Official Transcript of Proceedings ACRST-3253

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
506th Meeting

Docket Number: (not applicable)

PROCESS USING ADAMS
TEMPLATE: ACRS/ACNW-005

Location: Rockville, Maryland

Date: Friday, October 3, 2003

Work Order No.: NRC-1102 Pages 1-31

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

TR04

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

506th ACRS MEETING

+ + + + +

FRIDAY, OCTOBER 3, 2003

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The meeting came to order at 8:30 p.m. in room T2B3 of Two White Flint North, Rockville, Maryland, Mario V. Bonaca, Chairman, presiding.

Present:

Mario V. Bonaca	ACRS Chairman
Graham B. Wallis	ACRS Vice-Chairman
Graham M. Leitch	ACRS Member
Dana A. Powers	ACRS Member
Victor H. Ransom	ACRS Member
Stephen L. Rosen	ARCS Member-at-Large
Thomas S. Kress	ACRS
William J. Shack	ACRS
John D. Sieber	ACRS

Staff Present:

Steven Arndt	RES
Sher Bahadur	Associate Director, ACRS/ACNW
Sam Duraiswami	Technical Assistant, ACRS/ACNW
Medat El-Zeftawy	ACRS Staff
Michelle Evans	Engineering Research Application Branch
Tony Hsai	Engineering Research Application Branch
Howard J. Larson	Special Assistant, ACRS/ACNW
Mike Mayfield	Engineering Research Application Branch
Roman A. Shaffer	RES

I-N-D-E-X

AGENDA	PAGE
Review of Draft Final Revision to Regulatory Guide 1.168	4

P-R-O-C-E-E-D-I-N-G-S

8:30 a.m.

CHAIRMAN BONACA: The meeting will now come to order. This is the third day of the 506th meeting of the Advisory Committee on Reactor Safeguards. During today's meeting, the Committee will consider the following: Draft final revision to Regulatory Guide 1.168; verification, validation, review and audits for digital computer software used in safety systems of nuclear power plants; Subcommittee report on reactor fuels; future ACRS activities and report to the Planning and Procedures Subcommittee; reconciliation of ACRS comments and recommendations; proposed ACRS reports.

A portion of this meeting will be closed to discuss a proposed ACRS report on safeguards and security. This meeting is being conducted in accordance with the provisions of the Federal Advisory Committee Act. Mr. Sam Duraiswami is the Designated Federal Official for the initial portion of the meeting. We have received no written comments or requests for time to make oral statements from members of the public regarding today's sessions. A transcript of portions of the meeting is being kept and it is requested that speakers use one of the

microphones, identify themselves and speak with sufficient clarity and volume so that they can be readily heard.

Since we have no further comments regarding the agenda or items of interest, we'll move right away to the first item on the agenda here, which is the Draft final revision to Regulatory Guide 1.168. Mr. Sieber?

MR. SIEBER: Thank you, Mr. Chairman. I would point out that our Committee declined to review this standard when it was issued for public comments, and so the review that we're doing today is a review prior to final issuance of the standard for use. The Office of Nuclear Regulatory Research developed this standard, and at the time that it was under development it was known as Draft Guide 1123, and it was designed to replace the current version of Reg Guide 1.168, which was issued in 1997.

And the reason why it is being revised and reissued is because the underlying standards which are IEEE 1012 and 1028, have recently been revised themselves. So it is the Agency's duty then to review the new standard and to the extent that it's applicable to either endorse it in total or endorse it with some exceptions. And so we're in the process of

doing that.

Now, this Reg Guide 1.168 is one of seven reg guides that apply to digital systems in nuclear power plants, and the first one is 152, which is the criteria, 168, which is the one we're reviewing today, which is verification, validation, reviews and audits, and 169 to 173 also provide further structure in the development of computer software. So this is just one of a series.

The revision of the IEEE standard was not all that expensive, but it differs in a number of ways from the previous standard, and I'm sure that our presenters will let you know what those differences are. So without belaboring or stealing away any more of the presenters' material, I will introduce Mike Mayfield. He is overall responsible for this task and Steve Arndt and Roman Shaffer. Mike?

MR. MAYFIELD: Thank you. I have with me this morning Michelle Evans, the Chief of the Engineering Research Applications Branch. Roman Shaffer and Steve Arndt are members of her Branch that have responsibility for these activities. We are here today to seek Committee endorsement and I guess that's a nice way of saying we would like to get a letter endorsing staff publishing this update to the Reg

Guide.

And with that, I would introduce Roman. Roman's been with us several years, came to us out of graduate school, has kind of a varied background, and he took over this activity. We've had some turnover in staff, Roman took it over fairly late. We've asked Steve to join him this morning to deal with any questions you may have. Roman's one of our hard chargers, and we're looking forward to great things, so please feel free to abuse him this morning. Thank you. Roman?

DR. POWERS: How dare you?

(Laughter.)

MR. SIEBER: You won't abuse him because I've been doing it for the last few weeks.

MR. SHAFFER: Good morning. As Mike said, I'm Roman Shaffer and I've been with the NRC since June of 2000. I've recently taken over the project. I'm sure you all know Steven Arndt, Dr. Steven Arndt. He's here to help me, and I appreciate his attendance here.

We're here before the Committee to obtain a letter of endorsement to issue the final draft of Regulatory Guide 1.168 Revision 1. It's a long title, but essentially it covers two IEEE standard -- current

IEEE standards. I'll get into those a little bit later, but first I'd like to move to the second slide, the overview of what will be presented here this morning.

I'll give a little background information, try to define a little verification and validation exactly and provide an opening statement of some sort. Then we'll move on to the current guidance contained in Regulatory Guide 1.168 Revision 0. Revisions to this current guidance contained in Regulatory Guide 1.168 Revision 1. Resolution of the public comments we received on the draft guide and regulatory positions in the final draft guide to Revision 1. If you can't hear me or if I'm speaking too quickly, please let me know.

The Commission has requirements regarding quality and reliability of safety systems at nuclear power plants. These criteria are contained in Appendices A and B in 10 CFR Part 50. Software engineering practices rely in part on software verification and validation activities as well as reviews and audits to meet these requirements. NRC staff endorses consensus standards, such as IEEE standards, as acceptable methods for meeting these criteria.

Because sulfur V&V activities and reviews and audits are important to meeting the Commission's criteria, we've treated these two standards at the same time in this regulatory guide. In the current guide, in Revision 0 of Regulatory Guide 1.168, this current guidance was issued in September of 1997. It endorses two standards, IEEE Standard 1012-1986 and IEEE Standard 1028-1988.

DR. WALLIS: Why did it take so long? Are those the years, 1988?

MR. SHAFFER: Yes.

MR. SIEBER: Those are the old standards.

MR. SHAFFER: Those are the older standards.

MR. SIEBER: That's the old version, and now there's --

DR. POWERS: There's a new version coming up.

MR. SIEBER: The new version is here.

DR. POWERS: We're going to get to that.

MR. SHAFFER: In Revision 1 to the current guidance, we endorse the current standards, current versions of these standards. We undertook this work to revise current guidance contained in Regulatory Guide 1.168 in response to using nuclear reactor

regulation. This revision to the current guidance endorses two IEEE standards with exceptions, 1012-1998 and 1028-1997.

The main discussion this morning will be on the revisions -- the update to 1012-1986 because the current standard -- version of this standard was a significant rewrite in that it became a process standard and the provisions in the 1986 version were incorporated as one component in the 1998 version of IEEE Standard 1012. The update to 1028 was mostly in clarifying terms and using them consistently throughout the standard, and that standard, 1028-1997, gives criteria for performing adequate reviews, inspections, audits, walk-throughs, not so much how to enter these reviews or inspections or how to disposition the findings; it's just how to do a good review or audit, walk-through, et cetera. So, again, the main part of the discussion will cover 1012-1998 and regulatory positions -- the exceptions to this standard.

MR. LEITCH: Roman, does this standard address V&V with the -- in the manufacturing segment or the user or the regulatory or all of the above?

MR. SIEBER: Just software.

MR. LEITCH: Software, yes, right, but is

it directed -- my question is really is it directed towards the developer of the software or the user or the regulator or is it applicable to all of the above?

MR. SHAFFER: Yes.

MR. SIEBER: All.

MR. LEITCH: All of the above.

MR. ARNDT: This is Steve Arndt. It's a very comprehensive, broad standard. It was designed by IEEE to be all-encompassing for all kinds of different kind of software and all the different parts of the development process. The early part where you're actually defining the software, developing it, writing it, the implementation, the QA of incoming software, reuse, updating, all the different aspects. And it's also defined for a broad segment of the software population, which is why we have some exceptions because we're interested in using it in the nuclear area where we have some different applications.

DR. RANSOM: Does the NRC apply this to their own software?

MR. ARNDT: Funny you ask that. In the last couple of years, there's been some issues with the QA and quality associated with our internal software and the software we have contracted right for

us. So we've reviewed in several cases what kind of software QA and software validation and verification we should be using. In several cases, we have formally adopted this standard, the '98 version, as our standard with some exceptions and some modifications. In some cases, we're still discussing that. You'll hear next week about the sapphire code peer review, and that was one that we have decided to use this standard. As I said, there are some others that are undergoing discussion as to whether or not we should use this standard.

DR. WALLIS: And this covers all software?

MR. SIEBER: Safety-related software.

MR. ARNDT: This reg guide deals with safety-related INC software. The standard --

DR. WALLIS: That's very different from, say, reviewing a thermohydraulic code software.

MR. ARNDT: Yes. Yes, it is.

DR. WALLIS: And I don't think your intent is to apply this to thermohydraulic codes.

MR. ARNDT: The intent is not to apply the reg guide. The standard was written to be a broad standard with a lot of different --

DR. WALLIS: But what it's interested in is whether or not the software is true to the intent.

MR. ARNDT: That's correct.

DR. WALLIS: That's not to say that the function performed by the code itself is verified in any way. It's that if you put in an equation that the software truly represents that equation, it's not that the equation is a good one, right?

MR. ARNDT: The concept of verification and validation basically gets to that distinction. Verification is verifying that you wrote what you thought you wrote. You didn't write bugs into it. Validation goes to is it doing what the requirement said, to model things --

DR. WALLIS: Oh, that's very different. That's a huge task.

MR. ARNDT: It is a much more difficult task, and this has guidance on that.

CHAIRMAN BONACA: It includes comparison to --

MR. ARNDT: It includes how do you know what you wrote is proper, how did the requirements get put together and things like that.

DR. WALLIS: How does it compare with data and that sort of thing?

MR. ARNDT: Right. How does it compare with benchmarks, a number of things.

DR. WALLIS: That's a huge task.

MR. ARNDT: Yes. And this particular reg guide is dealing with a much, much smaller subset of that. It has to do with the actual safety system software.

DR. WALLIS: Well, if they could tell us how to validate thermohydraulic codes, that would be a real coup.

MR. ARNDT: That's why the implementation of a standard is not a trivial thing in things like a code or a thermohydraulic codes and things like that. But to answer Dr. Ransom's question, we are looking at it for in-house codes like that.

MR. MAYFIELD: This is Mike Mayfield. Steve, you may want to mention this international conference that's coming up.

MR. ARNDT: Yes, actually, thank you. One of the things that we're also doing from an NRC standpoint is looking at how these kinds of issues, as Dr. Wallis pointed out, is doable, what are the issues, what are the comparisons between things like real-time safety software and thermohydraulic codes and things like that. We're going to be having an NEA-sponsored workshop next summer, most likely in August, I don't think we've come to closure on the

dates, but I think it's going to be the second week of August of next year. It's going to be an international workshop on this specific issue: What are the techniques, what are the tools, what can we learn from this kind of work to apply to thermohydraulic codes --

DR. WALLIS: And the two on this are independent, because during the course of an accident if the code runs fast enough, you may want to run the thermohydraulic code in order to decide what decisions to make about where to come to some state at the plant.

MR. ARNDT: That has actually been discussed, particularly in Japan. They've been working on a program very similar to that.

DR. WALLIS: They're tied together.

MR. ARNDT: Yes. Did we beat that to death?

MR. SIEBER: Well, I think just to amplify Dr. Wallis' comments and questions a little bit, this standard actually does get to the phenomeninological modeling.

MR. ARNDT: It does.

MR. SIEBER: And it provides documentation so that you can follow what's going on in the coding

process, and I think that that is a leap forward as far as thermohydraulic codes are concerned. On the other hand, the application of this reg guide goes more to digital computers used as protection devices in power plants. Do we trip the reactor, and there's not so much of this phenominological modeling that goes on in those kinds of codes.

MR. ARNDT: That's correct.

MR. SIEBER: But the extension to other codes is -- it would make for an awful lot of paper but when you were all done I think you could have great faith in the product.

MR. SHAFFER: The Standards Committee that developed the standard was fairly broad. The members on the Standards Committee were fairly broad from the number of industries besides nuclear, such as medical and aerospace, so the regulatory positions taken in this revision to the current guidance have to do with taking exceptions to the standard to apply it to our systems, as mentioned.

The next slide move to the public comments and their resolution. The comment period on the draft guide was from March 5, 2003 to April 11, 2003. Two external stakeholders provides comments: South Carolina Electric and Gas Company and Progress Energy.

There were a total of four comment items, but there are only two really groupings. There's not very many comments, meaning it doesn't make sense to group them but that's the simplest way to handle them. These comments did speak to improved clarity.

MR. SIEBER: Those comments and their analysis and resolution is in Tab 16 of your books.

MR. SHAFFER: Both commenters, SCE&G and Progress, commented on the independence requirements in IEEE Standard 1012-1998. The concern was that staff was endorsing a -- potentially endorsing a level of control in excess of that in Appendix B. And Progress went further and said it may be broadly interpreted as a questioning existing organizational structure and independence. Our resolution was to agree with these comments and revise the draft guide accordingly. Next slide.

CHAIRMAN BONACA: So this means that they feel that the independence requirements in IEEE standards exceed the Appendix B requirements.

MR. ARNDT: Yes. The primary issue was having an independent organization do the V&V as opposed to a different part of one organization.

CHAIRMAN BONACA: I see what you mean.

MR. ARNDT: And that was beyond what we

traditionally require in Appendix B.

MR. SHAFFER: Yes. The standard talks about three forms of independence: Managerial, technical and financial independence. And NRC staff in the draft guide recommended that these three forms of independence be achieved as well as the separate organization.

DR. WALLIS: I don't quite understand this. This is making sure that the review is done by people who are independent of the main organization in some way?

MR. ARNDT: That's correct. And depending upon your interpretation of the standard, that would require someone actually in a different organization --

DR. WALLIS: Yes. You'd have to hire someone from outside your plant.

MR. ARNDT: Right. Right. And then that's beyond the current requirements within Appendix B.

MR. SIEBER: In fact, the early software that we wrote we did hire an outside contractor to do the V&V function, but it was opposed to the standard practice of engineering assurance where you had a branch within your own engineering department that did

the reviews, which was allowed by Appendix B. And so we wanted to make the computer software V&V function in the same kind of an organizational setting as you do regular engineering assurances.

CHAIRMAN BONACA: It is just a surprise that a requirement would exist for 1012. I mean this is regarding software verification and validation. I mean this means a level of understanding of the software that I believe only the people that developed it would have.

MR. ARNDT: That has been an open issue in the software business for quite some time. What are the qualifications of people performing V&V, not only their independence from the organization but also their knowledge of the type of software and the specific software. And that's -- even though it was incorporated in the standard the way it's stated, that's still a very open issue within the technical community. And because of the issue you bring up, there's a tradeoff between not having been involved with it and having a fresh eye and not having financial issues and things like that versus how well do you know it, how do you do it, and that's a very difficult balance to make. And, of course, we have the added issue of the previous guidance to deal with.

DR. WALLIS: Well, there's the question of accountability. I mean if a licensee does it himself, then he's accountable, but if he hires someone outside, then he has to do it himself anyway to be accountable --

MR. ARNDT: Exactly.

DR. WALLIS: -- so it doubles the work.

CHAIRMAN BONACA: And there are all kinds of issues there. I mean in some cases this may be proprietary software and who are you going to hire to do the verification and validation? I can see the concern.

MR. SHAFFER: Another comment from Progress was regarding the software grading process defined in 1012-1998. The nuclear industry uses a different approach to software quality than the one defined in 1012-1998. We use a -- the nuclear industry uses a two-tiered grading system: Safety and non-safety. The one defined in the standard is a four -- software integrity level one through four, four being the highest. Progress recommended that all safety system software at nuclear power plants be assigned safety software integrity level four, and we agreed with that and incorporated their recommendation.

DR. WALLIS: So there's nobody else who's protesting that?

MR. STEIN: No.

DR. WALLIS: One comment is suggesting it. No sign that other people would not approve of this?

MR. SHAFFER: Not to my knowledge.

MR. ARNDT: The real issue is the -- and that's one of the things that changed between the old standard and the new standard was to assign, in essence, an importance measure to software based on its criticality. And what is defined in the new standard is software integrity level, and they're based on things like if it fails, what are the consequences, what are the time frames and things like that. And it was originally in the standards were put together for this use in airplanes and things like that where if a computer program for routing the planes failed, it would not be as big a deal as if the flight --

MR. SIEBER: Hit the ground.

MR. ARNDT: -- computer failed and things like that. If you look at the definitions of the various skill levels, in all likelihood real-time safety systems would fall into category four anyway, because it's basically things that if it fails, the

consequence is immediate, and if it fails, the consequence has potentially severe aspects. The issue when we put out the draft was the concept of if you have a safety system that doesn't have those aspects, you could try and quantify it as a three or a two. The comment back was that, "That's not the way we're set up. We've got a QA program for safety systems and we have a QA program for everything else, and it doesn't make sense to add that evaluation to it," and of course the licensee is free so that this is just a preferred method to come back and say, "We would prefer to do it some other way," or they could come back under 5069, I think it is, the graded QA process, and also do it this way. So we don't preclude them from doing that, and we don't have any reason to believe anyone would want to do it a priori. In our graded QA applications, no one has come to us and said they wanted to do this for other reasons anyway. Did I answer your question? Okay.

MR. SHAFFER: Next slide. We're moving to the regulatory positions need, revision to the current guidance. First regulatory position is on critical software. Again, as we just discussed, safety system software in nuclear power plants should be assigned software integrity level four.

Second regulatory position is on software reliability and this reaffirms staff's position regarding quantitative reliability goals. We don't accept that as a sole means of meeting the Commission's requirements. When it comes to those systems, we like the hardware and software taken together to show some sort of indicator of -- provide assurance that the system meets the Commission's requirements. Next slide.

Next regulatory position is on independence and software verification and validation. Again, we talked about this earlier. This was the subject of one of the comments. There is guidance or requirements in the standard, 1012-1998, on managerial, technical and financial independence, and we consider these to meet the requirements in Appendix B, but this does not mean that they need someone outside their organization to perform software verification and validation.

Conformance of materials --

CHAIRMAN BONACA: How do you clarify this interpretation, I mean in the Reg Guide?

MR. ARNDT: Yes, in the Reg Guide. The structure is background, the statement that we endorse the standard is a means to meet the requirement, and

then the exceptions are written through the regulatory positions.

MR. SHAFFER: Conformance of materials is the next regulatory position, and this provides guidance on retrospective V&V of software not verified. That is reusable software.

Quality assurance is another regulatory position in that the standard -- there need to be additions to the provisions in IEEE Standard 1012-1998 in order to satisfy the criterion in Appendix B. We don't specify what those are, it's just additions need to be made.

Tools for software development is the next regulatory position, and this ensures that the tools used to develop the safety system software don't introduce errors or faults, and if they do, that the test methods will catch those. If this can't be demonstrated, then this regulatory guide -- the provisions in this regulatory guide will apply.

Regulatory Position 7 is verification and validation tasks. There are certain optional tasks or in the Standard 1012-1998 there are tasks identified as optional in the software V&V process. The staff position is some of these optional tasks are in fact part of a minimum set of activities for safety system

software, and they are given there: Audits, regression analysis, testing security systems, test evaluation and evaluation of user documentation. In Annex G to IEEE Standard 1012-1998, these are described in further detail.

DR. WALLIS: So the sort of thing you're verifying is that there aren't sort of typographical errors in a code. You're not verifying the robustness of the software in an environment where there might be random inputs that might disturb the software in some way?

MR. ARNDT: The verification is that the code operates correctly --

DR. WALLIS: Right.

MR. ARNDT: -- based on --

DR. WALLIS: Just like proofreading a manuscript really.

MR. ARNDT: Yes, in somewhat more complicated ways, because you can't go down every path in a software code, although these are much, much simpler than what you would think of in a computational code. So you do things like software audits, regression testing, things like that.

DR. WALLIS: It doesn't get hung up in some loop somewhere.

MR. ARNDT: Right, things like that. The validation part of it gets to things like test evaluation and things like that. You try and determine whether or not your tests are really testing the function of the system and things like that. And part of that is is there an opportunity for something like a random failure or things like that to bring down the system? There's always going to be failures, which goes to the reliability issue, but this is to validate that what you did is what you wanted to do.

MR. LEITCH: So these regulatory positions are in some cases exceptions to the standard or amplification to the standard?

MR. ARNDT: They are exceptions to the standard. They're saying if you do everything in the standard, you're going to be okay except in some cases you don't have to do as much, like the independence; in some cases you need to do more, like this one.

MR. LEITCH: Okay.

MR. ARNDT: So just think of it as here's the standard, that's everything you need to do. Take these pieces out, stick these pieces in, and you're set.

MR. LEITCH: Now, are these seven, I think you've referred to here, are they all they are or you

just telling us seven of the more important ones?

MR. SHAFFER: There's an eighth regulatory position on other codes and standards, and in that -- we use that in other regulatory guides. It just says if the endorsed standard references other standards, you need to take those one by one.

MR. LEITCH: So that's kind of an administrative --

MR. SHAFFER: Right. In conclusion, regulatory guide final, Draft Regulatory Guide 1.168 Revision 1 endorses current IEEE standards, IEEE Standard 1012-1998, IEEE Standard 1028-1997. The regulatory positions, which are exceptions to the standards, are consistent with the Commission's requirements and also with Standard Review Plan Chapter 7. There's no backfit issues. Our regulatory analysis show there's no backfit issues and whatever endorsement --

DR. WALLIS: So in terms of enforcement, you'd simply check that the licensee has gone through the process properly.

MR. SHAFFER: That's correct.

DR. WALLIS: You wouldn't dig any deeper than that, presumably. If they say they're following the standard, you believe it.

MR. ARNDT: Well, you really need to talk to NRR about enforcement issues, but the review is that they have done what they said they were going to do. And then if you want to go out and look at inspections, then you look at whether or not -- how they've done what they do.

CHAIRMAN BONACA: Could you give me a sense of what are the substantive changes of the IEEE standards that are being referred to Rev 1, referred to Rev 0?

MR. ARNDT: The biggest difference, as I think we've talked about earlier, is that -- well, biggest two differences in 1012 is that 1012 is a much more comprehensive document than it used to be. The older version was basically just a procedure for doing a V&V. The new one is much more detailed, how do you figure out what you're going to do, what kinds of issues you're going to have and things like that. It also introduced the software integrity level concept, the four graded systems, and maps very detailed, we've got whole sets of charts like that, that basically talks about if you have this kind of software and this kind of part of its development, these are the kinds of things you need for software integrity level four, five, three. So those are the two major differences,

as Roman pointed out earlier.

And the other standard is mostly clarification and cleaning up language, making sure it's self-consistent and things like that. As we've mentioned, we've determined that we're going not take advantage of the skill levels as such; however, the standard now has a lot more information about what it is you need to do for a skill level four than it previously had. Did I miss anything.

MR. ROSEN: Over the years, EPRI has been very active in the area of validation and verification of software. What has been their role, if any, in this process, or did you get any comments from EPRI?

MR. ARNDT: We did not. We have discussed this as well as other parts of the standard review plan with EPRI on a relatively frequent basis. And I actually was out at EPRI this summer, I think it was August, talking about software issues, and they did not raise this as an issue they wanted to weigh in on.

MR. MAYFIELD: Mr. Chairman, that concludes the staff's presentation unless the Committee has other questions. Again, we are requesting a letter to move forward on this. Thank you.

MR. SIEBER: Okay. If there are no other

questions, any member have a question they'd like to ask? I have these standards here and all the documentation if anybody would like to look at them. And if there are no questions, Mr. Chairman, I turn it back to you.

DR. RANSOM: I have a small one. The standard governing coding standards in the software, does it get into that level of detail?

MR. SIEBER: You mean like how closely do you adhere to Fortran 4?

DR. RANSOM: Right, that kind of thing or --

MR. ARNDT: No, it does not get into that level of detail.

DR. RANSOM: The testing, does it get involved with looking for things like dead code, conflicts?

MR. ARNDT: It talks about generic kinds of testing that you need to do. If you look at software testing metrics and things like that, the concept of looking at requirements testing versus coding testing versus regression testing and things like that, it will get down to that level of detail, but it won't say if you have this kind of buffer array, you need to do this kind of test.

MR. SIEBER: Any other questions. Okay, Mr. Chairman.

CHAIRMAN BONACA: Okay. Thank you very much for your presentation. I think we'll go off the record now and we'll take a long break. We're ahead of time and let's take a break until 20 of ten, and at that time we'll hear subcommittee report on reactor fuels.

(Whereupon, at 9:09 a.m., the ACRS open session was concluded.)

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 506th 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.

Eric Hendrixson

Eric Hendrixson
Official Reporter
Neal R. Gross & Co., Inc.

United States Nuclear Regulatory Commission

Regulatory Guide 1.168, Revision 1 "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

Roman A. Shaffer
Division of Engineering Technology
Office of Nuclear Regulatory Research

October 3, 2003

United States Nuclear Regulatory Commission

OVERVIEW

- BACKGROUND
- RG 1.168, REVISION 0
- RG 1.168, REVISION 1
- RESOLUTION OF PUBLIC COMMENTS
- REGULATORY POSITIONS
- CONCLUSION

BACKGROUND

- Software engineering practices rely, in part, on software Verification and Validation (V&V) activities as well as reviews and audits to meet the Commission's regulations regarding quality and reliability, e.g., Criteria contained in Appendices A and B to 10 CFR Part 50

- NRC staff endorses consensus standards (e.g., IEEE Standards) as acceptable methods for meeting these quality and reliability requirements

RG 1.168, REVISION 0

- Issued in September 1997
- Endorses two IEEE standards
  - IEEE Std 1012-1986
  - IEEE Std 1028-1988
- Exceptions taken to these standards
- Appendices are not endorsed, but some V&V tasks identified in IEEE Std 1012-1986 as "optional" are considered by NRC staff to be "acceptable methods"

RG 1.168, REVISION 1

- Responds to User Need Request NRR-2002-017

- RG 1.168, Revision 1, endorses two IEEE standards with exception
  - IEEE Standard 1012-1998, "IEEE Standard for Software Verification and Validation"
    - A process standard that defines the verification and validation processes in terms of specific activities and related tasks. In the 1998 revision, the guidance in IEEE Std 1012-1986 is incorporated as one component of the V&V process
  - IEEE Standard 1028-1997, "IEEE Standard for Software Reviews and Audits"
    - A standard defining five types of software review, together with procedures required for the execution of each review type

United States Nuclear Regulatory Commission

RESOLUTION OF PUBLIC COMMENTS

- Comment period March 5, 2003, to April 11, 2003
- Two external stakeholders provided comments
  - South Carolina Electric and Gas Company (SCE&G)
  - Progress Energy (Progress)

RESOLUTION OF PUBLIC COMMENTS (cont.)

- SCE&G and Progress both commented on *independence* requirements ("IV&V") in IEEE Std 1012-1998
  - Potential endorsement of "a level of control in excess of that imposed by" Criteria I and III of Appendix B to 10 CFR Part 50
  - Potential imposition of organizational structure re-alignment, and could "be broadly interpreted as questioning existing organization structure and independence"
- RESOLUTION

RESOLUTION OF PUBLIC COMMENTS (cont.)

- Progress commented on software grading process
  - Nuclear industry uses a different approach to software quality than the one defined in IEEE Std 1012-1998
  - Progress recommends that all safety system software be assigned highest software integrity level 4
- RESOLUTION

REGULATORY POSITIONS

1. CRITICAL SOFTWARE

Safety system software in nuclear power plants should be assigned software integrity level 4

2. SOFTWARE RELIABILITY

Staff does not endorse quantitative reliability goals as a sole indicator of meeting the Commission's regulations for reliability of digital safety systems

REGULATORY POSITIONS (cont.)

3. INDEPENDENCE OF SOFTWARE VERIFICATION AND VALIDATION

IEEE Std 1012-1998 guidance on managerial, technical, and financial independence satisfy requirements of Criterion I of Appendix B to 10 CFR Part 50, though this does *not* mean that a separate company is required to perform independent V&V of safety system software

4. CONFORMANCE OF MATERIALS

Guidance on retrospective V&V of software not verified under the standard (i.e., COTS software) can be found in Annex D, "V&V of Reusable Software," to IEEE Std 1012-1998

REGULATORY POSITIONS (cont.)

5. QUALITY ASSURANCE

Additions to the provisions contained in Clause 7.7.4 of IEEE Std 1012-1998 are necessary to satisfy Criterion XVII of Appendix B to 10 CFR Part 50 regarding records keeping

6. TOOLS FOR SOFTWARE DEVELOPMENT

If provisions contained in IEEE Std 7-4.3.2-1993 regarding V&V of software development tools cannot be demonstrated, provisions in RG 1.168, Revision 1, will apply

REGULATORY POSITIONS (cont.)

7. VERIFICATION AND VALIDATION TASKS

The following V&V tasks identified in Table 3 of IEEE Std 1012-1998 as "optional" are, in general, considered by NRC staff as part of the minimum set of V&V activities for safety system software:

a. Audits
b. Regression Analysis and Testing
c. Security Assessments
d. Test Evaluation
e. Evaluation of User Documentation

CONCLUSION

- REGULATORY GUIDE 1.168, REVISION 1 ENDORSES CURRENT IEEE STANDARDS
- REGULATORY POSITIONS ARE CONSISTENT WITH COMMISSION'S REQUIREMENTS AND SRP CHAPTER 7
- NO BACKFIT ISSUES
- LETTER OF ENDORSEMENT