Official Transcript of Proceedings ACRS-3330

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
527the Meeting

Docket Number: (not applicable)

PROCESS USING ADAMS
TEMPLATE: ACRS/ACNW-005

SISP - REVIEW COMPLETE

Location: Rockville, Maryland

Date: Friday, November 4, 2005

Work Order No.: NRC-694 Pages 1-122

NEAL R. GROSS AND CO., INC.
Court Reporters and Transcribers
1323 Rhode Island Avenue, N.W.
Washington, D.C. 20005
(202) 234-4433

TR04

DISCLAIMER

UNITED STATES NUCLEAR REGULATORY COMMISSION'S

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

November 4, 2005

The contents of this transcript of the proceeding of the United States Nuclear Regulatory Commission Advisory Committee on Reactor Safeguards, taken on November 4, 2005, as reported herein, is a record of the discussions recorded at the meeting held on the above date.

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

+ + + + +

527TH MEETING

+ + + + +

FRIDAY,

NOVEMBER 4, 2005

+ + + + +

The Committee met in Room T2B3 of the U.S. Nuclear Regulatory Commission, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland, at 8:30 a.m., Graham B. Wallis, Chair, presiding.

PRESENT:

GRAHAM B. WALLIS, ACRS Chairman

WILLIAM J. SHACK, ACRS Vice Chairman

JOHN D. SIEBER, ACRS Member-At-Large

GEORGE E. APOSTOLAKIS, ACRS Member

MARIO V. BONACA, ACRS Member

RICHARD S. DENNING, ACRS Member

THOMAS S. KRESS, ACRS Member

DANA A. POWERS, ACRS Member

VICTOR H. RANSOM, ACRS Member

I N D E X

P R O C E E D I N G S

8:29 A.M.

CHAIRMAN WALLIS: This is the second day of the 527th meeting of the Advisory Committee on Reactor Safeguards. During today's meeting, the Committee will consider the following: Digital Systems Research Plan; Status of Rulemaking on Post-Fire Operator Manual Actions; Future ACRS Activities/Report of the Planning Procedures Subcommittee; Reconciliation of ACRS Comments and Recommendations; Preparation for Meeting with the NRC Commissioners; and the Preparation of ACRS Reports.

This meeting is being conducted in accordance with the provisions of the Federal Advisory Committee Act. Mr. Sam Duraiswamy is the Designated Federal Official for the initial portion of the meeting.

We have received no written comments from members of the public regarding today's session. We have received a request from Mr. Alex Marion of NEI for time to make oral statements regarding the rulemaking on post-fire operator actions.

A transcript of portions of the meeting is being kept and it is requested that the speakers use one of the microphones, identify themselves and speak

with sufficient clarity and volume so that they can be readily heard.

During lunch time today, representatives of the Office of the Chief Financial Officer will provide a briefing to us regarding the revised policy for reporting labor hours.

That's all I have by way of introductory remarks. I will now hand over the chair to my esteemed colleague, George Apostolakis.

MEMBER APOSTOLAKIS: Thank you, Mr. Chairman. The Committee has been reviewing the Digital System Research Plan for more than a year now. We issued the first letter on June 2, 2004 in which we supported the efforts of the team that is developed the program and in that letter also there were several personal opinions written by me. Then the full Committee had an information meeting on May 6th of this year and then the Digital I&C Subcommittee met in June 14-15, 2005, and last month, October 20-21.

Today, we will be briefed on the plan by the staff and I believe they're requesting that we write a letter commenting on the plan. So to start the briefing by the staff, I will turn the presentation over to William Kemper, Chief of the Instrumentation and Control Section in the Office of

Nuclear Regulatory Research.

Bill?

MR. KEMPER: Thank you, George. Before I start, Rich Barrett is here.

Rich, do you want to say anything?

MR. BARRETT: No, that's okay, go ahead.

MR. KEMPER: Great. Good morning. I'm Bill Kemper. As George said, I'm the Section Chief of the Instrumentation and Control Engineering Section in the Office of Research. And I have my colleagues Steve Arndt here with me, who is a senior I&C engineer in our section as well. And between the two of us we will present the research plan.

We're here today to present the final draft research plan which covers the period 2005 to 2009. As George mentioned, we provided a fairly detailed overview of the research plan to the Committee back in May. Since that time we've continued to work proactively with our stakeholders, NRR, NMSS and NSIR to improve the research plan.

We've also, as George said, presented the plan to the I&C subcommittee through two different sessions which resulted really in three full days of interaction with the subcommittee and got a lot of very good insights from the subcommittee as well. We

appreciate the interactions with that committee and look forward to continued interactions with you all. It's really helpful to us quite frankly.

So today's presentation is going to be a higher level overview, if you will, than the last time we were here. And it will include the results of those interactions with the subcommittee, as well as our internal stakeholders.

We hope that these briefings on the research plan will provide the ACRS with sufficient information for the Committee to endorse our program to the Executive Director of Operations.

And also, we have a lot information, as before, to cover, in a relatively short period of time, so we will make our best effort to stay on schedule.

In terms of background, the current digital safety system review guidance is really contained in Chapter 7 of the Standard Review Plan which is several years old. That plan was produced in 1997. The SRP is adequate, but it's dated. We have already seen and anticipate receipt of more complicated and more extensive plant specific applications, thus the need to make the review process more effective, continues to grow.

The 2001 through 2004 research plan was primarily focused on NRR issues.

CHAIRMAN WALLIS: Did that plan succeed?

MR. KEMPER: We believe that we got a lot of good use from that plan, a lot of benefit to the Agency from that plan.

CHAIRMAN WALLIS: This new plan gives no reference to sort of approaches which were successful previously or anything like that, so it doesn't give the idea that you're building on anything.

MR. KEMPER: Well, it does indicate products that were produced through the efforts of the previous effort. There were various NUREGs that are mentioned throughout the various sections of the plan.

I do not have a compiled list of those things, but we could produce that for you, if you'd like at some time in the future. I'll go over this in just a minute. The current plan builds on the old plan.

CHAIRMAN WALLIS: You're going to tell us that, okay.

MR. KEMPER: Yes. However, in the past few years, the need to provide support to NSIR and NMSS has grown.

CHAIRMAN WALLIS: The output of this goes

to -- is going to be a chance in the SRP or something?

MR. KEMPER: It should result in changes to the SRP.

CHAIRMAN WALLIS: So how can academic work in universities which this seems to be directed at do anything for an SRP which is a regulatory document that is extraordinary unfamiliar territory for most universities?

MR. KEMPER: Well, that's just one of the outputs. Also, we expect to produce review, regulatory guidelines which we issue to the industry, numerous NUREGs that will provide the biggest --

CHAIRMAN WALLIS: Who is going to do that connection between this research and the real need?

MR. ARNDT: Steve Arndt. That's going to be done by a number of different people. Some of it will be done by other contractors. Some of it will be done by the research staff and some of it will be done jointly in collaboration with our stakeholders. For example, we're working right now on how to improve the technical tools and acceptable criteria for some of the on-going areas that are coming up in the regulatory space, for example, the on-line monitoring program that's been an academic exercise primarily for 10 or 15 years, but now is moving into the plants and

we expect license amendment requests within the next year.

CHAIRMAN WALLIS: Sometimes that's the most difficult part of the work.

MR. ARNDT: Exactly.

CHAIRMAN WALLIS: To make that connection between academic work and the real world.

MR. ARNDT: That's exactly the most difficult going from what is theoretically the right way to do it, to what is the specific acceptance criteria that is necessary. And as Bill will mention in a minute, the research plan is more geared this time for development of specific acceptance criteria to assist in review and update of the regulatory guidance.

MR. WATERMAN: This is Mike Waterman. Just as an addendum. In addition to developing acceptance criteria, we want to develop review procedures, step-by-step procedures that we have consistent reviews of safety system applications.

And additionally, we want to develop training curriculums that we can train and support our staff on how to use the review procedures, the tools and methodologies to assess acceptance criteria appropriately. So that's -- it's more of a product-

oriented function, where we want to put tools and procedures in the hands of our supported staff.

CHAIRMAN WALLIS: So the sequencing here is you first do the work in university and then someone looks at it and sees that it's suitable for your task and then tries to adapt it in some way to what you need?

MR. WATERMAN: Exactly. We want to develop --

CHAIRMAN WALLIS: I'd think you'd have to do it simultaneously, otherwise university may go off in some area which is very interesting, but doesn't really meet your needs.

MR. ARNDT: Professor Wallis, it's really a phrased approach and we'll get into this later in the presentation, but the 30-second version is we look out on the horizon, see what technologies might be important for us to understand. We develop the information or the technology or the tools. As that goes forward we will decide whether or not, if necessary, we have enough information, we have enough tools. If not, then we transition that into the tool development, the regulatory development, the Reg. Guide, whatever; then finally, the actual training and acceptance criteria and revision to the guidance.

MR. KEMPER: But in the final analysis, our contracting process really will control the scope of the work that's done by universities. We use cooperative agreements which are pretty well-defined, in terms of the goals and objectives when we work at universities. We use statements of work when we contract with independent contractors or laboratories which are very definitive in terms of what our scope is, the expected outcomes and the level of effort that should transpire.

So as I was saying, we've also noticed that NRR is not the only internal stakeholder that we should provide support to. For example, at fuel cycle facilities, there are fuel cycle facilities right now going through the licensing process that depend heavily on digital I&C systems. So we're participating with NRR to provide support to that effort.

So our current situation really that NRC is facing is a number of issues which I'm going to cover here. We expect that licensing, excuse me, that licensees will replace analog systems with digital systems as the existing analog systems become obsolete. Obsolescence of analog I&C systems is a real problem within the nuclear industry, and

routinely challenges the licensee staff in maintaining the maintenance of these systems. In some cases, licensees are having to resort to extraordinary measures to obtain replacement parts to keep these systems in operation. They're doing things such as mass procurements of RPSs and ESFASs, cabinets and all the peripherals associated with that; plants that have been shut down or where the construction was stopped at those plants. There's also somewhat emerging business with third party vendors to re-engineer these sector analog components such as pressure transmitters and nuclear instrumentation cabinets and modules and so forth, because the original OEMs or equipment manufacturers just won't support the equipment any more. They're either out of business or they shifted to the digital world because that's where the business interest is. And the rest of the sector process control is business.

So replacement of analog equipment with digital equipment is inevitable. There's no doubt about it. It's going to happen. Licensing these digital systems presents challenges to the NRC because of the increased complexity of the systems. Consolidation of discrete analog functions into a single digital process is typical. In the analog

world you have many things happening in parallel. All that is consolidated into one processor. It's all a sequential type of operation.

Also, potential consolidation of independent safety systems themselves into a single system such as combining RPSs and ESFASs on to one chip is something that we're seeing right now, being proposed to the Agency. And also, there's many new potential failure modes which we've discussed at length, involving digital equipment versus analog equipment.

There's also limited operating history of digital equipment in the nuclear safety-related applications. And to review licensee systems, it requires a significant amount of effort by the staff with specialized skills.

So current licensing guidelines provide information on what to review, but not necessarily how to review it or what the appropriate acceptance criteria should be. So that's really the angle that we're approaching here and the value that we're going to add to the regulatory process.

Also, there is a considerable industry interest in risk-informed digital safety system reviews, but the NRC does not yet have the needed

technical basis to support this kind of review.

MEMBER RANSOM: Does your definition of digital systems include wireless and optical transmission of data?

MR. KEMPER: Yes, it does. Also, in today's environment, cyber security safety-related digital systems is really important. And the staff is working, as we speak to develop regulatory guidance and we intend to assist them with acceptance criteria and some of the bases information needed to support that regulatory guidance in this area.

The operating history we have indicates that digital system failures may be of risk significance. For example, an analysis of the 1984 through 1987 accident sequence precursor or data indicated that a large number of risk-significant events includes I&C failures and that both safety and nonsafety systems contributed to these events.

In fact, 30 percent of the events were initiated by I&C system failures and an additional 10 percent of those events at least one I&C failure contributed to the progression of the event.

Also, an analysis of LER data show that many software system failures are context dependent, so it's not straight forward. In other words, it's

dependent upon the operational mode at the time, so the failure of digital systems various from one plant sequence to another and that many faults are introduced in testing and maintenance, as well as operations.

MEMBER APOSTOLAKIS: But that brings us back to a comment that was made some time ago regarding the distinction between a software-centric approach and a systems-centric approach. This is a very true statement, the failures are context dependent. However, in several places in the plan, you say, for example, that you will estimate the risk significance of the software. That is a little bit different than this because that implies that you are viewing the software as another component of the facility which, like a pump, will cover all or whatever. Whereas here, what you're saying is that really you can't do that because it's part of the integrated system, so I think it would be useful to recognize these things in the plan and make sure that the guys who are working on this issue are fully aware of it.

MR. ARNDT: The point here is that these are complicated systems that cannot be analyzed easily using the traditional methods we have available.

MEMBER APOSTOLAKIS: Right.

MR. ARNDT: And your point is well taken and in the areas which we'll talk about a little bit later in the presentation where we're looking at, particularly risk significance, but also other issues associated with software-driven systems, one of the big challenges for us is not only understanding the complexity, but also being able to differentiate which systems you need to analyze with very sophisticated methods and which ones you can get away with analyzing in a less significant way.

MEMBER APOSTOLAKIS: Which is an excellent idea and I'm not sure there is a section in the plan where this is addressed, the classification, in other words, because in some systems, you may, in fact, make sense to talk about the software as a separate component. In an actuation system, for example --

MR. ARNDT: Right. That is part of the research and we can go back and look at the plan before we finalize it and see if we can highlight that more specifically.

MEMBER APOSTOLAKIS: These two comment, these two issues that we just discussed I think are very important. The first one is classification.

MR. ARNDT: Right.

MEMBER APOSTOLAKIS: and the second one is to make sure that some of the items in the plan do reflect this context-dependence of the software, because if you read that section 3.3.4 or something like that, you clearly get the impression that you have a pump, you have a valve, you have the software. So what is the risk significance of the pump? What's the risk significance of the software? And that's not consistent with this.

MR. ARNDT: You're right.

MEMBER APOSTOLAKIS: It's obvious that you're appreciating the difficulty, but I think it should also be in the plan.

MR. ARNDT: Okay.

MEMBER APOSTOLAKIS: Because the guys who do the work may not appreciate it.

MR. KEMPER: Well, I believe and Steve will cover this in more detail during his portion of the presentation, but our risk element, I think, addresses that or attempts to address that as one total system. One concentric system, if you will. You can't really separate the software from the hardware. You have to treat it as a single system.

MEMBER APOSTOLAKIS: I noticed also at the subcommittee meetings, if one reads the plan without

talking to anybody, one gets a certain impression as to what the authors had in mind, but then when one talks to you, that there is really a much better picture, okay?

You gentlemen have thought through a lot of these issues, but a lot of that thinking is not in the plan and maybe you can try, if you have another chance to go over it, to make it reflect this kind of thinking. I don't recall a single case, but we asked the question and you didn't have an answer, but if you go to the plan, it's not always there.

MR. ARNDT: Fair enough. Thank you.

MEMBER APOSTOLAKIS: Okay, let's move on.

MR. KEMPER: Also a member of our staff, Mike Waterman, did a study that evaluated some potential common mode failures that have occurred in systems that are currently licensed in the U.S. over the past 10 years. And he produced a report, 20 some odd different events that represent software failures which could be construed to become mode failures under certain plant conditions and it includes things like the most recent Palo Verde Core Protection Calculator software bug you all probably heard about that. Palo Verde modified their RPS software to allow a failed sensor input signal to be ignored and maintain the

value of the last good signal. The licensee didn't ask for that, so I've been led to believe, but it happened. In fact, it missed the licensee's review and it was only discovered during a maintenance activity. Operations was made aware of it. They declared all four channels inoperable conservatively and resulted in a plant shutdown.

Also, there was a soft testing bug in the software for the Turkey Point load sequencers. They were upgraded to a digital system about 10 years ago and the system has a self-testing routine that is invoked quite a bit, but it's supposed to be interrupted when a real signal comes in. As it turns out, due to a bug, the real signal could not interrupt the self-testing routine and therefore when called upon, the system wouldn't properly actuate.

So these are just examples --

CHAIRMAN WALLIS: So this gets to my original question. What they're talking about here is giving some advice on the practice of how you detect false and so on in a plant.

MR. KEMPER: Yes.

CHAIRMAN WALLIS: That's very different from some academic doing a study on digital system faults. That could be very esoteric.

MEMBER APOSTOLAKIS: Maybe you need both.

CHAIRMAN WALLIS: Maybe we need both.

MEMBER APOSTOLAKIS: The field is so new.

CHAIRMAN WALLIS: We need some structure, intellectual structure coming from academia, but we've got to get down to the plant level.

MEMBER APOSTOLAKIS: Exactly. Just out of curiosity, is it really a problem for a regulator to say anecdotal evidence? If there is some suspicion shouldn't you get the damn evidence?

(Laughter.)

MR. KEMPER: Well, we chose that word just to say we haven't -- this is not a report that we intend to issue. We haven't spent a great amount of time putting this is in a format that we typically would issue to the public.

MEMBER APOSTOLAKIS: But you do what happened there?

MR. KEMPER: Oh yeah, we're very sure of the details that are in this table here.

MEMBER APOSTOLAKIS: Anecdotal evidence.

MR. KEMPER: I've got a copy of the table if anybody wants to take a look at it here.

MR. WATERMAN: This is Mike Waterman from Research. That isn't really a report. I was just

curious about well how many common mode failures have we had since say like 1990 or 1991, so I simply did a key word search on it. I think I started with digital systems or something like that, something simple. And I thought well, I'll get a couple here and then I'll have to refine it. And I found over 20 events just on that one key word and I was just building up a table for myself, if you will. It wasn't issued as a report or anything like that, just for my own reference. But I was kind of surprised by how many events have actually happened. When I went back sort of remembering all the different things and started adding them up mentally, I thought, yeah, I guess there have been a lot.

It turns out just about all the digital systems we've licensed at one time or another have had one problem or another occur in them and it's just like hm, maybe we ought to pay more attention to this.

MEMBER APOSTOLAKIS: Yes, it's fine to do that, but when you decide that on several occasions there is something going on, I presume you're going to find out exactly what happened?

MR. WATERMAN: Oh sure, the licensees always do their root cause analysis.

MR. KEMPER: Most of these are the results

of LER. It's documented. It's on the record.

MR. WATERMAN: Yes, these are LERs and event reports and Part 21 notices.

MR. KEMPER: It's just not our formal report that you can look and --

MEMBER APOSTOLAKIS: No, I understand.

MR. KEMPER: But the bottom line here is these operational events involving failures of digital I&C equipment indicates why this research is so extremely important. It's really critical that we understand how these systems behave and that we have objective performance criteria to review in licensee systems.

So all these things prompted a development of digital safety system research plan. In 1997, a National Academy of Science's report "Digital Implementation and Control Systems in Nuclear Power Plants" was reviewed. The Committee identified a number of key areas that should be explored, including system aspects of digital instrumentation and control technology, software quality assurance, common mode software failure potential, safety and reliability assessment methods, human factors and human machine interfaces and dedication in commercial off-the-shelf hardware.

In developing the previous research plan, the '01 to '04 plan, we research reviewed the NAS report recommendations and also I&C vendor-development efforts at the time and determined that the key areas for research really were in four areas: systems aspects of digital technology, software quality assurance, risk assessment of digital I&C systems and emerging I&C technology and applications.

CHAIRMAN WALLIS: And these four areas of research were actually carried out?

MR. KEMPER: They are in progress.

CHAIRMAN WALLIS: In progress?

MR. KEMPER: Yes. We haven't completed them. A research plan is a living document, if you will.

CHAIRMAN WALLIS: Whenever our review a research program, I want to know -- I usually look at the success of the previous one in order to evaluate my opinion of the second one.

MR. KEMPER: Right.

CHAIRMAN WALLIS: I don't want to get into that, except your written document gave me no clue as to whether or not the previous work was successful and where it was leading and all that kind of stuff.

MR. KEMPER: That's a good point. that

was pointed out also by the subcommittee and we intend to add a section to the research report that indicates the completed work.

MEMBER APOSTOLAKIS: Speaking of that, what is the plan? Are you planning to revise this document any time soon?

MR. KEMPER: Our plan is basically we're still looking at what came out of our last subcommittee meeting and any actionable items that came out of there we'll include that into the plan as quickly as we can and then we're hoping to wait until this Committee provides their letter to the Commission, excuse me, to the EDO and then we will issue that document under Carl Paperiello's signature to the other office directors with a copy to the Commission. That's the plan. And we intend to do that by the end of this year.

MEMBER APOSTOLAKIS: So that will be it?

MR. KEMPER: That will be it.

MEMBER APOSTOLAKIS: That's again for some period of time?

MR. KEMPER: Well, the plan is after that, I hope to update this on an annual basis. Rather than waiting another five years because it's such a dynamic world we live in. Things are going to change quickly

and so it makes more sense to me to update this on a shorter period.

MEMBER APOSTOLAKIS: Surely though some of the tasks of the previous plan will be completed soon and may have been completed already.

MR. KEMPER: That's right, they have been. For example, the Lightning Task. We talked to you all about that at the last committee meeting.

MEMBER APOSTOLAKIS: Yes.

MR. KEMPER: Many of the system -- research on the system aspects of digital systems are being completed.

MEMBER APOSTOLAKIS: And you said earlier you plan to have relatively frequently interactions with the subcommittee?

MR. KEMPER: Right.

MEMBER APOSTOLAKIS: I think this is an important topic, as we said earlier. It's fairly new. We all are really learning in various degrees, of course, and especially in some key areas, I would urge you to come to us before you have a completed product.

MR. KEMPER: Okay.

MEMBER APOSTOLAKIS: While your work is in progress, you have some ideas how to proceed and I think it would be useful to inform us and maybe get

some feedback.

MR. KEMPER: Absolutely. That's precisely what we would like to do.

So in developing the new research plan, we continue the programs that are in progress and refocus the outcome of the research projects to provide improved technical guidance for review of digital systems, to provide technical support in areas where program offices need to improve acceptance criteria and develop assessment tools and methodologies to improve the reviews.

Input to the plan was solicited from NRR program offices, NRR, NSIR, and NMSS. The draft plan was sent to those offices and thoroughly vetted with the technical folks in the three offices and comments have been incorporated. In fact, we held numerous meetings with the program offices to disposition their comments.

We also presented the results of these reviews in comment resolutions to the ACRS I&C subcommittee during the June meeting.

And as I said, the research plan has been reviewed by the subcommittee and comments are being incorporated.

So in the final analysis, we believe this

plan provides a flexible, adaptable framework for identifying NRR, NMSS and NSIR research initiatives needed to meet the challenge of licensing digital I&C systems for safety-related applications at nuclear facilities.

The research plan is structured to include the most important areas needed to support the program office. We have six programs identified in the plan. Four of them are carry overs from the previous plan with two new areas.

CHAIRMAN WALLIS: There's something really wrong with your previous slide. A framework for identifying NRR, NMSS and NSIR research initiatives? I don't understand that at all. You identify needs of those people and then you construct initiatives to meet them. I don't understand how this framework identifies those folks' research. This is your research.

MR. KEMPER: This research program --

CHAIRMAN WALLIS: Framework for carrying out research to meet the needs of those people. It doesn't make sense, that sentence.

MR. KEMPER: The plan provides a flexible, adaptable framework for identifying research initiatives needed to meet the challenges of the other

program offices in licensing digital I&C systems. That's what we're trying to say. In other words, they're our customers.

CHAIRMAN WALLIS: You'll put it right, okay.

MR. KEMPER: This plan is driven by the regulatory use of the products.

CHAIRMAN WALLIS: I hope so.

MR. KEMPER: It's not research just for the sake of research.

So the plan is structured, as I say, it has six programs. Four of them are carry overs, although there's new elements associated with each of those four areas and we have two new elements, security aspects of digital systems and advanced nuclear power plant digital systems.

These six programs represent 27 research projects at this point. We expect more will be produced as time goes on.

CHAIRMAN WALLIS: Now another thing I missed in all of this, you've got this very nice sounding scheme, you're going to do all these things. I had no awareness of the capability of the professional world out there to deliver any of this stuff. This could be just a pipe dream. We'll put

out this RFP, or whatever, and someone will do the work and magically the research product will appear. My sense of the field is it isn't like that. This is a rather beginning sort of field, particularly in security aspects, that people are struggling to come up with the right way to do things.

MEMBER APOSTOLAKIS: I mean, do you expect the plan to say this research will be done at such and such a place?

CHAIRMAN WALLIS: There are some people out there who are capable of doing it, otherwise, the whole thing is a dream.

MEMBER APOSTOLAKIS: Well, how would the plan reflect that?

CHAIRMAN WALLIS: I think you might have to say something about the realism of the plan somewhere.

MEMBER APOSTOLAKIS: That's a different --

MR. KEMPER: Well, if I could, the tasks in the plan represent the needs of program offices.

CHAIRMAN WALLIS: I understand that. That makes sense there.

MR. KEMPER: If the expertise doesn't exist, then we're going to have to work hard to try to find where that expertise is or grow that expertise.

CHAIRMAN WALLIS: Grow it, right.

MR. KEMPER: Within academia and --

CHAIRMAN WALLIS: Is there anything you can give us now? How far along are they in terms of meeting these needs?

MR. ARNDT: It depends a little bit on the particular area you're talking about and I'll highlight that a little bit when I talk about particular research programs.

To give you the 30-second answer, in some areas you're entirely correct, we have some real challenges associated with the ability to actually come up with enough specificity and techniques and methods and acceptance to get there. In some areas, we're surprisingly far along. There's been a lot of work either in various corners of the world or in various other safety critical applications that we hope to borrow from.

But as Bill mentioned, the idea is to work through those issues and improve the current regulatory process by providing the review procedures and the acceptance criteria. One of the biggest challenges associated with this, a lot of these technologies, is you can look at it, but frequently there's not the definitive acceptance criteria. How

good is good enough?

CHAIRMAN WALLIS: So there may be some areas where you simply figure out what you need to do in the next plan?

MR. ARNDT: Yes.

CHAIRMAN WALLIS: In order to get these research products that you want. I don't know if it's going to be all delivered at the end of this program.

MR. ARNDT: Right, and we'll highlight that issue.

MEMBER POWERS: Am I correct that you had prepared some fairly useful reviews of the field and indeed have presented that before the American Nuclear Society to kind of assess the field in this area?

MR. ARNDT: In several specific areas, one of the parts of the task is simply to understand the state-of-the-art and to know which areas we want to investigate further. The particular area that Dr. Powers is talking about is in the risk area. One of the areas we wanted to look at is what is the state-of-the-art? And we presented a paper in June at the ANS meeting, but that's true in several of the other areas as well. We have to understand where the state-of-the-art is and whether or not it is sufficiently well known to convert to the state-of-the-practice.

It's really fortunately or unfortunately, depending on your perspective of research, what we do is we convert the state-of-the-art to a practical document or a practical procedure or practical set of acceptance criteria for our regulatory counterparts to use.

MEMBER POWERS: I would just comment that the paper in this particular area was excellent and I thought it was a real contribution made to the Society to present this review of the state-of-the-art. And solicit input from the Society members on what they thought. That represents what I think is a good practice for the research program to share what their thinking is on a subject.

MR. KEMPER: I was going to say that's very productive because as it turns out all of us in the world are trying to solve the same problems because everybody in the world, in the nuclear world anyway, is trying to deploy digital instrumentation and control systems in their plant.

MEMBER APOSTOLAKIS: Yes.

MR. KEMPER: So we're all grappling with the same issue. So as a result of that there's a lot of information, a lot of energy being expounded throughout the world. It really is productive for us to do just what you said.

MEMBER POWERS: I think it's -- I know for a fact the paper elicited lots of thinking and discussion and you get free peer review there. It maybe worth what you paid for it, but it's -- I may you may get a real nugget there.

MR. KEMPER: Absolutely.

MEMBER APOSTOLAKIS: But just as an example, talking about peer review, you don't seem to mention any peer review in the plan for individual projects. Are you the only reviewers?

MR. KEMPER: Well, we have a peer-review process within the Office of Research.

MEMBER APOSTOLAKIS: Okay.

MR. KEMPER: That can be invoked any time we choose to do it. We do internal peer reviews ourselves, but for example, Steven did a project, started a project on software metrics where he called upon a peer review by various industry experts, if you will, in this field and got formal input from them and included that into the report itself, actually. We do that when the need arises.

MEMBER APOSTOLAKIS: Do you remember when we had the presentation here some time ago of work that was done at the University of Maryland and at the University of Virginia where the committee members

challenged several of the fundamental assumptions of the researchers who are, in my view, seemed to be surprised that they were challenged at such a fundamental level when they had used these approaches for railways and so on and nobody could challenge them.

Who is doing this challenging this time around? Is it you or the ACRS or somebody else?

MR. ARNDT: It depends on the particular project and the particular level of knowledge that exists in the industry and the particular level of controversy that exists, associated with particular concepts. In some cases, we try and get that input from knowledgeable sources, including the ACRS subcommittee, but also sources that are out there. For example, one of the peer reviews we did drew from members of the 1997 NAS Committee that were knowledgeable of both the general software, the general digital reliability community. In the case of the current digital system reliability program, we're drawing from people who are working digital system -- general reliability, but have some expertise in digital systems, like some of the people at Idaho, some of the people like Nathan Smith, Siu, I'm sorry, things like that, who are both internal and external.

It's a challenge because we have both conflict of interest issues and the fact that these areas in most cases are very small set of people are working in them and there's some level of controversy associated with it.

MEMBER APOSTOLAKIS: So what you're saying is that there some peer review, but you just didn't make it very formal in the plan?

MR. KEMPER: That's correct. And also, I'll be frank with you, that's why we're very excited about your subcommittee's existence as well because you all serve a lot of help for us, quite honestly, in asking those questions and challenging those concepts.

MEMBER APOSTOLAKIS: I'll tell you, flattery works with me. Let's move on.

(Laughter.)

MR. KEMPER: Okay, moving right along here.

MEMBER RANSOM: I would hope that you've looked at Japan because 15 years ago when I visited Japan with Ken Hanson on an assessment mission there, the Japanese were at this stage, actually doing research with digital systems for what they called advanced nuclear plants. So I would guess they have quite a bit of experience in this area. I don't know,

are you aware of that?

MR. KEMPER: Yes, yes, they do. Japan as well as Korea is another, and Taiwan as well. Many of the Asian nations are well along in a deployment of digital controls.

MEMBER APOSTOLAKIS: The Europeans have done a lot of work.

MR. KEMPER: That's true. I didn't mean to exclude the Europeans, but yes, specifically, you're right.

MEMBER POWERS: Koreans seem to be extremely aggressive in funding the universities to do particular studies and things like that.

I'm sure Steve is very aware of it, just his work for the ANS because we nearly always have a session on that particular area.

MR. KEMPER: That's correct.

MEMBER APOSTOLAKIS: I get a paper from Korea just about every other week on digital systems. They are extremely active.

MR. KEMPER: Yes, they are very much so.

MEMBER APOSTOLAKIS: They don't have an ACRS there, I don't think.

(Laughter.)

CHAIRMAN WALLIS: Regarding peer review,

I think you can expect the ACRS to give you a very high level review, but don't expect it to be the kind of peer review you really need.

MEMBER APOSTOLAKIS: The subcommittee gets into fair detail.

CHAIRMAN WALLIS: I think you need a peer review of experts in the field and real experts in the field.

MR. KEMPER: A fair comment, I appreciate that.

MEMBER POWERS: I thought you said there were no experts, only specialists.

CHAIRMAN WALLIS: I didn't say that. I don't know where you get that quote from.

MEMBER APOSTOLAKIS: From your long record.

(Laughter.)

MEMBER POWERS: You said everybody was struggling with how to proceed here.

(Laughter.)

CHAIRMAN WALLIS: No, I was asking --

MEMBER APOSTOLAKIS: We're still on Slide 7.

MR. KEMPER: Yes, I'm trying to move on here as quickly as I can.

In the final analysis, the research plan's broad base focusing on improving traditional review methods for reviewing existing digital technologies, analysis of emerging technologies and evaluation of issues arising from the application of digital technology. Also the plan focuses on improving the assurance of digital I&C system reliability which comprises many systems and components in the mitigating systems and security cornerstones of the reactor oversight process.

So how do we prioritize these projects? Well, this is the plan here. Basically, the inputs used to determine the priority of the research included completing on-going work, program office inputs, and also a balance between current regulatory issues such as diversity and defense-in-depth security; issues that are anticipated to be regulatory issues in the short term, such as field programmable gate arrays, on-line monitoring.

These are systems that are currently being -- they're over the horizon. They're almost right in front of us. We expect them to be deployed here soon and submitted for approval; and also following emerging technologies that might require future licensing reviews. Smart transmitters are examples.

The projects also support the NRC strategic plan, as indicated in Section 4 of the research plan. Each program has strategies supported indicated by them and as indicated in Section 4 of the research plan, each project has a relative priority, high, medium and low. These priorities were determined based on operational experience, program office request, such as user needs, and likely application schedule for the specific issue involved.

The projects have been scheduled based on available budget as well and resources. So we have a certain budget in resource and a certain number of I&C engineers and of course, that has to be a part of this equation here. As a result, the research plan is very useful in supporting the RES budgeting process.

That concludes my portion of the presentation. At this point I'm going to turn it over to Steven t to provide an overview of the program areas of the research plan.

MR. ARNDT: Okay, this next part of the presentation is just to give you an overview of some of the projects that are in the program. What we're going to try and do is work through this part of the presentation rather quickly, just to give you an overview of what we're doing, why we're doing it, how

we came up with the particular programs in there and just a little bit of a flavor for what some of those programs are.

As Bill mentioned earlier, the program is specifically designed to balance between looking over the horizon, trying to see what new technologies are available, what's going to happen. As we get more and more information about the particular programs, then we can decide whether or not we need to do specific research programs to develop specific regulatory guidance.

Most of that work is in the emerging technologies applications program which is Section 3.5 of the plan. Those programs will either be developed and worked in that particular section or moved into other parts of the program as they become more specific user needs.

The other parts of the plan are organized in a particular structure that just allows us to understand what we're doing and what we're trying to solve and issues like that.

I'm going to go through this. It's not in the order in which it's most convenient, 3.1, 3.2, 3.3. I'm going to go through it in a slightly different order because we did not get to some of

these areas when we talked to them in May. So we re-ordered it a little bit to make sure we get to the issues that we didn't address at the May meeting.

VICE CHAIRMAN SHACK: What fraction of this work is sort of actually directed at specific user needs?

MR. KEMPER: If I could -- let's see. I'm going to have to take a guess here. I would say maybe 20 percent has existing user needs. The rest of it was anticipatory research, although now that the research plan has been reviewed and we've collaborated with our offices, we no longer consider any of this work as anticipatory any more, although there may not be a specific user need number driving that, if it's an approved projects and research plan, we consider that the same as a user need.

MR. ARNDT: The first area I'm going to go over fairly briefly is the security aspects of digital systems. This is an area that if you go back to the earlier research plan, we had a very small little section and that was only added as part of ACRS discussions. Previously, this was an area that was covered in the regulatory review process in various areas of the standard review plan under some of the general design criteria, but we wanted to look

generally at this issue to see if it was a major issue.

Obviously, since 9/11, that has been elevated both in the general agency concern and also in the research concern of the plan. Attention is not only to safety systems, but also non-safety systems associated with security aspects within the plant: security computers, access control and also the various risk-significance of non-safety system applications.

We're also looking at how security issues are going to play out in the era of upgrading to digital systems. The increased use of digital systems, particularly in safety systems, but also non-safety systems and security systems is an issue. The current regulation consists of the particular rules and regulations that are already in part 50 and other places in the regulation, as well as the specific orders that were issued after 9/11.

We are in the process of supporting the rule making associated with this in NSIR and that's one part of this program, but also we're looking at the particular programs that have been approved, and will be put into licensing processes in the near future to understand the cyber vulnerabilities.

Just for your information, the color coding scheme that I have here is the blocks that are in yellow are programs that we plan on doing, but have not yet started. The blocks in green are the parts of the plan that actually have on-going research. So that gives you just a general feel for how much of this is currently working and how much of it is going to be --

MEMBER APOSTOLAKIS: So in future presentations, perhaps it would help if you had an extra box there with a different color saying work or part of the work here has been completed to satisfy Professor Wallis. Saying the previous plan for -- I know security was not done. In future, you can say the previous time we sponsored this kind of research and we have this product.

That would be very useful to everyone.

MR. ARNDT: Okay, and in this case this presentation is too high level to see that.

MEMBER APOSTOLAKIS: I understand.

MR. ARNDT: But there are certain projects under this general program that we have completed and --

VICE CHAIRMAN SHACK: You can put a progress bar.

MR. ARNDT: Yes. We can find some kind of graphic to make it look a little bit more apparent.

MEMBER APOSTOLAKIS: Hot red.

MR. ARNDT: Hot pink or something. As I just mentioned under the previous program, and as part of the early part of this program, we've completed some research in this area, both with under the research plan by the Office of Research, as well as some work that has been conducted by NSIR to look at specific potential issues.

During the subcommittee meeting, we went into a fairly high level of detail, both in general and in proprietary and safeguards information, so I won't go into it in detail here, but the research we did led us to the conclusion that additional work needs to be done to more clearly identify particular issues that might present challenges in new digital systems, particularly in areas like the protocols that are necessary, the communications that go on in digital systems, how you need to ensure that improper communication is prohibited, things that are associated with how do you deal with permanently installed connections for maintenance and things like that to reduce the likelihood that you could have a cyber vulnerability.

There's also been a lot of work associated with understanding what the criteria should be. The projects that are highlighted there, the power reactor pilot study and the licensee self-assessment methodology was work that was done with the industry and NSIR to develop a strategy for doing the analysis.

However, this is fairly high level information. Details of what is an acceptable methodology and what is an acceptable protocol and what is acceptable communication architecture is something that we're going to look at the future to try and understand and what the characteristics of these systems need to be to be acceptable.

One example of the work is the project that we'll focus on, the specific issues associated with communication protocol of assessments, evaluating safety/nonsafety interconnections, evaluating internal architecture of digital systems from the cyber security standpoint. These systems were originally designed to be interconnected and to be flexible and to have the capability to accomplish the protection and control function. The rules on which they were designed under never really looked at the concept of someone trying to hack into them as opposed to random failures or failures like that.

So we want to go back and look at it from a different perspective and look at much more detail into methodology that various people might use to attack these systems and what the appropriate methodologies would be to design architectures to prevent that and what the acceptance criteria would be and the policy associated with those.

Next I'm going to go over again fairly briefly the risk assessment portion. This is an on-going area of research, very active. We had at the subcommittee meeting an extensive briefing by the EPRI on their methodology and their proposed methodology. We talked extensively about some of the research that we have on-going, both the development of analysis of what data there is out there, both nuclear data and non-nuclear data, as well as the programs that we have on-going to look at the issues that Professor Apostolakis was mentioning earlier. What are the methods that are necessary, what level detail does the model have to be, how do you integrate this into current risk methodologies?

To briefly summarize the current situation, there's a lot of interest in doing this kind of work in the industry. There's a number of reasons why that is being driven. Some of the

traditional deterministic analyses drives the designers down a particular path that they would not necessarily like to go. So they're interested in understanding and looking at whether or not risk-informed or risk insights can get you to a different design concept.

EPRI has proposed a methodology. The NRC is also looking at various methodologies.

MEMBER APOSTOLAKIS: Have you reviewed the EPRI methodology?

MR. ARNDT: Yes.

MEMBER APOSTOLAKIS: Do you have an assessment of it?

MR. ARNDT: Let me be careful here. EPRI asked the Agency to do a review of the topical report. That is a specific regulatory act that looks at is it acceptable or not. That has not been done. The Agency has not done a formal review.

Now if you use the small case "R" review, have we reviewed what's in the document and assessed what we like and what we don't like about their proposed methodology, the answer is yes. And we did that for two reasons. One, as an input to NRR to determine if they're going to review it, if they consider it to be acceptable for review, enough

information, details and things like that.

The other aspect was to look at is there something in what they're doing that could be used in our research program for the Agency. We've done both of those and there are certainly some aspects of what EPRI has proposed that we can integrate into our research and we're doing that. However, we do have some issues with the methodologies that they proposed as well as some of the data that they've proposed.

MR. KEMPER: And the results of that review has actually been documented and sent out to EPRI.

MEMBER APOSTOLAKIS: I'd like to see that. Can I see that?

MR. ARNDT: Sure.

MEMBER APOSTOLAKIS: It looked to me like it was just a sensitivity study.

MR. ARNDT: There are some significant information that needs to be looked at and gone through.

We've also looked at a number of other things that have been proposed both in the nuclear industry and the non-nuclear industry. That third bullet there, there's a lack of generally accepted methodology to predict digital systems, failure

probability is, of course, almost a motherhood statement, but the converse to that is also true. There's a lot of methodologies out there with varying levels of pedigree and varying levels of implementation success that we're trying to use and understand and build on.

MEMBER APOSTOLAKIS: This is again an example of when you really have to be careful with the language.

MR. ARNDT: Yes.

MEMBER APOSTOLAKIS: This again presumes that there is such a thing as a failure probability of the software.

MR. ARNDT: Yes.

MEMBER APOSTOLAKIS: You might say there is a lack of generally accepted methodology to evaluate, to estimate the failure probability of a system that has in it digital software.

MR. ARNDT: Right.

MEMBER APOSTOLAKIS: That's really the correct way of saying it because after all, what we're interested in is a system performance.

MR. ARNDT: Right.

MEMBER APOSTOLAKIS: This presumes again there is such a thing as a failure probability of the

software.

If you recall, since you mentioned it in the National Academy report, there was a strong disagreement among the members as to what is the appropriate way. So that is coming back to you?

MR. ARNDT: Yes, and that is still an open technical issue and I suspect it will be for the foreseeable future. And really, the issue we have is there currently does not, in our opinion, there currently is not a sufficient level of acceptance to use this in the regulatory process, but it is rapidly coming to that, I think, in some areas technically, but more importantly directly coming to that in the regulatory process as licensees want to use this. We need one, either to have a good technical basis for saying no, you can't; or two, have a good technical basis for saying yes, you can, but if you do so you have these limitations on the use of this implementation of risk-informed or risk insights in digital systems.

MEMBER APOSTOLAKIS: As you know, what makes this whole field very difficult is that it deals with issues that are not dealt with in traditional reliability and risk assessment.

MR. ARNDT: Right.

MEMBER APOSTOLAKIS: Namely, to design a specific case analysis. And if you look at the PRA, we never really say the probability that this thing was manufactured incorrectly. We always assume it starts correctly and then we have some time dependence and so and that's what makes this extremely difficult. There are no methods out there.

MR. ARNDT: And point of fact, it's even more complicated than that because if you look at what data we have, it's actually a rather complicated convolution of specification issues, design issues, maintenance issues, actual coding issues and other things, some of which can be relatively straight forwardly modeled, some of which can't and some of which have different aspects to it.

The real issue is how much of this can we do and how much of it do we need to do. One of the issues that has been raised several times, including in the subcommittee is, as more and more systems include digital controls and digital protection systems, the plant PRAs, in essence, are becoming outdated, simply because they're not trying to address them, not only for the digital systems themselves, but of the embedded controls in a lot of the other large spinning parts and valves and things like that.

So the research program is designed as Dr. Powers pointed out, to look at the known capability of available models, both academic research level as well as actual implemented models in other technologies and what available technologies and data that are out there and use these methodologies to examine the most promising ones to see whether or not we can develop both regulatory guidance in this area, what's necessary, what the limitations are, what the specifics are, as well as internal check tools and methodologies to examine the analysis ourselves.

CHAIRMAN WALLIS: Do you have an idea of how adequate this information is that you're going to look at? Is it very sparse or is there a huge amount of it or is it of the right sort and that kind of thing?

MR. ARNDT: We've done several analyses of the methodologies, both looking from the traditional -- if we were to do this in a traditional PRA, using traditional methods, how would we do it and what are the limitations.

We've also looked at it from the opposite way, saying all right, if you take the most sophisticated methods that have been proposed, the most exotic stuff that's out there in the research

area, what are the ones that one, been used --

CHAIRMAN WALLIS: I was talking about the data rather than method. Is there a base -- in other areas of research you say we don't have enough data, so we have to do an experiment or we have to do something. Are you at the point where you put all the data in and you just have to analyze it or do you have to create it somehow?

MR. ARNDT: We have two issues with respect to data. We don't have a whole lot of data. There's two reasons for that. One, the systems have not been deployed all that long and two, many cases detailed root cause analysis is not done. The card doesn't work, throw it over your shoulder, put a new card in.

The other part of it is even if you have the data, you have to structure in such a way that you can actually use it. That is in some ways an even worse problem than the lack of data itself because some of the data analysis you can steal from other industries and you can build up data sources from cards and components and other things. The problem is the models frequently don't have the sophistication to get down to the point where you can use that built up data and you can't structure the data bases in such a

way that they support the models that we have.

So we're trying to do -- attack this on a number of areas. We have a couple of on-going data analyses and data-gathering projects. One is the International Database Program that's run out of OECD which is the Computer System Important to Safety database, the COMPSIS database which is gathering nuclear plant-specific data. Another is the on-going work we have at Brookhaven National Lab to gather generic component-type data.

Implicit in both of those is also looking at how do you structure this data and how do you put it together in a rational way to deal with it. The other part of that is in the analysis methodology, we're looking at how do you build experiments or tests or how do you write the analysis software or analysis methods to support testing information or analysis information instead of completely doing it on data. For example, if you want to understand how systems fail, you can look at mutation testing, or fault injection testing and things like that. Can you use that data to predict what you're actually going to get in a reliability kind of standpoint.

MEMBER APOSTOLAKIS: But it seems to me, Steve, that one of the true tests of a proposed

methodology is to take a piece of software, analyze it, find the fault which then the designer of the software admits it's a fault. Because just having data, you know, I don't know you can always do things and say well, my methodology caught this. And that was the first paper back in 1984, I think it was, in a master's thesis when they took a piece of software that was developed by Berkeley for one of their rockets experiments and they just did a simple 403 analysis and my goodness, they found an error.

We did the same thing at MIT and the designer was one of our guys. He finally admitted that there was an error there. He would have divided by zero under certain conditions, but his counter argument was that the probability that you would ever need to do that was so small that it really didn't matter.

I think that's a true test of a methodology. Now of course, most of the time you don't find anything because these systems are tested and reviewed and so on, so is that proof that it's not a good methodology? I don't know. It probably isn't because if there is no error there, you're not going to find it.

MR. ARNDT: One of the primary issues

we're trying to deal with in the supporting analysis part of the digital system risk area, as you know, you can't just have a risk model with reliability. We need something to support the reliability numbers, be it data analysis or whatever, is looking at those particular methodologies and for example, one of the methodologies is fault injection testing and there's been several examples of them finding these kind of issues. Another one is looking at state space analysis methods. They're basically a much more sophisticated software fault tree, to see if you can gain that kind of information.

MEMBER APOSTOLAKIS: But we're still on slide 17.

MR. ARNDT: Yes, I'm going to start working on it. Let me just recap this quickly.

MEMBER APOSTOLAKIS: No, Dr. Kress.

MEMBER KRESS: Eventually, you will want to take a piece of software and associated hardware and come up with -- you look at where it shows up in an event tree, for example, where it's called upon to do something to create some change in the system and what you want is the probability that this software/hardware combination will or will not screw up this event. You want to know, yes or no,

probability.

That's how you would use it in a PRA.

MR. ARNDT: Right.

MEMBER KRESS: Now the starting is starting from that is what your need is. I can see how you can get a probability of a hardware failure. That's just like other components, but you also need to add that probability that the software will fail, will fail to give the right output that would be needed to create this event.

MR. ARNDT: That's correct.

MEMBER KRESS: This seems to me like you ought to be able to take a simulator and you look at the exercise input space that this thing is going to see during sequences, severe accident sequences and you have uncertainties in that input space. You have uncertainties in the models that create the evolution of the sequence, up to the point where the event is taken.

Now you could Monte Carlo sample all that uncertainty and your problem is with a simulator you could actually look and see if there was a faulty output, but that's not all of it because no matter what you do, you're not going to sample all of the input space. But it seems to me like you could make

some judgment like what fraction of the input space did I sample and the fraction I didn't sample then you could say -- let's assume that fraction has an error in it and that ratio gives you the probability. Now is that one of your approaches?

MR. ARNDT: That is, believe it or not, a very simplistic way of looking at some of the methodologies that are out there.

MEMBER KRESS: Okay.

MR. ARNDT: And that's basically a concept of what is known as coverage that is to say how much of the model did you look at and you can make certain predictions on the amount of reliability or the bound of the reliability based on how much of the --

MEMBER KRESS: So that is one of the methods you're investigating?

MR. ARNDT: Yes. It's actually a little bit more complicated than that, but I won't go into that.

MEMBER KRESS: I was simplifying it, but I just now thought of it.

MR. ARNDT: The other issue really is how do these things interact with the rest of the PRA?

MEMBER KRESS: Yes.

MR. ARNDT: And that's really a major

challenge and when we talk about developing and testing methods, we're looking at how do you not only develop the methods, but how do you integrate it with the real PRA and that's very challenging because of the relative sophistication of traditional PRAs and what's necessary here.

But what we're trying to do is as the last bullets talk about is pilots and methods come up with issues and as Professor Apostolakis mentioned earlier, one of the big issues is to make a determination of what level modeling is necessary for what kinds of systems.

At the risk of truncating this prematurely, I really have to go on.

Another major area is software quality assurance and this is primarily an issue associated with how do we do our job of assessing the software in terms of the actual assessment methodologies, as well as how do you credit the various internal processes of the software and the hardware such as self-testing methods and things like that.

As Professor Wallis mentioned earlier, one of the big issues is there's a lot of stuff out there that has been done in the theoretical area, but very little of that is found practical application in

reviews. The way we currently review is we look at the system in the software specifications. We look at the development process. And we do some audits and thread analysis of the software products, the specification, the test plans, the coding and things like that.

The problem is, of course, that this can never be complete because of the complexity of these systems. It's very time consuming. It requires a high level of skill for the reviewers, not only the actual software analysis methodologies, but also how this thing is going to be used in the plant. And that's not something we find in every individual. As a matter of fact, we have a very limited set of people who can do that.

And in most cases, acceptance criteria is not quantitative. How many thread reviews do you have to do to have a good understanding that you're probably not going to have a problem. It's not something that easily quantifiable.

The current state-of-the-art in software system safety assessment, there's a lot of different methodologies that have been proposed and many of them have been just esoteric lab bench type things and some of them have been exercised in fairly sophisticated

systems in the aviation business, the transportation business and in NASA and other things. But the level of detail for real time safety critical applications in the nuclear business in most cases is very low or none. These include various software system analysis methods, Markov analysis, dynamic flow modeling and things like that.

MEMBER APOSTOLAKIS: Anyway, the latter, Tom, has a lot of the elements you mentioned.

MEMBER KRESS: Yes.

MR. ARNDT: Software metrics analysis, if you look at how the system is built and how the software is developed and what particular things they do, you can get a feel for are you getting all the bugs out? Are you testing it properly? Have you added bugs during the system? You can understand in a more quantitative way how good the software is likely to be.

There's a number of formal methods analyses which is basically the concept of formal proving of the software coding. This was something that was very, very popular about 10 to 15 years ago, fell out of favor because of the limitations associated with it. There are a lot of things you can't do very well with formal proof methods,

particularly in sequential time systems. That is starting to become a big deal now again, particularly in Europe. EDF has a major program in this area.

You can learn a lot and add a lot of additional insights by looking at formal provers, and then various testing techniques, data flow testing, mutation testing, fault injection testing. Some nuclear industry vendors are starting to look at these kinds of techniques to not only understand what they're going to find, but the potential vulnerabilities for particular places in the software.

CHAIRMAN WALLIS: You have to move on. You're putting a fault in, unless you find a fault that's already there. So a fault to catch a fault doesn't sound quite right. Can you explain that to me?

MR. ARNDT: There's a whole theory behind it. I'd be happy to do that.

The research in this area is basically focused on looking at the various methods and seeing whether or not there's any short-term applications to these methodologies that could be used to improve the review process.

We're currently looking at three of these areas: fault injection testing, the formal methods

analysis and the software metrics. And the idea again is to find ways to improve the criteria and the procedures that we use to make it more reliable and increase the probability that we're going to find things, if they're there, or understand the structure of the software better, so we can make a more quantitative consistent judgment of the software. And that's basically what this slide says.

MEMBER APOSTOLAKIS: Do you really need to address this issue?

MR. ARNDT: Say again?

MEMBER APOSTOLAKIS: Do you need to address the system aspects? Maybe you can go to the emerging digital technology?

CHAIRMAN WALLIS: I think you've got to jump ahead. There's an awful lot of material.

MR. ARNDT: Okay, I'll give you the two second version. There's a number of different projects in this area. The only one we're currently working on is the environmental stressors, however, there's a number of issues, particularly the defense-in-depth and diversity issues that we need to work on proactively. So that will be the next one that we start.

In the emerging technologies area, these

are the things that are over the horizon that we're trying to get smart about so we know whether or not we need to do more detailed analysis.

VICE CHAIRMAN SHACK: What is the time scale for starting these areas where you haven't -- we've seen an awful lot of yellow boxes here.

MR. KEMPER: That's laid out in actually Section 4 of the plan. We have scheduled first quarter like FY07, FY08, that sort of thing.

MR. ARNDT: To be in this plan it has to at least start within the time frame of 05 to 09, so it's anywhere from going on now which is a green box to starting in 07, 08 or 09.

MR. KEMPER: And obviously, these time lines will change. As priorities change, new projects come up and resources change as well.

MR. ARNDT: Basically, as the owners and the licensees and things continue to improve, we need to keep an eye on what's going on. We have both the specific projects. We also have a catch-all project that specifically goes out every two or three years and looks at the wide variety of what's going on in the digital system industry and looks at specific things that might work their way into specific applications. For example, we did the first one about

three years ago and one of the things that it highlighted was field programmable gate arrays which is now part of the research program.

So the on-going projects include the emerging technology evaluations which I just mentioned, the on-line monitoring which is something that we expect an actual application later this year and getting smart about tomorrow's technology.

This is just a basic overview of field programmable gate arrays which is starting to become a very big issue, as I mentioned earlier. It's one of the areas that EPRI -- I'm sorry, EDF is looking at very highly. Toshiba is also looking at this very highly. So it's something that we expect to have to deal with very soon and the big issue there is these things shift the complexity that might otherwise be in software to hardware designs and the tools that are necessary to design the hardware. And that's something that our review process really aren't geared toward.

MR. KEMPER: Now these FPGAs appear to be the next generation, if you will, of computer control systems and the benefit is that it has a way of eliminating software reliability issues. It's hard program, like a sea of gates that a program wants and

once that happens, you don't have to consider software failures if you will.

MR. ARNDT: We gave a last area which is the advanced nuclear power plant digital systems. This was originally put in the plan to be a catch-all for that research we're going to need to do to support the kind of advanced control rooms and advanced digital systems we expect to see in the next generation of reactors.

MEMBER APOSTOLAKIS: Shouldn't one of these at least be green? I mean we're already in the process of reviewing the ESBWR.

MR. KEMPER: You would think --

MEMBER APOSTOLAKIS: Can you help us with that?

MR. KEMPER: You would think that they would be.

MEMBER APOSTOLAKIS: I'm sorry?

MR. KEMPER: You would think so, but as it turns out, each one has a different story. The AP 1000 design, for example, has already been certified. ESBWR, we've been told by the vendor that they intend to use the ABWR process control system for that design. ACR 700, we don't have a design certification on the table yet. And pebble bed is too far out into

the future to know really what's going on.

EPR is probably the next best hope we've got of really getting meaningful process controls, research work started on that.

MEMBER APOSTOLAKIS: But your research here is participatory so you should start something before the EPR comes --

MR. ARNDT: Yes. We're in a bit of a bind right now because the designers and the vendors are telling us that they're planning on using current generation technology in these plants. At the same time, our gut feel says this is a first time we're going to have an opportunity to design a new glass cockpit time of system and we would really expect them to use the new technology that's becoming available to them to do more sophisticated protection and control systems.

So our kind of gut feel is telling us one thing and the vendors are telling us something else. So we're in a bit of a box here.

EPR is certainly going to be using some of the things they've learned from the N4 reactor development as well as some of the things that they've learned from their application of their standard platform which is the Teleperm platform in Europe.

But we haven't really got any insight on that.

MEMBER APOSTOLAKIS: Well, the PRA subcommittee is supposed to review the PRA of the ASBWR and I understand we're going to have a problem with the digital part.

MR. KEMPER: Very likely.

MEMBER APOSTOLAKIS: That is a user need. We're not a user, are we?

MR. KEMPER: You could be.

MEMBER KRESS: Let us know where we can help.

MR. KEMPER: Accuser.

(Laughter.)

MR. ARNDT: The areas, depending upon what actually comes in, we hope to look at, things like more use of artificial intelligence, autonomous controls and new instruments and things like that. And because of that, we've broken the research into instruments controls and risk issues associated with -- like you just mentioned, but we currently don't have a research plan in these areas.

So what we plan on doing is basically watch this area and trying to build into these programs.

At this point, I'm going to summarize and

turn it back over to George. We've developed this plan based on what we've learned over the last few years the research of the previous plan. It's based on a broad program, more consistent processes for regulating the applications. We particularly designed the program to look at bringing the technology into review guidance and acceptance criteria. We look forward to working with ACRS not only the implementation of the plan, but also the particular research areas as Professor Apostolakis has mentioned. We want to come back and vet some of these things, both as they come to conclusion, but also as intermediate milestones are achieved. And we also want to have the ACRS provide us input on how the plan can be better.

MEMBER APOSTOLAKIS: In fact, that's a very important point and maybe we can have a meeting or maybe meet with Mr. Thornsbury to give us some idea of what you see in the next year or two, where you would seem some subcommittee meetings or whatever.

MR. ARNDT: Okay.

MEMBER APOSTOLAKIS: It's really important. This is a very new area for everyone, so we should try to do it the way we did the Regulatory Guide 1174.

MR. KEMPER: Right, there you go.

MEMBER APOSTOLAKIS: And the participatory mode.

MR. KEMPER: Yes.

MR. ARNDT: Absolutely.

MEMBER APOSTOLAKIS: Any questions for the gentlemen presenters?

CHAIRMAN WALLIS: It seems to me you're going to have very carefully monitor the work. We find some examples in other areas which are much more dimensional and a contractor has gone off and done something and fields a report and it's a bad report. Well, it doesn't have to be a bad report. If it's properly monitored along the way, it's going to be caught early. And I think particularly in this area where I think you can take all kinds of paths, really close to what they're doing and help steer them. Give them enough freedom of thought, of course, but not let them go off and produce something which isn't what you need.

MR. KEMPER: That's a very high priority of ours, quite honestly. It's a point very well made.

MEMBER APOSTOLAKIS: Mr. Thadani will say a few words.

MR. THADANI: Yes. Early on in the review

of fuel reactor designs, the staff had utilized a design acceptance criteria process approach to approve digital-based systems such as protection system and so on. The motivation then certainly was that these reactors probably are not going to come on line for 15 to 20 years and the technology will have advanced significantly. And so there was a sense that perhaps we don't need to expend a lot of energy on this issue.

However, the environment seems to have changed. I'm a little bit surprised that you said that there's no research going on in terms of new reactors, given the people are talking about coming in with COLs in a couple of years. That surprises me quite a bit.

We're using an approach that was conceived probably 10 years ago.

MR. KEMPER: You're right. I find it hard to believe that a vendor will propose a brand-new advanced design with 10-year-old process control technology, but that's -- when we engaged them, that's what we've been told on a couple of occasions.

MEMBER APOSTOLAKIS: That's certainly an issue that needs further exploration.

CHAIRMAN WALLIS: One reason they might do that is because they don't have to review anything

that's more modern, on a scale that you wouldn't know how to review anything more modern. Therefore, they would be very conservative in their choice of equipment. So there's this problem of how far do you have to stay ahead of the vendors or you'd have to anticipate or do you have to just follow them all of the time.

MR. CAIRAMAZ: This is Matt Cairamaz, NRR. We were using the same process that we used for the advanced reactors back in 1999 for these new advance reactors also because for example, the EPR is going to be using the Teleperm XS platform which we already approved. And the AP 1000 and the COMMON Q platform which we approved. And the latest IEEE standard on the acceptance criteria for digital systems is we're going to issue the Reg. Guide 1.1.2 which has been through the ACRS already.

MEMBER APOSTOLAKIS: Which again, brings up the perennial problem. Since NRR can make all these decisions and be happy, why do we need this? We're going to go back to 1999? So if we're happy with what we did in 1999, there is no reason to do any of this.

Matt, it's not just your problem.

MR. CAIRAMAZ: One of the user needs that

we did, we did request our researchers to keep an eye for the advance technology that we used in nuclear plants and come up with guidance for us to review and that's what this is about.

MEMBER APOSTOLAKIS: Any other comments or questions to the presenters, the staff?

MR. KEMPER: I noticed Mike Mayfield joined us. Mike, did you want to make any comments?

MEMBER APOSTOLAKIS: Do you have any questions to the presenters, Mike?

(Laughter.)

MEMBER APOSTOLAKIS: You had your question in the past already.

MR. MAYFIELD: When you put it that way, I guess the one point that NRR wanted to make and I was hoping to be able to sit next to Rich when we were making it, a couple of times the staff has been before the Committee and there plainly were disagreements and differences of opinion.

Over the last few months we, both offices, have worked hard, staff and both offices have worked hard to communicate better, to work through areas where there was misunderstanding.

We're not 100 percent there, but we're a long ways further down that road than we were four or

five months ago and I think that's a tribute actually to the staff on both sides, from both offices to have gone into an open dialogue and have gotten us to a point where there is very strong agreement, not complete, but strong agreement on the vast majority of the work. So I think that's something that I've been very happy to see. I think Rich is similarly pleased with the progress we've made.

MEMBER APOSTOLAKIS: I am very pleased to hear that too.

Okay, thank you very much, gentlemen. This was very informative as usual and we will try to get your letter by the end of tomorrow.

MR. KEMPER: Thank you very much.

MEMBER APOSTOLAKIS: Mr. Chairman, back to you.

CHAIRMAN WALLIS: George, you'd made it almost exactly on time. Congratulations. We'll take a break until 10:15.

(Whereupon, the foregoing matter went off the record at 10:00 a.m. and went back on the record at 10:17 a.m.)

MEMBER DENNING: Thank you.

We are now going to hear from the staff regarding their recommendations to withdraw the draft

final rule regarding post fire operator manual actions.

In addition, Mr. Alex Marion of Nuclear Energy Institute has requested five minutes to share the NEI perspective after the staff's presentation.

The ACRS has previously reviewed this subject during a fire protection subcommittee meeting in October of 2004. And then a full committee meeting, the 517th full committee meeting in November of 2004.

In a letter dated November 19th, 2004, the ACRS recommended that the staff proposed rule on post fire operator manual actions be published for public comment. There were 14 sets of comments that were received.

After reviewing the public comments, the staff concluded that the rule would not result in a reduction in exemption requests and decided that the draft rule should be withdrawn. And that's what they're for with us today is to discuss that.

The principle issue that is involved is the requirement for automatic fire suppression systems as a prerequisite for the acceptability of manual actions regardless of fire hazard in the area. And I think that what faces us today is the decision as to

whether to accept the recommendation for withdrawal or whether to make a recommendation that the staff try to work a little bit harder to come to accommodation on a rule that would work.

And I think Senil Weerakkody, Chief of the Fire Protection Branch, will start off the discussion.

MR. WEERAKKODY: Yes. I'm Senil Weerakkody, Chief of the Fire Protection Branch.

Alex, could you go to Slide No. 2 please? What I'm here for is first I want to introduce Alex Klein. He's in my branch. He has been leading the manual action rulemaking effort for the last two years. So he's going to be providing you the presentation as to what public comments we got and why we chose to make the recommendation after reviewing the public comments.

Then Dave Diec -- he's from the Rulemaking Branch. He's been the rulemaking lead for the manual action rule.

The purpose of today's meeting is to inform the ACRS as to why after reviewing the public comment we are planning to recommend to the Commissioners that we withdraw the manual action rulemaking. And our objective is to get your endorsement for that action.

With that, I'm going to hand over to Dave.

MEMBER APOSTOLAKIS: So that's it? You're just withdrawing? No plans for anything else?

CHAIRMAN WALLIS: That surprise me. I mean there was a problem that the rule addressed. Are you just simply going to forget it?

MR. WEERAKKODY: No, there are -- we have a closure plan.

CHAIRMAN WALLIS: You have an alternative plan?

MR. WEERAKKODY: Yes.

CHAIRMAN WALLIS: Are you going to tell us anything about that?

MR. WEERAKKODY: Yes, we can.

CHAIRMAN WALLIS: Oh, okay.

MR. WEERAKKODY: I don't know whether this was part of our presentation but we have a closure plan in terms of bringing the whole issue to a conclusion through enforcement. And if you need, we can go into details of that. We prepared the presentation more focused on the detection and suppression issue.

MEMBER DENNING: I don't think we'll have to go into that in detail but we definitely would like to hear at a high level what that plan is.

MR. WEERAKKODY: We could do that.

MR. DIEC: Thank you. Thank you, Senil.

I guess I don't have to introduce myself again. Let me go directly into the background of the issue a little bit.

Back in November of 2004, we came forward and presented our proposed rule to the committee and asked for endorsement to have the proposal published for public comment.

Shortly after that, we received the endorsement letter from the committee, you know, agreeing with our recommendation to publish the rule for public comments. Also in that letter one of the committee members did raise a number of issues of which Alex will discuss in detail regarding the role of the suppression system and risk informed, performance-based opportunities.

W the staff published a rule back in March 2005 with the comment period ending in May 2005. During the opening comment period, the staff held a Category 3 public meeting to discuss the issue regarding about what the rule means and clarify to our best opportunity to make the rule more transparent and also receive a number of comments and feedback from the industry early in the process regarding about

their position about the proposed rule.

And the comment from the industry echoed mostly of which the ACRS member raised about the -- they wrote up a suppression system. And in September of this year, we also had a Category 2 meeting to convey to the public and stakeholders of our proposed recommendation to the Commission to withdraw the operating manual action rulemaking.

MEMBER APOSTOLAKIS: What category is the Category 2? Can you explain?

MR. DIEC: Category 3 is pretty much an interactive meeting of which we make more availability to ourselves to answer questions with the public involvement. Category 2 basically allows us an opportunity to present our case. And also affords the public appropriate time to make their comment as well. But not the interactive.

Our next step is to consolidate all the insights from reviewing of the public comments after May 2005 and developing our disposition to such comments. Our plan, of which you alluded to earlier, is a policy paper that lays out the staff proposed recommendation and direction moving forward.

With that, I'm going to transfer over to Alex. His presentation will go into greater detail.

MR. KLEIN: Thank you. My name is Alex Klein. I'm a Senior Fire Protection Engineer. I work in the office of NRR. I report directly to Senil Weerakkody.

Next slide please. We were actually here a year ago exactly to the day briefing you folks on the proposed rule. And what I'd like to do is just give you idea of what the key topics are that I'm going to spend some time on. I'll go through these very quickly and then we'll get into some detail as I get into the subsequent slides.

The first two bullets on safety and compliance and the purpose of the rule I'll discuss very, very briefly. I think most of you folks are already aware of what's going on there.

I'll spend time -- actually more time on the third bullet on the major stakeholder comments because it is, I believe, what the committee is interested in most. And furthermore, it's the area that the staff has received comments on and questions both from the ACRS and comments from the public.

And then the last couple of bullets I'll discuss the closure plan which, I think, has some interest on here at this committee. And then a brief discussion on our scheduling conclusion.

Next slide please? With regard to maintaining safety and compliance, as you all know, when we s tarted this rulemaking, we did state that feasible and reliable GII operator manual actions are safety in spite of them being in noncompliance.

We've been continuing inspections and we have enforced our regulations whenever we found non-feasible operator manual elections. When e found feasible manual actions, we have cited these manual actions as non-compliances. And request that the licensee include those items in their corrective action program.

We plan to continue this inspection activity with a focus on any manual actions that are risk significant.

Next slide please.

CHAIRMAN WALLIS: Now is this a major burden going all this inspection and handling everyone of these manual actions individually?

MR. KLEIN: This -- the inspections are part of our reactor oversight process under the Triangle Fire Protection Inspections. Inspectors go through that process and if they come across any non-complaint operator manual actions, then we'll determine the significance.

CHAIRMAN WALLIS: But how much of a burden? I thought part of the rule was to clarify things and remove the burden of having to decide on each one of these manual actions.

MR. KLEIN: Part of the rule, if it had gone through, part of the proposed rule would have removed that part of the burden. However, as part of the inspection process, if the proposed rule had moved forward, inspectors would still determine and inspect the licensee's feasibility and reliability determinations of that operator.

CHAIRMAN WALLIS: They still do much the same work?

MR. KLEIN: I'm sorry.

CHAIRMAN WALLIS: They still do much the same work if the rule had gone forward?

MR. KLEIN: It may very well be, yes, sir.

VICE CHAIRMAN SHACK: But if you find it is feasible, do you still have to go through a significance determination process for the finding?

MR. KLEIN: Today yes.

VICE CHAIRMAN SHACK: Today? How about -- okay, I mean and that will continue to be true?

MR. KLEIN: Under -- if the proposed

rulemaking is withdrawn, yes.

CHAIRMAN WALLIS: If it went in -- if the proposed rule went through, would it reduce this burden of the significance determination?

MR. KLEIN: If a licensee implements an operator manual action under the proposed rule that is determined to be feasible and reliable, then we do not go through that process. However, if an inspector determines that or questions the determination of feasibility and reliability by the licensee, then we may very well reenter the SDP, yes.

MEMBER DENNING: But if the rule went through, then he could very well be in compliance with the rule depending on what the conditions of the rule are.

MR. KLEIN: That's correct, yes.

MEMBER APOSTOLAKIS: Could you say a few words about what you mean by feasible?

MR. KLEIN: We talked about this last year. And yes, I can address that. We have a set of criteria that we have in the proposed rule to establish the feasible of an operator manual action. That basically establishes that the operator manual action can be done.

And, of course, with your input initially

in the development of this rulemaking, we also developed reliability criteria to establish and to ensure that the action can be done on a more likely basis with high probability of success.

With respect to the purpose of rulemaking, I'll spend a very brief amount of time on this slide because we're all very well aware. The primary purpose of the rulemaking was listed in SECY-03-0100. And two of the primary purposes of that rulemaking was one, to codify the use of manual actions and its acceptance criteria, which we did under the proposed rule.

And the primary purpose was to avoid the need for numerous exemption requests. And that, I think, is one of the things that we're going to talk about in some level of detail. And I'll talk about it in some subsequent slides.

I want to point out to you the staff requirements memorandum that the Commission issued to the staff in January of this year that approved publishing the proposed rule.

The Commission directed the staff to engage stakeholders to get a clear understanding that the proposed rule would indeed achieve its underlying purpose of avoiding the need to process numerous

exemption requests. We received written comments from a variety of stakeholders at the close of that comment period.

The SRMs also directed the staff to add a statement to the proposed rule, supporting language, a statement of consideration that clearly pointed out the Commission's view with regard to exemption requests. And what I've done is I've placed a quote on there.

And what we believe is that the Commission's statement makes clear their view regarding exemption requests and the options available to licensees with respect to operator manual actions.

Next slide. As the ACRS member indicated after the close of the public comment period on May 23rd, 2005, we received 14 sets of comments. Of the 14 sets of comments that we received, five were from individuals of which four opposed the rule outright and one provided detailed technical comments.

Detailed technical comments were also received from the Nuclear Information and Resource Services, NIRS, a public interest group who also opposed the rule. But they advocated codifying acceptance criteria of the proposed rule Section 3(p).

We also received -- the majority of the

comments that we did receive were from industry, industry consultants, and from NEI. And I'll go over those major comments in detail in a couple more slides.

In addition to the comments received to the proposed rule, the NRC had previously received comments from several hundred people, individuals opposing our plan to issue the operator manual action rulemaking. These comments were received under our Federal Register notice to publish an enforcement discretion policy back in November of 2003.

In terms of the rulemaking process, the staff analyzed the comments, considered the comments made by the stakeholders. Many of the comments were the same or similar in nature so you'll see that I've grouped them together in a couple more slides. And I'll highlight some of these.

MEMBER APOSTOLAKIS: Is it common to have several hundred individuals comment on anything? Or was it a campaign behind it?

MS. McKENNA: This is Eileen McKenna. I'm the Branch Chief in Financial and Policy in NRR. We have -- I think you're right. Many of these comments were almost form letters and repetitive-types of things. And we do see, on occasion, campaigns if you

will, websites where people can find proposed comments to submit, and we will get repetitive comments.

So I don't think it is unusual in that regard. We had one on one of our rulemakings. It was petition on design basis threat where we had that experience as well.

CHAIRMAN WALLIS: I think these comments from industry and from NEI were the same, weren't they, as had already been made at our meeting here a year ago. So we didn't really need to go out for public comment to know what their response was. Isn't that true?

MR. KLEIN: That's true to some extent.

CHAIRMAN WALLIS: So but you still put the rule out and then getting the same comments again, you decided to back off.

MR. KLEIN: Yes, sir.

CHAIRMAN WALLIS: You didn't back off before. But nothing had changed.

MR. KLEIN: I'll ask the rulemaking branch folks to respond to that. But what I can say is that the comments that we did receive from the industry were in public meetings and were verbal. I think that there is a process that the staff needs to go through when we go through proposed rulemaking.

CHAIRMAN WALLIS: Yes, I understand that. I understand.

MS. McKENNA: I think that's correct.

MR. KLEIN: Right.

MS. McKENNA: And also that by putting the notice in the Register, we can solicit comments from any stakeholder who chooses to comment, not just those who are participating in the meetings.

CHAIRMAN WALLIS: Yes, but it still means that it changed your mind. And you already had the information before. I'm a bit surprised that just getting it written down changed your mind when getting it orally didn't.

MEMBER DENNING: You can proceed.

CHAIRMAN WALLIS: But anyway, go ahead.

MR. KLEIN: Next slide please. This slide lists the major stakeholder comments. The comments that are bolded, if you'll note at the top, are those that I'll go into more detail in the next few slides. And those bolder comments are also those that this Committee had some recent questions and comments on. And to which I'd like to address individually.

If you'll allow, I would just like to briefly go over each of these comments with the intent of addressing each of the bolded comments in some

subsequent slides.

With respect to the requirement for automatic suppression, the comment was made by the industry and by NEI that that requirement is unnecessary. The comments were primarily directed, however, at the requirement -- even though the comments were made, the requirement includes fire detection and suppression. The comments were primarily made with respect to automatic fire suppression. And again, I'll get back to that in a little more detail.

With respect to the comment made that numerous exemptions will still be needed, as you are aware, one of the primary purposes for the rulemaking was to avoid the need for licensees to prepare exemption requests. And, however, many industry comments were made stating that numerous exemptions or costly modifications will be necessary in that the proposed rule would not achieve its intended purpose.

With respect to the alternative rule language, alternative rule language was proposed by NEI in their comment letter.

CHAIRMAN WALLIS: I think you're on Slide 14 now?

MR. KLEIN: No, sir.

CHAIRMAN WALLIS: Well, I'm following you. And you seem to be --

MEMBER DENNING: He's going to go over them again.

CHAIRMAN WALLIS: Oh, you're going to go over them again. I see.

MR. KLEIN: In very brief detail. I just wanted to give you a flavor for each of these if I may.

CHAIRMAN WALLIS: Excuse me.

MR. KLEIN: The alternative rule language that NEI proposed basically defined certain terms in 3(g)(1) and proposes no changes to existing wording in 3(g)(2). And stated that the criteria that's in the proposed Rule 3(p) is not necessary.

With respect to the inspection procedure, there was a comment made by NEI that their position is that the inspection procedure criteria that is listed in the back of that inspection procedure provides sufficient criteria for determining the feasibility of operator manual actions. And again, I'll get back into that in a little more detail.

The next four I'll discuss fairly quickly. Even though the time margin and time margin factor was an issue that we discussed last year in some great

detail, there were a number of comments that were made from the industry with respect to time margin and the time margin factor that is contained in the draft regulatory guide.

With respect to time margin requirement, a number of commenters indicated that the licensee's thermal hydraulic analysis and calculations and other types of analyses have inherent conservatisms that accounts for the time margin.

The comments also objected to the time margin factor of two stating that it is arbitrary, it is unprecedented, and not consistent with requirements for other plan programs such as emergency operating procedures.

The staff has taken this comment into consideration in the treatment of any criteria that may be issued for internal staff guidance. However, we would retain the concept of time margin. We believe that that's a very important concept to retain.

With respect to comments on the proposed rules of backfit, some commenters continue to state that the proposed rules of backfit and that the use of operator manual actions is within the regulations. The staff disagrees with these assertions.

As stated in the past -- and as supported by CRGR, the regulations do not identify the use of an operator manual action as one of the three means of compliance in Section 3(g)(2) of Appendix R.

There was a comment made with respect to missing an opportunity to risk inform and performance base this rule. The NRC disagrees with this contention in that we've already promulgated a risk informed performance-based rule under 10 CFR 50.48(c) that addresses fire protection as a complete program.

There were comments made by the public interest groups that asserted that the proposed rule abandons defense-in-depth. And that it would undermine the Agency's safety oversight and abandon its enforcement responsibility.

It was further asserted that the proposed rule would overlook security-related fires.

The staff does not agree with these assertions. We believe that we've provided the bases for the proposed rule and that it adequately addresses defense-in-depth.

The reactor oversight process and our inspection of plants continue to be done in accordance with our processes and policies. Enforcement would also continue in accordance with our procedures and

policies.

With respect to security-related fires, the staff recognized this when we wrote the proposed rule. We decided during the proposed rulemaking process during the proposed rulemaking period, that the security-related fires needed to be addressed on a more global and comprehensive basis rather than piecemeal through individual rules.

Next slide please. Industry stated that the requirement for an automatic fire suppression system is not necessary and that the installation of such systems would be costly without a clear safety enhancement and will likely result in more exemption requests. They also stated that existing fire hazards analyses have already determined where an automatic fire suppression system is required in the plant.

The staff has considered the comments and continues to maintain that the fire detectors and automatic fire suppression system requirement in the proposed rule is essential to ensure defense-in-depth and is fundamental to fire protection regulations. And we discussed this with you folks in great depth a year ago. And the same with the fire protection subcommittee.

Under the proposed rule, licensees would

be allowed to implement operator manual actions as a fourth compliance option to the requirements of 3(g)(2) where redundant trains are located in the same fire area. This fourth compliance option relies on the success of the operator manual action to safely shut down the plant in the event of a fire.

Because of the relatively high failure probability of an operator manual action, the staff believes that the defense-in-depth provided by automatic suppression is essential.

With respect to fire hazards analysis, fire hazards analysis is a deterministic type analysis and is done by considering items such as, you know, the type and quantity of combustibles, the location of the hazards, the geometry of the area, and other factors such as ventilation and available manual firefighting capability. However, a fire hazards analysis does not account for the failure of the manual action.

For these reasons, the staff included the requirement for automatic fire suppression in the proposed rule.

MEMBER DENNING: Let's spend a few minutes on this --

MR. KLEIN: Yes.

MEMBER DENNING: -- because I think this is the essence of whether we can -- how you proceed.

The one alternative that the industry now has is to go through the risk-informed process. And if one looks at how manual actions are going to be taken into account in that process, and it is somewhat speculative, but basically we can almost be assured that based upon risk assessment and the risk significance of an area that the arguments will be made that manual actions should be approved without the requirement for fire suppression systems based upon the low risk from that area. There will be arguments about the low risk from that area.

And the way the process is set up, I suspect that those arguments will be accepted. I mean the process isn't critical of that. So that I see for areas that have this low-risk significance, that they'll be allowed to have manual actions without fire suppression systems.

The industry argument about the fire hazards analysis is pretty similar. That is, they say that we go through a fire hazards analysis and we determined that combustible loading is not high enough to really sustain fires in an area. And it doesn't need sprinkler systems.

So they've already gone through that analysis for an area. And based upon that, they said we don't need a fire sprinkler for that area.

But with the rule you now have it, it would be required, that even though the fire hazard analysis said it didn't need a sprinkler, you would need a sprinkler because you have the manual action. So that I think that what we wind up with is quite an inconsistency between how the same room would be treated in Plant A that goes through risk-informed analysis and Plant B that is identical but goes through the deterministic analysis.

And they really would wind up in the same place, then I don't see why we would be so sticky about this question of do we really have to have the sprinkler system in addition to the manual action when we do have some evidence that fire isn't at the same level of concerns as those areas where there are sprinklers.

So again I raise the question along those lines.

MR. KLEIN: Let me respond with respect to the 805 process. Yes, I agree, it is a risk-informed method of establishing a new fire protection licensing basis. And perhaps there may be situations where it

may very well be appropriate to implement an operator manual action.

With respect to whether a suppression system is required or not, when you look at the risk, one other aspect that an 805 licensee would have to make a determination on is the effect that say removal or not putting in place a suppression system is their determination of adequacy of defense-in-depth.

So a licensee under the 805 process would not simply look at the risk numbers. They would also make that determination of whether or not a suppression system is required --

MEMBER DENNING: Yes.

MR. KLEIN: -- with the defense-in-depth.

MEMBER DENNING: Yes. But I would be willing to make a little bet as to how that answer comes out for the majority of those cases. There's one other thing I'd like to pursue and that is the inspection guide that is used now which determines whether -- in the inspection process whether a noncompliance is really a serious noncompliance or a not serious non-compliance.

And it says in the inspection guide that in those cases, it is okay that you don't have to shut the plant down and fix something because the safety --

because these are low safety concerns.

I didn't see anywhere in the inspection guide where the requirement would exist for fire suppression in that determination. Am I wrong? Is there a requirement? In order to be found to be a low safety significance for a manual action, in that inspection guide, do you have to have a fire suppression system operable? Automatic?

MR. KLEIN: Yes. Let me respond to that. If I can go to Slide 15 please?

The inspection procedure was written and had attached to it the criteria. And the acceptance criteria in the inspection procedure was provided back in March of 2003. And that was provided for inspectors to determine whether or not an operator manual action is feasible with respect to a licensee being able to take credit for that operator manual action as a temporary compensatory measure.

So with respect to how we use the criteria in the inspection procedure, it was done under that type of consideration with respect to an interim compensatory measure.

With respect to whether or not suppression was actually listed as a requirement as one of the criteria, the criteria were provided to establish the

feasibility of the operator manual action. The requirement for automatic suppression or detection is part of the rule under 3(g)(2).

So an inspector would come in and make that determine that judgment and determine the risk when they go through the STP process considering wither or not automatic suppression would provide that level of defense-in-depth and safety required.

So in terms of it not being listed in the criteria, I think it was because we listed the criteria only to establish the feasibility of the operator manual action. Now I'll ask any of the staff to clarify what I've said because I wasn't here when they issued the inspection procedure back in March of 2003. But, however, I believe that's the basis for it.

And I don't know of Senil has any additional comments to make.

MR. WEERAKKODY: The criteria that they put together in the inspection guidance -- obviously the inspection guidance doesn't go through the same rigorous review process the rule criteria goes through was a tentative mission for us to move forward with this issue by a rulemaking or any other means and then keep the plant safe during that time.

There is a big difference between what were existing under inspection guidance, which is an internal document. When we entered the rulemaking process, rightfully so, we come to you, we go to all the stakeholders and we get feedback. And one of the things we learned was that feasibility was just not sufficient.

We need to have feasibility and reliability for these manual actions for a self-implementing rule because once the rule is approved, the licensees could, on their own, approve these manual actions. So the quality or the objective of the criteria is going to be a step up in a rule as opposed to inspection criteria.

MEMBER DENNING: I understand your position.

MR. KLEIN: Okay. Let me add something about the fire hazards analysis aspect of it also. And maybe we can go to Slide 13 because I think that has some connection to it.

With respect to the comments that were made with the numerous exemptions, when we try to write a rule, we try to write the rule, as Senil indicated, we try to write a rule that is objective, that's clear, and is such that it is inspectible and

enforceable.

And if we try to put a rule in place where we provide a licensee exceptions to where, for example, a suppression system may not be required because there are no combustibles at all in their fire area, I believe.

And I believe that it is the position of the Agency that it may not necessarily cover all situations out there in the plant because each case of an operator manual action in a specific location in a plant is specific to that configuration and the plant's ability to have suppression in that area.

We further believe that if we provide language, rule language, that would provide exceptions that we would not be contributing to clarity in our regulations again because of the specificity of the situations. And that's basically why we have the requirement for automatic suppression as part of the rule.

MR. WEERAKKODY: One thing I'd really like to add to this important topic based on the questions you asked Dr. Denning, with respect to suppression, if you -- we are in no way holding 805 and non-805 plants with different safety standards with respect to manual actions. If you go to the 805 code document and the

main rule, all licensees who go to 805, unless their manual action already is approved, they have to re-analyze each of those manual actions using performance-based/risk-informed methods.

And as you can recall with our discussions on the reg guide and the number of questions you had on MEFS, LFS, you found out how much analysis the licensee has to do and document in order to use manual actions in an area without suppression.

So you are correct. And 805 plant can have situations of manual actions without suppression but they will do it after following a very deliberate, very thorough process with five PRAs and, you know, they are using money to do all that analysis.

MEMBER DENNING: You can return to your --

MR. KLEIN: Thank you. Let's stay on Slide 13 then. And I think we covered most of these items.

The staff understands that numerous exemptions would be submitted. And I think that we're talking about -- the crux of the matter is the fact that we have the requirement for automatic suppression in the proposed rule.

And I discussed with you previously in a couple of slides the bases for why we believe

automatic suppression is appropriate for ensuring defense-in-depth.

So if I could just go on to the next slide, Slide 14 with respect to the alternative rule language proposed by NEI. As I indicated, NEI did submit some proposed alternative rule language. The staff did consider this alternative rule language but we did conclude that the language would not ensure defense-in-depth.

Basically the language would allow the use of manual actions in areas with redundant trains under the assumption that the manual action is successful in ensuring that one train remains free of fire damage. Aside from the conflict that this would impose with Section 3(g)(2) and 3(g)(3), the alternative language does not ensure feasibility and reliability of the operator manual action absent acceptance criteria as part of the rule which was not proposed in the NEI rule language.

Furthermore, we believe that the lack of again, the automatic fire suppression system is essential to defense-in-depth as we previously discussed. So it is for those reasons that the NRC -- that the staff concluded that the alternative rule language would not adequately address our concerns.

Let me skip over Slide 15 I think. Unless the Committee has some further questions with respect to the inspection procedure, I'll skip over that one.

CHAIRMAN WALLIS: Well, all your slides so far seem to reap up the public comments and support issuing the rule. I don't have any rationale yet for withdrawing it.

MR. KLEIN: I'll get to that if I may.

This slide basically states the recommendation that the staff will make to the Commission to withdraw the proposed rule.

CHAIRMAN WALLIS: It doesn't follow from what you just said though.

MR. KLEIN: I'm sorry?

CHAIRMAN WALLIS: Okay. You're going to tell us the rationale after that?

MR. KLEIN: Yes, sir. Slide 17, if I may.

Okay, the industry certainly was very clear in their response stating that a substantial number of exemptions would still be needed under the proposed rule. Given the industry's positions and assertions, the primary purpose of the rulemaking certainly would not be achieved.

The assertion of the large number of exemption requests would also not meet the

Commission's staff requirements memorandum view of exemption requests. That's the slide that I had up there previously.

The SRM provided the Commission's view that although the exemption process is available, the Commission considers the rulemaking or 10 CFR 50.48(c), which is NFP 805, more desirable in order to minimize the need for future exemption requests.

Since a substantial number of exemptions would still be needed, it's clear that the Commission's view and direction would not be met. 10 CFR 50148(c) is available to licensees as a risk-informed alternative to minimize exemption requests and solve the kinds of issues being addressed in this proposed rule.

This alternative also meets the Commission's SRM view and direction without a new rule. Furthermore, the majority of the comments from the industry and the public clearly did not support the proposed rule as written.

And I've got some quotes here which I'll just skip over with respect to time.

And so basically, based on the above reasoning, the staff will make a recommendation to the Commission to withdraw the proposed rule.

CHAIRMAN WALLIS: Well, I'm not sure you've been deterred by stakeholder comments in the past. And that's not the real reason for voiding a rule.

MR. KLEIN: Well, it is -- I mean part of the reason is the Commission in its SRM really does say if you determine that it isn't going to reduce the number of exemptions --

CHAIRMAN WALLIS: I understand -- I can understand that rationale. But the fact that a few comments from industry object isn't really a good reason for backing off since all your previous rationale supported the rule.

MR. WEERAKKODY: Can I add something Dr. Wallis?

One of the things that I think Alex is going to mention or has not mentioned yet is that when we issued Appendix R, the old fire protection rule, and we turn around and issued about a thousand exemptions, and that's kind of like backdooring or circumventing the rule. So with that background, you know, we can't issue a rule with the full knowledge that the only way to comply with the rule is by pursuing another hundreds of exemptions. That's unacceptable to how we do business.

We had to do it for Appendix R because the courts asked that we do so.

MEMBER DENNING: But isn't there a set of problems out there where there actually are fixed suppression systems. And by including this, they will not have to ask for exemptions for those?

MR. KLEIN: That's correct. If you look under the requirements for Section 3(g)(2), 3(g)(2)(b), which is a 20-foot separation requires a licensee to have installed automatic suppression and detection. Section 3(g)(2)(c) with a one-hour fire barrier also requires detection and suppression.

So really what it comes down to is Section 3(g)(2)(a) which is the three-hour fire barrier which was deemed adequate enough for train separation at the time Appendix R was written without automatic suppression.

MEMBER DENNING: Okay. Continue.

MR. KLEIN: Okay. So are we on Slide 18, yes, our closure plan, which I think that you'd like some discussion on. Of course we're developing a policy paper that will recommend withdrawal of the proposed rule. That's ongoing right now as we speak.

The staff also plans to issue a regulatory issue summary that will communicate our regulatory

compliance expectations.

CHAIRMAN WALLIS: If they look something like the rule you are withdrawing, nothing much will change except it won't be a rule. It will just be a somewhat weaker document. You still seem to have the same expectations.

MR. KLEIN: What we will reiterate, Dr. Wallis, in the risks is our compliance expectations with regard to the fact that the use of operator manual actions under 3(g)(2) is prohibited by regulation unless a licensee has an exemption to that effect.

CHAIRMAN WALLIS: So it's just status quo then?

MR. KLEIN: Yes, it is. In effect it is, yes, sir.

CHAIRMAN WALLIS: You know you haven't cured the problem.

MEMBER DENNING: In actuality --

MR. KLEIN: Well, with respect to curing a problem with numerous exemption requests, if that's characterized as the problem, as Senil indicated, if we do issue the proposed rule as written, and if licensee do come in with exemption requests, then we are not providing a good regulatory practice.

CHAIRMAN WALLIS: The rule doesn't solve the problem. But the problem is still there. And you're going to solve it in the traditional way essentially.

MR. KLEIN: That's one way of solving it. The other option, of course, is for a licensee to come in under 50.48(c).

CHAIRMAN WALLIS: Right.

MR. KLEIN: So there is that option available to a licensee.

Senil?

MR. WEERAKKODY: And when we -- if the Committee approves and then if we withdraw the rule, we have plans to -- and, you know, I can't go to the details because these are pre-decisional at this point, we have current enforcement disciplines in place for manual actions and circuits. We have plans to give the licensees a reasonable time frame to develop plans and come into compliance.

MR. KLEIN: Okay, the last bullet I think I talked to you about already. That the staff continues to inspect operator manual actions through the reactor oversight process.

My last slide basically is a -- with respect to schedule, the policy paper is scheduled to

go to the Commission by the end of calendar 2005. And we plan to issue the risks in the spring of 2006 assuming that the Commission favorably approves our recommendation to withdraw the rule.

In conclusion, the staff believes that the proposed rule should be withdrawn and we are asking ACRS endorsement of our recommendation.

That concludes my presentation.

MEMBER DENNING: Does anybody have any questions for the staff? We are going to have a few minutes to a presentation by Mr. Marion following our discussion.

CHAIRMAN WALLIS: After Mr. Marion's presentation we may have some questions for the staff --

MEMBER DENNING: Staff still.

CHAIRMAN WALLIS: I'm not quite sure how that will work out.

MEMBER DENNING: Sure. Any questions now? Dana?

MEMBER POWERS: Somewhat off the subject but just a little bit on philosophy. In thinking about your proposed rule, you have given some emphasis to automatic suppression yet we never credit automatic suppression with extinguishing a fire. Is that true?

MR. KLEIN: I'm trying to understand your question. Are you saying --

MEMBER POWERS: I haven't asked one really yet.

(Laughter.)

MR. KLEIN: All right. Well, you asked me if that's true.

MR. WEERAKKODY: No, that's not. I heard the question. I think that's not true depending on the suppression system. Some we rely on to suppress fire. Some we rely on to extinguish fires.

MEMBER POWERS: Can you point me to something where we credit an automatic system of extinguishing a fire.

MR. FRUMKIN: Well, this is Dan Frumkin of the staff. One of the nuances in automatic suppress systems is the gaseous versus the water suppression systems. And gaseous suppression systems are, by definition, extinguishing systems.

And the water suppression systems, we have deluge what are, I think, extinguishing systems and the automatic sprinkler systems which most people are familiar with are the control systems.

And that's where NFPA comes in and says some of these are extinguishing and some of them are

control systems. From a regulatory standpoint in the fire protection significance determination process, for example, a large amount of credit is given for automatic systems to extinguish fires.

If they operate in enough time, you can get one or two orders of magnitude of credit for extinguishing a credit from an automatic system or if you don't extinguish it you do make the scenario go away. It could be a very small fire after that. So there's a lot of credit in practicality space at NFPA and also in risk space in our significance processes.

MEMBER POWERS: Are these probabilities that you would ascribe to extinguishing based on experiment?

MR. FRUMKIN: Are they based on experiment? I think that they're based on statistics and this history of fires and how many fires had, you know, gone past that point. But that was developed during the fire SDP and the NUREG 6850 statistical machinations with the fire events database, EPRIs and Sandia's.

MEMBER DENNING: It would be useful to see what the statistics are for gaseous systems actually extinguishing.

MEMBER DENNING: Other questions Dan?

MEMBER POWERS: I'm too off the topic to pursue this.

MEMBER DENNING: Okay. Well, thank you very much. And now, Mr. Marion, would you step up front and guide us?

MR. MARION: Good morning. My name is Alex Marion, Senior Director of Engineering at the Nuclear Energy Institute. And I appreciate the opportunity to offer a few perspectives from the industry relative to this particular rulemaking.

The industry essentially supports rulemaking in this area. We think it is important to establish acceptance criteria but which licensees can demonstrate their ability to execute an operator manual action if there is a fire in a nuclear power plant.

And approximately three years ago, we reached an agreement with the NRC on that concept and we also reached an agreement that rulemaking was the appropriate vehicle to use to provide some stability in the process going forward.

Now prior to any stability in this particular area, there have been two processes that have been involved over the last 25, 30 years relative to the treatment of manual actions. One was the NRC

expectation that utilities who wanted to credit manual actions for 3(g)(2) areas would issue a formal exception request to the NRC.

However, that has not been written anywhere. It is not explicitly stated in NRC regulations nor is it explicitly stated in NRC regulatory guidance.

The second practice has been one where the NRC has reviewed and approved operator manual actions in a more informal manner. And it has been documented in safety evaluation reports and inspection reports.

We provided that kind of information to the NRC approximately three years ago. That was the basis of the recognition, I think, on their part that there were these dual approaches and we needed to provide some consistent process going forward.

And that's why fundamentally we supported th rulemaking. We still support the rulemaking. The only provisions of the rulemaking that we took issue with was the requirement or proposed requirement for automatic suppression. And our basic argument in that regard was that it was arbitrary.

But more importantly from a practical sense, the utility fire hazards analysis and utility actions for demonstrating compliance with 10 CFR 4058

as well as Appendix R had already identified that particular areas of the plan that have significant fire hazards such that automatic suppression is necessary.

So to add it as an additional requirements in areas where you're you are going to execute operator manual actions makes no sense from a fire protection point of view.

And the second provision of the proposed rulemaking that we took issue with was this time margin which was effectively a penalty on the use of operator manual actions. And we still believe that there is need for stability in this process going forward. We support the inspection procedure acceptance criteria that has been in place now for approximately two-and-a-half years.

We, as a matter of fact, had an appendix to NEI 001 that identified similar acceptance criteria. And we removed that appendix when NRC published the inspection procedure. Because it didn't make any sense to have redundant information in an industry document as well as an NRC document.

We intend to submit --

MEMBER POWERS: There are no major cases--

MR. MARION: Pardon?

MEMBER POWERS: -- of where there is that redundant information?

MR. MARION: I'm sorry.

MEMBER POWERS: No -- we don't have any major situations where there is that kind of redundant information?

(Laughter.)

MEMBER POWERS: I think it is actually fairly common.

MR. MARION: Yes, it is. It is. But, you know, we wanted to basically quite frankly give credit to the NRC for articulating the acceptance criteria in their inspection procedure. So operator manual actions for the past couple of years have been reviewed against that acceptance criteria.

And as I mentioned before, the regulations aren't explicit in this area in terms of requiring an exemption request. It's an interpretation but it is more fundamental that that.

There are two sets that are referred to as Appendix R plants and those that are referred to as NUREG 0800 plants. And the timeline for the differentiation between the two categories of facilities of 1979 -- those licensed before '79 and those after.

And for the plants that have been licensed under 0800, they have a standard license condition that allows them to do an evaluation of changes to their fire protection program. And if that evaluation doesn't reduce the effectiveness of the fire protection feature. And they are allowed to proceed with making that change.

And a lot of utilities that have received informal, if you will, non-exemption type of approval for the use of operator manual actions fall into the category.

So the problem still exists. This is the sae problem we've had for the last 25, 30 years today. You still have two approaches that are being used.

We support the rulemaking. We don't support those two provisions. We intend to submit acceptance criteria to the NRC for review and approval hopefully the first week of December.

Let me just say a word about fire hazards analysis. It is deterministic but it is fundamental to evaluating the fire hazard you have in a given area so that a licensee can identify the appropriate fire protection features to deal effectively with that hazard.

And I don't believe the staff was trying

to downplay the significance of fire hazards analysis in the comments this morning. But I just wanted to point out that it is deterministic. But it is the only means you have now to do that kind of an evaluation.

And let me just indicate that it is also one of the key aspects to the defense-in-depth concept. In defense-in-depth are four elements, if you will, prevention, detection, mitigation, and recovery.

Operator manual actions identify what kind of features you need to put in place to detect a fire, based upon the hazards again. What kind of features do you need to put in place to prevent a fire, again based upon the hazards in a given area.

And then what you need to do to mitigate. And then from the standpoint of recovery, you are relying on operator manual actions to get the plant in a safe condition.

And lastly I'd like to say that I'm quite frankly disappointed as to where we are now. We were under the impression that we were on a success path to provide some predictability and stability to the process going forward. And if the staff recommends, and I suspect that they will continue to do so as they

presented this morning, that the rulemaking activity be ceased, we're back to where we were three years ago.

We're back to an unpredictable process. We're back to a licensing basis at plants that represents two approaches, one with formal exemption requests and another with informal acceptance by the NRC. And we haven't solved anything.

I'm hoping that the staff can review and approve our acceptance criteria that we intend to submit. That criteria will be consistent with what is in the inspection procedure that was referred to earlier.

We have done a review against other NRC guidance documents and the only aspect that we are not considering is this time margin factor penalty. And we are not including the proposed requirement for automatic suppression.

And that concludes my comments. And I thank you for the opportunity. And I'll be more than happy to answer any questions.

MEMBER DENNING: Yes. A couple quick questions. First, you say that you are still supportive of the rulemaking process. But if the rule went forward as it exists today are you just

indifferent? Or would you prefer not to see the rule as it is being proposed today?

MR. MARION: If the rule was issued today as proposed, and this includes the two provisions that we are fundamentally against, it will require an increased number of exemptions basically to do with those two provisions.

As I think Senil indicated, there are approximately a thousand exemptions that have been issued on Appendix R already. You'll probably get as many, all right, based upon the automatic suppression provision in that regulation.

CHAIRMAN WALLIS: Did you answer his question? Would you be in favor of this rule going forward --

MEMBER DENNING: As it is today.

MR. MARION: With those two --

CHAIRMAN WALLIS: The question we face is to recommend whether it goes forward or not.

MR. MARION: Yes. The rule, as proposed, we do not support.

MEMBER DENNING: You don't support it --

MR. MARION: No.

MEMBER DENNING: -- as proposed.

MR. MARION: Primarily because of those

two provisions.

CHAIRMAN WALLIS: So you support a rule but not this rule.

MR. MARION: We propose a rule that focuses on acceptance criteria to demonstrate the feasibility of manual action.

CHAIRMAN WALLIS: So you're not opposed to a withdrawal of this rule?

MR. MARION: Not opposed to withdrawing this rule --

CHAIRMAN WALLIS: Thank you --

MR. MARION: -- as proposed.

CHAIRMAN WALLIS: -- for clarifying things.

MEMBER DENNING: Yes. Okay? Any other questions?

(No response.)

MEMBER DENNING: If not, then thank you very much. And I turn it back to you, Graham.

CHAIRMAN WALLIS: Thank you. I think we've done very well.

Now we have another item on the agenda. And we look forward to that. If the staff will come forward, we have a meeting on the report of the Planning and Procedures Subcommittee. And we'll move

right to that.

We don't need the transcript. Thank you very much for the transcript. We don't need it any more.

(Whereupon, the above-entitled meeting was concluded at 11:18 a.m.)

CERTIFICATE

This is to certify that the attached proceedings before the United States Nuclear Regulatory Commission in the matter of:

Name of Proceeding: Advisory Committee on Reactor Safeguards 527th Meeting

Docket Number: n/a

Location: Rockville, MD

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.

Katherine Sykora
Official Reporter
Neal R. Gross & Co., Inc.

NRC DIGITAL SYSTEM RESEARCH PLAN FY 2005 THROUGH FY 2009

Advisory Committee on Reactor Safeguards
November 4, 2005

William E. Kemper
Steven A. Arndt
Engineering Research Application Branch
Division of Engineering Technology
Office of Nuclear Regulatory Research
(301-415-6502, saa@nrc.gov)
(301-415-5974, wek@nrc.gov)

BACKGROUND

- The current digital system review guidance (SRP Chapter 7) is several years old (1997)
- We have already seen and anticipate receipt of more complicated and more extensive plant specific applications, thus the need to make the review process more effective continues to grow
- The FY2001-2004 NRC digital system research program plan was primarily focused on NRR issues
- In the past few years the need to provide support to NSIR and NMSS issues has grown

CURRENT SITUATION

- Issues facing NRC
  - We expect that licensees will replace analog systems with digital systems as the existing analog systems become obsolete
  - Licensing these digital systems presents challenges to NRC because of the
    - Increased complexity of the systems
      - Consolidation of discrete analog functions into a single digital system
      - Potential consolidation of independent safety systems into a single digital system
      - Potential new failure modes
    - Limited operating history of digital equipment in nuclear safety related applications
    - Significant effort required by staff with specialized skills
  - Current licensing guidelines provide information on what to review, but not necessarily how to review it, or what the appropriate acceptance criteria should be
  - There is industry interest in risk-informed digital system reviews, but the NRC does not yet have the needed technical bases to support this kind of review

CURRENT SITUATION

- In today's environment, cyber security of safety related digital systems is essential, and staff is working to develop regulatory guidance and acceptance criteria
- The operating history we have indicates digital systems failures may be risk significant
  - An analysis of 1984-1997 ASP data indicated that a large number of risk significant events includes I&C failures and that both safety and non-safety systems contributed to these events
  - An analysis of LER data showed that many software system failures are context-dependent (e.g. dependent upon the operational mode at the time of failure) and that many faults are introduced in testing, operations and maintenance
  - Anecdotal evidence shows potential issues (Palo Verde's Core Protection Calculator and Turkey Point's load sequencers)

DEVELOPMENT OF THE NEW PLAN

- In the 1997 NAS report "Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues" the review committee identified a number of key areas that should be explored including;
  - Systems Aspects of Digital Instrumentation and Control Technology
  - Software Quality Assurance
  - Common-Mode Software Failure Potential
  - Safety and Reliability Assessment Methods
  - Human Factors and Human-Machine Interfaces
  - Dedication of Commercial Off-the Shelf Hardware
- In developing the "NRC Research Plan for Digital I&C for FY 2001-2004" RES reviewed the 1997 NAS report recommendations and I&C vendor development efforts at that time and determined that the key areas for research were
  - Systems Aspects of Digital Technology
  - Software Quality Assurance
  - Risk Assessment of Digital I&C Systems
  - Emerging I&C Technology and Applications

DEVELOPMENT OF THE DIGITAL SAFETY SYSTEM RESEARCH PLAN FY 2005-2009

- The new research plan was developed to
  - Provide improved technical guidance for review of digital systems
  - Provide technical support in areas where program offices need improved acceptance criteria
  - Develop assessment tools and methodologies to improve reviews
- Input was solicited from NRC program offices (NRR, NSIR and NMSS)
- Draft plan was vetted with program offices and comments have been incorporated
- The new research plan has been reviewed by the ACRS Digital I&C Subcommittee and comments are being incorporated
- Provides a flexible, adaptable framework for identifying NRR, NMSS, and NSIR research initiatives needed to meet the challenges of licensing digital I&C systems for safety related applications at nuclear facilities

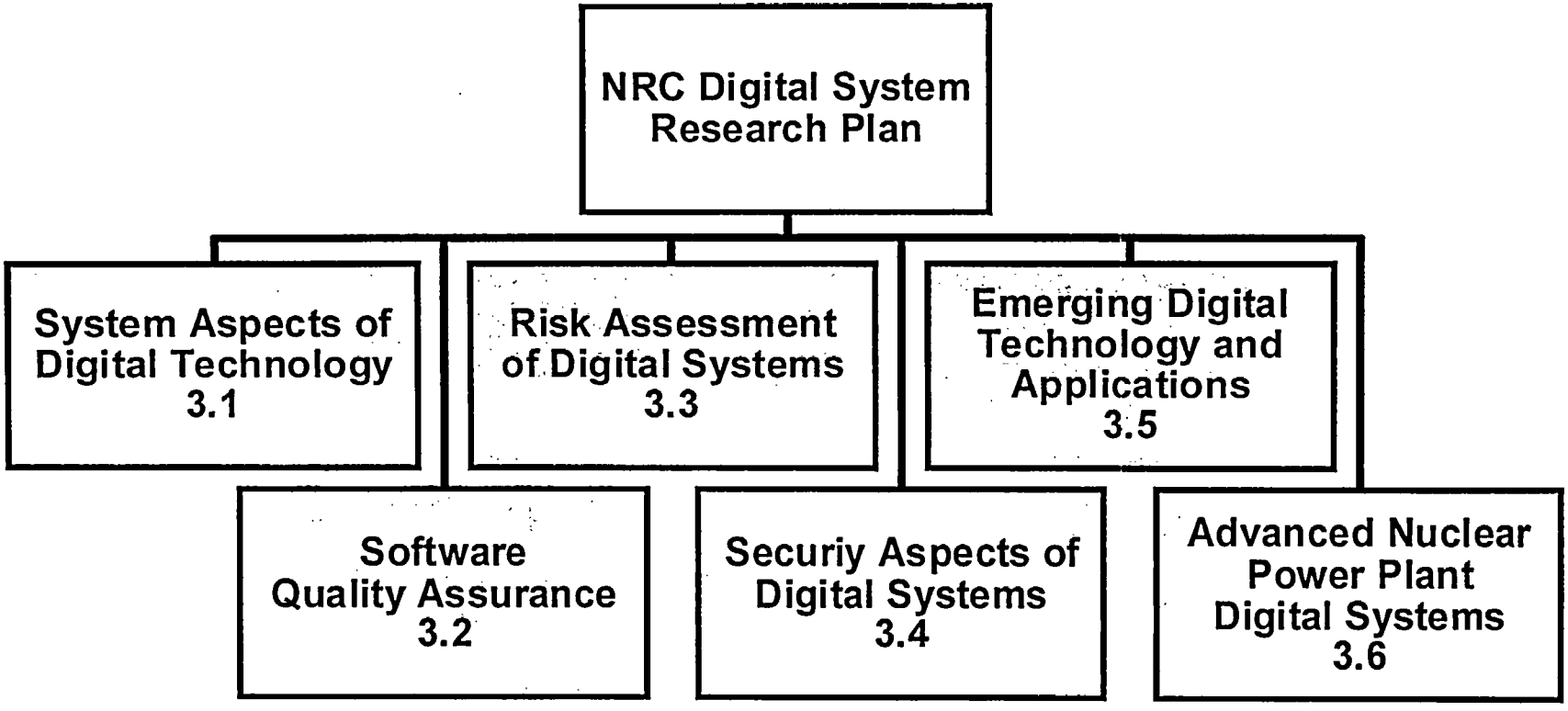
RESEARCH FOCUS

- Structured to include the most important research areas needed to support the program offices
  - Systems Aspects of Digital Technology
  - Software Quality Assurance
  - Risk Assessment of Digital I&C Systems
  - Security Aspects of Digital Systems
  - Emerging Digital Technology and Applications
  - Advanced Nuclear Power Plant Digital Systems
- Broad-based, focusing on improving traditional review methods for
  - Review of existing digital technologies
  - Analysis of emergent technologies
  - Evaluation of issues arising from the application of digital technologies
  - Focus is on improving the assurance of digital I&C system reliability

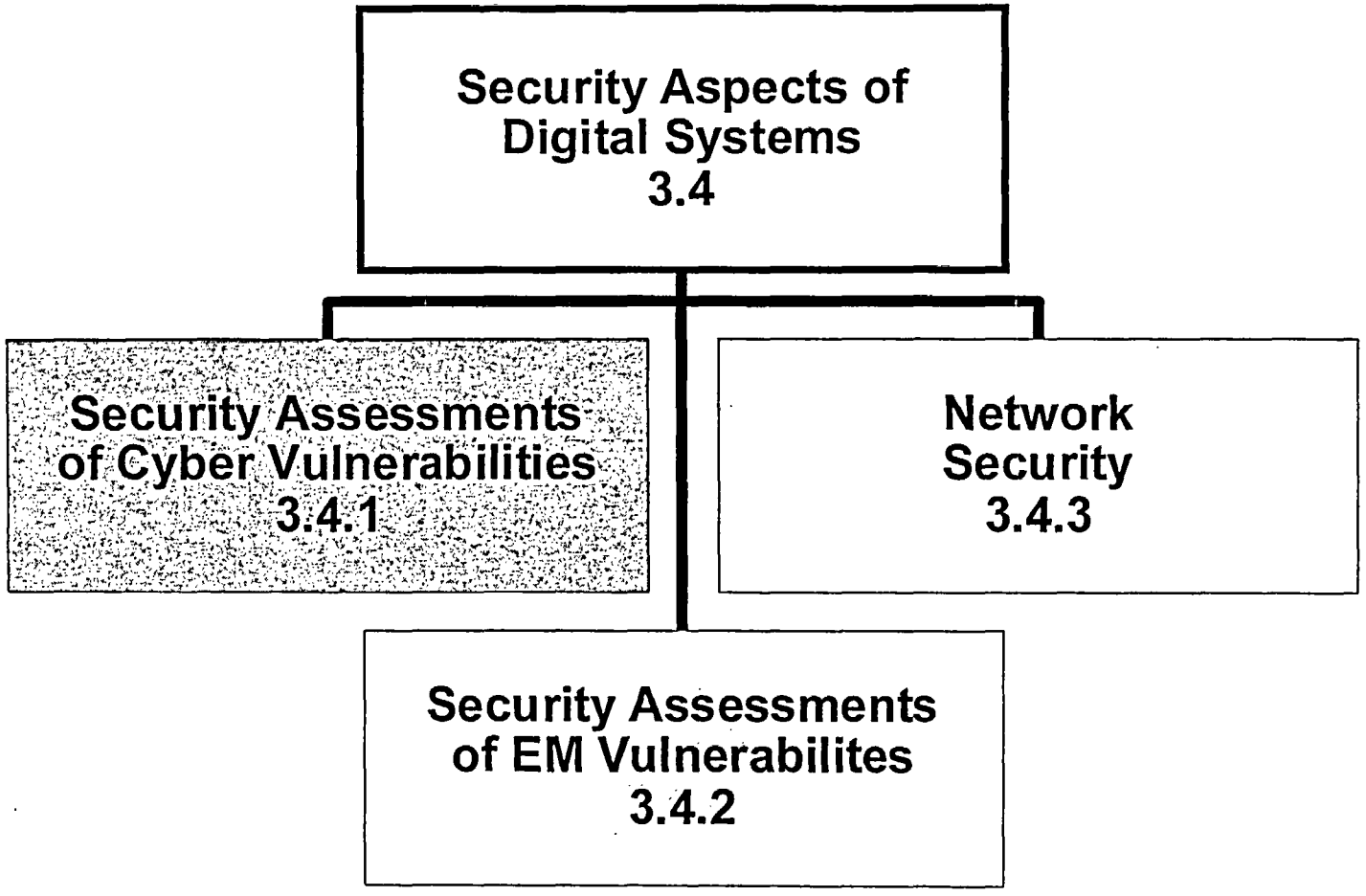
PRIORITIES FOR CONDUCTING THE RESEARCH

- Inputs included
  - Completing ongoing work
  - Program office inputs
  - Balanced between
    - Current regulatory issues (EMI/RFI, D3, Security)
    - Issues that are anticipated to be regulatory issues in the short term (FPGAs, OLM, digital system risk)
    - Following emerging technology that might require future licensing reviews (smart transmitters, self testing methods)
- Supports NRC strategic plan strategies
- Incorporated in the Plan (in Section 4) as
  - Relative priority (high, medium and low)
  - Determined based on operational experience, program office requests and likely application schedule
  - Projects scheduled based on priority and available resources
- Used to support RES budget process

RESEARCH PROGRAMS



SECURITY ASPECTS OF DIGITAL SYSTEMS



SECURITY ASPECTS OF DIGITAL SYSTEMS

- Cyber security is an NRC concern that has been heightened since the events on 9/11
  - Attention to non-safety as well as safety systems
  - New look at safety systems
- Digital system security requires addressing potential vulnerabilities during system development and after installation
- Current regulation, orders and guidance establishes security criteria for the use of digital systems

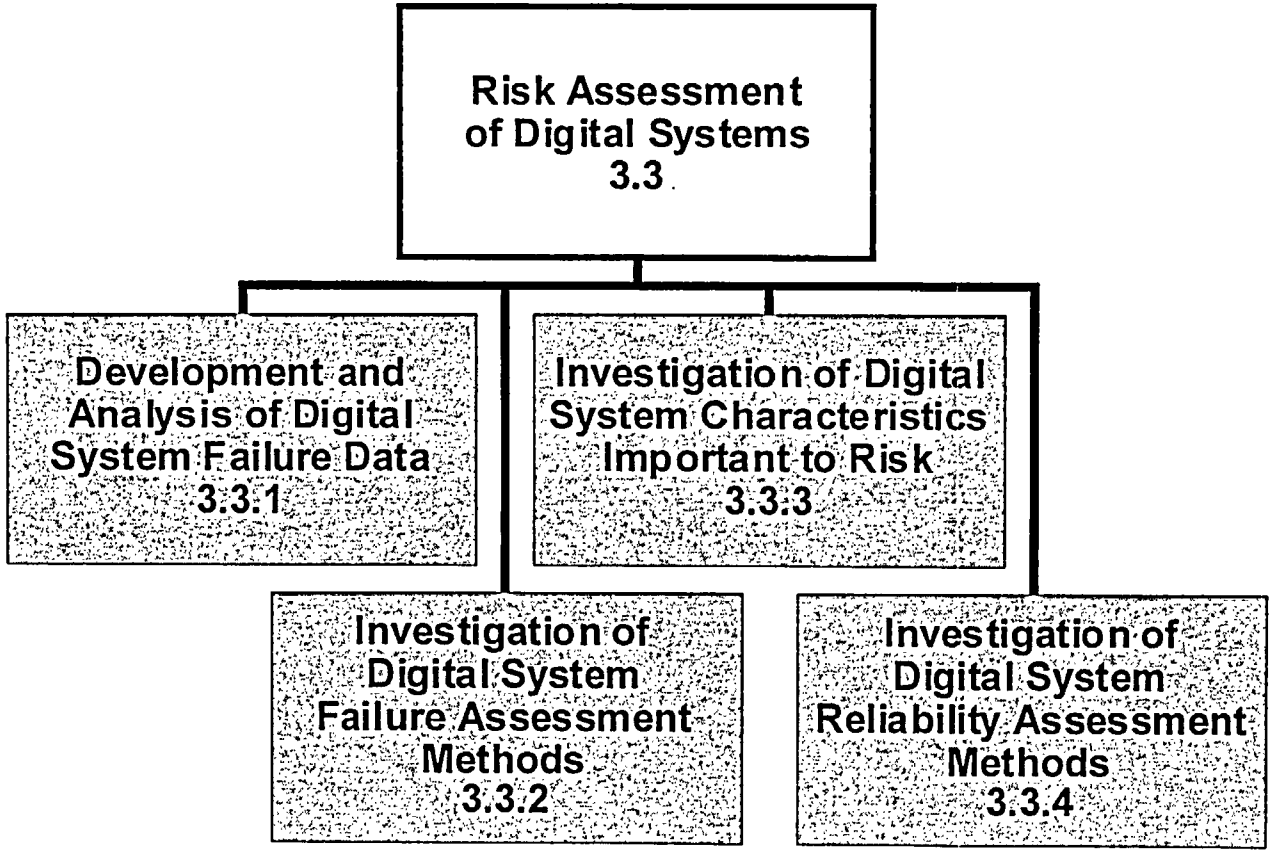
SECURITY ASPECTS OF DIGITAL SYSTEMS

- Additional guidance is needed to develop detailed acceptance criteria and review procedures, and training for reviewers
- Past research indicates that additional information is needed
  - Safety System Isolation Study
  - Protocol Robustness Analyses
  - Network Security Tool Vulnerability Case Study
  - NSIR projects
    - Power Reactor Pilot Study
    - Licensee Self-Assessment Methodology
- This program includes three project areas
  - Security Assessments of Cyber Vulnerabilities
  - Security Assessments of EM Vulnerabilities
  - Network Security

SECURITY ASPECTS OF DIGITAL SYSTEMS

- As an example the security assessments of cyber vulnerabilities research project will conduct detailed
  - Safety System Assessments,
  - Communication Protocol Assessments and
  - Evaluations of safety ⇔ non-safety system interconnections
- This research will produce
  - Test reports, including mitigation measures
  - Taxonomy of potential vulnerabilities
  - Methodologies (including procedures and tools) for reviews and inspections
  - Acceptance criteria
  - Policy and regulatory recommendations

RISK ASSESSMENT OF DIGITAL SYSTEMS



DIGITAL SYSTEM RISK PROGRAM

- Licensees are replacing analog systems with digital systems
- Licensing these digital systems presents challenges to NRC
  - Consolidation of many analog functions in one digital system challenges traditional diversity and defense-in-depth methods
  - Industry has expressed interest in incorporating risk insights in the reviews of these systems or using risk-informed regulation as an alternate method for licensing these systems (EPRI)
  - Lack of a generally accepted methodology to predict digital system (software) failure probability
  - Research into the limitations of digital systems reliability modeling to support the needed analysis does not currently support expanded use of risk information in licensing digital systems
- As the NRC licensees replace analog systems with digital systems, the current PRAs are not keeping up with these changes
- NRC risk analysis tools and data do not currently support this kind of analysis. NRC risk guidelines currently do not provide acceptance criteria for digital system reviews

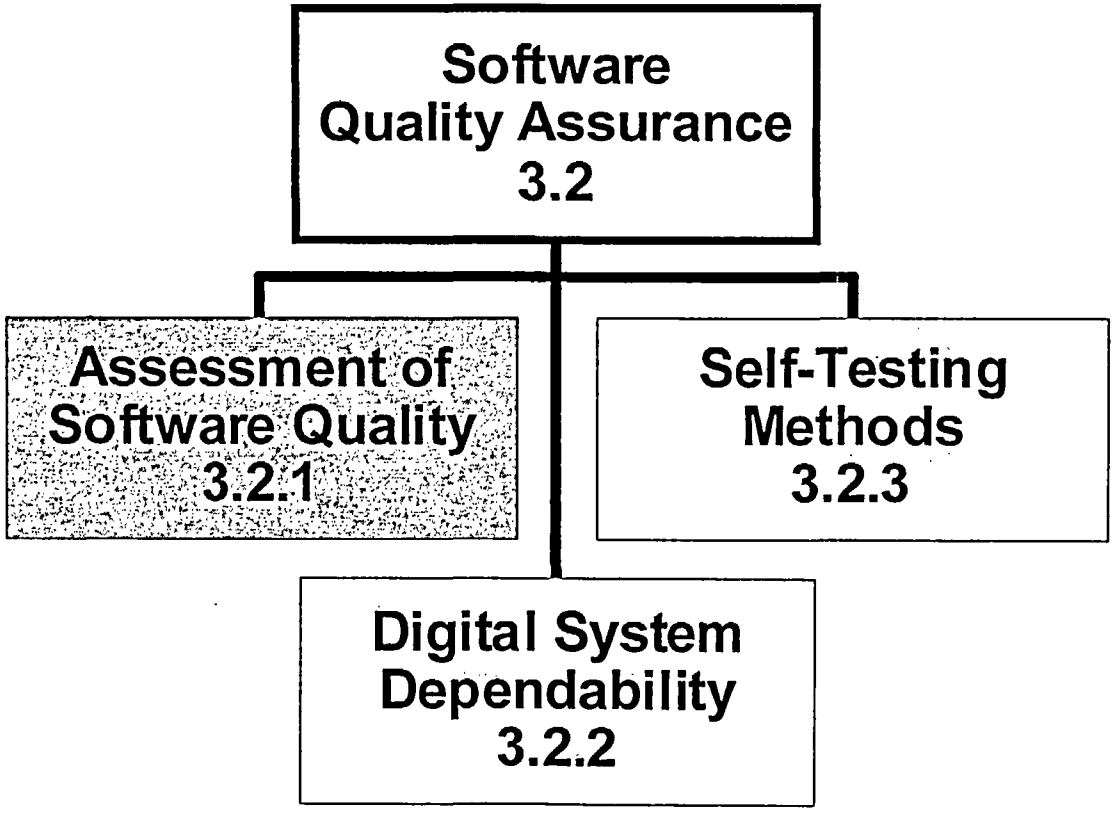
DIGITAL SYSTEM RISK PROGRAM

- The research program is designed to use available information, including failure data and known capabilities of available methods to develop the review methodology
- Available methods and tools for including digital system models will be examined and the most promising ones will be investigated in detail
- Review of current data and development of application-specific databases is on-going and will be used to support methods development

DIGITAL SYSTEM RISK PROGRAM

- Research is oriented toward developing regulator guidance and providing consistent processes for assessing risk based digital safety system applications
  - Gathering, understanding and using failure data
  - Assessing what modeling methods might be acceptable
  - Determining which systems need to be modeled and at what level of detail
  - Developing and testing methods
  - Developing regulatory acceptance criteria
- New methods for integrating current digital system models into PRAs will be developed
  - Pilot methods using both traditional methods and dynamic methods using models
  - Benchmarks of the capabilities of several methods will be completed
  - Uses and limitations of methods will be explored

SOFTWARE QUALITY ASSURANCE



SOFTWARE QUALITY ASSURANCE

- NRC SRP Chapter 7, Rev. 4, June 1997 provides regulatory guidance for reviewing digital safety systems
- NRC SRP Chapter 7 BTP HICB-14 identifies digital system development attributes that should be reviewed, but does not provide detailed guidance on the process for confirming that the software conforms to acceptance criteria
- As part of its review of digital safety systems, NRC evaluates safety related software quality by reviewing
  - System and software specifications
  - Development processes (e.g., V&V, CM) and
  - Software development products (e.g., SRS, SDD, Test plans, Code listings, RTM)
- SQA evaluations are performed manually, since assessment tools or other means of obtaining quantitative measures of software quality are not available
  - Time consuming
  - Highly dependent on the skill and experience of the individual reviewer
  - Acceptance criteria is not quantitative

SOFTWARE QUALITY ASSURANCE

- The current state-of-the-art in software system safety assessment includes a number of methods and tools for quantitatively assessing the quality of software:
  - Software system analysis techniques (e.g., Petri-net analysis, Markov Analysis, Dynamic Flow Modeling)
  - Software metrics
  - Formal verification methods
  - Testing Techniques (e.g., Data Flow Testing, Fault Injection, and Mutation Testing)
- None of the these methods have found wide-spread uses in the nuclear industry

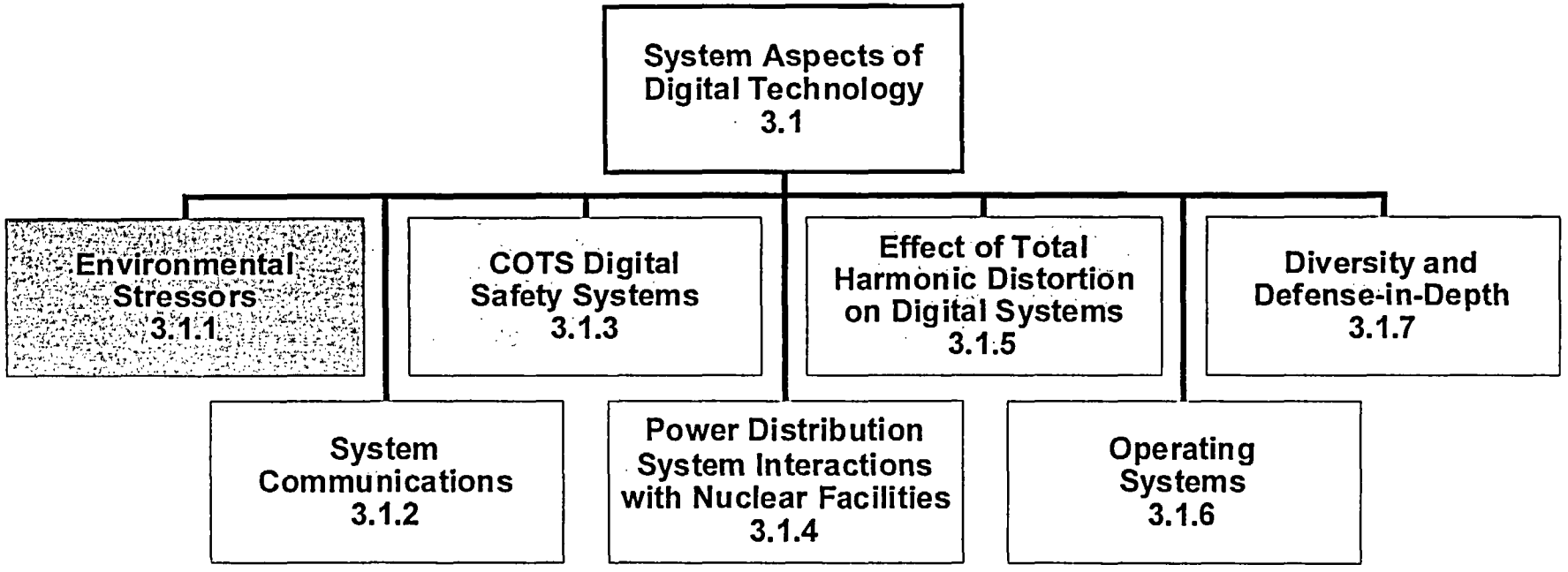
SOFTWARE QUALITY ASSURANCE

- Given the complexity and sophistication of current digital safety systems, the goal of research in this area is to provide independent assessment methods and specific acceptance criteria that can supplement and augment the existing guidance in Chapter 7 of the SRP
- Research in this area will focus on methods that have likely short term application without the need to do extensive development and apply these to nuclear industry applications
  - Fault injection testing has been used by a number of industries including some nuclear platform suppliers
  - Formal methods have been used in several industries to support safety critical applications
  - Software metrics are currently used for software quality control and continuous improvement (e.g., for programs at CMM level 4 and 5 respectively)

SOFTWARE QUALITY ASSURANCE

- As an example, there have been a number of software errors in nuclear applications, like the Turkey Point 3 load sequencer failure that would be very difficult to find using the current review process that focuses primarily on a review of the software development process and a limited number of thread audits
- This research area currently focuses on developing methods to help assess software quality and reliability using tools and analysis methods that
  - Permit the reviewer to review more of the code with the same amount of effort
  - Assess the added benefits of self testing and improved development processes
  - Provide objective acceptance criteria and review procedures that augment and supplement existing SRP guidance for approving (or denying) digital safety system license applications

SYSTEM ASPECTS OF DIGITAL TECHNOLOGY



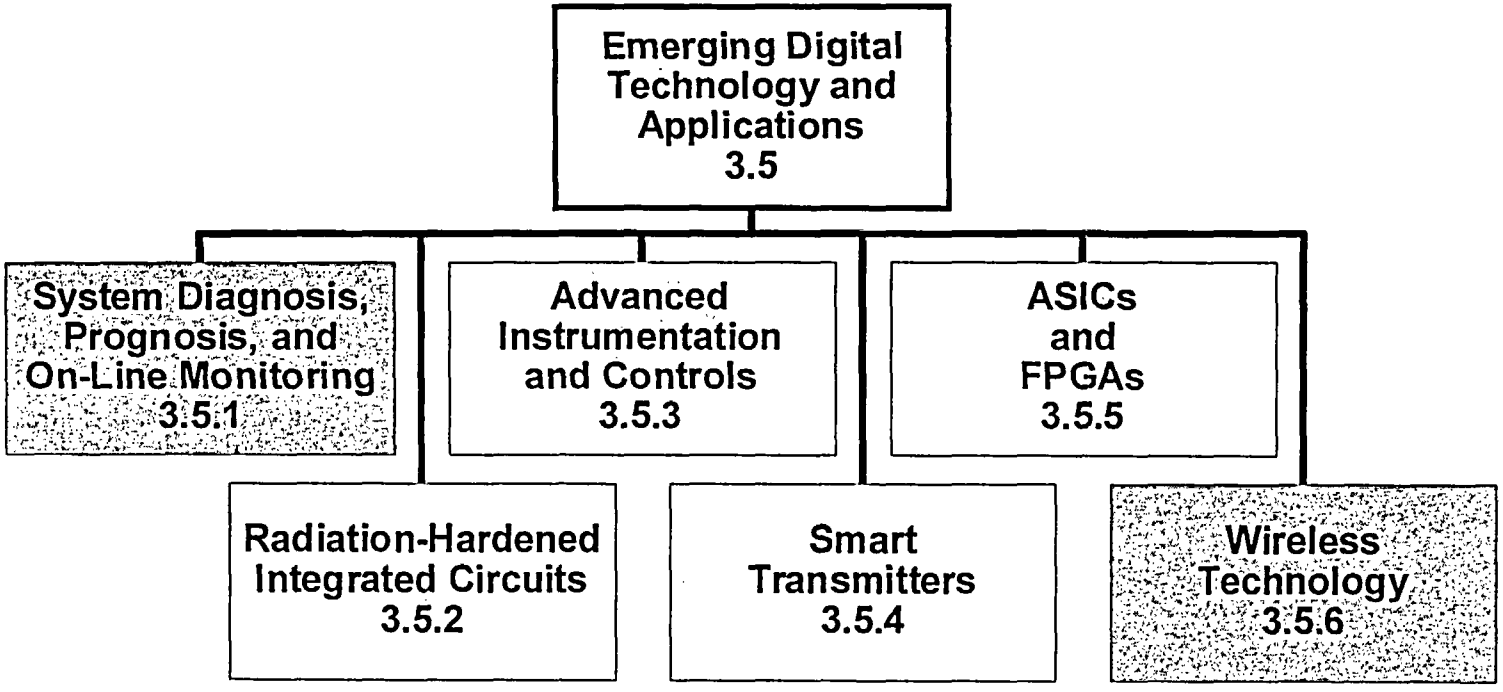
SYSTEM ASPECTS OF DIGITAL TECHNOLOGY

- System aspects of digital technology involve factors, both internal and external, that affect the performance of a digital system as a whole
- This research will address aspects of digital systems that can adversely affect safety due to
  - Environmental stressors
  - Systems interactions associated with power distribution and total harmonic distortion effects
  - Operating systems and system communications
  - Diversity and defense-in-depth analysis

SYSTEM ASPECTS OF DIGITAL TECHNOLOGY

- As an example, systems interactions associated with power distribution and total harmonic distortion effects are safety issues because newer digital components are more sensitive to power quality and power distribution
  - Higher IC circuit densities
  - Lower voltage requirements for memory states
  - Non-linear loading that can effect power quality
- Current criteria adequate for current designs, but as above increases new criteria may be needed
- There have been several events in which these effects have caused a digital system failures
- The goal of the research is to provide detailed acceptance criteria (IC density and/or power quality) to support regulatory reviews

EMERGING DIGITAL TECHNOLOGY AND APPLICATIONS



EMERGING DIGITAL TECHNOLOGY AND APPLICATIONS

- Vendors, licensees, owners groups, and nuclear industry will continue to develop and propose new technologies for nuclear facilities
- A detailed understanding of these emerging technologies is critical for NMSS, NRR, and NSIR staff to license these technologies in safety related applications in an effective and consistent manner
- This part of the research program will include an effort to identify important emerging technology, investigate technologies that may have a regulatory impact and develop the needed information and regulatory guidance before a licensee submits an application

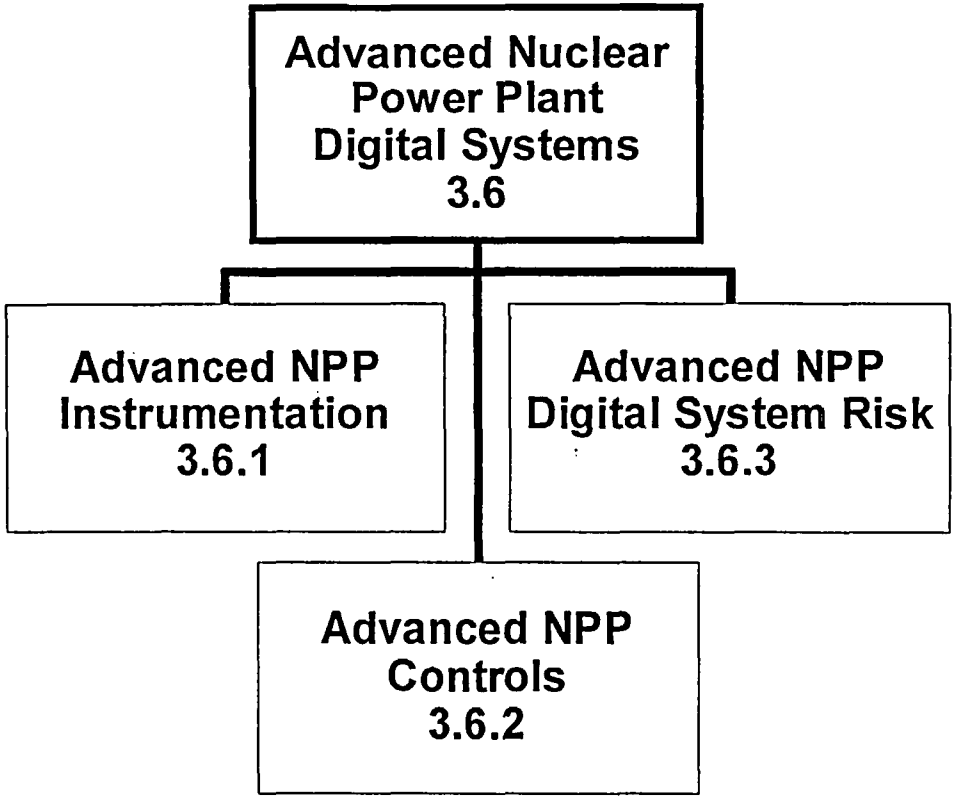
EMERGING DIGITAL TECHNOLOGY AND APPLICATIONS

- The research program in this area includes
  - Developing technology specific information on the potential application
  - Developing assessment tools and review methodologies
  - Revising regulatory guidance to support unique features of each new technology and establish acceptance criteria
  - Adopting the SRP for unique technologies
  - Developing the supporting training curricula
- Ongoing projects include
  - Emerging technology evaluations (every 2-4 years)
  - On-line monitoring
  - Wireless technology
- Future projects include
  - System diagnosis and prognosis
  - Advanced instrumentation and controls
  - Radiation-hardened integrated circuits
  - ASICs and FPGAs
  - Smart transmitters

EMERGING DIGITAL TECHNOLOGY AND APPLICATIONS

- As an example, application specific integrated circuits (ASICs) and field programmable gate arrays (FPGAs) are now starting to be used in safety applications
- FPGAs are currently being used by Toshiba in safety systems for international nuclear applications
- FPGAs shift the complexity that might otherwise be in software to the hardware and design tools
- Current review guidance is based on software driven systems
- This research will
  - Evaluate the safety aspects (design, V&V, etc.) of ASICs and FPGAs
  - Develop safety assessment techniques and acceptance criteria for these devices
  - Support modifications of current regulatory guidance (SRP) to include this emerging technology

ADVANCED NPP DIGITAL SYSTEMS



ADVANCED NPP DIGITAL SYSTEMS

- Advanced reactor designs could result in new instrumentation and control technologies, and might present new regulatory challenges
- To date, new reactor vendors have not identified any new technologies, however as the actual implementation come closer, advanced I&C designs are expected to be incorporated
- Research projects are dependent on advanced reactor design pre-application reviews and COL applications
  - EPR
  - AP1000
  - ESBWR
  - ACR-700
  - PBMR

ADVANCED NPP DIGITAL SYSTEMS

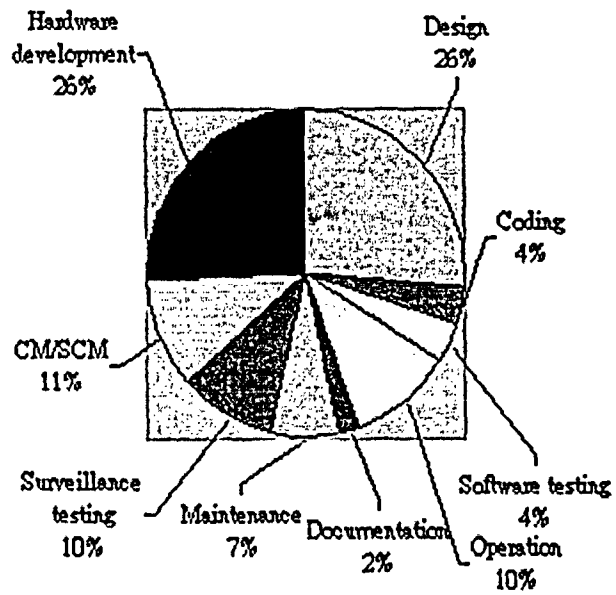
- Advanced reactor designs may apply new I&C technologies in safety, important to safety and non-safety systems
  - Robotics, artificial intelligence, autonomous controls, fully integrated DCS, new instrumentation, etc.
  - Research is organized into three basic areas
    - Advanced nuclear power plant instrumentation
    - Advanced nuclear power plant controls
    - Advanced nuclear power plant digital system risk
- No research in progress at this time

SUMMARY

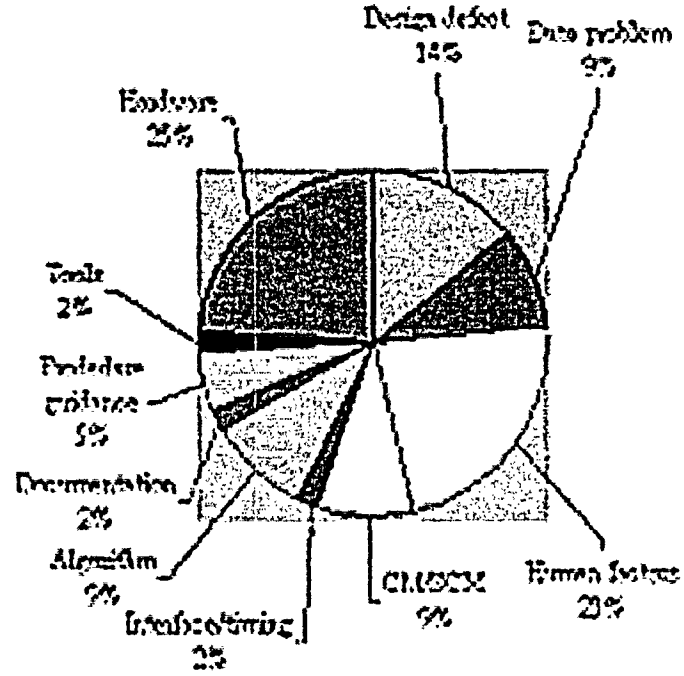
- NRC Digital System Research Plan FY 2005-2009
  Provides a flexible, adaptable framework for supporting NRR, NMSS and NSIR regulatory requirements
  - Broad-based program oriented toward providing more consistent processes for regulating nuclear applications
  - improving review methods for new applications of existing technologies, advanced technologies and new issues
  - developing regulatory acceptance criteria
- The staff requests that the ACRS endorse the plan and continue to provide inputs on how to improve the research program
- RES is looking forward to working closely with the ACRS as the research is implemented

BACK-UP SLIDES

CURRENT SITUATION

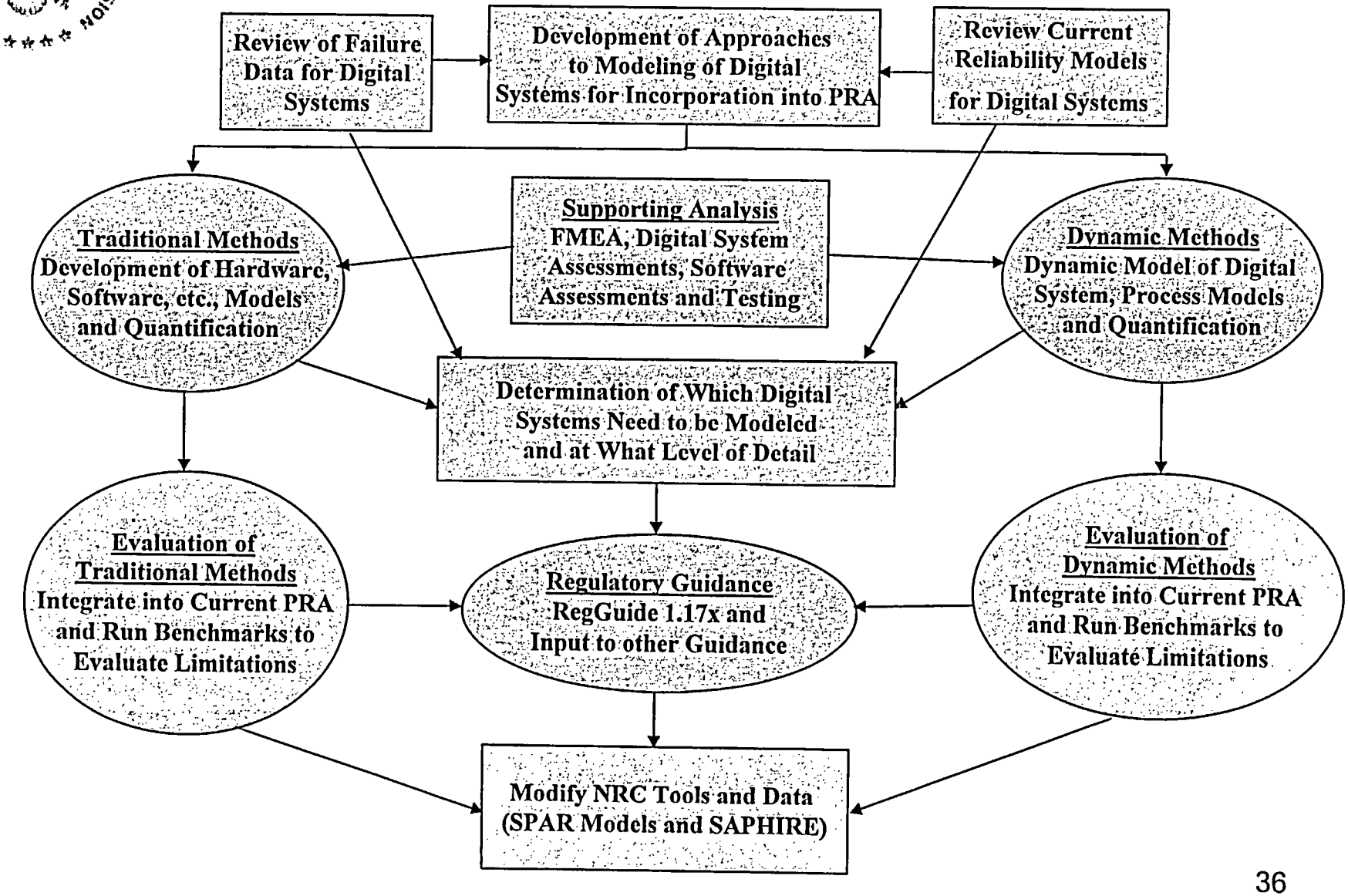


Stage where fault was inserted

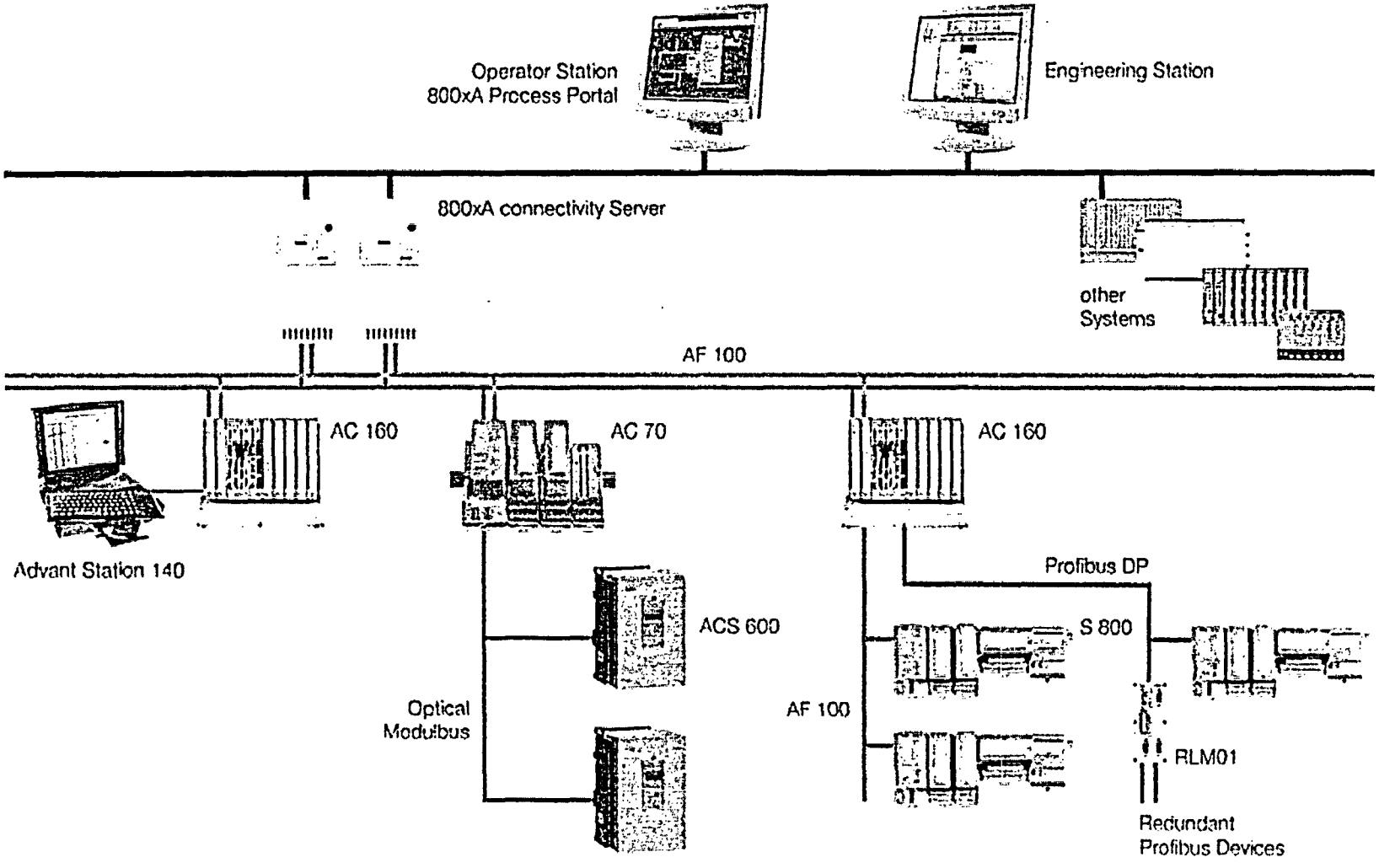


Type of fault

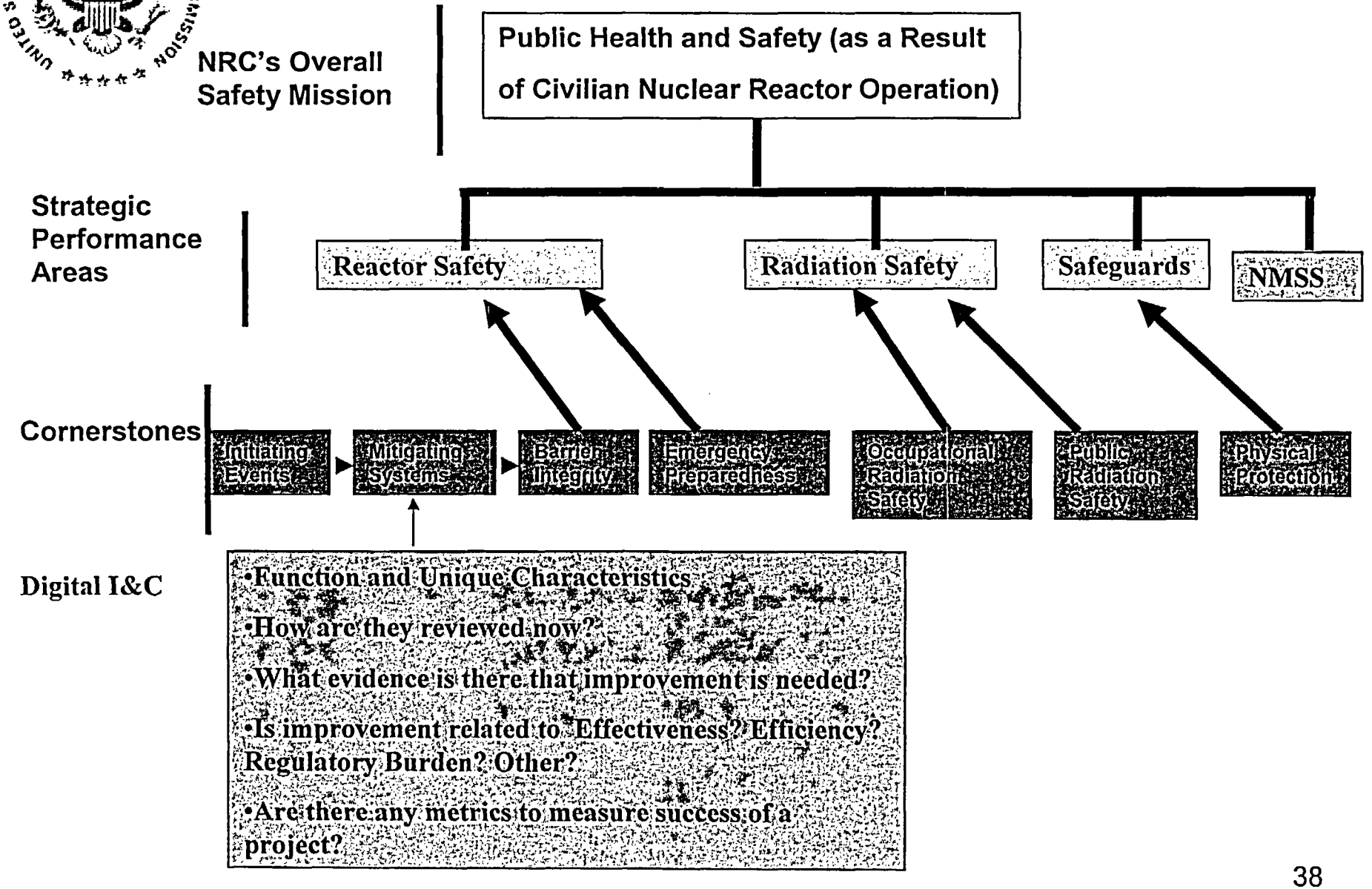
NRC Digital System Risk Program



SECURITY ASPECTS OF DIGITAL SYSTEMS



Building on the Reactor Oversight Process



Operator Manual Actions Rulemaking

Sunil Weerakkody, Chief

Fire Protection Branch
Division of Risk Assessment
Office of Nuclear Reactor Regulation

Operator Manual Actions Rulemaking

- Staff introductions
- Purpose

Operator Manual Actions Rulemaking

David Diec, Project Manager

Financial, Policy and Rulemaking Branch
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

Operator Manual Actions Rulemaking

- Background:
  - Staff briefed ACRS in November 2004
  - Staff published proposed rule in March 2005
    Proposed rule comment period ended in May 2005
  - Staff received early feedback on proposed rule in a Category 3 public meeting in April 2005
  - Staff held Category 2 public meeting in September 2005

Next Steps in Rulemaking Process

- Incorporate insights from public comments
- Develop dispositions of public comments
- Develop policy paper with Staff recommendation

Operator Manual Actions Rulemaking

Alexander Klein,
Sr. Fire Protection Engineer

Fire Protection Branch
Division of Risk Assessment
Office of Nuclear Reactor Regulation

Key Topics

- Maintaining Safety and Compliance
- Purposes of Rulemaking
- Major Stakeholder Comments
  - ACRS questions
- Staff Recommendation
  - Basis for recommendation
- Closure Plan
- Schedule and Conclusion

Maintaining Safety and Compliance

- Continue Inspections of Manual Actions
- Issue Violations Against Non-Feasible Manual Actions

Purposes of Rulemaking

- Primary purposes of the proposed rule SECY-03-0100
  - Codify the use of manual actions and its acceptance criteria
  - Avoid the need to process numerous exemption requests
- SRM dated January 18, 2005 stated:
  - "the staff should engage stakeholders to get a clear understanding…the proposed rule would achieve its underlying purpose"
  - "although the exemption process is available…the Commission considers the…rulemaking…or 10 CFR 50.48(c) more desirable in order to minimize the need for future exemption requests"

Major Stakeholder Comments

- Public Comments
  - Staff received 14 sets of comments
  - Several hundred individuals commented on November 2003 Federal Register Notice
  - The staff analyzed and considered the comments

Major Stakeholder Comments

- Major comments
  - **Requirement for automatic suppression is unnecessary [Industry, NEI], [ACRS question]**
  - **Numerous exemptions will still be needed [Industry], [ACRS question]**
  - **Alternative rule language proposed [NEI], [ACRS question]**
  - **IP71111.05T criteria endorsed [NEI], [ACRS question]**

  - Objected to the time margin and factor [Industry, NEI]
  - Proposed rule is a backfit [Industry, NEI]
  - Missing an opportunity to risk-inform, performance-base the rule [Industry]
  - Proposed rule abandons defense-in-depth; overlooks security related fires; undermines safety oversight [Public Interest Group]

Major Stakeholder Comment

- Requirement for automatic suppression is unnecessary
  - Industry and NEI object to the requirement
    - Fire hazards analysis
  - Staff concludes that the requirement for automatic suppression is essential to maintain defense-in-depth
    - One success path with an operator manual action
    - Relatively high failure probability of an operator manual action
    - Fire hazards analyses are deterministic

Major Stakeholder Comment

- Numerous exemptions will be needed
  - Industry comment based primarily on requirement for automatic suppression
- Staff position
  - Staff concludes that this would require writing exceptions to the rule to cover all situations
    - Poses a challenge to ensuring safety
    - Each situation is case-specific
    - 10CFR50.48(c), NFPA 805 approach is available

Major Stakeholder Comment

- Alternative rule language proposed by NEI
  - Defines several terms in III.G.1
  - Does not change III.G.2
  - Eliminates III.P

- Staff position
  - Staff considered the alternative rule language
  - Staff concluded that alternative language could lead to operator manual actions in areas where there are redundant trains
  - Some operator manual actions may have high probability of failure resulting in an unsafe plant condition
  - Alternative rule language does not ensure defense-in-depth

Major Stakeholder Comment

- IP71111.05T criteria endorsed by NEI
  - NEI claims IP71111.05T provides criteria for determining feasibility of manual actions
- Staff position
  - Staff developed the proposed rule acceptance criteria as part of a self-implementing rule
    - Staff wrote the acceptance criteria to be objective, inspectable and enforceable
    - Staff wrote the criteria to also ensure reliability

Staff Recommendation

- The staff will recommend to the Commission that the proposed rule on operator manual actions be withdrawn

Bases for Recommendation

- Industry comments stating that numerous exemptions will still be needed
  - Does not achieve a primary purpose
  - Does not meet the Commission SRM view
- Option of 10 CFR 50.48(c) is available to industry
  - Addresses Commission SRM direction
- Comments from stakeholders did not support the proposed rule
  - Industry
  - Public

Closure Plan

- Staff is developing a Policy Paper that will recommend withdrawal of the proposed rule
- Staff plans to issue a Regulatory Issue Summary (RIS) that will communicate our regulatory compliance expectations
- Staff continues inspecting operator manual actions through the Reactor Oversight Process

Schedule and Conclusion

- Schedule
  - Staff plans to submit the policy paper to the Commission by the end of calendar 2005
  - Staff plans to issue a RIS Spring 2006

- Conclusion
  - Staff believes the proposed rule should be withdrawn
  - Staff requests ACRS endorsement of our recommendation