of our equipment is designed to meet that spec, and I've got to say where applicable because things like the nuclear instrumentation signals are not exposed to a test of that sort.

But all of the field wires that go out to the switch gear, motor control centers, that kind of stuff, all of the sensor, four to 20 am sensor, thermocouple RTD signal paths. All of those are qualified to withstand the IEEE surge and continue to function afterwards.

As far as physical is concerned, we have always, of course, because we're in the nuclear business, had to build and qualify our equipment to meet seismic requirements. Our experience has been that the tough part of that is the cabinets.

Generally speaking, cabinets and card cages are the challenge. Circuit board behave pretty much the way they're supposed to if you keep them from wobbling around. That's been sustained in a number of tests we've made recently.

As far as temperature goes, we have a -- I guess you could say a dual set of requirements, I think very much like CE mentioned. We qualify our equipment to 120 degrees Fahrenheit. We don't ever expect it to run that --

MR. MICHELSON: That's room temperature.

MR. REID: Yes. 120 room temperature, yes. Typically the specs we use say you ought to be able to survive at that for eight to ten hours, some number in that time range. Our normal operating conditions we limit to about 104 F. In most cases, we'd hope it would be lower than that.

MR. CARROLL: How does the operator know that stuff is not surviving?

MR. REID: There are a couple of ways. It depends on why it's not, of course, to begin with. But we have a --

MR. CARROLL: I'm thinking the temperature going up and --

MR. REID: Somehow I knew you were going to ask that question. One of the things we did when we designed the circuit boards for the new system, we designed a special board that is especially a monitor board. It plugs into the Intel multi-bus. One of its jobs, amongst other things, is to monitor temperatures in different places in the cabinet and issue an alert.

You can do what you want to with the alert, but its only job is to tell the rest of the system that temperatures have exceeded allowable values. That same board also looks at the voltages on the power supplies and if the voltages go out of spec, it will alarm that and we can tell it to trip the system to protect the outputs from doing dumb things.

MR. MICHELSON: Are these located in the multiplexing transmitting cabinets?

MR. REID: Yes. Let me say something about that. Our system architecture is a little different from what other people have talked about. I can't find my picture. We do not have what you would call multiplexers, per se, in our system. We have cabinets where functions are performed and where those functions are first performed, we perform an A-to-D conversion and --

MR. MICHELSON: Where are these cabinets located, though?

MR. REID: They are typically located in rooms near the control room.

MR. MICHELSON: Maybe it would be easier if you start with the sensor out on the pipe somewhere and kind of --

MR. REID: Let me walk --

MR. MICHELSON: -- which is done analog and which is done digitally.

MR. REID: First of all, with the exception or rod position indication, there are no digitizing multiplexing type electronics in containment in a Westinghouse design.

MR. MICHELSON: Outside of containment, what do you do?

MR. REID: Outside containment, we bring the wires up to the cabinets typically. Here is a case where the integrated protection cabinets, there will be four different rooms in the plant. Those wires will be brought directly from the containment to those cabinets. In other words, there is no multiplexing at that point.

Once we get the signal into that cabinet, we will do an A-to-D conversion on the signal, check the normal things you do once you first get hold of a signal.

MR. MICHELSON: Do those cabinets contain the temperature sensors that you're referring to?

MR. REID: Yes. That's right. It's a standard module that goes in every one of our Intel multi-bus --

MR. MICHELSON: Where do they normally go in elevation in the cabinet?

MR. REID: It's about the middle.

MR. MICHELSON: About the middle.

MR. REID: Incidentally, I laughed a little bit this morning. Somebody was asking about where the power supplies were in the cabinets. We went through the same gyrations over the years. In the past, we always put them in the bottom because it was easier to seismically qualify. That's where they are now.

As it turns out, we can qualify them.

MR. MICHELSON: Now, your hot spot from the viewpoint of power supplies is up in the top somewhere.

MR. REID: That's right, which gives us an even better draft and we're not pulling the hot air over the cabinet.

MR. MICHELSON: But you sense the temperature in the middle of a cabinet.

MR. REID: I said the board is in the middle of the cabinet. The board has several sensors which are distributed throughout the cabinet.

MR. MICHELSON: They're hard-wired to the board?

MR. REID: Yes. It is able to monitor the bus voltages because all of the voltages are brought onto the bus. But there is a separate temperature sensor, several of them that are located at different points in the cabinet.

MR. CARROLL: What other magic does this

monitoring board do?

MR. REID: It resets the microprocessor in the event that something -- it is the one that starts the processor up when you first turn on power. But mostly it's there to do the diagnostics --

MR. CARROLL: Temperature and high and low voltage.

MR. REID: Yes.

MR. MICHELSON: It shuts all power off to the board if it gets low voltage?

MR. REID: Right now it simply tells the operator something has gone wrong.

MR. MICHELSON: Even on voltage.

MR. REID: No. On voltage, it shuts the system down, but I can't remember how we do it. You've got to shut the system down. Otherwise, there's no point in monitoring --

MR. MICHELSON: You start worrying about what it's doing if the voltage gets too low.

MR. REID: Yes. It turns out the supply, you've only got a quarter-of-a-volt tolerance before the microprocessors start getting upset. The other systems are much more tolerant.

MR. MICHELSON: It almost has to be automatic in order to --

MR. REID: I'd have to check, but I'm virtually --

MR. MICHELSON: You're not trying to protect the cabinets so much as you are trying to prevent unwanted actions from occurring.

MR. REID: That's right. We're trying to protect the function to make sure we don't do something that's inappropriate.

MR. MICHELSON: So you provide under-voltage protection to do that.

MR. REID: And over. Over is more important.

MR. MICHELSON: You don't worry about frequency at all?

MR. REID: No. We're monitoring DC voltages.

MR. MICHELSON: That's right.

MR. REID: There are plus and minus 15 volts provided for the I/O boards and then a combination of five volts and some other stuff that's provided for the microprocessor board.

So those power supplies have a fairly wide threshold for input voltages. But once we get through those, we're looking at straight DC.

MR. WYLIE: Excuse me, Mr. Reid. We're going to have to wrap the meeting up. We have another meeting starting at 3:00.

MR. REID: Okay. I had, I think, pretty much --

the only other thing I was going to mention is --

MR. MICHELSON: Humidity, are you going to provide for a condensing atmosphere?

MR. REID: No. Ninety percent non-condensing.

MR. MICHELSON: That's at all locations?

MR. REID: Excuse me?

MR. MICHELSON: That's throughout in the reactor auxiliary building?

MR. REID: Yes. Some of our equipment is designed or at least you can get some benefit by placing it close to things like motor control centers, because it allows you to shorten the big heavy wires that go between the motor control center and the control circuits, and then multiplex the signals back up into the control room.

Those cabinets are out in a more loosely controlled environment. For the Class 1-E cabinets, specifically on AP-600 where we have passive cooling requirements, those have been all pulled back into the area that has guaranteed cooling after a loss of off-site power.

The other thing I just wanted to mention is -- and I'm not really qualified to talk about it in too much detail -- but we do, in fact, have -- on AP-600, we've put together a reliability, availability and maintainability plan. One of its objectives is to take the EPRI requirements for the various availability requirements and begin to allocate those and parse them out to the different parts of the system.

I think I have about four hours of the unavailability per year that's allocated to all of the I&C. So it represents a challenge, but we are, in fact, doing a structured process in order to take those requirements and parse them out and make sure that we've got a budget and that everybody is working to those objectives.

That was my last slide. If there are any other questions, I'd be happy to answer them.

MR. WYLIE: Thank you, Mr. Reid. I'd like to thank all the presenters today for fine presentations. I think that the Subcommittee will get together later and decide what we want to do from here forward. I call the meeting adjourned.

[Whereupon, at 3:00 p.m., the Subcommittee was recessed.]

REPORTER'S CERTIFICATE

This is to certify that the attached proceedings before the United States Nuclear Regulatory Commission

n the matter of:

NAME OF PROCEEDING: ACRS Reliability Assurance

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.

Michael O'Pauls

Official Reporter
Ann Riley & Associates, Ltd.

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: ACRS Reliability Assurance

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.

Mary C. Larkin

Official Reporter
Ann Riley & Associates, Ltd.

ALWR RELIABILITY ASSURANCE INSTRUMENTATION AND CONTROL

- DESIGN CRITERIA
- REGULATORY GUIDES
- NATIONAL STANDARDS
- ENGINEERING SPECIFICATIONS
- DESIGN PRACTICES
- STAFF EXPERIENCE, KNOWLEDGE, AND JUDGEMENT

- EXISTING DESIGN REVIEW
- PLANT MODIFICATION REVIEW
- ALWR REVIEW

DESIGN REVIEW CRITERIA

- PAST LICENSING REVIEWS
- STANDARD REVIEW PLAN
  - SEISMIC, EQ, APPENDIX B, IEEE 279

- RECENT REVIEWS
  - CPC, RESAR, CESSAR, RETROFITS AND MODIFICATIONS

- ADDITIONAL REVIEW GUIDANCE
  - SOFTWARE IEEE/IEC
    - VERIFICATION AND VALIDATION
    - CONFIGURATION MANAGEMEN
  - HARDWARE IEEE/IEC
    - ELECTRICAL ENVIRONMENT

- FUTURE APPLICATIONS
- NRC RESEARCH REQUESTS
  - SOFTWARE CRITERIA
  - ISOLATION DEVICES
  - MULTIPLEXING/ FIBER OPTICS

FUTURE APPLICATIONS

- EPRI ALWR (EVOLUTIONARY)
- GENERAL ELECTRIC ABWR
- COMBUSTION ENGINEERING SYSTEM 80+
- EPRI ALWR (PASSIVE)
- WESTINGHOUSE AP600
- GENERAL ELECTRIC SBWR
- COMBUSTION ENGINEERING SIR
- ABB/CE PIUS
- MHTGR/CANDU/.....
- RETROFITS AND UPGRADES

PROVEN TECHNOLOGY

- OPERATIONAL HISTORY
  - TIME IN SERVICE
  - SIMILARITY OF APPLICATION
  - NUMBER OF UNITS
- TESTING
- ANALYSIS
- SIMILARITY TO PREVIOUS DESIGNS

ALWR PASSIVE ISSUES

- I&C CRITERIA FOR PASSIVE SYSTEMS
  - EXISTING CRITERIA AND REVIEW GUIDANCE
  - NEW GUIDANCE AS NEEDED

- NO SAFETY GRADE AC POWER SUPPLY
  - HVAC FOR ELECTRONICS

REVIEW ISSUES

- SOFTWARE
  - V&V
  - CONFIGURATION MANAGEMENT

- PREVIOUS REVIEWS
  - TEMPERATURE TESTING

- FAILURE MODES

- MILD ENVIRONMENTAL TESTING
  - TEMPERATURE
  - HUMIDITY
  - RADIATION
  - FIRE SUPPRESSION
  - ELECTROMAGNETIC INTERFERENCE

ONGOING DEVELOPMENT

- STANDARDS DEVELOPMENT
  - ANSI
  - IEEE
  - ISA
  - IEC
  - NRC - REGULATORY GUIDES AND SRP

- INTERNATIONAL TECHNICAL EXCHANGES
  - REGULATORY
  - VENDORS
  - UTILITY
  - RESEARCH
  - FRANCE / UNITED KINGDOM / CANADA / GERMANY / SWEDEN / NORWAY

- NRC RESEARCH
  - NRR USER NEEDS

I&C HARDWARE
RECENT EMI - EMC REVIEWS

- DIGITAL REPLACEMENTS FOR ANALOG
  - PALISADES, HADDAM NECK, BEAVER VALLEY
    GENERAL ELECTRIC NUMAC

- COMMON MODE FAILURES
- COMPLEX UPGRADES
  AUTO TEST AND CALIBRATION
- CONDUCTED NOISE
  - HIGH FREQUENCIES
  - POWER LINES
  - CRITERIA - IEEE 518, 1050, ANSI C63.12

- EMI RADIATION EFFECTS
- SHIELDING
- GROUNDING
  SINGLE POINT VS MULTIPOINT
- SURGE WITHSTAND

- RESULTS TO DATE
  - OLD CRITERIA
  - ORIGINAL CABLES & ROUTING
  - POWER, LOCATIONS

I&C HARDWARE

ALWR DESIGN REVIEWS EMI/EMC

- EPRI ALWR I&C DESIGN GOALS
- GE ABWR UPGRADE TO DIGITAL I&C
- CE SYSTEM 80+ UPGRADE TO DIGITAL

- DESIGN APPROACHES
  - DISTRIBUTED MICROS OR MULTI UNITS
  - MULTIPLEX DATA SYSTEMS
  - AUTO TEST AND CALIBRATION
  - FAULT LOCATION

- EMI PROTECTION IDENTIFIED
  - NO CONSISTENT APPROACH
  - EACH SUPPLIER HAS OWN CRITERIA

- SURGE WITHSTAND
  - DESIGN NOT TO THIS DETAIL

- OVERALL
  - SIMILAR MILITARY
  - APPLICATIONS REQUIRE COMPATABILITY CONTROL

NUPLEX 80+

HARDWARE RELIABILITY

KEN SCAROLA

MANAGER, ADVANCED CONTROL COMPLEX ENGINEERING

NUPLEX 80+ HARDWARE RELIABILITY

- o FIELD PROVEN PRODUCTS
- o EQUIPMENT QUALIFICATION
- o QUALITY ASSURANCE AND CONFIGURATION CONTROLS
- o FAULT TOLERANT DESIGN
- o AUTOMATIC TESTING
- o STANDARDIZATION
- o AVAILABILITY ANALYSIS TECHNIQUES

PROVEN PRODUCTS

- o NUPLEX 80+ IS COMPOSED (ALMOST ENTIRELY) OF COMMERCIALLY AVAILABLE PRODUCTS WITH PROVEN INDUSTRIAL AND UTILITY PERFORMANCE:
  - PROGRAMMABLE LOGIC CONTROLLERS
  - PC-AT COMPUTERS
  - MINI COMPUTERS
  - CRT WORKSTATIONS
  - ELECTRO-LUMINESCENT DISPLAY WORKSTATIONS
  - COPPER AND FIBER-OPTIC COMMUNICATION NETWORKS
- o MOST OF THESE ARE USED IN NUCLEAR APPLICATIONS (INCLUDING CLASS 1E)
- o PRODUCTS ARE INTEGRATED WITH INDUSTRY STANDARD INTERFACES
  - RS-232, 485
  - ARCNET
  - ETHERNET
  - VME-BUS
  - STD-BUS
  - PC-BUS
- o NUPLEX 80+ TECHNOLOGY WILL NOT BE DEBUGGED BY THE NUCLEAR INDUSTRY.

EQUIPMENT QUALIFICATION

o ANALYSIS AND/OR TESTING IS PERFORMED TO VERIFY COMMERCIAL PRODUCT PERFORMANCE IN THE FOLLOWING AREAS:

- SEISMIC - IEEE-344
- TEMPERATURE - IEEE-323
- HUMIDITY - IEEE-323
- RADIATION - IEEE-323
- EMI - MIL-STD-461
- SURGE WITHSTAND - IEEE-472
- FAULT ISOLATION - IEEE-384 (RG1.75)

o MANUFACTURERS TESTING OR FIELD EXPERIENCE IS SUBSTITUTED WHERE EQUIVALENCE CAN BE JUSTIFIED.

o IN ADDITION, PRODUCTS ARE EVALUATED FOR AGE RELATED FAILURE MECHANISMS.

ENVIRONMEMNTAL CONDITIONS - OUTSIDE CONTAINMENT
(MILD ENVIRONMENT)

MAIN CONTROL ROOM - CABINET OR PANEL AMBIENT CONDITIONS

	NORMAL	ABNORMAL
TEMPERATURE	73 - 78 °F	85 °F (8 HOURS)
HUMIDITY	20 - 60 %	60 %
PRESSURE	ATMOSPHERIC	
RADIATION	2×10^{2} RAD GAMMA (TID)	

EQUIPMENT ROOM/REMOTE SHUTDOWN ROOM - CABINET OR PANEL AMBIENT CONDITIONS

	NORMAL	ABNORMAL
TEMPERATURE	65 - 85 °F	104 °F (8 HOURS)
HUMIDITY	40 - 60 %	90 %
PRESSURE	ATMOSPHERIC	
RADIATION	2×10^{2} RAD GAMMA (TID)	

PLANT FIELD LOCATIONS - CABINET OR PANEL AMBIENT CONDITIONS

	NORMAL	ABNORMAL
TEMPERATURE	32 - 104 °F	122 °F (8 HOURS)
HUMIDITY	20 - 90 %	90 %
PRESSURE	ATMOSPHERIC	
RADIATION	1×10^{3} RAD GAMMA (TID)	

5.3.4 Qualification Test Acceptance Criteria

The qualification test unit will be subjected to EMI test signal levels and frequency ranges as specified for the equipment. Proper test unit operation and performance (i.e., software execution, response time, data stability, communication integrity, analog conversion accuracy,...etc.) at the maximum levels defined or the point of discontinuity shall establish the EMI qualification baseline.

Any anomaly or discontinuity observed beyond test unit tolerance limits that would impair the safety related performance of the unit during the application of EMI test signals will constitute susceptibility to the applied EMI test signal. Upon identification of susceptibility, that portion of testing will again be performed to confirm repeatability and the susceptible condition(s) will be documented as the qualification baseline.

Modification may be applied to eliminate the observed EMI susceptibility however, it must be demonstrated by test and/or analysis that the modification does not effect prior EMI qualification results. EMI qualification testing may then be continued to completion.

5.3.5 Site EMI Characterization

A site survey will be performed upon completion of system installation to characterize the installed EMI environment. This characterization will address the synergistic effects of simultaneous operation of multiple systems. EMI characterization is performed to confirm that the EMI operating environment of the equipment is within its qualification baseline.

QUALITY ASSURANCE AND CONFIGURATION CONTROLS

- o ABB/C-E MAINTAINS AN INDUSTRY APPROVED QA/QC PROGRAM
- o COMMERCIAL SUPPLIERS ARE AUDITED FOR INTERNAL QUALITY PROGRAMS INCLUDING:
  - CONFIGURATION CONTROLS
  - DEFICIENCY REPORTING
  - CORRECTIVE ACTIONS
- o ABB/C-E HOLDS DEDICATION RESPONSIBILITIES
  - FAILURE MODES AND EFFECTS EVALUATION
  - 10CFR21 REPORTING

FAULT TOLERANT DESIGN

- o REDUNDANCY THROUGH MULTIPLE INDEPENDENT CHANNELS IN SAFETY SYSTEMS
  - PLANT PROTECTION SYSTEM
  - ENGINEER SAFETY FEATURE COMPONENT CONTROL SYSTEM
  - DISCRETE INDICATION AND ALARM SYSTEM
- o PPS FAILS-SAFE TO INITIATE REACTOR TRIP AND ESFAS
- o FAULT TOLERANCE THROUGH DUAL CPUs AND COMMUNICATION LINKS IN NON-SAFETY SYSTEMS
  - CONTROL SYSTEMS
  - DATA PROCESSING SYSTEM
- o FAULT PARTITIONING THROUGH SEGMENTATION IN ALL SYSTEMS
- o COMMON MODE FAILURE TOLERANCE THROUGH INTER-SYSTEM DIVERSITY

  PPS - CONTROL SYSTEMS
  E-CCS - CONTROL SYSTEMS
  DIAS - DPS

SYS80+ RT FUNCTION vs TRIP PROCESSOR ASSIGNMENT

\ TRIPS \ TRANSIENTS \	SG1 lo P	SG2 lo P	CONT hi P	SG1 lo L	SG2 lo L	SG1 dP	SG2 dP	SG1 hi L	SG2 hi L	PZR lo P	PZR hi P	LOG PWR	DNBR lo	LPD hi	VOPT	CONT hihi
FW temp decrease	1*	2*											CPC*	CPC	1	
FW flow increase								1	2				CPC	CPC		
Main steam flow increase	1	2											CPC	CPC	1	
IOSGADV	1	2											CPC			
SLB i/o containment	1	2											CPC			
LOL											1,2					
TTRIP											1,2					
Loss of cond vacuum								1	2		1,2					
MSIV closure											1,2					
Loss of non-emerg AC to station aux													CPC			
Loss of norm FW flo				1	2						1,2					
Loss of RC flow													CPC			
1 RCP seizure													CPC			
RCP shaft break						1	2									
Uncont CEA withdraw at low pwr											1,2		CPC	CPC	1	
at power													CPC			
1 f/l CEA drop																
s/u of inactive RCP																
Core flow rate incr																
Inadvert deboration											1,2	2	CPC	CPC	1	
CEA ejection															1	
CVCS malfunction											1,2					
SG tube rupture													CPC			
LOCA										2			CPC			

1* - BISTABLE PROCESSOR 1
2* - BISTABLE PROCESSOR 2
CPC* - CORE PROTECTION CALCULATOR

TABLE 1

System 80+ RT Function vs Trip Processor Assignment

AUTOMATIC TESTING

- ALL SYSTEMS EMPLOY SELF DIAGNOSTICS:
  - MEMORY READ/WRITE CHECKS
  - COMMUNICATION ERROR DETECTION
  - WATCHDOG TIMERS
  - ANALOG TO DIGITAL ACCURACY
- SAFETY SYSTEMS ALSO INCLUDE PROGRAM MEMORY CHECKSUM VERIFICATION
- PLANT PROTECTION SYSTEM ALSO INCLUDES CONTINUOUS AUTOMATIC FUNCTIONAL TESTING
  - ONE CHANNEL AT A TIME
  - SHORT DURATION TO PREVENT PROPAGATION
  - CANNOT BLOCK VALID TRIP PROPAGATION

Slide179/7

STANDARDIZATION

- o PRESENT PLANTS CONTAIN NUMEROUS COMPONENTS FROM NUMEROUS ELECTRONIC SUPPLIERS.
- o MANY ARE CUSTOM BUILT FOR THE NUCLEAR INDUSTRY
- o THIS IS THE RESULT OF ANALOG TECHNOLOGY AND DISTRIBUTED RESPONSIBILITY FOR THE I&C COMPLEX
- o THE RESULT IS DEFENSE IN-DEPTH (THROUGH DIVERSITY)

  HOWEVER, SIGNIFICANT DIFFICULTY IN:

  - PERSONNEL TRAINING
  - SPARE PARTS
  - REPAIR TIME
- o NUPLEX 80+ MAXIMIZES STANDARDIZATION WHILE MAINTAINING A MINIMUM LEVEL OF DIVERSITY.
- o THIS RESULTS IN:
  - IMPROVED PERSONNEL MAINTENANCE SKILLS
  - REDUCED SPARE PARTS INVENTORY
  - SHORTER MEAN TIME TO REPAIR*
  - ADEQUATE DEFENSE-IN-DEPTH

* ALSO ACHIEVED THROUGH SYSTEM SELF-DIAGNOSTICS

AVAILABILITY ANALYSIS TECHNIQUES

o ANALYSIS IS CONDUCTED AT SEVERAL LEVELS:

- SUBSYSTEM
- CHANNEL
- SYSTEM
- CONTROL COMPLEX (INTER-SYSTEM)

o IDENTIFIES AVAILABILITY OF KEY SYSTEM FUNCTIONS (AT VARIOUS PLANT LOCATIONS)

o ANALYSIS PRESENTLY CONSIDERS:

- COMPONENT MTBF
- MEAN TIME TO REPAIR
- FAILURE MODES AND EFFECTS

o METHODS FOR CONSIDERING OTHER FACTORS ARE STILL BEING DEVELOPED:

- SOFTWARE RELIABILITY
- HUMAN ERROR
- SELF-DIAGNOSTICS/AUTOMATIC TESTING

o GENERAL CONCLUSIONS:

COMPONENT MTBF 2 - 10 YEARS
MTTR .5 - 2 HOURS
FMEA - MINIMAL DUE TO:
- REDUNDANCY
- MULTIPLICITY
- SEGMENTATION
- DIVERSITY
- FAIL-SAFE DESIGN

o TYPICAL SYSTEM FUNCTION AVAILABILITY IN MCR > 99.98%

Westinghouse Electric Corporation

RELIABILITY AND MAINTAINABILITY ANALYSIS

ENVIRONMENTAL DESIGN

Design Features to Support Maintenance (Cont'd)

- Logic Programming Interface
  - Functional graphic representation of logic
  - Logic uses verified software modules
  - Logic testing included
  - Changes implemented in PROM
- AC Power Distribution
  - Limit extent of system to be powered down during repair
  - Multiple circuit breakers and switches in cabinet allow local isolation of failed equipment
  - Support for two independent AC feeds provided

RELIABILITY AND MAINTAINABILITY ANALYSIS

ENVIRONMENTAL DESIGN

ELECTRICAL

- ELECTROMAGNETIC INTERFERENCE
- RADIO FREQUENCY INTERFERENCE
- IEEE SURGE WITHSTAND

PHYSICAL

- SEISMIC
- TEMPERATURE
- HUMIDITY
- RADIATION

ENVIRONMENTAL DESIGN

IPS – Designed for Maintenance

- Integrated automatic functional testers 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

Design Features to Support Maintenance (Cont'd)

- Logic Programming Interface
  - Functional graphic representation of logic
  - Logic uses verified software modules
  - Logic testing included
  - Changes implemented in PROM
- AC Power Distribution
  - Limit extent of system to be powered down during repair
  - Multiple circuit breakers and switches in cabinet allow local isolation of failed equipment
  - Support for two independent AC feeds provided

Design Features to Support Maintenance

- Modular Design
  - Replaceable modules with plug and socket connections
  - Hardware diagnostics identify failed module
  - Modular software facilitates design changes
- Mechanical Keying
  - Prevents improper board insertion
  - Covers input/output modules
- Software Keying
  - Ensures that computer hardware is intact
  - Covers computer modules
- Maintenance Console
  - Low level inpsection of software and system status
  - Inspect memory and data values
  - Read software configuration data
  - Cannot interfere with normal operation

Design Features to Support Maintenance

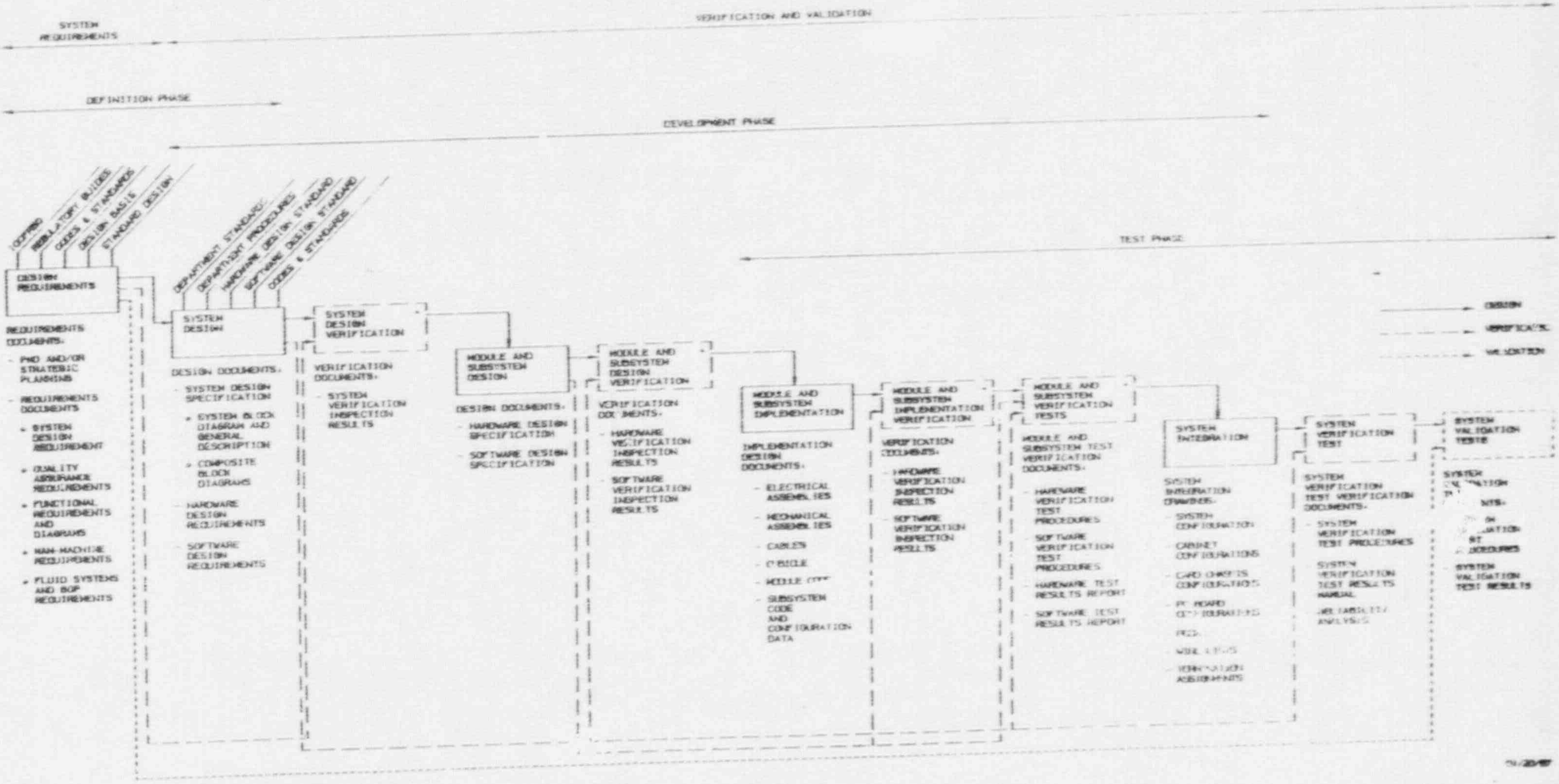
MAINTENANCE CLASS	Automatic Tester	Self Diagnostics	Maintenance Console	Logic Programming Interface	AC Power Distribution	Modular Design	Mechanical Keying	Software Keying
PREVENTIVE								
Calibration	X	X						
Function Checks	X							
CORRECTIVE								
Fault Detection	X	X						
Localization	X	X	X					
Isolation					X			
Replacement/ Repair						X		
Confirmation	X	X					X	X
ADAPTIVE								
Calibration Data Changes			X					
Functional Changes				X		X		

(Column group heading: DESIGN FEATURES)

ZT09 ZTB DISC 111

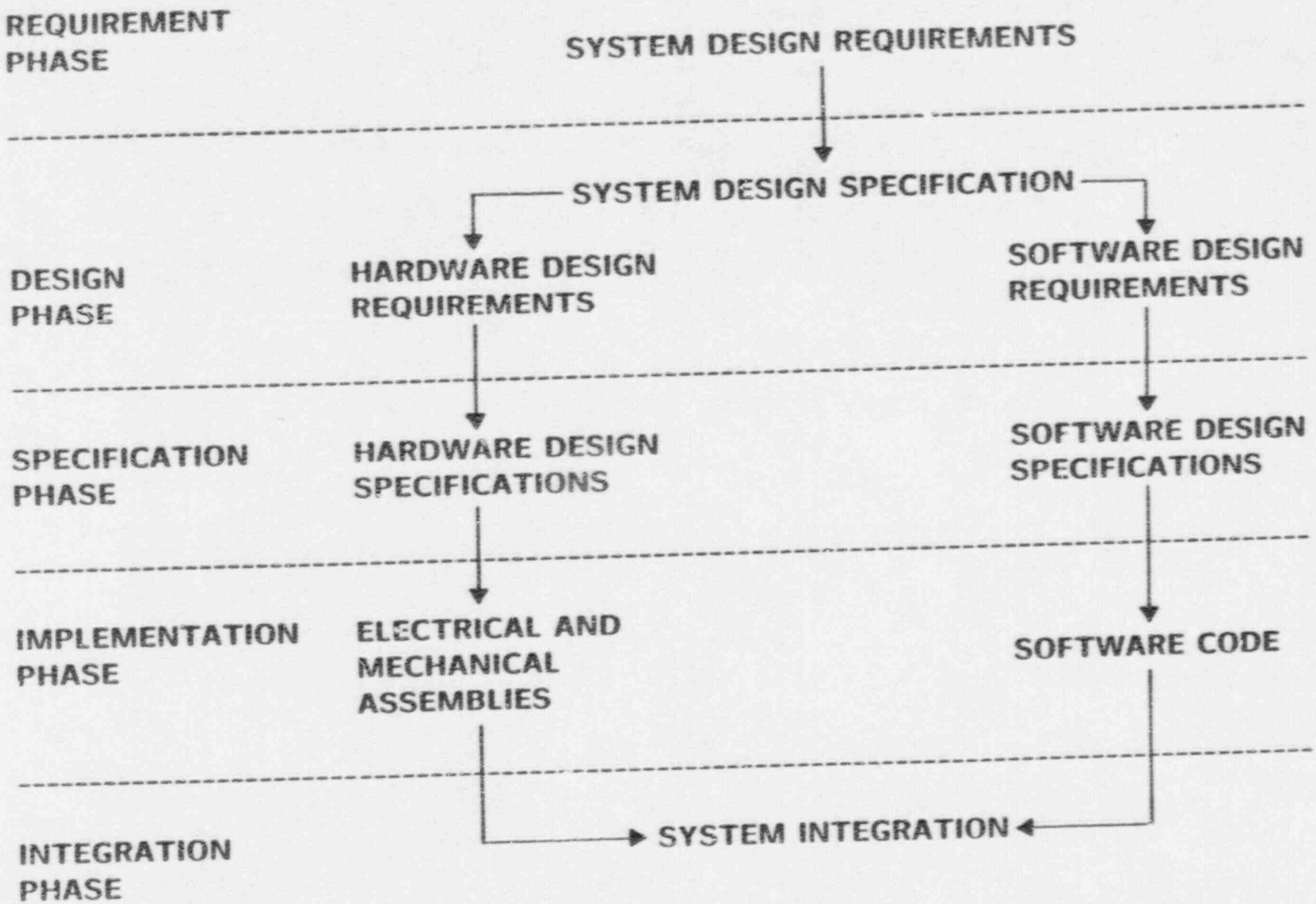
RELIABILITY, TESTABILITY & MAINTAINABILITY

SYSTEM DEVELOPMENT/IMPLEMENTATION PROCESS (SYSDIP)

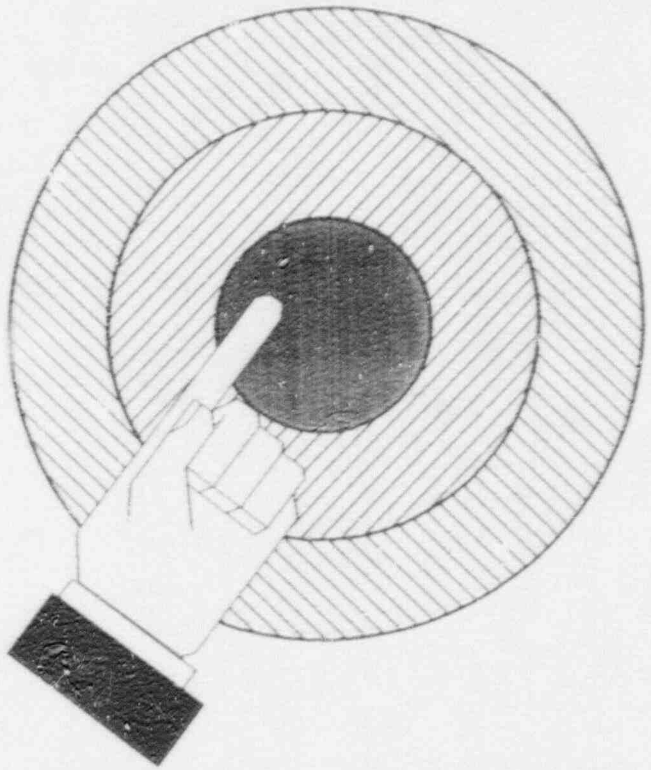


* VERIFICATION REQUIRED FOR SAFETY SYSTEMS ONLY

DESIGN PROCESS



Westinghouse Design Philosophy



MAINTENANCE FEATURES

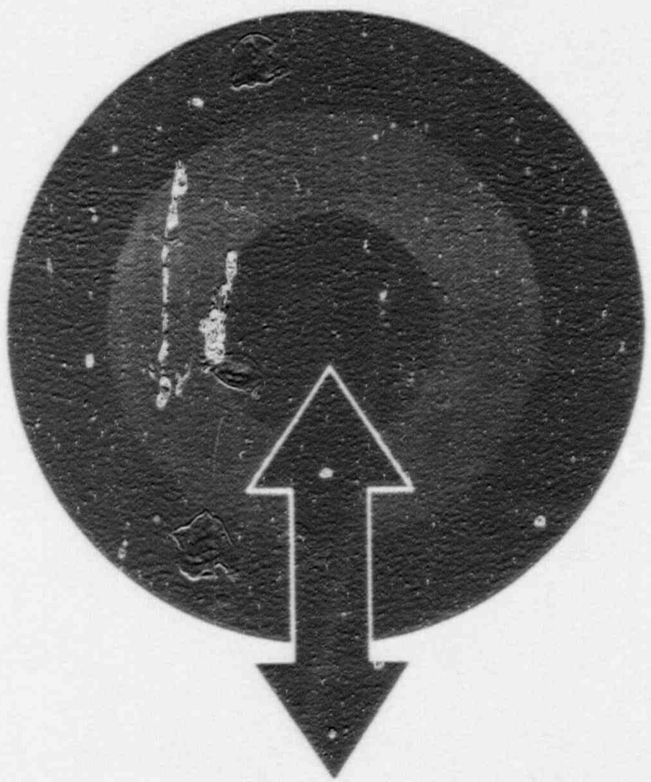
Characteristics:

- Complex functions
- Diffuse symptons
- Key to reliability

Design Approach:

- Automatic tester
- Comprehensive diagnostics
- Plug-in modules

Equipment Design Philosophy



Interfaces to Other Systems

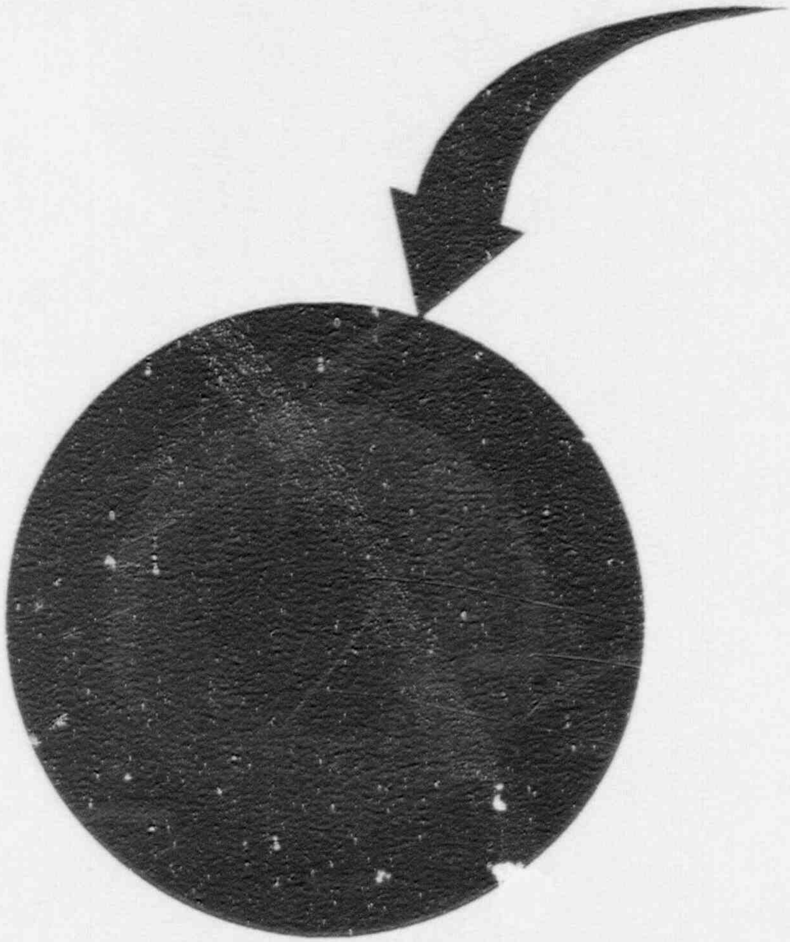
Characteristics:

- Multiple vendor interfaces
- Potential for interaction
- Requirements often vague

Design Approach:

- Use international standards
- Use fiber optic data links
- Keep data format flexible

Equipment Design Philosophy



Packaging

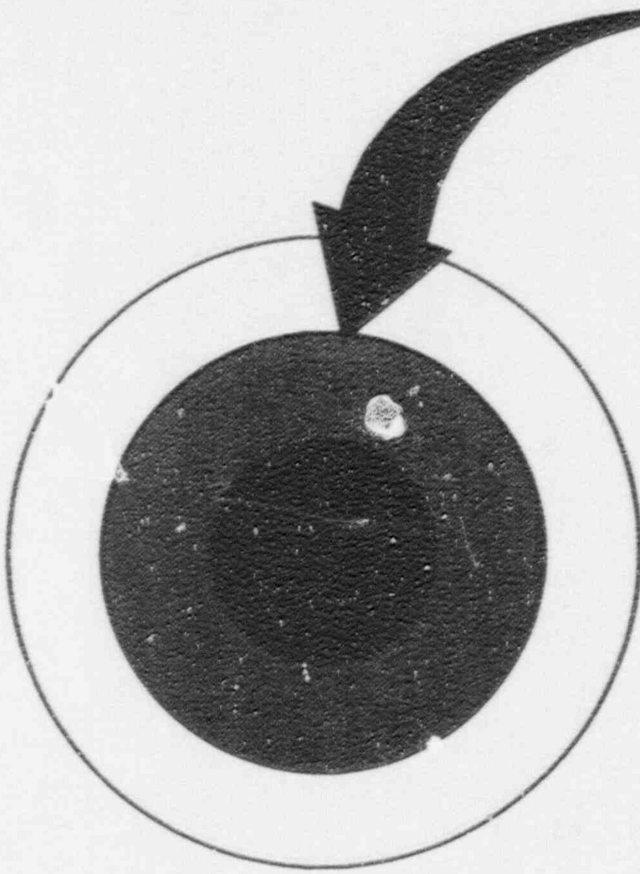
Cnaracteristics:

- Seismic integrity
- Protection from interference
- Control of access

Design Approach:

- Ⓦ designed cabinet
- EMI/ RFI shielding
- Modular replaceable units

Equipment Design Philosophy



Input/ Output Modules

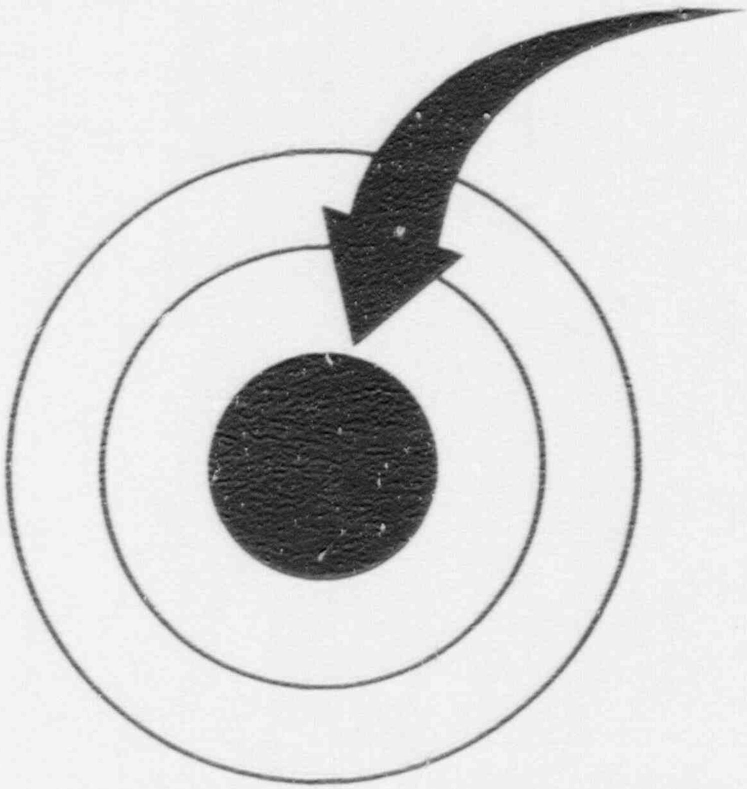
Characteristics:

- Established technology
- Relatively large numbers
- Impact by Nuclear requirements

Design Approach:

- Custom design by Ⓦ
- Integrate with diagnostics
- Design verification testing

Equipment Design Philosophy



Core Digital Processors

Characteristics:

- Rapid technology evolution
- Large development cost
- Other industries set standard
- Complex modules

Design Approach:

- Purchase from vendor
- Select board level modules
- Relies on broad-based experience
- Standard interface to next layer

DESIGN PROCESS / SYSTEMS DESIGN

Benefits of Westinghouse Digital I&C

AREAS OF BENEFIT

FEATURES	SCHEDULE	INSTALLATION	PLANT INTERFACES	PLANT COSTS	WORKING ARRANGEMENT	DISTANCE	TRAINING	HUMAN ENGINEERING	PLANT SAFETY/LICENSING	PLANT AVAILABILITY	PLANT OPERABILITY	MAINTENANCE	TECHNICAL INDEPENDENCE	OBSOLENCE	FLEXIBILITY FOR THE FUTURE
MICROPROCESSOR TECHNOLOGY			X			X	X		X	X	X	X	X	X	X
DISTRIBUTED PROCESSING ARCHITECTURE	X	X	X	X					X	X	X				X
MODULAR DESIGN	X	X	X				X			X		X		X	X
SEPARATION OF FUNCTIONAL AND EQUIPMENT CONFIGURATION	X	X	X		X	X	X						X	X	X
REDUNDANCY									X	X		X			
FAIL SAFE/FAULT TOLERANT									X	X		X			
IMPROVED CONTROL AND PROTECTION ALGORITHMS				X						X	X				X
EXPANDED CONTROL AND PROTECTION RANGES				X						X	X				X
ACCOMODATION OF DEDICATED AND "SOFT" CONTROLS			X					X			X				X
FUNCTIONAL, PHYSICAL, PROCEDURAL, AND ALARM DISPLAYS							X	X	X		X	X			X
WINDOWING, PAGING, ZOOMING, DISPLAY ACCESS							X	X			X				X
INTEGRATED REAL TIME DATABASE MANAGEMENT	X	X		X	X	X									X
PLANT PERFORMANCE CALCULATIONS											X	X	X		
DATA ARCHIVING AND RETRIEVAL									X	X	X	X			
ACCURATE AND STABLE									X	X	X	X			
CONTINUOUS SELF DIAGNOSTICS	X	X							X	X		X			
ENGINEER/MAINTENANCE WORKSTATION	X	X					X		X	X		X			
INTEGRATED AUTOMATIC TESTER	X	X							X	X		X			
MULTIPLEXING	X	X	X	X											X
OPTICAL ISOLATION			X						X	X					

I&C Architecture Characteristics

- Modular Design
- Digital
- High Performance where necessary
- Distributed Processing
- Data Highway and Data Link Communications
- Physically Distributable
- Hierarchial Architecture for Communication and Data Transfer
- Fiber Optic Cabling
- Fault-Tolerant Design
- Clean separation within safety equipment and between safety and non-safety equipment
- Improved Control and Protection Algorithms
- Information Presentation in Context with Navigational Aids

Primary Design Objectives (Continued)

- To reduce the impact of hardware failures on plant operation by providing redundancy and fault tolerance
- To enhance equipment reliability through the application of continuous diagnostics that localize faults soon after their occurrence thereby minimizing the time required for failure detection and repair
- To facilitate maintenance through the use of easily replaceable modules and built-in diagnostic and trouble-shooting equipment
- To facilitate the periodic functional test requirement by the inclusion of an integrated functional tester

Primary Design Objectives

- To meet the stringent requirements of nuclear class 1E equipment including seismic, separation, environment, testability, reliability, and quality

- To reduce the cost and schedule associated with cabling of the actuated equipment control circuits through the application of multiplexing technology

- To simplify plant layout through the application of standard cabinet sizes and modular system configuration

- To provide a logic programming interface that may be used by plant application or process control engineers

- To facilitate the equipment manufacture and plant construction schedule by separation of the functional design from the equipment configuration and allowing the two to proceed in parallel even to the point of commissioning

OBJECTIVES OF

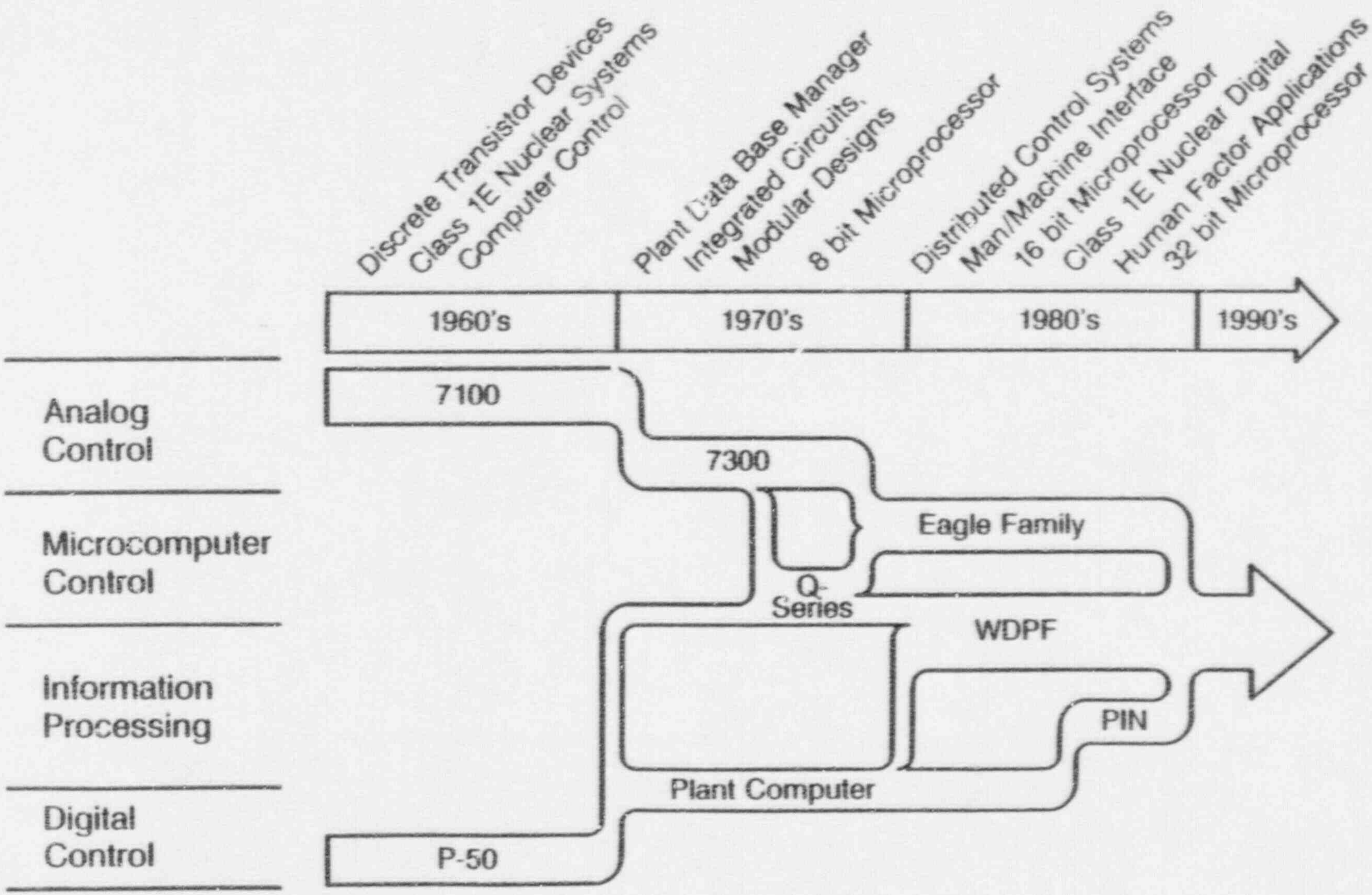
WESTINGHOUSE I&C SYSTEM DESIGNS

USE DIGITAL TECHNOLOGY TO PROVIDE IMPROVEMENTS IN:

- COST
- SCHEDULE
- CONSTRUCTABILITY
- MAINTAINABILITY
- OPERABILITY
- FLEXIBILITY
- RELIABILITY
- LICENSEABILITY

INTEGRATE AND UNIFY THE TOTAL PLANT I&C SYSTEMS

Instrumentation & Computer Product Evolution



OVERVIEW AND OBJECTIVES

(2)

Westinghouse Electric Corporation

RELIABILITY OF SOLID STATE DEVICES IN ADVANCED REACTORS

PRESENTATION TO THE ACRS SUBCOMMITTEE

ON

RELIABILITY ASSURANCE

FEBRUARY 5, 1991

J. B. REID

Westinghouse Electric Corporation

RELIABILITY, AVAILABILITY & MAINTAINABILITY PLAN

- MONITOR SUPPLIERS
- PROGRAM REVIEWS
- DATA COLLECTION AND ANALYSIS
- CORRECTION
- MODELING
- ALLOCATION
- PREDICTION
- FMECA
- MAINTAINABILITY ANALYSIS
- MAINTAINABILITY DESIGN CRITERIA