

**NUCLEAR REGULATORY COMMISSION**

ORIGINAL

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

TROY

1 UNITED STATES OF AMERICA  
2 NUCLEAR REGULATORY COMMISSION

3 + + + + +

4 ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

5 506th ACRS MEETING

6 + + + + +

7 FRIDAY, OCTOBER 3, 2003

8 + + + + +

9 ROCKVILLE, MARYLAND

10 + + + + +

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

14 Present:

15 Mario V. Bonaca	ACRS Chairman
16 Graham B. Wallis	ACRS Vice-Chairman
17 Graham M. Leitch	ACRS Member
18 Dana A. Powers	ACRS Member
19 Victor H. Ransom	ACRS Member
20 Stephen L. Rosen	ARCS Member-at-Large
21 Thomas S. Kress	ACRS
22 William J. Shack	ACRS
23 John D. Sieber	ACRS

24  
25  
**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1     Staff Present:

2     Steven Arndt                   RES

3     Sher Bahadur                   Associate Director, ACRS/ACNW

4     Sam Duraiswami                 Technical Assistant, ACRS/ACNW

5     Medat El-Zeftawy               ACRS Staff

6     Michelle Evans                 Engineering Research Application

7                                     Branch

8     Tony Hsai                       Engineering Research Application

9                                     Branch

10    Howard J. Larson               Special Assistant, ACRS/ACNW

11    Mike Mayfield                 Engineering Research Application

12                                     Branch

13    Roman A. Shaffer               RES

14

15

16

17

18

19

20

21

22

23

24

25

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

I-N-D-E-X

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

AGENDA

PAGE

Review of Draft Final Revision to Regulatory Guide 1.168 4

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

## 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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

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

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

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

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 doing that.

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

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

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

1 Guide.

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

12 DR. POWERS: How dare you?

13 (Laughter.)

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

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

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealgross.com

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

5 I'll give a little background information,  
6 try to define a little verification and validation  
7 exactly and provide an opening statement of some sort.  
8 Then we'll move on to the current guidance contained  
9 in Regulatory Guide 1.168 Revision 0. Revisions to  
10 this current guidance contained in Regulatory Guide  
11 1.168 Revision 1. Resolution of the public comments  
12 we received on the draft guide and regulatory  
13 positions in the final draft guide to Revision 1. If  
14 you can't hear me or if I'm speaking too quickly,  
15 please let me know.

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

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

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

11                   MR. SHAFFER: Yes.

12                   MR. SIEBER: Those are the old standards.

13                   MR. SHAFFER: Those are the older  
14 standards.

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

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

19                   MR. SIEBER: The new version is here.

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

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

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

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

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

24 MR. SIEBER: Just software.

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

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

4 MR. SHAFFER: Yes.

5 MR. SIEBER: All.

6 MR. LEITCH: All of the above.

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

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

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

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

12 DR. WALLIS: And this covers all software?

13 MR. SIEBER: Safety-related software.

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

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

18 MR. ARNDT: Yes. Yes, it is.

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

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

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 MR. ARNDT: That's correct.

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

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

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

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

17 CHAIRMAN BONACA: It includes comparison  
18 to --

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

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

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 DR. WALLIS: That's a huge task.

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

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

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

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

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

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

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

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

16 DR. WALLIS: They're tied together.

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

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

23 MR. ARNDT: It does.

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

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

8 MR. ARNDT: That's correct.

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

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

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

24 CHAIRMAN BONACA: I see what you mean.

25 MR. ARNDT: And that was beyond what we

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 traditionally require in Appendix B.

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

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

12 MR. ARNDT: That's correct. And depending  
13 upon your interpretation of the standard, that would  
14 require someone actually in a different organization  
15 --

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

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

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

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

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

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

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

6 MR. ARNDT: Exactly.

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

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

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

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

3 MR. STEIN: No.

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

6 MR. SHAFFER: Not to my knowledge.

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

20 MR. SIEBER: Hit the ground.

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

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

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

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

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

20           Conformance of materials --

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

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 then the exceptions are written through the regulatory  
2 positions.

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

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

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

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

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

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

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

14 DR. WALLIS: Right.

15 MR. ARNDT: -- based on --

16 DR. WALLIS: Just like proofreading a  
17 manuscript really.

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

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

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

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

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

19 MR. LEITCH: Okay.

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

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

1 just telling us seven of the more important ones?

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

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

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

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

22 MR. SHAFFER: That's correct.

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

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

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

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

1 as Roman pointed out earlier.

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

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

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

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

25 MR. SIEBER: Okay. If there are no other

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

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

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

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

11 DR. RANSOM: Right, that kind of thing or  
12 --

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

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

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

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

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

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

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

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

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

506<sup>th</sup> 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  
Official Reporter  
Neal R. Gross & Co., Inc.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS  
1323 RHODE ISLAND AVE., N.W.  
WASHINGTON, D.C. 20005-3701



# 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



# United States Nuclear Regulatory Commission

## 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



# United States Nuclear Regulatory Commission

## 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”



# United States Nuclear Regulatory Commission

## 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)



## United States Nuclear Regulatory Commission

### 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



## United States Nuclear Regulatory Commission

### 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



---

# United States Nuclear Regulatory Commission

---

## 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



## United States Nuclear Regulatory Commission

### 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



---

## United States Nuclear Regulatory Commission

---

### 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



# United States Nuclear Regulatory Commission

## 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



# United States Nuclear Regulatory Commission

## 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