Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Wednesday, June 5, 2013

Work Order No.: NRC-4286 Pages 1-140

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

1
2
3
4 DISCLAIMER
5
6
7 UNITED STATES NUCLEAR REGULATORY COMMISSION'S
8 ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
9
10
11 The contents of this transcript of the
12 proceeding of the United States Nuclear Regulatory
13 Commission Advisory Committee on Reactor Safeguards,
14 as reported herein, is a record of the discussions
15 recorded at the meeting.
16
17 This transcript has not been reviewed,
18 corrected, and edited, and it may contain
19 inaccuracies.
20
21
22
23

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

605TH MEETING

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

WEDNESDAY

JUNE 5, 2013

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Advisory Committee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B1, 11545 Rockville Pike, at 8:30 a.m., J. Sam Armijo, Chairman, presiding.

COMMITTEE MEMBERS:

J. SAM ARMIJO, Chairman

JOHN W. STETKAR, Vice Chairman

HAROLD B. RAY, Member-at-Large

DENNIS C. BLEY, Member

CHARLES H. BROWN, JR. Member

MICHAEL L. CORRADINI, Member

DANA A. POWERS, Member

JOY REMPE, Member

MICHAEL T. RYAN, Member

STEPHEN P. SCHULTZ, Member

WILLIAM J. SHACK, Member

GORDON R. SKILLMAN, Member

NRC STAFF PRESENT:

MARK BANKS, Designated Federal Official

EDWIN M. HACKETT, Executive Director

CHRISTINA ANTONESCU

STEVEN ARNDT

ERIC BOWMAN

MICHAEL CASE

MICHAEL CHEOK

SHANA HELTON

EILEEN MCKENNA

TIM REED

KARL STURZEBECHER

JOHN THORP

ALSO PRESENT:

RONALD BALLINGER

*Present via telephone

A G E N D A

Opening Remarks by ACRS Chairman..... 4

Station Blackout Mitigation Strategies

Rulemaking..... 6

Revisions to Six Regulatory Guides on

Use of Digital Software..... 89

P R O C E E D I N G S

8:29 a.m.

Opening Remarks

CHAIRMAN ARMIJO: The meeting will now come to order. This is the first day of the 605th meeting of the Advisory Committee on Reactor Safeguards. During today's meeting, the Committee will consider the following:

First, Station Blackout Mitigation Strategies Rulemaking. Second, Revisions to Six Regulatory Guides on the Use of Digital Computer Software in the Safety Systems in Nuclear Power Plants. Third, Assessment of the Quality of Selected NRC Research Projects, and fourth, Preparation of ACRS reports.

This meeting is being conducted in accordance with the provisions of the Federal Advisory Committee Act. Mr. Mark Banks is the Designated Federal Official for the initial portion of the meeting. We have received no written comments or requests to make oral statements from members of the public regarding today's sessions.

There will be a phone bridge line. To preclude interruption of the meeting, the phone will be placed in a listening mode during the presentations

and Committee discussion. 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.

I would like to open with an item of interest. Drs. Peter Riccardella and Ronald Ballinger have been selected as new members of the ACRS. Dr. Ballinger, who is joining us here today as an invited expert, has over 40 years of experience with metallurgy and materials in nuclear power applications, and is currently a Professor of Nuclear Science and Engineering at the Massachusetts Institute of Technology.

Dr. Ballinger has worked on cooperative research programs at EPRI, has served or is serving on several Department of Energy committees regarding disposition of waste streams at DOE sites, and evaluation of advanced reactor options. He has authored or co-authored over 100 scientific papers, and is a member of several professional societies, including the American Nuclear Society and ASTM.

Dr. Ballinger has worked previously with ACRS as a consultant on issues related to steam generator, tube degradation and leakage. Welcome

aboard, Ron.

(Applause.)

CHAIRMAN ARMIJO: Dr. Pete Riccardella has over 45 years of experience in the nuclear industry. In particular, he is an authority in the application of fracture mechanics to nuclear pressure vessels and fissures. Dr. Riccardella has had significant involvement with the American Society of Mechanical Engineers during his career.

In 2001, he became an honorary member of ASME Section 11 Subcommittee on Nuclear Power Plant In-Service Inspection, and in 2005, was named an ASME Fellow. Dr. Riccardella was a founding member of Structural Integrity Associates, which has been an industry leader in failure prevention and failure analysis.

We hope to have them both on board as official ACRS members by this fall. Again, welcome aboard. With that, I'd like to turn the meeting over to Dr. Bill Shack, who will lead us through the presentation on Station Blackout Mitigation Strategies. Bill.

Station Blackout Mitigation Strategies

MEMBER SHACK: Okay. Again, one of the recommendations of the near-term task force was to

essentially develop a new station blackout rule that would cover extended station blackouts. In the meantime, we've issued an order, EA.12-049, which again mitigating strategies, again which addresses extended blackouts.

What the staff is here to present to us today is a regulatory basis to go forward with a new station blackout rule, that in a way addresses the concern of the Near Term Task Force, and essentially perhaps codifies the order and makes it generically applicable.

Again, they'll be talking about the regulatory basis to do that and some rule concepts. Mike Cheok wants to make the presentation.

MR. CHEOK: Thank you, Dr. Shack. Again, good morning. My name is Mike Cheok. I'm the Deputy Director in the Division of Engineering in NRR. It's a pleasure for us to be here to talk today at ACRS on our efforts, on our rulemaking efforts for station blackout mitigating strategies, and to provide you with a status of our leading strategies for those.

At this point, the staff has issued and completed a draft regulatory basis, and have issued this for a 45-day comment period. This comment period ended last week on May the 28th. Our objective today

is to discuss this reg basis with you, and to get your comments.

Over the next month, the staff will be working on a Commission Assistance Note or MR. CASE: Note to inform the Commissioners of our progress. We will incorporate your comments and your feedback into our Commission Assistance Note.

Over the longer term, the staff will be working on the draft rulemaking, the draft package, and it will use your comments today to start our initial writing of the draft rule.

So from, going from the reg basis to the draft rulemaking to the final rule, we will continue to update the ACRS as requested, and we will come back and talk to you about the status of what we're going to be doing.

So today, we will have Tim Reed, who will talk about the reg basis. We will Eric Bowman, who will talk about the status of the mitigating strategies order, and Eileen McKenna from NRO will entertain any questions that deal with reactors. So Tim.

MR. REED: Okay, thanks Mike. It's a pleasure to be back in front of the ACRS again today. Mike just covered the purpose slide, so I don't think

we need to do that again. So I'll move to Slide 3. A lot of this going to be familiar to you folks, because you've heard a lot of it more than about a month ago, I guess it was.

So I'll shorten this, real condensed on the background, so we can have an opportunity to try to get through all of this material in an hour and a half. So I'll breeze through this background kind of quickly, and get to I think what is much more important, and that's the actual concepts, which is the balance of this presentation.

But as we've pointed out, we've briefed the Subcommittee on Regulatory Policies and Practices twice. We briefed you at committee in December 2012, and then also here recently on April 23rd. So most of you are familiar with a lot of this information.

The scope and schedule for this regulatory action station blackout mitigation strategies rulemaking was substantially changed by COMSECY-13-0002. That was issued in January of this year and then we've got an SRM, agreeing with the scope and schedule from the Commission in March.

What that basically did was the third bullet there, revised the scope to basically address all of the actions stemming from NTTF Recommendations

4 and 7 into this rulemaking, and to place, put in place a much more normal rulemaking schedule.

In other words, now we -- in fact, as Mike just mentioned, we actually had an opportunity to develop the reg basis federally, put that out for comment for 45 days. Now we'll have a proposed rule stage and a final rule stage, and under the former schedule that wasn't possible.

Of course, this was justified because of the scope of the mitigation strategies order, EA.12-049, that was issued on March 12th of 2012. Basically, it's addressing, in large measure, a recommendation for and addressing those issues, any safety issues, in basically about the fastest schedule possible with licensees.

So that was -- the very good answer, we're addressing safety as fast as possible with the order, and allows us to do rulemaking on something a lot closer to a normal rulemaking process. You see --

MEMBER SHACK: A question there.

MR. REED: Yes sir.

MEMBER SHACK: When I looked on the rulemaking website, there were very few comments on this rule. Is that just because they were late in posting?

MR. REED: There's some coming in kind of late. We have now ten sets, and I expect an additional set coming from NEI, with the real detailed comments from NEI on June 20th. So --

(Simultaneous speaking.)

MEMBER SHACK: You still have some coming in well past the deadline?

MR. REED: Yeah, yeah. Sometimes it takes a while for some of that to get processed, depending on which forum it comes through, whether it comes regulation.gov or through the mail or whatever. So it can take a while. Shana?

MS. HELTON: Hi. This is Shana Helton, NRRN. I'd just like to note that, you know, we always, as a matter of practice, try to consider late-filed comments to the extent practical, unless there's some extenuating circumstances. In this case, it's just the regulatory basis stage.

If we can consider the comments as we finalize the regulatory basis, that's fine. Even if we can't, if they come in too late for our due date, then we can consider any late-filed comments as part of the development of the proposed rule package.

MR. REED: Absolutely. That's -- a lot of the most -- we took the opportunity, when we put the

reg basis out, really the draft rule concepts in the appendix is the most important part for me anyway, and most of the substantive comments are coming in on that.

A lot of that work is going to be realistically done in the proposed rule stage, and I think NEI's comments will be addressed largely in that stage. Yes. So right now, I'm aware of 10 sets. Very good comments, in fact, from mostly the new reactor designers.

So and I'll try to address those as I go through. I've gone through that one time very quickly, so if I see something on a slide, I'll try to mention where I got feedback there, as we go through this.

So we mentioned that the -- I got the, by the way I got the schedule on there as June 30th, 2014. That's next, end of next June, next year for the proposed rule, and any supporting draft guidance to the Commission. So that's the current rulemaking schedule.

Then we've lined up the final rule to line up with the ultimately implementation of EA.12-049, with December 2016, because the drop dead date right now for the mitigation strategies order is December

31st of 2006. So we're trying to line these two things up here, so they work in lock step like that.

So and then 45 day comment period, ten sets of comments. It was actually at 48, I think, days that ended on May 28th, because we had a holiday. So that's the background.

Slide 4, the basis for this rulemaking is actually kind of straightforward, as opposed to what it can be sometimes on rulemakings truthfully as well. Because we have a mitigation strategies order that was issued to all current licensees, all licensed power reactors in fact, including Vogtle and Summer, two COLs.

Obviously, those requirements are in any form aren't in any form of the Code of Federal Regulations, that what we typically do in NRC in rulemaking, we make those what I, the language I'm using, is make those generically applicable.

So that we have a stable, known set of requirements for everybody to comply with. It's not something that's going to be shifting with each order or license condition in the future. It's the best way to do things, because it's an open format. It allows us to learn lessons from the implementation of the order, allows us perhaps to have some flexibility.

We have a lot more time and generic flexibility, and it's done when we did the orders, which were done in extraordinarily expedited fashion. So that's all part of this rulemaking. But in fact, I think the rulemaking is an absolute certainty, of course, because of this situation.

So we don't really have a situation where we have to go through and justify our rulemaking like we might typically have some of the other Fukushima actions, okay.

And of course, the orders, especially because the current station blackout requirements, which for the United States reside in 10 C.F.R. 50.63, did not really do what we wanted to be done. This is -- obviously, this is stemming from a very severe event, which could damage onsite and offsite AC power sources, don't damage the entire site.

It can go for quite a long time, and it certainly can devastate offsite AC power sources, and that creates completely different situation than what 50.63 was looking at. And since it's a low duration event, you get into other issues like spent fuel pool cooling, which 50.63 was not concerned with.

The order is applying these requirements to all modes of operation, and so I suspect that the

rulemaking would do so also, and of course 50.63 did not do that. So 50.63 was as, I think everybody's aware, was a cost-justified substantial safety enhancement, which turned to be cost-justified. So as that was demonstrated to be cost-justified by NUREG-1776.

So it was a very successful regulation for what it did, but it's got kind of a different focus than the mitigating strategies. But having said that, and ELAP is a severe blackout that goes on essentially for -- I will get to the next slide here.

But so they kind of went together nicely, as we'll see here in a minute. So that's the reason why we're doing this rulemaking. I think that wouldn't be a surprise to anyone.

Now I'm going to get to, I think, the rest of this really is trying to get to these draft rule concepts that were in the appendix, and these slides are largely look like the slides that I presented last month. We didn't have an opportunity really to go through all the comments that we've got right now and try to change some of this.

But if we did, if I could pull the rulemaking group together, I think you'd see a lot of this changing already, because I think we're probably

too restrictive on the new reactor designers, have a little bit too much of a current licensee mind set. But nonetheless, as I go through, I'll try to reflect some of the comments that we've had, and I'll try to mention that as we go through.

One of the things we did to try to provoke external stakeholder feedback in the draft rule concepts is we put out an ELAP definition, and the very first thing you'll notice about that is I don't have a loss of normal access to the ultimate heat sink there.

That was in the order, okay, and we intentionally did not put that in here. The idea was to provoke comments, see what people thought about the fact that why should you assume the loss of normal access to ultimate heat sink unless it's -- if it's a direct consequence of ELAP, of course it's assumed, and if you would expect it to occur from the external event. In other words, that equipment is not reasonably protected; of course you would assume it to occur. But why would you assume it any other way?

So that was put out there to provoke comment. We got some pretty interesting comments so far. We're looking at that. There seems to be some agreement that if you have a divers, robust type of

heat sink powered source, then maybe it should be allowed. It provides, consistent with the supplemental AC power, which you'll see later, some opportunities for engineers, I think, to design in physical protection here. It might be advantage over human reliance.

So that was kind of the intent there. Clearly though, if -- one of the interesting things I got is people didn't like the way I separated the little pieces of the ELAP definition. It's kind of confusing. It's all those things added together down there at the bottom of the slide.

MEMBER CORRADINI: So can I ask a question, since I wasn't at the Subcommittee meeting. What does "extend indefinitely" mean?

MR. REED: That's another --

(Simultaneous speaking.)

MEMBER CORRADINI: I mean so are you saying that there's no probability, there's no cutoff frequency? I know you don't really mean that. So what are you thinking?

MR. REED: I think actually we got feedback to that extent right now, and that's something I think we'll need to think about, I think the order needs to think about. We have a multiple

phased approach right now for current licensees, with the last phase being a reliance on offsite resources, okay. But then at what point do you say you're okay?

MEMBER CORRADINI: Right. But so I mean let's just take the current, let's just take the current situation. As you said, this was for a different purpose. It had some sort of cost-benefit analysis that's attached to it. But with the current rule, you have to show that you can essentially recover within some time period.

So what's that probability versus -- I mean there must be estimates of all this. So has staff at least gotten some feeling as to what you want to extend it to, or are you letting the rulemaking proceed such that you'll just see what input you get?

I'm still struggling with are you going to give a suggestion, a straw man? Are you going to let it just sit out there, because indefinite definitely makes to me no sense, personally. It just seems way too big.

MR. REED: Yeah, it's impossible. I know what you're saying, but I think this is a case where I think we need to see what is implemented. I mean for example, you could have a success criteria that says once you've established offsite assistance, and

basically that line of assistance is established, you can say okay, you're successful.

In other words, you're doing what you can do. That would be one way. I don't know how we're going to call success. I mean obviously, you can't for some of these scenarios say you're going to be successful.

I can't say, for example, I'm going to get the cold shutdown or something, given a situation like you've destroyed the facility. There may not be a successful mitigating event.

But what you do have is all this equipment, the strategies, the guidance in place. You have it planned out. You have it worked through. You have a good chance of mitigating that you didn't have before. That's definitely better than what existed in 50.63, which was typically the scoping periods were designed to have about a 90 percent chance of recovery within those, yeah.

So this is an indefinite thing now. I mean indefinite being I want you to be able to go well beyond that, to some point where we can say okay, realistically we're going to start getting power back on site. You're going to realistically now reestablish some of the normal --

MEMBER BLEY: So Tim said outside assistance, and we have the flex program that's going on at the same time.

MR. REED: Exactly.

MEMBER BLEY: So I think what he's saying is, and you can correct me, they've got to be able to look long enough that whatever comes in from offsite to support them comes up there.

MEMBER CORRADINI: Well I mean I was expecting you to say back to me that you don't want to define what indefinite is, because you'll allow for multiple definitions of success. So if that's the case, that's fine. I'm just curious if you have some examples of success.

So one is essentially you extend by flex. You extend, you essentially are able to reestablish. That's a definition, not the only one. Is that your point?

MR. REED: That would be one.

MR. CHEOK: And I think another point could be indefinitely might not be time base. It could be a situation base. So you would say define a success statement. If you can get to, achieve to that success state, and that's how we will define when the SBO ends. So it may not be time-based; it could be

performance-based.

MR. BOWMAN: If I could, this is Eric Bowman. I'm the staff lead for the mitigating strategies order.

The inclusion of the phrase "extends indefinitely" as it occurred under the mitigating strategy order and as is being carried forward into the station blackout mitigating strategies rulemaking is based in large part on addressing shortfalls that we had the (b)(5)(B) mitigating strategies, where we set the mission times for the strategies at 12 hours, and didn't look to the use of offsite resources to extend the mission times.

So under that set of strategies, because it was not envisioned as being a large regional catastrophe, that would prevent calling a local supplier of diesel fuel from coming in and refilling the fuel tanks for the portable pumps they use there, we felt that it was acceptable to merely require sufficient fuel and water resources for a 12-hour mission time.

Here, looking at what occurred at Fukushima, we felt it was more appropriate to include the requirement extending indefinitely, meaning that there has to be some kind of provisions made for the

delivery of fuel from offsite or the use of the large fuel tanks that are onsite to refuel the pumps, to the extent that it's possible, and you could think of a success path that maintaining or restoring core cooling, for example, is one of the requirements.

If they manage to restore power, AC power to the electrical buses and get back to a normal circumstances where they're using the normal systems for the maintenance of core cooling, they're going to be able to do that indefinitely, until something else happens perhaps. But the idea is we don't have an end point for the need to maintain the safety functions.

MEMBER CORRADINI: But I think this could end up -- we don't know yet obviously. But I think you could end up not saying the word "indefinite" in a rulemaking, but a phased thing with offsite assistance or something like that, to get away from something which is impossible to comply with.

MR. REED: Right. But I think I see where you guys are going with this. But I'm, at least the way it's phrased here, and I was looking through some of the backup reading material, I was confused. I think I understand a little bit more.

MEMBER REMPE: When you start relying on offsite sources, what happens if there's a bridge out

for repair for a month or something like that? Is that going to be part of it; they'll have to report that this will occur?

MR. REED: Yes. Transportation issues are going to be in here too. We have some language -- I think do we have it on here, the slides, or we didn't have that? I think we didn't. But transportation to the site is an issue in a severe event like that.

MEMBER REMPE: Restoring normal operations. Suddenly, you know, that --

MR. REED: Yeah. That would be like an earthquake takes out the bridge.

MEMBER REMPE: But I mean just for maintenance.

MR. REED: Oh.

MEMBER CORRADINI: Her point is you're operating perfectly fine operationally, but your plan to satisfy this rule has this key bridge having to be there.

MEMBER REMPE: Right.

MEMBER CORRADINI: So that if something happens, this is going to be transported by that. That bridge is out for a month. So all of the sudden, your station blackout success path is compromised. I think that's it.

MEMBER REMPE: Right, exactly. So is there going to be reporting, you know, they've got to start telling you when the bridge is going to go out for a month, and then you'd have alternate plans? I mean I was reading the material too. I was just thinking of what ifs that could occur.

MR. BOWMAN: Well, the requirement as it's listed in the EA.12-049 mitigating strategies order is for the licenses to develop, implement and maintain the guidance and strategies. So the licensees have an obligation, if the bridge goes out, to figure out an alternate method of delivery of the offsite resources.

Whether or not it's reportable is not addressed in the order, but would be addressed elsewhere.

MEMBER CORRADINI: Okay, but just I'm -- I mean I was trying to turn around the first -- I'm still stuck on the first sentence, and then I'll stop. What you're really saying is you want it basically to show long-term decay heat removal under, excuse the rephrasing, under all circumstances.

That's really what you're saying. Under all circumstances, you want to show that you can successfully remove decay heat, remove decay heat from

the core and the fuel and the spent fuel pool, and maintain the containment function.

MR. REED: I'm a little -- I would say you have to have strategies, guidance and equipment in place that has reasonable capability of doing that. You may not be in fact successful. Okay. So I'm a little -- on the success criteria with a situation like this.

MEMBER CORRADINI: That's fine, okay. That's fine. I'll stop. Thank you very much.

MR. REED: But I see what you're saying.

MEMBER REMPE: Thinking about the reportability thing and implementation on a reasonable chance of success, I'm just wondering again if you start having to report when a bridge is out for a month, well is it a week or a month.

The implementation of this is what was really I was struggling with when I was reading this, and how fine in detail are we going to go to.

VICE CHAIRMAN STETKAR: I mean emergency plans face the same issues in terms of evacuation routes and things like that. People deal with that.

MEMBER REMPE: And how do they deal with it? I mean --

VICE CHAIRMAN STETKAR: I don't know.

They don't report it.

MEMBER REMPE: So they don't report. They just ignore it. So if the bridge was out --

VICE CHAIRMAN STETKAR: No, no. They don't ignore the bridge is out. They have to have alternates in place, I believe. But they don't have to -- I think John's point is they don't have to, it's not a reportable event, from the licensee's perspective.

MEMBER SCHULTZ: Tim, are you going to talk further about Mike's point, that the focus ought to be for the rule to be performance-based, to get away from words like "indefinitely" or just the general description --

MR. REED: Right. I'll probably be saying that several times, and not only from the comments here, but from the comments from the new reactor designers I've gotten reg basis. I think we will probably, are too restrictive. Well, we're trying to get past a very high level performance requirement go down, I think it would be a little bit restrictive on what a new designer could do to solve this problem.

So absolutely. I think we're probably going to have to be a little more performance-based on what these concepts have. So I think we'll be leaning

that way. I don't know. I mean it's just me looking at it. But absolutely I agree with that, so -- that's just me, though.

MEMBER SCHULTZ: Because that helps to tie it in with the current rule.

MR. REED: Yes.

MEMBER SCHULTZ: That's part of the objective, is at some point in the rulemaking, it is going to integrate, I hope very well with the current rule. That's one of the goals, and that would help to get a focus in a different way than just saying well, we're going to handle beyond design basis events, without identifying what they are and what the bounds are.

MR. REED: Right.

MEMBER SCHULTZ: And understanding that like the current implementation of station blackout, it is site-dependent, both in terms of location, as well as number of reactors --

MR. REED: Absolutely.

MEMBER SCHULTZ: --capabilities and so forth.

MR. REED: And hazards, yeah absolutely. I agree.

MEMBER RYAN: Tim, it strikes me that all

the sub-bullets on specifically the current concept that includes on short-term intervals, some of those things probably aren't as big of a deal as if it's a very long period of time, and then an intermediate period of time.

So all those, in terms of the intensity of what you're going to deal with is time-dependent. Are you going to deal with that at all? For example, complete loss of AC power to the essential and non-essential switch gear. That lasts longer and the backup system, you know, might not be working. Have you thought about the time-dependence of all this?

MR. REED: Yeah. In fact Eric, I'll chime in. I think the way I think about this is it's an event that occurs say at T equals zero, okay, and depending on the initial conditions are the mitigating actions you have to take. These are a simple set of assumptions that we're going to assume at the beginning. It may be worse than this.

But the actions you have to take at each point of time after T equals zero are dependent on what happened. So the very first action might be, okay, you're in the control room trying to figure out what happened obviously. But then you might think okay, I need to start stripping batteries, or I may

need to go and do, for the power send for a central charger, or I may need to go to a turbine-driven aux feedwater pump room.

Depending on what you have to -- or go look at water sources. Okay, as you go through the sequence for that event, you need to figure out how long it is until you have to take action. So the time constraints are absolutely the great key, and that's part of the implementation of the order. Folks are trying to work that problem right now.

MEMBER RYAN: Okay. So that's covered.

MR. REED: So all these things really, you know, they really sit in a time domain, if you will.

MEMBER RYAN: That's kind of what I'm thinking if you give them a list. They all have to have --

MR. REED: Yeah, absolutely.

MEMBER RYAN: Without understanding the time sequencing of all these things, either singularly or interacting in some way, you really don't know where you are on the intensity scale.

MR. REED: That's right.

MR. BOWMAN: Yeah. This is Eric Bowman. The other thing that needs to be borne in mind is that there's a relationship of this set of requirements

with the station blackout requirements.

They've got the loss of all AC emergency operating procedures that they'll be going through, and in large part the initial actions will all be the same, as though they're going down the standard station blackout procedure they already have.

But at some point there will be a decision point where they'll get a response. Got to obtain -- with an alternate AC power source reliant licensee, the current procedure says go start the alternate AC source and place it on the buses.

If the response that the AC, the alternate AC power source doesn't start, if the response is not obtained, then it branches off into doing these mitigating strategies.

MEMBER RYAN: Got you. So it's got to be kind of a very complicated web of decision-making where, you know, in one set of circumstances that decision could make lots of sense, and if something else precludes you making that decision, that whole pathway is kind of shut off.

MR. REED: Absolutely, exactly.

MEMBER RYAN: It's a very complicated network of decisions, not just --

MEMBER BLEY: Something I think would help

the Committee, because some of us have never participated in a rulemaking, some of us have, would be something like a critical path chart. I know you do those out of this rulemaking process, and how it will interact with other rulemakings, like the one about integrating procedures.

I think what you were just talking about somehow tends to overlap what's to be going on over there. I think maybe next time we get together, that would be very helpful.

MR. REED: Yeah. We have a whole slide of different circumstances kind of right in the center of it. So it's a challenge.

MEMBER RYAN: I know you do, yeah.

MR. REED: I'm certainly aware of that. But anyway, this is -- these sub-bullets were meant to try to define the specific elements of this entire ELAP condition, and I'm not sure, I think it created some confusion.

First of all, I don't think, for example, we got comments that hey, why are you saying safety-related batteries, and I think that's a good comment. If those are reasonably protected batteries, I think we will allow power from reasonably protected batteries.

They may have to be strapped for size. They may have to be changed from what they are now, to make sure they are reasonably robust structures. But for example, that's one comment that I've got.

Also, going back to an initial comment earlier, if in fact the supplemental AC power sources survive and are in the proposed rule, and by the way, they're strongly supported by designers, that would be one way. That would be one success criteria of restoring power using a supplemental AC power or robust source.

So this was meant to give the individual concepts of what this condition was, and to get comments on it. It was, we got a lot of comments on this, and we'll see what we go, where we go from here on that, if there's anything else in there that comes to mind to bring out on this slide.

VICE CHAIRMAN STETKAR: During the Subcommittee meeting, we had some discussion about all of these little bits and pieces and words and sub-bullets, and how people might creatively interpret what they might mean at a particular plant and how they might justify the fact that they don't need to meet the intent of this rule, because they don't satisfy any of those specific conditions there.

Have you received a lot of feedback? You already mentioned, I think, comments on each of these individual line items. Well, do you have say safety-related batteries and kind of use a Joe battery rather than a safety-related battery?

The question I have is are we trying to be so specific that we're walking ourselves into little finely-defined corners that don't really address the concern? The concern being, I'll use the word "indefinitely," an indefinite loss of all AC power sources to any system, SSCs, that are needed for decay heat removal from the core and the spent fuel, period. I mean that's it.

How that is achieved at a particular plant. Whether it's loss of power to the essential and non-essential, or whether it's an or, or whether it's some two out of three of this and six out of seven of those other things is a site-specific issue. The fundamental concept needs to be elaborated.

MR. REED: I agree. Actually, the comments in this Committee we had those kind of comments, and the comments we got back on the reg basis on this were kind of leaning us towards going more to performance-based, allowing more flexibility. Having, licensees will have all these tools in the

tool kit, if you will, and they'll use them as they see fit, depending on what happens. And so if we get too much definition here --

VICE CHAIRMAN STETKAR: That's what I was saying.

(Simultaneous speaking.)

VICE CHAIRMAN STETKAR: You now have some feedback, and if a lot of the feedback is coming about in terms of discussions of specific and and/or logic, or what you call an essential or what you call a safety-related, that might be a clue that we're heading down a path towards over-specificity.

MR. REED: Absolutely, too prescriptive at the reg requirements level, and this is one of the good things about putting those draft concepts out there and getting feedback.

Before you even get to the proposed rule stage, that can avoid some of that. Now I'm not going to solve all the problems in the world, but I'm sure I'll get good comments on the proposed rule, okay.

VICE CHAIRMAN STETKAR: But I mean at the rulemaking level, it's one thing. In terms of implementing regulatory guidance, there could be better definition of --

MR. REED: I think if the regulatory

guidance --

(Simultaneous speaking.)

VICE CHAIRMAN STETKAR: --of specific conditions as that comes up.

MR. REED: Absolutely. So I think I agree in spirit with what you're saying. It's been, I think, three times now today. So that's, I think, kind of the feedback I've gotten on the ELAP definitions so far. I think you're going to get some more comments from NEI on June 20th, and it's probably going to some of this loss of heat sink stuff.

So I'll wait to see and when that comes in, I'll reserve, depends where we end up on this. But I think we definitely need to be at a more performance-based level with this definition.

MEMBER BLEY: Just going back to that Subcommittee, Eric said it this way, but I don't think he quite said it. The big thing that we're worried about is when you have a discrete list like this, it'll turn out either you've forgotten something that you could put in that list, or somebody will --

MR. REED: Use it.

MEMBER BLEY: Break things apart and other pieces and say it only applies to this, and you'll have much difficulty.

MR. REED: Some lawyer, I mean. I know exactly what you're saying.

(Simultaneous speaking.)

MR. REED: So yeah. I definitely agree with that. So but that was, it was good to get that feedback from the committee and from stakeholders on that. So any more comments on this slide?

(No response.)

MR. REED: I'll go to Slide 6 then. This kind of the harder thing, the mitigating strategies themselves. In fact, on this slide, this looks -- I think it's almost exactly the same as what I presented to the Subcommittee. One thing I wouldn't have on this slide was as the third sub-bullet there, "equipment would be required to sufficient design capacity."

It actually should go on the next slide. So ignore that for a second. But the rest of it is really kind of the guidance and strategies and those kinds of requirements, the first one being of course develop, implement and maintain guidance and strategies to maintain or restore core cooling containment, and spent fuel pool cooling capabilities.

So that's identical to the order. That is the heart and soul of this requirement, and it's

actually a pretty strong argument, that the minute you start dropping down below that, you start getting yourself in trouble. If we stay at that level a little bit more, almost the attachment to the order, you're okay.

But we've tried to get a little bit more detail, where we've gotten, I think, we're getting ourselves into some areas where maybe we're not doing the very best thing for the rulemaking or for safety, for that matter. But --

MEMBER BLEY: I have a question about the word "strategies." I like the word "strategies," and to me that implies laying out the functional description of how you're going to survive this event. It could mean to somebody else laying out very detailed, specific procedures akin to the EOPs that we have.

My concern with that is when the real event doesn't quite match it, it may not be helpful. So I'm wondering if you've defined "strategies" and what you think we're looking for in that area.

MR. REED: We haven't, and I'm sure Eric's going to jump in here too, we haven't defined strategies, but we're thinking exactly what you're thinking. You really can't have a step-by-step thing

for a situation where you don't even know what the damage state's going to be obviously.

MEMBER BLEY: So if that event occurs, that will be better than if that event doesn't occur.

MR. REED: These really are strategies, but they're not just amorphous things. They are, they're a set of guidance and strategies, with staging and deployment routes and work through; there's an engineering basis work. There are time constraints built into these things.

So when you look at what's being done, if you look at the integrated plans of what's being done, there's a lot of work that is being done. Even though they're strategies, they give you a very good chance that they would be in fact successful in being deployed.

And certainly for probably a lot of scenarios, we're not even thinking about it. You know, so they're looking at flexible, but they are engineered, and yeah, it may not work, you know, exactly the way you thought. You might have to take a different pathway, and this in fact has contingencies, that there's more than one connection and there's these other aspects of these strategies that reflect the fact that this is a pretty undefined

situation you're going to be addressing.

But yeah, you're absolutely right. That's the thing I think really gets done in an EOP, you know, and then once you step into these strategies, you're in a world that's a lot less defined, and you have to be more flexible there, to allow the folks at the site to probably do the best thing they can at that time, you know.

MR. BOWMAN: This is Eric. The way I would think of it, the guidance, per the phrase "guidance and strategies" is what is getting to the procedures. The strategies can be a more inclusive term that covers things such as one of the things industry is doing in response to the order is a set of contractual relationships between the licensees and the offsite resource provider that's running regional response centers.

The implementation and maintenance of that contract is part of the strategies they're doing, to allow them to maintain and restore the functions. So it's -- we haven't gone and defined what guidance and strategies means. It's gotten a certain cachet to it as a term of art that's been used since 2002, when the Order EA-02-026 was issued with Section (b)(5)(B) for that set of mitigating strategies.

MR. REED: But we'd be supporting detailed procedures on the use of this, and that proceduralized and it should be. But yeah, the strategies are obviously more.

MR. BOWMAN: And so in large part, we can't really define exactly what the strategies are going to be, because the initial conditions for the entrance into the use of the guidance and strategies aren't entirely well defined. Something has happened, and some of your other structures, systems and components will either survive whatever happened or they won't.

So these guidance and strategies give the licensees tools, if you will, and a tool box to choose from, similar to what goes on with the severe accident management guidelines.

MR. REED: Let's see. So similar to the rare -- be required to be adapted in all modes, and maybe we'll say something. We got an interesting comment on those, and simply suggested that maybe we should say when irradiated fuels in the reactor vessel are in the spent fuel pool.

I kind of like that. It gets to -- I would like tech specs in this thing, and that's an interesting concept I think we might have to give some

consideration to. I like that comment, but that's just me.

MR. BOWMAN: I do too.

MR. REED: Oh, well that's two. I'm sure we add it up and we need more votes for that. We got some comments, "mitigating strategies must be required to consider contingencies." We got an interesting comment here, and it's a concern here about the backup to the backup to the backup. When you guys going say the end of this thing?

So yeah, I don't think we're -- we're not expecting licensees to do something they're not actually doing right now in the order. So I think we need to clarify the word "contingencies."

You know, at some point, you know, you've got to stop this. We're talking about extremely remote events. I don't even expect anything like Fukushima to happen in the United States ever. I think this equipment could be used in other less severe events and probably will be used in less severe events.

But you know, when you're talking about something this remote, you know, how far do you go and what's needed? So contingencies --

MEMBER SKILLMAN: Tim, what is your

current vision of contingencies? How far are you thinking it should go?

MR. BOWMAN: Yeah, let me address that. Where it is addressed, the contingencies that are existent in the program that's responsive to the Order EA.12-049. All the licensees are required to have a capability to use a portable pump as a means of providing water, either make that for the reactor pressure vessel or reactor coolant system, or the steam generators, depending on the plant design.

That is a contingency. For example, if there is some reason why there is no alternate power available because of actual damage to the DC buses and the AC buses, as a result of the initiating event.

MR. REED: Actually, I see -- to be honest with you, I see -- you may want to get to this area in a second, but I see us being within the regulatory scope of the order for this rulemaking, because one of the things, as I read through basically the information that supported the blackout rule, the post-blackout rule and the reevaluation of risk in 2005, you look at all that information about low station blackout risk.

Obviously not external, put the external events to the side for a second. That risk is

absolutely very low and going lower because of mitigating strategies. It certainly wouldn't support additional regulatory action, or even expending reg resources.

I mean the last step turned it down below to the minus 5 on main core damage frequency basis. So that risk is, we're separating that and I'm saying that's 2.1, and physical protection is NTTF 2.1. That's out there, and that needs to be done, you know. That's the real, in my opinion, the real lesson learned.

But in terms of the scope, I would probably be very closely inside the umbrella of the order, with lessons learned and feedback and fixing what doesn't work or what's impractical and what needs to be changed from the order, and perhaps with additional flexibility.

So that's kind of a -- right now, that's kind of my overriding current thought on where we would be going, in terms of trying to meet our backfit reg analysis processes, you know. I don't think we can go beyond the order right now and see there's any justification for it.

So that's kind of a general answer you're going to get on a lot of these things. But in terms

of what is imposed, it's already in places. Those were in the side that said a backfit on current licensees if I stay within that. Once I go beyond it, it gets very tough. I don't see that I can satisfy these processes and go beyond that.

MEMBER SKILLMAN: Well, you know, I can understand coolant, core, protecting containment and protecting the fuel in the spent fuel pool. But there are a couple of other things that come quickly to mind. You don't want to dump your waste gas decay tanks inadvertently.

You need at least 1/100th of a light bulb in your control room. You've got to be able to see, and you probably need to ventilate it. So there are a couple of other functions that are essential in order to accommodate that first box. There's not particularly complicated. Designers know very well they have to do it.

But I think as we look at this, we ought to be careful that we're not short-sighted, and to the discussion we had on this issue of "extends indefinitely," of a proponent of maintaining that phrase, because kind of sets of lifeboat standard. That says "hey, you're in trouble. You've got to be able to do something here."

There are a lot of clever ways to respond to that, but at least it sets the concept that kind of gets everybody's attention. So and there's room in that for a performance-type response, but stating that the way you've stated it, at least in my mind, in a minimum of words, communicates the problem.

MR. REED: We could do that in a real language level, maybe -- and we could do it in supporting considerations that provides the meaning and intent of the rule language. There's others. There are ways of doing that, try to make everybody happy. I don't know how that would work, but --

MEMBER SKILLMAN: I was going to draw on this idea of contingencies and I agree with you. How far do you go? Well, not too much further. But let's make sure that as far as we go, it encompasses the things that the operators of the plant really have to attend to. That's cooling the core, cooling the fuel in the spent fuel pool, probably protecting some portion of the radionuclide inventory, where it might be.

Whether it's in waste and gas containment tanks or it's your sluicing devices that you do not want to inadvertently dump to the floor or those types of things. There's a minimum lighting and some

minimum ventilation are essential, in order to safety operate the unit.

MR. BOWMAN: Oh yeah, and this is Eric Bowman again. We do have, I believe, all of those items are covered at the guidance level as being supportive systems that are necessary to continue with the maintenance and restoration of the overarching safety functions, core cooling, spent fuel pool cooling and containment.

To make it more performance-based, we were looking to the amount of lumens as opposed to the wattage of the lighting, because we have seen a lot of licensees that are shifting to LED lighting in order to preserve their batteries.

MR. REED: The lighting's key, HVAC can be key. There's lot of support equipment that actually is key.

MEMBER SKILLMAN: Thank you.

MR. REED: Working down through this slide, of course, as mentioned earlier, the mitigating strategies will be, in fact are being integrated into the existing emergency operating procedures station blackout, for a station blackout. That is, that's occurring.

As we mentioned earlier about, you know,

the response not obtained stage; you know, you can't recover offsite power, AC power. You can't recover onsite AC power. You're going to the beginning strategies where you don't, can't recover your alternate AC power source, then you go into these strategies.

So they work, they do link in there, and there's difficult decisions that have to be made by people in the control room about when you have to go the mitigating strategies, and you've probably got to do some of that when it makes sense to do it. They're not all different, as Eric mentioned. Some of these are exactly the same. So that's good, there's an overlap.

But for these kinds of severe events, I'm not sure it's completely impossible to make some of these decisions earlier, because if it's a true severe event, and it gets us into what we're talking about here. I think you'll see the grid destroyed pretty substantially.

If the grid's not destroyed substantially, that's the best source of AC power you want to generally get back. So there should be hopefully early on, in one of these situations, we've got a pretty good feel of when you're going to get that

power back, and that could, I think, hopefully perform all the actions that you take now.

But that innovation is a challenge, and trying to make that as smooth is possible is part of the implementation of the strategies into the EOPs.

MEMBER-AT-LARGE RAY: I don't think you mean the grid destroyed. You mean the connection to the grid.

MR. REED: Yeah. Yeah, probably. Yeah, hopefully the grid's not destroyed, but yes. Yes sir. If the grid's destroyed, we're really in trouble. So let's see, of course the strategies would have to culminate and be able to use offsite assistance from the regional support centers.

There's two of those going in place, and that make affect, you know, the success. We'll have to see what we're getting in this thing, and also there's a lot of feedback from the order and how we actually terminate or end is going to cause success to the end of the strategy.

Then this framework, this new set of strategies themselves, making any strategies fit inside this other rulemaking that we talked about earlier, that's the NTTF Recommendation 8 rulemaking, which is trying to integrate all this stuff. It's

trying to integrate the emergency operating procedures, the severe accident management guidelines, the extensive damage mitigation guidelines, and now this new set of mitigation strategies into one --

Well, I shouldn't say one, but a set of guidance, strategies and procedures, such that there's clean transitions, there's command and control, that maybe when you exercise and train, you're doing the entire set. You're working through that. That's that recommendation I know they bridge to at least once or maybe more. So I was there for one of them.

We would try to use that rulemaking to the extent possible, and not have redundant or overlapping, you know, requirements if possible. Now if that one doesn't survive, then if that doesn't link, for example, back to the reg analysis, then I would probably, I would have those requirements in my mitigation strategies rulemaking. So and work with those folks and what that should be for the mitigating strategies.

So that's all I had to say on that slide. Any questions or comments?

(No response.)

MR. REED: On the design requirements slide, this is another interesting area where I got

some feedback from some of the designers. We have, at least I did, I have kind of a mindset that they install the equipment that's relied on first, in current licensees, is safety-related stuff. So it goes without saying that stuff needs the special requirements of design for safety-related, typically Class 1, 2 and 3 safety-related equipment. It's going to be very robust.

So I don't see that I have to do a lot for that. But a new reactor designer should have a little more freedom. So that's, we should be talking about any equipment-installed work order should be reasonably protected, should be able to perform the functions as needed in these situations. It doesn't have to be safety-related, as long as it's reasonably protected and performing functions needed for these situations.

So we've got some of that, some of the feedback on that so far on the design requirements. So I think again, you know, this kind of goes back to this idea in the definition, where we're possibly getting a little bit too detailed in some of these areas. We've got to be careful and set up at a high enough performance from this base level, and perhaps even on the design, it might make sense that this

stuff really resides in guidance, and not be up at the rule level.

We stay at a very performance-based level of the rule, and keep the design requirements down out of the rule, to avoid problems. Or a new reactor would have to come in and then come up with an exemption, and that would create unnecessary burdens.

So this was a set of ideas that we put out there, draft concepts that were -- and we got some feedback. They're pretty straightforward. Of course, it's got to perform the functions you need. It's got to be protected. It hopefully can be independent from the installed stuff to some level.

The equipment itself, the N plus 1 sets of this equipment needs to be designed, stored and protected. You're trying to minimize that equipment being knocked out by the same event that knocks everything else. So you're trying to avoid common mode and common cause failures, that has the protection from the effects of these events.

Then when you design in-state and deploy, you want to of course do that in such a manner that it doesn't destroy the equipment that it's being hooked into. You're going to have to rely to some level on I'll call it a process path and an electrical path.

So that's, you know, distribution systems you want, and you want to make sure that that works too. So that's just basic engineering.

CHAIRMAN ARMIJO: I have a question. If a licensee complies with the orders that were issued as a result of Fukushima, what other things are on this list that he isn't already going to do?

MR. REED: Does he cover it is what you're asking?

CHAIRMAN ARMIJO: Yeah. I'm just saying, isn't this what we're already doing?

MR. REED: I believe, I am not --

CHAIRMAN ARMIJO: We already want them to do it.

MR. REED: Yeah. I believe almost everything. I'm a little bit, I'm a little hesitant on the testing and inspection assurance level. But I believe they would be, but I'm not -- what I'm trying to do is write language mostly for a new reactor.

CHAIRMAN ARMIJO: Yeah, I understand, I understand.

MR. REED: And that's why I keep saying I'm probably too restrictive. But I would -- probably this goes back to a comment I made earlier. If you're in compliance with this order, I don't think I'm going

to be imposing right now, based on everything I know, anything additional. So you should be in compliance with the rule, hopefully. Now on the --

(Simultaneous speaking.)

MR. REED: We do have a change control requirement that's not in the order; it's in the guidance. So there's some differences here, but I don't think they end up being too substantial at all. At the present time, I see that that's where we'd go, at 50,000 feet. That can change. I mean --

MEMBER SHACK: Well, the flexibility you allow for the supplemental source is different from the order.

MR. REED: That's the thing. That's one thing. Flexibility, that's a voluntary flexibility, and that hopefully gets people away from relying on humans as much, and that's a good thing, I think. I think it's better way.

MEMBER SHACK: So we had some discussion at the Subcommittee that, you know, you've built one more Maginot Line, you know. The Guderian comes with the Panzers through the Ardennes somewhere --

CHAIRMAN ARMIJO: Flexibility is good.

MR. REED: Flexibility is good.

CHAIRMAN ARMIJO: When you don't know

what's going to happen.

MR. REED: Yeah, it is. I think relying on humans in these kinds of events is not a good thing too. So there's two edges to that sword.

CHAIRMAN ARMIJO: That's all we've got. That's what we are.

MR. REED: That's a very interesting, because you really haven't considered the feasibility and reliability of the manual actions associated with the mitigating order very much.

MEMBER SHACK: That's right.

MR. REED: You know, there's certainly something to be said for installed equipment that doesn't require any manual actions, or certainly less reliance, less reliance on them.

MEMBER SHACK: Yeah, yeah.

MR. REED: Absolutely. That's the main thing. To me, that's one thing I sort of see, you know, in the rule, is there really ought to be more emphasis on the feasibility and reliability of the actions that are -- the guidance has very little at the moment, either the ISG or the 1206, and that seems to me somehow that slipped through and we didn't comment on it at the time.

VICE CHAIRMAN STETKAR: Tim, we tend to

all be engineers and like to think about designing things, pumps and pipes and valves and electrical buses and all that kind of stuff. One of the problems with the existing station blackout rule and everything that we've discussed is that implicitly, all of those things had presumptions about what would go wrong, how it would go wrong, how long that condition would last, and how you could get out of it, and we're discovering that some of those presumptions perhaps should have been challenged.

When we start to talk about design requirements and options and strategies and things like that, is there an inherent presumption that the things that you plug into inside the nuclear power plant, called switch gear for example, are by definition not affected by this event?

Because if I had to develop a strategy for that contingency, I might think of a couple of different options. The reason I bring it up is that emergency diesel generators and piping, for example, tend to be, from a seismic perspective anyway, rather robust pieces of equipment.

In fact, if you look at seismic risk studies that have been done, typically the fragilities of electrical switch gear, control signal cabinets,

depending on their mountings and locations in the building, tend to -- they tend to have lower capacities. Still well above the safe shutdown earthquake, but lower capacities than the generators themselves.

And therefore, if the presumption is that we're just going to bring in another power supply and plug it into something that by definition is there, that might not exist. So I guess my question is when we're starting to talk about, you know, design details and options, at least at the rulemaking level, is there some inherent presumption that it's there?

Because just because the electrical buses are down, my point is that the ways of getting water to the core through piping systems are, might very well be intact. So I don't know. When I start to read some of these, a little bit more details here on some of your slides.

MR. REED: On one side of me, you know, I don't like saying beyond design basis, okay. I don't like as a regulator, because I can't -- I don't know what that means in terms of what I'm putting out there. If I was a licensee, I wouldn't know how to comply with that. If I was an engineer, I don't know how to design for that.

So but you need to have some definition starting with what are we talking about. What are the requirements, what I need to comply with, what I need to design to. Now as a practical reality, we do that. But then clearly, that's not necessarily going to be, win the day.

So that's the other side of this thing, and that's where you're going. You go in place and you do, some of the safety-related set of equipment is going to be robust and available. In fact, it may not be. So that comes back to while there should be some contingencies --

MR. BOWMAN: That's a contingency we discuss with the -- and it's not just bring the portable pump over. But it's also the manual start for the emergency core cooling systems like reactor core, isolation cooling or turbine-driven AFW. So it's addressed to a certain extent there. We don't -- we aren't looking as far as your turbine-driven AFW pump will not work.

MR. REED: I think that's a melt, it doesn't work, for example.

MR. BOWMAN: That might be a residual risk.

MR. REED: Yeah. There's some I don't

think you're going to be successful. That's why I've been saying, you know.

VICE CHAIRMAN STETKAR: No. I'm just saying -- the only reason I brought it up is that because this is called extended loss of AC power, we tend to start thinking about electrical things and strategies that tend to get electricity back to places where we can then distribute it to the rest of the plant.

As long as you keep focused at fundamental functions of core decay heat removal, however you can accomplish that, and make sure you have strategies in place to do that, whether it's, you know, hose connections to a piping system and making sure you have a diesel-driven pump that has enough pressure and flow capacity, for example, as one of your possible strategies.

MR. REED: You can hang in there with a turbine-driven pump on the primary side --

(Simultaneous speaking.)

VICE CHAIRMAN STETKAR: The only reason I bring it up is, you know, we're going to get to the next slide and talk about the super diesel generators, that's supposed to be really excellently good diesel generators. That doesn't necessarily solve, you know,

solve all of the problems.

MR. REED: I was going to say, if there aren't any more questions, then we can go to the --

(Simultaneous speaking.)

MEMBER SKILLMAN: To what extent, in your development of the requirements, have you considered lessons learned from blackouts? I know of two. I was involved in one in 1965. I watched New York City go black, and all of Long Island, and then ultimately the East Coast. But I was looking at downtown Manhattan when the lights went out. There was one in what, 2007-2008, that started up in the First Energy system and proceeded east and west.

In the first one, there were no nukes. Indian Point wasn't there, Oyster Creek wasn't there. There were some early builds up in New England, but nothing really going on. So we've never tested anything like this in real time.

Unless there was a test from the one in 2006-2007-2008, and a test where the stations were actually built, and a total loss of offsite power. To what extent have lessons from those experiences been factored into this?

MR. REED: I haven't considered those lessons at all, to be honest with you. Actually, I

was at Turkey Point in 1985 when they had, I think they lost the power to Miami. I was there at that site at that time. I was the aux feedwater system engineer. So all three aux feedwater pumps were electronic, and they went in and reset those.

VICE CHAIRMAN STETKAR: Big surprise.

(Laughter.)

MEMBER SKILLMAN: So we had SOR, we had SOR-99-01, which kind of laid out a number of the lessons learned. But I'm just wondering if there are some lessons that would be valuable here, because you know, if you thought you had offsite support you didn't, at least in the 1965 event.

There was no one to call, because they were just as black as you were. There were no lights, there was nothing. I mean the bridges were out, everything was out. Toll gates were up. The whole city just literally came to a halt.

I can just imagine that event in 2013 at Indian Point. What do you do? So I have a hunch that there may be some lessons that are useful. I think you probably circled the wagons in terms of providing AC power. But as John was pointing to, there are some other issues out there that have to do with the infrastructure that you might be depending upon.

If there's no one to call, because the phones aren't working. Well, maybe the cell phone towers would be down because they're not powered, you know, who do you talk to?

MEMBER-AT-LARGE RAY: Well but a loss of -- I mean a grid blackout and a station blackout are two very different things. Loss of offsite power is an operational occurrence that --

MEMBER SKILLMAN: That happens routinely.

MEMBER-AT-LARGE RAY: The plant is designed and tested for. We're talking about something here which causes a station blackout.

MEMBER SKILLMAN: I got that.

MEMBER-AT-LARGE RAY: A whole different ball game.

MEMBER SKILLMAN: And I'm saying that there have been several.

MEMBER-AT-LARGE RAY: Station blackouts, extended station blackouts I mean?

MEMBER SKILLMAN: No, not extended station blackouts.

MEMBER-AT-LARGE RAY: No. That's the issue on the table.

VICE CHAIRMAN STETKAR: There's been a few short-term station blackouts.

(Simultaneous speaking.)

MR. REED: I think Vogtle's the only station blackout, I believe.

VICE CHAIRMAN STETKAR: Huh?

MR. REED: I believe Vogtle's the only station blackout --

VICE CHAIRMAN STETKAR: Susquehanna, I think, had one, you know. That had some common cause. This was years ago. But they've all been short-term.

MEMBER SKILLMAN: There's some lessons there that might be valuable at this early stage of rulemaking. That's my only point.

MR. REED: Okay. Is there anything else on Slide 7?

(No response.)

MR. REED: I want to go to the supplemental AC power source. I was, this was actually strongly supported, and in fact South Texas 3 and 4 absolutely loves it, and they have, I guess, two gas turbine generators I believe that are above the 50-foot level, I believe. So they have, and either one can supply Units 3 and 4. So they like this a lot, and they think they're very robust and they would be there.

So and other designers like this too. I

think there's some flexibility to use something like this. I think the current, you're making a very good point, and this is something that I personally --

VICE CHAIRMAN STETKAR: I was going to say. Those gas turbines still plug into the same place.

MR. REED: Yeah, I know, and the diesel generators themselves are really robust, you know.

VICE CHAIRMAN STETKAR: They are.

MR. REED: And I just don't know how much better you can do as far as equipment and diesel generators. They're trains essentially. So it's almost, you know, but you could take --

VICE CHAIRMAN STETKAR: Now they don't do so good in flooding, for example, if you have a flooding --

MR. REED: Yeah. Clearly that's a --

VICE CHAIRMAN STETKAR: --and things like that, speaking not particularly for seismic.

MR. REED: This doesn't rule taking something that you already have on site and making it a little bit better, first of all. This is flexible enough to use an existing thing, not adding another Maginot Line, you know, for example. But the idea --

VICE CHAIRMAN STETKAR: --was the current

one.

MR. REED: Yeah. Using the current Maginot Line and just moving it, I guess. But that was, this was the idea to allow this. You know, there was obviously not a lot in the order, and it changed the entire complexion of the mitigation strategy. So like I said, we got strong support from designers, and that to me is interesting.

So they see it as an opportunity maybe to do more engineered installed type approaches. I personally think that's the best place. I think that's the best place to be in terms of safety.

MEMBER CORRADINI: This would be in addition to diesel generators?

MR. REED: You could use -- you could. I'm not ruling out your current diesel generators and doing something more. Presumably, your current diesel generators probably are aligned to one safety bus. You may not have as much cross-connection, maybe not diverse ways of connecting.

MEMBER BLEY: Plus they're isolated.

(Simultaneous speaking.)

MR. REED: Sometimes they're not too separated, you know.

MEMBER BLEY: The older plants weren't.

In the newer are really separated.

MR. REED: I think you could so some things, and it may be as a practical matter, for a current licensee. But this may be mostly for new reactor, new design. You're not talking about huge amounts of cost to try to do something like this.

I'm trying to allow for, you know, an approach that would be less reliant on a lot of people running around with supplemental portable equipment.

MEMBER CORRADINI: But this is, just a clarification again, since I wasn't in the Subcommittee. This is not, to get back to Sam's point, I'm trying to draw an umbrella around this. This is not part of the current order. This is something over and above.

MR. REED: This is an idea that definitely is not in the order. It's a flexibility that the rulemaking group, working group thought let's throw it out there and get feedback on it. I've said to people, I've said in a Category 3 public meeting, we may not, you may not see this in a proposed rule because obviously management at a higher level, including the Commission hasn't, certainly to date, hasn't agreed with this. So we had different views on --

MEMBER CORRADINI: This again is the rule might be too much detail at, you know, what specific implementation -- but I guess where my question was coming from was it sounds good, but what's the probability of failure of this compared to everything else I'm worried about?

If I have such an extreme event that's going to knock out everything else, it strikes me that this thing's going to be toast, just like everything else would be toast.

MS. McKENNA: Well, I think that one of the key points of this really was in the flooding scenario, but that's where if you protected some source for a different flood level, it might have a better chance of survival than so much for seismic conditions. I think that really was the driver for this.

CHAIRMAN ARMIJO: Right. I mean so is this a different machine? Is it gas turbine as opposed to diesel, or is it a location issue?

MS. McKENNA: I think that it's more probably a location. The second bullet does talk about diverse, but it doesn't have to be diesel versus a gas turbine to be diverse or, you know.

CHAIRMAN ARMIJO: Yeah, sure.

MR. REED: But if you have a particular hazard, such that for that location, having a diverse machine, it's pretty likely that this one will make it for this event, this one will make it for this other one. That's a good thing, but it may not be for every site and situation.

CHAIRMAN ARMIJO: But we found from Fukushima that the air-cooled diesel that didn't get flooded saved Units 5 and 6. Is that what we're talking about here, something like that, in a favorable location, protected against flooding?

MR. REED: Air coolant is another great thing is to have the supporting system of cooling, yeah. So yeah, probably with its own supply of fuel bunkered.

CHAIRMAN ARMIJO: Of course, the Japanese are now putting everything under the sun on their plants, gas turbines, every piece of equipment they can buy, they're using it. I'm not sure they all work.

MR. REED: It's interesting, because we come back to -- if the event takes off the diesel generators --

MEMBER CORRADINI: I mean all sorts of questions pop in my head, which is how close it is to the plant, how big is it, right? What is the danger

from having all this natural gas piping nearby for another accident that I can imagine? I mean there's a plethora of things that pop in my head that make this not necessarily as good as it sounds at first blush.

MR. REED: No, that's exactly -- that's why I want to hear it, that kind of feedback.

MEMBER CORRADINI: Yeah.

MR. REED: I'm not sure either.

MEMBER CORRADINI: That's fine. I just want to understand. So it's not, I just want to put it in context with what Sam was asking. That's fine.

MR. REED: But we offer the flexibility I think you allow a designer, they may in fact build, come away with a way to skin the cat that's a lot better than the mitigated strategies. So I'm not convinced that I know the right answer.

But if somebody, a new reactor designer comes in and says here's what I got, we can look and go whoa, that is really good. And so until I see it, I don't know. So that's the ideas put out there with that idea. And you see the concepts that we put out there in -- it tends to be kind of the strongest link in the chain, if you will, but not unnecessarily strong if the entire facility's destroyed.

This also comes back to another thing that, you know, I think I said in the Subcommittee, and people ought to keep in mind. If your plant's not physically protected properly, 25 extra feet of water comes across the facility, it doesn't matter. It really doesn't matter.

You know, you've got to physically protect the plant to some level properly, and frankly Fukushima was not, you know. So I think if you do that, then this stuff probably will be pretty useful for a lot of events, and you won't get a lot of stuff destroyed.

But then it might a whole lot of extra equipment. So but yeah. So they work together, and in fact that's kind of the way we're going, you know. We're adding 2.1 to the physical protection, and we're doing many strategies, and you don't see me suggesting, for example, additional physical margin and mitigation strategies, because I'm saying that should be over in 2.1.

That's where you should do that. That's really GDC-2, you know, so -- and that's what that effort's all about.

MEMBER SCHULTZ: Tim?

MR. REED: Yes sir.

MEMBER SCHULTZ: I just heard you say that this is an alternative to mitigating strategies, and it's a bit confusing, because I thought this was a way in which to meet the elements of mitigating strategies, except when you get down to the point where you mitigating strategies says then you need to rely upon offsite resources as well.

I can see a licensee for a new reactor saying "I don't need anybody else. I can install something like this. So I don't think I need that." That would be way out in terms of the likelihood.

MR. REED: I think a new reactor designer would in fact try to go that, all the way to that point. In other words, I'm going to put in an engineering approach, and I don't need anything at all. But I would say really? You don't anything?

MEMBER SCHULTZ: And discussion would ensue, you're right.

MR. REED: Yeah. I can't personally not see of a design that wouldn't need at least a final phase.

VICE CHAIRMAN STETKAR: Yeah. I was going to say, we talked about this a little bit, and I think in my notes from the Subcommittee meeting is you characterized this as an alternative to what you call

the Phase 2 response.

MEMBER SCHULTZ: Yeah. That's why I wanted to clarify it here.

VICE CHAIRMAN STETKAR: But it wouldn't necessarily obviate the need for a longer term Phase 3, you know, supply fuel or whatever.

MR. REED: Yeah, I figure you would probably be in Phase 3. But you might be able to get a lot of the others, you might be able to get most of the rest of it out and basically you're into Phase 3, potentially. I'm not going to say you can't.

MEMBER SCHULTZ: I believe that's what you need to do, in order to integrate this option as part of the overall rulemaking strategy.

MR. REED: Yes. We have to -- I agree with you, and if we don't do that, I don't think it will be a success.

MEMBER SCHULTZ: I agree. Thank you.

MR. REED: And like I said, we really, we threw all our concepts out there for this reason. We don't, the stuff may not survive it. But that's the whole idea, is we go out with regulatory basis, that's an opportunity to get a lot of good thoughts from folks, and you can get a lot better rule language that way. So that was the whole spirit here.

So are there other comments on the supplemental AC power source slide?

(No response.)

MR. REED: Okay. I've got until ten o'clock, don't I? So I'm trying to adjust myself to make it. I'm watching my -- we've done a couple of slides in ten minutes.

So at the Subcommittee, we had change control and linkage slides, I combined them together. Change control is something when you're in this realm when you're not in the safety or design basis world, 50.59 doesn't work. I'm sure you've talked about Recommendation 1, especially treatments of change control.

If you're going to do something in this realm, you've got to pretty much put it in there, put it in this regulation so that whatever treatments you want, whatever control you want on configuration, it's got to be in there.

So that's the idea in change control. Certainly, this is important stuff. It was mitigating strategies order. We need to maintain the configuration over time. That's the idea.

So we have to have some sort of control. This is a very high level control, change control

thing. It's not, nothing real sophisticated. I don't have any criteria like 50.59. I'm not sure we could even do that. We had one suggestion, not too surprising at all, that they suggested that hey, why don't you follow along the 50.54(p), 50.54(q) reduction of effectiveness kind of change control, which is something I also thought about.

So that's the one feedback we had in this area. Most of the people here are pretty familiar with 50.59. I'm an old 50.59 person. But so that's really the idea here, that there should be at least some nominal change control requirement, and clearly you want to maintain compliance with your regulations obviously, and your guidance and your commitments and everything else.

So certainly that would be as part of it, but I think at some point if you wanted to make changes to what the staff has already looked at and reviewed, then I think we need to see that. If it gets outside the envelope of, you know, what's being done for the current licensees under the mitigating strategies order, we have obviously inspections involved.

So that will provide a licensing framework, if you will. If you're outside that, maybe

that's where we look at change control. But that's speaking at real time right now. So that's change control.

Linkage to 50.63. Got some interesting comments here, also with the overall integrated type of rulemaking. The comments here were not too surprising. While I think the industry supports having a link, a nominal link obviously, these are being implemented at a symptom-based EOP level.

But having a link; anything more than that can probably create unintended impacts. Licensees know what it means to comply with 50.63 and supporting guidance. So from a licensee standpoint, they know what that means. And when you start to link regulations, link to the new set between, to a separate set, you've got to be careful that we're not causing impacts.

So the first thing we were thinking of is well we probably would want to keep 50.63 as a separate entity, so I don't have thousands of procedures, programs, topicals, reports, NUREGs, everything over the last 20 plus years that all refer to 50.63 becoming something, or not labeled correctly and need pointers and everything else.

You don't want to do that obviously, but

this idea here was pretty simple. It was recognizing these do link together, and this is a concept that perhaps a lot of people that are involved with the nuts and bolts just don't realize, that they think mitigating strategies is one thing; station blackouts is another.

What's mitigating strategies for a ELAP condition was really a bad SBO, and so guess what? They link together, right into the same procedure, the EOP. So a lot of them was simply to recognize that in the regulations, almost for a clarity standpoint. But so --

MEMBER BLEY: So if you think more in the long term, rather than in the first year or so, does it really make sense to keep them separate?

MR. REED: This is an interesting idea. Like if you're a new reactor designer, okay, long-term, you could come in with one set, make any strategies, address everything. One shot. Beyond design external events, if you want to call it that, exposure to fires, normal blackouts. One set of equipment, one set of strategies, one rule.

I think I can see that happening, so for you could have a new, a new like I'm not sure where we'd put this thing, Part 52 or somewhere. But a new

reactor, they could do it in fell swoop, and that would probably be great for a new reactor type of situation. That would be horrible for a current licensee. We'd have to go through and figure out what did I just, what happened? How do I need all this? What do I have to change?

So if we do it, I think we'd have to totally separate and have a new integrated set of requirements for new reactors looking forward. I think you could that. In fact that -- if I was to start all over and we didn't have anything in place, that would be exactly what we would have.

We'd have one set of mitigating strategies that would do basically everything. Whether it's an explosion or fire, whether it's external event, whether it's a normal blackout, it would handle them all. In fact, they probably will.

VICE CHAIRMAN STETKAR: So I guess what I was thinking is I don't know how much chaos is here for existing plants, but we'll be needing 50.63. We'll have some new requirements that are probably much more heavily overlapped than even you said. I mean you're dealing with the same thing, just longer term. You're extending your ability to deal with it.

Having a completely separate set, five-ten

years from now, the administrative burden of tracking those notable things might more than overwhelm, you know, than biting the bullet and addressing it all at one time. I don't know if anybody's thought hard about that. I'm sure the industry reaction at first is don't touch this, because we know what we're doing.

But I don't know if people, and we'll hear from them some time in the future probably.

MR. REED: It could happen.

VICE CHAIRMAN STETKAR: I don't know if they think, you know, what about five years from now? Are we really buying a lot of overhead by having two separate -- that was one of the questions that went out to the public comments, wasn't it? What kind of feedback did we get?

MR. REED: And you know, a current licensee I think could come in and say you know what? I can meet 50.63, 50.54(hh)(2) and 50.XXX with one set of stuff.

(Simultaneous speaking.)

MR. REED: He's a numerologist. But with one set of stuff. We'd be fine with that, and they could still have three separate requirements, and one set that's accepted as a Mod 3. But it would be nice to have it in one spot, but if I do that, I think I do

create a lot of paper impact, if nothing else.

MEMBER CORRADINI: I didn't hear that conclusion. So you agree with the fact that one could satisfy all three with one set of --

MR. REED: No doubt, yeah.

MEMBER CORRADINI: Okay. But then your thinking is that still you would maintain three separate recording logs?

MR. REED: Three separate requirements, so that those who don't want to do that are not adversely impacted or intentionally through changing all the programs, procedures and everything else.

MEMBER CORRADINI: Good God. I'm sorry that is not --

(Simultaneous speaking.)

MEMBER CORRADINI: That's my immediate reaction.

MR. REED: That's a rulemaker trying to minimize impact to -- Shana, go ahead.

MS. HELTON: Hey Tim, this is Shana Helton, and correct me, Tim, if I've got it wrong, but as we move into the proposed rule stage and we do a full-fledged regulatory analysis, these are the kind of considerations that we take into effect, or take into account.

As Tim alluded, you know, there's Paperwork Reduction Act, burden requirements. So we'll look at the public feedback that we get, you know. I think it's a very good question, a very good comment, and I appreciate the feedback from the Committee. But I think, you know, we haven't yet done the regulatory analysis, and that will really shed the light on kind of what the radiance is from a cost-benefit standpoint.

MEMBER BLEY: I have a related question. If you defined ELAP in the more general simpler terms, like Mr. Stetkar suggested, one could envision a fairly simple rule, but with guidance and detail of how you meet that rule, that would kind of replace all of it.

MR. REED: I actually can see this thing going that way eventually. When we go through all the gnashing of the teeth and everything, when all is said and done --

MEMBER BLEY: Here's the guidance. You do what you were doing and you're good on what was 50.63.

MR. REED: Yeah.

MEMBER SHACK: But I'm not sure what the advantage is.

MEMBER BLEY: I'm not either.

(Simultaneous speaking.)

MEMBER SHACK: You know, that kind of guidance and stuff, it's a matter of comfort and fear.

MEMBER BLEY: I look at it as a three-tiered rule. The 50.63 takes care of sort of the most common kinds of station blackout situations.

MR. REED: The short term.

MEMBER BLEY: And people are sort of used to that. High up, this is on maintaining reliability of the AC systems, because you really don't want to have to go to a mitigating system. I look at the mitigating systems order is the next level of things. Lots of stuff has gone wrong. I've got to recover.

Then, you know, it's 50.54(hh), you know, everything shot to pieces, you know, the one last shot at it. So I to me see there's three regimes here that are covered, and I think it's worthwhile keeping them separate, and linking them as they go from one to the other.

Trying to put them all in one rule, where you really have different expectations. I mean my expectations when I've got lots of damage are different than I do when I'm in my sort of normal operating condition, and I've lost power.

MR. REED: Yeah. Sometimes if I roll them

up to one high level thing, I can inadvertently impose impact for what you're saying, where somebody says "Wait a second. I don't need to do that for this," you know. I'm like I can't figure out what are the permutations here.

MEMBER BLEY: So I'm not at all sure of that. I have to think a lot more about it, to make sure it doesn't --

(Simultaneous speaking.)

MEMBER SHACK: It isn't clear one way perhaps to the other. I personally like the three-tier approach, because sort of that's the way I think of it. But I kind of agree.

MEMBER POWERS: I can see that it is an implementation, if I was doing it.

MEMBER SHACK: You could do that.

MEMBER POWERS: But it seems to me that a rule that says "thou shalt code," until you can get to a state where you don't need the code as a very straightforward rule, and strictly a performance-based rule. Very little in it. Perhaps a lot of guidance, but a very simple rule, and maybe the guy that has to comply has three tiers and all kinds of complexity. But the rule, it seems to me, it's very --

(Simultaneous speaking.)

MR. REED: Since you're acceptable meeting it that way, a new reactor can meet it a different way, but it's one rule.

MEMBER BLEY: And maybe once you really go through it, there will be three regimes of response.

MEMBER POWERS: How many regimes there are is how you break things down and think about things. But the simpler the rule, the more you make available engineering expertise that relies on the licensee, and the less you have to rely on the engineering expertise of you on your team. I always like to put the burden on somebody else.

MR. REED: That's one side of it. If you're a licensee and you just opened this up, and I'm not sure that you, Mr. NRC, are going to play nicely in the sandbox --

MEMBER POWERS: Well, that's for, that's the function of the regulatory guide, to say here's one way to cope with this, and what gets you out future trouble is when a guy comes in with his graphite-moderated sodium-cooled fusion reactor, you don't have to change the rule.

MR. REED: Yeah. That's what's great about the performance-based rule, absolutely.

MEMBER POWERS: Yeah, that they're technology-neutral.

MEMBER CORRADINI: Yeah. Are you in favor of that? I just want to get that on the record.

(Laughter.)

MEMBER CORRADINI: I just thought, I thought I heard something, but maybe I heard something else. So I just want to get it on the record.

MEMBER POWERS: No. I mean my favorite rule of all the rules is the 10 C.F.R. 100.33, that says don't care how you do it; just go ahead when the radionuclides exceed 25 rem site boundary. Don't care. Don't tell me anything about how you did it. Just don't do that, and it's totally technology-neutral, totally --

(Simultaneous speaking.)

MEMBER SHACK: --condenser on the Mark 1.

(Simultaneous speaking.)

MEMBER POWERS: I would laugh, except I didn't hear you.

MR. REED: Last slide. I think I'm violating the agenda. This is --

MEMBER POWERS: The penalties for doing that are relatively minor.

CHAIRMAN ARMIJO: They're pretty harsh.

MR. REED: This delineates the next steps. Right now, we're considering ten sets, and we'll get another set here in a week or so of comments and revising the reg basis and finalizing that. We have, as Mike mentioned in the very beginning, a requirement to provide a Commission Assistance Note. That's due on July 8th and July 1 to the EDO.

So that's my early metric, if you will. So as I say here in that sub-bullet, if the Committee's going to decide to write a letter and put it out, I'd appreciate that sooner than later. That would help inform that MR. CASE: Note. If possible, I'd like to reflect any views if I can.

And we will, of course, be proceeding into proposed rulemaking after that. So we'll finalize the reg basis. We'll put it out in an FRN, to show the stakeholders that we've done that, and then we'll move forward into rulemaking, and then go to the proposed rule, which is the next stage is January 2014. Mike?

MR. CHEOK: I was just going to add real quickly, if we do not get a formal letter from the Committee, we will obviously also take into account the comments we go today and factor them into our CA Note.

MR. REED: Yeah, whatever way. I mean

today or any other way, creative way, I definitely want all the comments we can get, because there's a lot of good interaction here today, similar to what some of the external stakeholders, and similar to what the working group has already had. So but a lot of these you can see from more than one side.

So we're trying to figure out what the best way is. Anyway, that's the next step. That's all I've got.

MEMBER BLEY: I have a question. Once we have this rule, and once people propose their strategies, or lay out their strategies, I'm assuming my strategies include using some of the flex ideas and maybe shipping a generator onto site if I need it, either by truck or heloing the thing in, and Ron Ballinger was pointing out to me earlier that how the military has helicopters with fairly large generators on board with hookups.

I don't know if those would be available or if the industry is looking at those. But industry's putting together, as I understand it, and INPO is participating in catalogues of where things are, how they can move them and that sort of thing.

But once those strategies are defined in meeting the rule, you guys explore to somebody who's

exploring how in fact NRC will somehow follow that planning, to be able to get equipment in and adjudge how reliable that might be for different events on the site.

MR. BOWMAN: At the guidance level, what we have set up in NEI 12-06, the document we endorsed for the guidance for the order, which would very likely be carried forward into the rulemaking, one of the requirements for the offsite resources is that it be amenable to inspection by the NRC.

Our intent is to treat it similar to how we treat Appendix B suppliers. I've been in discussions with the Vendor Inspection branches in NRO on the way forward for that. So that's the type of oversight we'll be having.

MEMBER BLEY: Okay.

MR. REED: Any more comments?

(No response.)

MEMBER SHACK: Thank you very much. Ten slides, right on time. Back to you, Mr. Chairman.

CHAIRMAN ARMIJO: Okay. Thank you, Bill. Thank you, Tim. We're going to take a break and we'll reconvene at 10:20.

(Whereupon, the above-entitled matter went off the record at 10:05 a.m. and resumed at 10:22

a.m.)

CHAIRMAN ARMIJO: Okay, we're going to start. Okay, we're back in session, and our next topic is on the revisions of Six Regulatory Guides that Charlie Brown will lead us through.

Mr. Brown.

Revision of Six Regulatory Guides

MEMBER BROWN: Okay, yes. The staff is in the process of doing the Reg Guide updates. These six Reg Guides are on software development processes. They are all interconnected, and as anybody who attended our exciting meeting could testify to, which there were only three of us there, but that's okay.

So I'm going to introduce Mike Case real fast here, so he can make an introductory comment, and then they will proceed on with getting you through. We need to make one observation first. These were first issued in 1997. There have been no changes to any of them with one exception in that interim.

So that's, it's important to get these particular Reg Guides out, and so that's just to set a little bit of a tone for your thought processes and your discussions. Mr. Case, you can then make your comments.

MR. CASE: Thanks. I'm Mike Case, the

Director of Engineering and Research. Karl used to work for me. He's now over in NRR. So he's finishing up this assignment for the Office of Research. So we appreciate his ability to stick with us and get these things through.

Just a couple of thoughts. This is the sort of an agenda item that is a change of pace from the last one. In last one, we were doing something that was important and urgent, as far as rulemakings can be urgent. This one -- Reg Guide update program, and I just wanted to give you a quick status. There's about 554 Reg Guides in NRC's Reg Guide program, and you all have been participating in getting them up to date. We are about two-thirds of the way done. So these are being driven by the Reg Guide Update program.

So they're not remarkable changes, but it's getting us in the same -- it doesn't quite get us to the same century, but it gets us in the same general area.

MEMBER BROWN: The comments on the Reg Guides are you guys still haven't caught up.

MR. CASE: But it gets us a large part of the way there. So I just want to -- it has had the benefit of something that you reviewed. Karl's going to report on how we dealt with some of the comments,

and I think it's an important thing, and we're looking forward to a letter that probably summarizes those comments, and hopefully releases us to make them final and get them out. Thank you.

MEMBER BROWN: Karl, you're on.

MR. STURZEBECHER: This will be my presentation. Is it on here, Christine, or do I put my own --

MEMBER BROWN: Christina, how does he find his presentation? A momentary glitch in computer operations.

MR. STURZEBECHER: Good morning. My name is Karl Sturzebecher. I'm with NRR right now. As Mike explained, I was with the Office of Research, and I'm going to go through six software reg guides that we've been working on.

The purpose of the meeting, I'm going to go through a background of what was the goals, how did we go about this effort, what was the overall results. We've gone through a quick iteration of what, how the Reg Guides and associated standards fit with the software life cycle.

I have a layout, a matrix layout that shows the IEEE guides, how many different revs have gone since 1997, when we made the first set of six, and

then I'll get into, review six Reg Guides, and I'll step through the Subcommittee's findings, and what we're doing to work on those particular points.

I have a slide that's going to demonstrate the color code key and how I'm going to present these six guides, so I can do it in a rather structured and fast way, in showing the topics and how they've changed. I have a conclusion. I'll go through the six Reg Guides using that template, and then I have a conclusion.

So the goal for these six Reg Guides that were released in 1997 is basically just to update to the latest IEEE standards. In general, there's no change to the approach used, and we'll look further into that. I show you how there's some refinements that have happened.

How did we go about this effort? Well, the guides we first started with, the draft from Oakridge National Labs, and then the NRC picked that up from there with a ten-person team, that consisted of NSIR, NRR, NRO and Research, and they had subteams for each guide, and then we used a stakeholder document process to keep track of the changes as we went through them.

As for outside influence, we've been talking to JPL, NASA, EDF, a railroad software test engineer.

So we've been getting a flavor of what other industries do, and where we sit in that situation.

What was the overall results? Well, the lead -- you're going to see that the lead documents have changed quite a lot. While there's some basic documents in here, there are standards that haven't varied at all. The concept still hold for after 20 years. They're still in the same way you do; certain things stays the same, like unit test.

And like I've mentioned before, the approach has been refined, and I'll give you an example. Like the first Reg Guide we're going to go through, the 1.173, it takes certain topics like software quality management and deletes it, and downplays V&V, because the V&V really sits in the other Reg Guide in 1012.

So the idea is that it's becoming more refined and you're going to see that. Reg Guide 1.170 through 829, IEEE 829, expands significantly in the number of documents. So there's some differences going on, and then yet some of the guides stayed the same.

There are cross-cutting topics. Integrity is a big one that steps between the different standards and also the guides. Security, that's the latest topic that's been going on, and we've addressed

that. We'll go through that. Tools and release management delivery, which a lot of the standards have brought that topic in, and I'm going to talk about that.

So I will give you a quick run-through, that if you start with the software life cycle, the first Reg Guide, 1.173, is the umbrella. It's what the project architect picks up and starts with, and it's associated with 1074.

Now the architect's type or the architect, he's going to start working with planning the activities, and he's going to need to set up requirements, and is going to refer to Reg Guide 1.172, which is based IEEE Standard 830.

Then when you get into the design activities, and you're setting up this particular life cycle process, you're going to start looking at unit tests and you'll reference this particular guide. The implementation activities is when you take the concept and go into code, and integration is when you take unit testing of certain parts of the code, and you begin to link them and you do branch testing.

Eventually, that creates a component, and then you step up the next part, where you go to a system test. Now throughout this entire life cycle,

you have your software test documentation, and that's our Reg Guide 1.170, based on 829.

This document follows each of the steps going through, while using configuration management, and we get into validation activities or testing and I put that one up, and then here's the two-base Reg Guides like I mentioned, configuration management and the verification/validation processes, Reg. Guide 1.168, which is used all the way through the life cycle. Then you have your installation activities and finally operating maintenance activities. That ends it.

MEMBER REMPE: So before you leave, you get -- I looked through some of the comments from the public, and there were some concerns expressed about some of these standards that are being referenced by these Reg Guides being out of date.

So let's pick on 1.168, and actually there's 1012 actually has a 2012 IEEE standard, and the response given back to the member of the public was well, the revised standard actually incorporates other aspects that are not covered by this Reg Guide.

What I was wondering is again, we're referring to standards that are, have been superseded. Could a person or could the NRC's process be a little

more up to date, by at least say while we looked at this IEEE standard, we're only going to consider that aspect of the 1012-2012 standard, instead of tying ourselves back to the older versions of the standards, and being a little more up to date in the process?

MR. STURZEBECHER: That is true. 1012-2012 came out this past summer. I was in the process of going public for the public comments at that particular point.

Just from a standpoint of how we look at our stakeholders and go through the review process, it's hard to step back and pick up a guide, and then retro everything to follow through, especially in trying to carry off six.

We already did that once with 829, the 2008. We were referencing, I'm going to go to the next slide here. For 829, the part that came from Oakridge was using the 1998 version. So my question is when I got the project was well, why aren't we using the 2008?

So I stepped that up, because and that's a huge change, because from 1983 to 1998, it was only a format change. From there, the documentation -- 829 is almost twice the size. So that was enough labor there, just to get the team to re-orientate and start again on that.

So when 1012 comes out, and we had many discussions about this, some heated, about going to that, there is the other aspect is that now you're introducing hardware and systems. So we already systems sufficiently, I believe, with the SIPs the way they're laid out.

As for hardware, that's a whole another subject, and you know. But the scope of the project was really just to come up to speed on the standards we have. There's been some talk of starting a new set of hardware Reg Guides, and maybe that should be something in the future that we should look at.

But frankly, I think where we caught the particular set of standards, they've worked well together as it stands. I don't think you can really say the gang of six, based on software, you can start including hardware. But you're right. We could have said well, just take the software aspect of it, and that is --

MEMBER REMPE: There were some new changes in the 2012 versus the 2008 software, I guess, the question is.

MR. STURZEBECHER: Right. It just expanded three times its size and said okay, when you want to -- you use the same set of tables and everything, but

use it for hardware and use it for systems. It's possible. I mean I went through it and we could have done it, but I just don't know.

There was other aspects that I see, like if you look at 830, you know. That vision in the IEC, it just takes the 1998 and drops it into that document. That's okay, fine. The 828, it hasn't really changed either. But when you hooking on IEC and you start going that direction, like 12-207, they have a whole different philosophy of how they do their software life cycle.

They integrate integration management, and they integrate the V&V into the process, and they start to lose the whole idea of unit test. The unit test is really the base block of these guides. It is the building block for setting up your testing.

So there's certain directions that I've heard and talked to on this particular direction. When we talked to NASA, they followed the same pattern, and I think I'm pretty pleased with what we have. So at this point, I think further on, that should be a consideration.

MR. CASE: Karl, let me add from a process perspective, I'm also the Scanners executive. So I get that comment all the time. So from a process

perspective, what we did in the Reg Guide Update program, what we invented is a five-year periodic review.

So what I expect will happen is although we didn't come up to the latest standard, the Reg Guides will come up for view once again.

So hopefully, we'll develop a much better pattern of picking the Reg Guides up five years from now and incorporating some of the latest standards. From a process point of view, that's how I get pass this how come you haven't endorsed my latest standard.

MR. STURZEBECHER: I got the signal, yes. All right. So here's the matrix --

VICE CHAIRMAN STETKAR: Karl, I hate to do this to you. Go back to the previous slide. I just want to make sure I understand something, because I kind of liked -- no, the other slide. Go backwards.

(Off record discussion.)

VICE CHAIRMAN STETKAR: Configuration management down in the lower left-hand corner there at least on this cartoon seems to apply only to the design, specification and design activities. Doesn't it actually extend all the way through the whole life cycle, through operations and maintenance?

MR. STURZEBECHER: Sure. Yeah, it does.

VICE CHAIRMAN STETKAR: Okay.

(Simultaneous speaking.)

VICE CHAIRMAN STETKAR: I just wanted to make sure that I wasn't missing something here, because I went back to the Reg Guide.

MR. STURZEBECHER: You're right.

VICE CHAIRMAN STETKAR: Okay, fine.

MR. STURZEBECHER: Yeah. It's --

VICE CHAIRMAN STETKAR: Keep going. You've satisfied me. I'm happy.

CHAIRMAN ARMIJO: Karl, I've got a top level question. When you're doing this upgrades, and maybe this is in general on Reg Guide updates, I mean do you ever consider combining them, just to say "Hey look, like I see unit testing and then test documentation." It seems to me like that would be a nice, complete package that says this is how we test software and this is how you document it.

I just wondered if that ever is a possibility, and is it actually a problem?

MR. STURZEBECHER: We did consider that. We thought about just putting them all in one set.

CHAIRMAN ARMIJO: Yeah.

MR. STURZEBECHER: But then again, you lose that ability to change one versus the other. There

really isn't a lot of changes going on with unit tests, but it is the basic building block, as I said. It is a little bit separate from the software test documentation. When you get further in it, you'll see why that guide expanded, and what it's --

CHAIRMAN ARMIJO: Well, it looks like it's very complicated.

MR. STURZEBECHER: It relates to unit test. When we get there, I'll show you.

CHAIRMAN ARMIJO: Okay.

MEMBER BROWN: That's reflected on this. If you notice the complexity in terms of changes, 170 and 173 are the highest, and 170 was the test documentation. Yeah and --

CHAIRMAN ARMIJO: It would seem to me it would be more complex to do it --

(Simultaneous speaking.)

CHAIRMAN ARMIJO: --the document, but you did.

MEMBER BROWN: Sam, when I looked that them, that made sense to -- it's a set of standards and an order that everybody's familiar with, and if you go start mixing these things up, people are going to lose the picture on how, you know, what's expected from them.

So integrating is good in some cases, and in other cases, it just mushes things. It just adds confusion. So I understand your point. It's just that --

MR. STURZEBECHER: The point is that the audience who uses these things understands it this way.

MEMBER BROWN: Exactly, and all the standards, you know, the standards kind of mesh that way.

CHAIRMAN ARMIJO: Yeah. Like the Standards Committee could have combined them. So I just wondered if there was any reason, and you're saying hey, there's good reasons, but let's move on.

MEMBER BROWN: Yeah. Okay Karl, keep moving.

MR. STURZEBECHER: Okay. Now I'm moving into the review of the six Reg Guides. When we went through this whole set of changes with the Digital I&C Subcommittee, they came up with six different suggestions for us to improve what we've done.

The first one is basically the coverage of Reg Guide should include more than just safety grade systems. We agree to that, except that the way it's situated in the Part A, we're specific on just safety

systems for now.

MEMBER BLEY: Part A of --

MR. STURZEBECHER: Of the guide --

MEMBER BLEY: It does state that, yeah.

MR. STURZEBECHER: Yeah. So I really didn't change that.

MEMBER BROWN: I'm going to help Karl out a little bit on this. There's a footnote in every one of the Reg Guides, and we'll talk about this when we're going through the letter. Footnote 1 says "This only applies to safety-related," these documents, safety-related stuff, but not systems important to safety.

So there's a separation. That's the same words in the 1997 versions, as are in the new versions. John raised the issue in the meeting about why is this systems important safety not at the same level of or some level, nor defined, relative to software standards and qualification, that the safety system are, and we're going to talk about that in our letter, and they don't have an answer for that. We're going to have to --

VICE CHAIRMAN STETKAR: For the purposes of this meeting, you've decided to retain that scope?

MEMBER BROWN: Yes.

MEMBER BLEY: And what Karl had said, Part of the Reg Guides?

MEMBER BROWN: That's right.

MEMBER BLEY: Yeah. So yeah, on the reg we agree. The Reg Guides do say that. We were hoping that it wouldn't.

MEMBER BROWN: We're not -- so that's still an open issue that we've got to talk about. The other five are the ones that they were going to do something with. So if you can move on through those.

MR. STURZEBECHER: Okay. For each one of these, I'm going to show in the diagrams where they drop in, and I'll be able to explain a little bit more detail. But the first one is on Reg Guide 1.173, which we'll get into shortly, and that was a comment that our cybersecurity language needed to be consistent in Part B, and one of the regulatory positions, 3, with Reg Guide 1.152.

We're working on that. We've already repaired Part B with the proper, the same language as in 1.152, and the Reg Guide or Position No. 3, where it's going to take those particular line items out, because they do not match. They're more for building security and that's not what my presentation is about in the first place, when you talk about building

security versus just having 1.152.

MEMBER BROWN: You do reference 1.152 in the document?

MR. STURZEBECHER: Yes, we do. We just need to keep consistency with the language, like you said.

VICE CHAIRMAN STETKAR: Our reason, for those who weren't there, 1.173 was in some sense an outlier from the other Reg Guides. The other ones sort of took the same reference language to 1.152.

MR. STURZEBECHER: And the only guide, because it's the overarching one that we put in Part C, we actually state go look at Reg Guide 5.71. And the staff felt that that was enough at that point. There's other places in other guides you wouldn't put security in at all.

Number 3, Reg Guide 1.170. That's the documentation one. There is a sentence in there when we take an exception to a particular table in Appendix B, that was trying to mix Integrity Level 3 and 4 together, and basically took an exception to mixing 3 in there and just saying hold at 4.

We had a sentence in there that was trying to explain why, and we're going to remove that sentence. It's already been done.

Reg Guide 1.170, No. 4 there, "Add failure

recovery software testing to the Reg Guide or the Position 4." That is called system testing, and we're working on a paragraph that will do what was asked for on that. And that's an important point, because if you're going through coding and you have a failure or a bug.

You need, if you had to come back to a particular starting point. So what's recovery testing software? So it was a very good item to bring up.

No. 5, Reg. Guide 1.169, add test cases and test documentation to the RP-6, and I think test documentation's there, I have to double-check. But we're going to put test case is a line item to highlight and emphasize that part for, when you're dealing with configuration management, whether it's an item that you check. I'll show you later on that.

The last one is Reg Guide 1.168, which we want to realign the paragraphs in there. We had a discussion about a statement on independence, and a disagreement with the way the boxes were shown on Figure 1 of 1012. There were three little boxes we want to remove.

We have a paragraph that's in there that it doesn't sit well, doesn't read right. So we're working on that. We're kind of getting a little -- it

doesn't flow well, and the second paragraph kind of sets the tone for releasing the reason for why you just did it.

MEMBER BROWN: That's the triangle diagram that had some lower level stuff that you all said we don't agree with those, and it wasn't consistent in the words?

MR. STURZEBECHER: Yeah.

MEMBER BROWN: And it was confusing, okay. There was a little bit of contradiction. So that point that was brought up. I've forgotten who brought that one up, but --

MR. STURZEBECHER: Okay.

MEMBER BROWN: So keep going.

MR. STURZEBECHER: So let's stop for a second. This is going to be how I'm going to step you through each guide. We're going to start with the IEEE standard on your left, and work across to the new, and then you're going to see whether it's endorsed without exception, it passes right onto the life cycle, the software project life cycle process.

Other ones that have been added that are new, and you see the callout little bubbles there, the callout with the new, we took an exception where we used the color red, and yellow is the delete. Green

is for existing, circles a particular item in the standard that's been there. We may have an emphasis we wanted to put.

We put red in, and I have using purple in a purple callout box for public comments, to show where the public comments came into this process we did for upgrading these docs.

CHAIRMAN ARMIJO: Does that mean they're incorporated, or they're --

MR. STURZEBECHER: Yes, yes.

CHAIRMAN ARMIJO: Okay. Not just somebody send in a suggestion.

MR. STURZEBECHER: I'll start with Reg Guide 1.172. All right. This guide follows exactly 1074, endorses it, and what it does is by using the standard, it sets the direction up for the project architect for building the software project.

Once he builds this particular life software project, life cycle process, you're going to have a product at the end which would hope to be that software product with some high, I don't want to say adaptations, but it's going to have to be the requirements that you put forward, that it is fairly well designed.

So the first step, let me run through this

quick, is he's going to need to start the life cycle process. You need to establish the requirements. That means you're going to refer to Reg Guide 1.172. You're going to have to select a software project life cycle model.

Now when I'm reading through these five steps, this is basically the first Clause 3 and 4 of IEEE 1074. So this is the first steps that this, that the project architect's going to do. So in building the model, a model is defined as it's a framework of processes of activities within a life cycle, and usually it starts with an idealized working of the problem. It becomes an architecture orientated around a supporting set of activities.

I'll show you later that 1074 moved this exercise into the Annex. They kind of de-emphasized that and it's set forth, just saying well, it's really up to the project architect, depending on the industry, to pick their model and go forward from there.

The next step is to develop the software project life cycle, and that's where you're going to start pulling the activities from the Annex A, and we'll go through that, where there are certain activities required and certain activities that you

can add if needed, that fill in this center piece.

Then you're going to establish this software project life cycle process using all these different activities, following this particular life cycle that you see in the middle, and then you need to validate the process with the stakeholders, to make sure that you've met. I mean you can even do a V&V at that point if you wanted to, just to see that the process is set up right, correctly.

So now I'm going to make a transition to the Annex that I was talking about for the third bullet down, and when they're pulling from it, the Annex A, the activities. So have the Reg Guide on the right-hand side. The left is the 1995 version. The center is the 2006.

So the first stage in this animation, and I'll go slow through it, is to show what change in 1074. Just to give you some background, it's still using the same life cycle process.

The 1995 version had a set of processes. This new one has activities. So it's broken down by activities, because obviously if you're trying to make a life cycle process, why would you have a set of processes? It just kind of gets confusing with the language on that.

This particular standard reshuffled a lot of the activities. There were a couple of big moves, but they go through that, and it's more refined. So they moved the software model, like I was telling you, from Clause 2 into the Annex. The software quality process was deleted. Title change on this integral process, which later becomes support, selection of activity groups.

And then we have the V&V process, which was deleted. It's still there in the form that you're going to do an evaluation, an audit and so on, but it's more at a peer to peer level for Reg Guide 1.168, for the years when you really want to do a true V&V on things.

So this shows the shift of how the guide changed, and it's pretty complicated. You can see the overview dropped over. The project management processes went to Annex A.1. The pre-development set of processes are now in Annex 2, and I shouldn't be using the word "processes," because they're now really called Annex activities in 1074. But there you see the whole line.

Now it's in red. I'm going to go through each set of items that changed. Now when we built the software project life cycle process, that was a key

concept in implementing the Standard 3 and 4. So we've already stepped through that.

Project management section, added a security, set of security objectives in Annex A.1, and that related to our Reg Guide Position 1(d), where we added what's called "secure analysis," and that's appointed to Reg Guide 1.152 and 571.

Now this is where the Subcommittee came in and said we need to adjust this, and make it exactly like Reg Guide 1.152. So that will be done, and so there's the animation to show that, and I talked to that earlier.

The project planning. In this change to the 2006 version, all of the planning processes are now activities. They're all moved into Annex A.1. So you have this brand new set of planning activities. So they de-emphasized more of the project management and started emphasizing up front that you need to do more planning, which will only make sense if you're a project manager, and they added release management.

Also in Annex A.3, for the development, during the development process, you're going to have that managed software release where that's when you take a particular software product that you finished. You've got to be able to know what Rev it is and keep

the configuration management straight for issuing them out.

Okay. So here is planned system transition, and this is an existing clause and now it's in Annex A.1, A.2-3. We created a regulatory position. The team felt that we needed to emphasize this, and this was just a reminder to the licensee that safety software needs to be evaluated by the 50.59 process.

MEMBER BROWN: I want to make one comment relative -- so you understand that one. That's a little confusing. If you read the IEEE standard, it effectively said that transition planning should -- is only required for when you're completely replacing all the software or revising the system. There are exceptions that says hold it guys.

You've got to do this in accordance with 50.59. All safety changes to the software need to be managed under the 50.59 process. Now so that's an exception they took, and I think that's what you're referring to; is that correct?

MR. STURZEBECHER: Yes.

MEMBER BROWN: So that's what that means. So there's nothing wrong with what they've got, but you've got to say no, hold it. You've got to do it to everything, not just when you take the whole thing out

and put a whole new one in, which was an allowance in the IEEE standard.

MR. STURZEBECHER: Software importation activities group, and this is the set up for activities in the standard that's new, and it's for evaluating the software importation required. We already have that in our regulatory Position 1, which is basically refers to the EPRI for pre-existing or commercially off the shelf software.

We reference a topical report that we have endorsed. That was one of the public comments that came in, and said you need to put the citation in there and the date. So we took care of that, and that has been updated to the Guide.

Okay, the next step is down in post development, and this is where you need to identify software improvement needs. This is a new section. Remember how we deleted the SQM? Well, this is kind of where it fits in place in the process now.

They put it into this area, and these three new activities, identifying the improvement, implementing the problem reporting and then reapplying it back to the software project life cycle process. So there's your quality link right there.

85. It has a new name, "Support Section of

Activity Groups." There was some difficulty in really seeing what's shuffled into this from the original guide. A lot of it is new. It's about evaluations, conducting reviews, a traceability matrix for conducting the audits, and reporting the evaluations.

Other subsections still holds configuration management in there, document development and training. Those were existing.

The last was the Annex D through F, which includes mapping information, model examples, glossary and a bibliography. We have a new Regulatory Position 6 that outlines each one of those particular annexes.

So that guide helped the project architect set up a particular process, and they would turn to this particular Reg Guide to develop the software requirements specifications. So Reg Guide 1.172 again follows directly a 30, I believe 30, let's see here. One of the issues, or if you want to put it one sentence, it's basically what do you do for the Reg Guide?

You're creating a software requirements specification that delineates the function accurately, without adding constraints. So it comes down to this point that even words that you use to try and explain a particular requirement in software have to be exact.

All parties have to understand what the word means and where you're going with it.

There's traceability from the original baseline. When you make your first revision of that particular requirement in your future developments, and the guide and the standard is written that it supports the life cycle process.

I didn't do any animation with this one, because it's pretty simple. You can see that there's only one change between the 1993 version and the 1998. That was the addition of Annex B, which is five lines for compliance to the EAI 12207 1997 version.

The unambiguous subsection or subclause in 4, we did create a Regulatory Position 2, and this is a new subsection called "Unambiguity." There was a public comment about how we've written it.

We were basically conveying that if you're going to set up your software requirements, that sometimes are generally derived from an associated software product, and to do this for a safety system requirement, you need to make sure the interpretation in the SRS should be unambiguous.

So it's just re-emphasizing that. The public comment was we didn't write it very well. So we rewrote it and that's been completed.

MEMBER BROWN: The point here was just we wanted a clear specification, not an ambiguous one.

MR. STURZEBECHER: Not ambiguous.

MEMBER BROWN: That's the English version of this particular additional stuff. Other than that, this was pretty benign.

MR. STURZEBECHER: In Clause 5 of the 830-1998 version, there is a subclause about security. We took exception to this and we got in again with the regulatory position 6(b), and we talk about security analysis, and we state in there that we need to refer to the SDOE from Reg Guide 1.152, which is Secure Development Operating Environment.

MEMBER BROWN: When you wrote that, I went back and looked. You say you took an exception. You didn't really say you took an exception to that in the Reg Guide. So any --

MR. STURZEBECHER: You want to --

MEMBER BROWN: I want to be -- all of the rest of the places where you took an exception, you said "We take exception to this, and here's what we want." In this case, you just stated what you wanted.

MR. STURZEBECHER: Yeah, we just stated what we wanted. What items that are in that particular --

MEMBER BROWN: I'm going to get beat up by

the members here, because I said there were no exceptions to this.

MEMBER REMPE: Now that you've told us to beat you up.

MEMBER BROWN: If you want to rewrite it --

MEMBER BLEY: Maybe this is an addition rather than exception.

MEMBER BROWN: That's the way I read it, that they added that to it. They weren't taking exception to anything there. They just added --

MEMBER BLEY: Added more requirements.

MEMBER BROWN: That's the way I read it, after I read the way you stated it before.

MR. STURZEBECHER: Yeah, because when you look at the --

MEMBER BROWN: Well, you don't have to mouse-milk this. You can go ahead and go on. I just wanted to make that point --

MEMBER POWERS: Do you have any idea what mouse-milking is? It's a baby term, I think.

(Laughter.)

(Simultaneous speaking.)

MEMBER POWERS: Why do you have those? You're always telling people not to do that.

MEMBER BROWN: Okay, Karl. We can go onto

this now, and go to the next item, okay?

PARTICIPANT: Actually 6(b) says "is not endorsed." So that sounds like an exception.

MEMBER BLEY: No. They have a lot of the annexes that they don't endorse in here, in these various Reg Guides, in the --

MEMBER BROWN: So that's not -- I made that point in the letter also, that they, you know, where they don't endorse an annex, they don't. It's very clear when they do, and it's very clear when they don't. So that was, in terms of clear writing, that was good.

MR. STURZEBECHER: Yeah, and maybe we should. I missed one earlier.

MEMBER BROWN: It's not an exception.

MR. STURZEBECHER: It's not an exception, but you know, the items are listed --

MEMBER BROWN: Let's go on, Karl.

MR. STURZEBECHER: Yeah. Okay. Unit testing. Here's another. This is based on IEEE 1008. There's literally no changes to the standard, and it provides emphasis on unit testing, just like I explained before. This is the smallest piece of software that can be independently tested.

Right now, the only thing we've done to the

Reg Guide is we've modified Regulatory Position 5, and we've also laced through the Guide references to 829, because like the Chairman said before, the unit testing and software documentation are pretty close, and they are, and this one is pointing to 829, saying here is where you need to look for where unit testing will be used in Reg Guide 1.170, and then the Regulatory Position 6, which outlines the Annexes A through D.

MEMBER SCHULTZ: And it needs to go back to the 1983 version, because the 2008 version doesn't comply, or doesn't provide those sections.

MR. STURZEBECHER: Yeah. It used to reference 1983, and now we're telling -- maybe I should have put 2008 there instead. Make that clear, yeah. In the Reg Guide, it says go to the -- originally, it said 1983, yeah. My mistake on the slide, so you might want to change that.

MEMBER SCHULTZ: Okay, thank you.

MR. STURZEBECHER: Okay. This is going to be a busy one, Test Documentation. Okay. This Reg Guide follows 829-2008 directly. Again, the objective is to create a software test plan and you can read the rest there, methodically documenting some of the requirements with reportability demonstration of the

unit component system and testing.

It follows the common framework of the life cycle process, and it applies to developing software with the life cycle, the pre-existing or pre-developed software. This is where we begin to introduce Integrity Level 4, the traceability and anomalies.

This Reg Guide had the largest set of changes. Literally this standard doubled in size. It's impressive, I think, the work that was done on this particular standard, how the details they went through to create another set of documents that overarch it.

Literally, it goes from being one-dimensional, the first version, to being three-dimensional in this sense, because they have, they've addressed these other issues of anomalies that may happen, how do you handle that, how do you record that, what kind of logs you use and it's traceable, and they had that integrity, four levels, four steps of integrity and we just stick to Level 4.

So in 1983 is on the left, we've got 2008, the new version in the middle, and our Reg Guide 1.170. Right off the bat, the scope's deleted. It's not part of the new one. The test item transmittal report is gone. The test incident report is gone, and

the appendices are gone. 1983 is too far out, a long time ago.

Where the particular parts did meet, you can see how the test plan number three moved into Level Test Plan Clause 9. Four, the test design specifications, became Level Test Design, Clause 10, and Test Case Specifications became Level Test Case 11, Clause 11, and the test procedures became a Level Test Procedure.

And you keep saying "Level" in front of everything. But when you're actually doing the work, you're working on a Unit Test A. You take the word "level" out and you drop it in front of there, and you call it "unit test, Unit A Test Plan," and you can begin to create your configuration management of parent, daughters and work breakdown structure using that particular nomenclature here.

So you can see how the 1983 version was really a core part of this new standard. So it looks like it's going through 2008. Okay. So the first part, Clause 1 and 2, basically how you use the standard. It's kind of a structured set of, you know, instructions. So you really need just to read through the entire document to understand it.

I'm going to start here with software system

integrity levels. Now in Integrity Level 4, we made a change to our Regulatory Position 1, which is Test Programs. We've added in there that you need to maintain Level 4. That's just a small change in there.

MEMBER BROWN: Well, that's not -- let me, I want to emphasize that a little bit, because in fact, the IEEE standard allowed the acceptance of a lesser level of software integrity, based on a risk analysis from one of the annexes, and I think the staff appropriately looked at that and said look, for safety systems software, we want Integrity Level 4, and that's very much in tune, as you probably well imagine, with my general thought processes.

I really like that, because they told people what they wanted, and I thought that was an important thing, a point to get across, in terms of their insistence. It's very specific and said they can only apply Level 4, should be assigned to all nuclear plants safety systems, and they developed that.

CHAIRMAN ARMIJO: Well that's a built-in requirement.

MEMBER BROWN: Yeah, that's very specific. Well, it's a Reg Guide.

CHAIRMAN ARMIJO: It's a back door

requirement.

MEMBER BROWN: But it's very specific as to what they want. So if they come in with something other than that, they're going to --

CHAIRMAN ARMIJO: It's going to be painful.

MEMBER BROWN: It should be painful, let's put it that way. The fact is they should say no about 4,000 times before they look at it. That's an offhand comment. Anyway, I just wanted to make sure you understood that.

MR. STURZEBECHER: So that goes right up front in that regulatory position. In Regulatory Position 6, we do have integrity levels, a new section there, and it takes exception to the Annex B and Table B-3, because in that particular annex, we'll get to that later, but it basically says that they tried to mix in with a risk assessment scheme of Level 3 with Level 4. So we take, we put that exception there.

The public comment we had for Regulatory Position 1 was they didn't like the language, because when you look at Regulatory Position 1, there's a list of items we add, ask the licensee to look at, along with the master test plan, and it wasn't clear whether we were saying the Master Test Plan and A through G, or one or the other. So we cleaned that up.

Now this is one of the little Subcommittee's comments were when we took exception to that Annex B, we had that one sentence in there, and it's going to be deleted. So I'm showing --

MEMBER BROWN: That's the likely cause.

MR. STURZEBECHER: The likely cause, yeah. Likely to cause, yes. Okay. So Clause 5 is Test Processes. It follows the life cycle. It really outlines exactly how the stages when you route through it, that you're supposed to set your documentation up with the life cycle.

It also had a statement about testing tasks that in Clause 5, that we wanted to point in our Regulatory Position 7 here, that if you read through Annex C, Table C.1, that it emphasizes it better than what's in Clause 5. So we just made that addition with that Regulatory Position 7.

Regulatory Position 9, which is associated with Clause 5, because Clause 5 has a Table 3 in there, which identifies security issues in the life cycle that should be addressed, but it doesn't include the very beginning at Acquisition Supply, Planning and Concept, which is picks up from concept and goes on. So we made the revision that in the plan, you need to consider security all the way from the start.

Test Documentation. This points to two aspects that we brought up in Regulatory Position 3. There's a Clause 6.4 that says, you know, if you want to minimize your documentation, just lower your integrity level, and we're saying no, we don't accept that.

At the same time, we also brought up that it's okay to use test logs and to reduce documentation at the open entry, and that can be a tool in which you repeat the same particular procedure, and just have an open entry where you drop in the next item that you're calibrating or working on.

MEMBER BROWN: You really covered that in Position 8, if I remember correctly?

MR. STURZEBECHER: Yeah. Yeah, I did.

MEMBER BROWN: And you took exception to that.

MR. STURZEBECHER: And that's the next one. Yes Charlie. Okay, yeah. On Position 8, we're saying if you're going to use that tool, it's got to be usually accessible for electronic validation for a safety concern. So those three particular items were all hinged upon Clause 6.

We'll go to Clause 7, Test Documentation, Address and Mapping. This is, it's kind of -- as a

clause, it's not really, I would say exciting. But it has some really strong relevance that maybe they should strengthen in the future, because it points to -- it starts laying out where you're supposed to go and take all these particular documents that you want to address, and how do you lay them out and have the work breakdown structure in testing. So it's a very important clause.

We finally get to the Master Test Plan, and if you're running through a set of tests and you have your tests, your level test logs, your anomaly reports and then say you document this with a level and then a test status report. This all ends up in the master test report.

There's a clause there that -- I think we went down too far -- there's a clause there, in Master Test Clause 8, at 8.2.3.3, where we wanted to emphasize that they had a deviation policy, and that we need to establish this and record using the proper documents.

So that's all Regulatory Position 2 was, is it emphasizes that, that change that we put in there.

Then we have -- I've already clicked, good, the AR 14, 15 and 16. It was three clauses, and this is a new set of clauses that, excuse me, really is a

complete improvement over the ones that were deleted on the left there, the test item transmittal report and the test incident report. I really couldn't find anything directly related between the two.

They were rewritten. So that's the tail end, after you've gone through this process and you've done your testing, and how to report your anomalies, your bugs in the software. We make note of that in Regulatory Position 1(g), and say highlight the use of this level test log and the anomaly report documentation.

Last is the annexes, and A through H, we put that in Regulatory Position 10.

MEMBER BROWN: I don't remember. Did you all endorse all of those annexes in this particular Reg Guide?

MR. STURZEBECHER: No.

MEMBER BROWN: I didn't think you did. Okay. Just that I remember one of them, you said you did pretty much all the exceptions.

MR. STURZEBECHER: Yeah, Table C.

MEMBER BROWN: Yeah. I'd have to go back and look. I just, because I couldn't remember which Reg Guide we did. But you stated that. You can go ahead. That's a confusing question on my part.

MR. STURZEBECHER: Yes. Here's where we're going to add the failure recovery software testing, right, in Regulatory Position 4. That's when you're testing your code and it fails. Where does it go? You need to have it fall back and have the documentation that shows that your recovery software testing is working.

Reg Guide 1.169, Configuration Management. This follows 8/28/2005 directly. The Guide follows it directly, and the objective here is to use the configuration management plan, the activities reporting, the software, the system history and the baseline to final use.

There weren't really that many changes, and this is a medium level set of changes. It's not like some of the other standards which didn't change it all. But there are a few things.

MEMBER BROWN: Is that through IEEE 828?

MR. STURZEBECHER: Yeah. Here's some tweaking to say that the standard matches the other standards, and that's -- we'll go through that next year, changes in words that they did.

The appendix becomes an annex, so you see 1990 going to 2005. The introduction is split up into overview, definitions and acronyms. In Clause 3, we

added a couple of tasks for doing the software configuration management process, and those were costs, surveillance of activities and types of risks. They were very minor updates.

This is where the release management and delivery comes in. They've added that in, and we did the same with Regulatory Position 12. So they just re-emphasized that need. We also made a note of it in several other areas, line items like in Regulatory Position 4, in the line item there, because it's basically saying make sure you include this.

We also had a paragraph that we said control the development of your commercial contracts, as part of the whole configuration management scheme. Regulatory Position 7, that refers to the EPRI topical report, and that's how you dedicate a particular commercially off the shelf software, and again, the public comments stating about our citation and when we accepted that report needed to be put in there. So that was changed.

Basic word changes throughout the two standards, from the 1990, 2005. "Tailoring" was changed to "adapting." Nothing exciting, and then the annex becomes Regulatory Position 14. A is the Bibliography and B is Relationship to Other Standards.

Then on the Regulatory Guide, we had this outdated reference to Standard 1012-1987, which is no longer in use, so that was deleted. There was a public comment that removing a line item that said "Commercial software items that are safety software, or safety system software."

Those items, when you look at the Reg Guide, is about safety system software. So it is redundant that we had line item, so we took that out. This is where we put the test case, added that into Regulatory Position 6. It's called "Documentation." So that's where they added that, so that's covered.

Reg Guide 1.168. This one was interesting, because it has two standards it refers to. Again, it follows 1012-2004 version, 1028-2008 directly. This is one guide that was updated from the original 1997 group. It was updated in 2004 and now we're updating it today, 1013. The Reg Guide --

MEMBER BROWN: Is this the interim one that went to 2004?

MR. STURZEBECHER: Yes.

MEMBER BROWN: But it was just, it was editorial. There was very little, if anything, in the difference between the two standards.

MR. STURZEBECHER: Right.

MEMBER BROWN: Because that's a comment you made during the Subcommittee meeting.

MR. STURZEBECHER: There's a few additions, minor additions to 1028, and I'll show you the next on 1012. There are a lot more minor things put in there, but no big changes at all. In fact, we look at 1028, we go through it. This is one where it deleted the anomaly classes, the Annex A.

The anomaly classes were some sort of taxonomy. It wasn't really useful. Anomaly ranking was shifted over into 2008. It has the same wording and structure, starting with catastrophic, critical and working your way down, as 1012, but it just doesn't have any numbers. Level 4, 3, 2, 1.

These were minor changes. In Clause 4, it added life cycle and a planning line item. The next level we're going to call out shows in Clause 5, with the add spec descriptions. In Section 6, 6.1, gave software topics for the inspector to look at. 6.3, added some inspection items, documentation, quality, procurement and software history. So really general small things. I might not even have wanted to put them on, but they had no effect on the standard.

So this is the last one. This is your 1012-1998, the 1012-2004. These two figures were moved

into the back end of Clause 7. 7.6 was moved into 6.1 of 2004. It's again the reporting requirements, which makes sense to fix under Clause 6, which is about V&V reporting. So that was taken care of. Then the annex was moved over, A through H.

As to Scope and Field Application, some minor details of how you go. Like now you can include commercially off the shelf items for this. This is where Clause 4, where they added integrity levels 1 through 4, the description. Also in 5, where it has integrity levels the highest, the V&V intensity should be just as high.

We included this in our title. It was just a title change in our Regulatory Position 1, was "Critical Software." We just changed it to software integrity. There wasn't anything different than that, because this guide is pretty up to date, Charles was saying.

The public comment on this one is there is a contradiction between what we said in Reg Guide 1.70 and Reg Guide 1.68. In 1.70, it was about Annex B, but we took an exception to being B.1 and B.3.

We didn't have it in here, so we added that paragraph. This is the same paragraph that has that "likely" sentence that we want to delete. So it's

just we're repairing it, but we're also following up with what the Subcommittee said to do.

The process management has four process improvement tasks. The process development adds life cycle security, and that's laid out through the life cycle that they now acknowledge look at security.

There was a clause in 7.74 about security, and we reference it just again, or we note that you should look at and use SDOE activities, that that should be part of your V&V activity, to check the SDOE.

This was another adder, small adder with 7. It adds 6 under reports. That's all it was. Nothing major. Now the annex, I have it separated here, two different colors. One was existing and one was partly the new, some of the new changes they made. That was Annex B, B.1. That's the one we took exception to. The original Annex B.3, we took exception to that too, and that's how it ties up with Regulatory Position 1.

In Regulatory Position 3, we added this paragraph. That's what we talked about before. We disagreed with the Figure 1, the three bottom boxes on the triangle, and the Subcommittee says we need to work on that paragraph. So we're going to straighten that out, because it doesn't flow right.

The last callout here is Table C.1 adds additional independence, which is not acceptable, and we took exception to that, because they try to mix in an idea of conditional independence. So it will just be purely "independent."

Public comment to include a topical report citation, and that was taken care of in Regulatory Position 4. That's the end.

MEMBER BROWN: Okay. Before you leave that slide, go back. The two interesting ones in there were the Regulatory Position 3, where it talks about the little block about independence of software, V&V exceptions. If you look at IEEE 1012, there's a figure called a "Relationship of Verification and Validation to Other Project Responsibilities."

That's a little triangle showing, you know, the major step and then it drops down to subgroups, and they pigeon-holed them, those little subgroups. They said, hey, look, we're not going to agree with how you pigeonhole. That's got to be, you've got to tell us what you're going to do in the big picture when you go through and lay it out, as opposed to allowing that, the pre-defining what was acceptable or not, relative to an organizational standpoint. That was in Annex C, excuse me, Annex F, Figure F.1.

So Position 3 actually takes exception to those subordinate relationships. That's what it does. I mean it's fairly easily stated.

The other one is the conditional independence. When you do V&V but you've technical independence, managerial independence and financial independence from the development organization. If it's rigorous, those are completely independent from the development organization.

The IEEE standard allowed a less than rigorous independence, based on, you know, some evaluation and an analysis that you did, and the staff or NRC staff took exception to that and said, to that form of independence and said that that's not acceptable. You need rigorous independence.

Again, this is a Reg Guide, and if somebody wants to do something slightly off normal, doesn't mean they can't come in and talk about it. It's just they set the metric in a particular place, which at least the Subcommittee members didn't disagree with that. Is that correct Dennis and John, on materials?

So those are the two major items in my mind, relative to this particular one. So other than that, didn't want to steal your thunder, but I think you're now complete; correct?

MR. STURZEBECHER: Yes, I am.

MEMBER BROWN: So I guess I would open the floor to questions, if anybody has any additional question.

MR. STURZEBECHER: I've just got one more slide.

MEMBER BROWN: Oh, you've got one more slide. I'm sorry. I apologize for that.

(Simultaneous speaking.)

MR. STURZEBECHER: Yeah. It just shows that we've worked on this. We've looked at it and all the common topics were contemplated. We matrixed through the guides, and key public comments were addressed, and they are ready for publication of the changes we need to make.

VICE CHAIRMAN STETKAR: Now you mentioned that Karl has evolved past these. If we recommend that they're not issued, does that mean he gets pulled back in? Just a piece of information.

(Simultaneous speaking.)

(Laughter.)

MEMBER BROWN: If there are any other questions from the members?

MEMBER REMPE: Throughout the presentation, I heard you say we're fixing a paragraph here or

there. Are you still doing that or are they done?

MR. STURZEBECHER: Part of them were done.

MEMBER BROWN: Is this relative to the questions that you -- thank you.

VICE CHAIR STETKAR: Are you going to -- are you going to show us what you did? I mean yes, Christina.

MS. ANTONESCU: Yeah. Yes, they're planning to give us the copies of all the regulations.

VICE CHAIR STETKAR: I don't think we need another Subcommittee meeting. We just would like to see what you did.

DR. ARNDT: Sorry, Steven Arndt, ACRS.

(Laughter.)

DR. ARNDT: Sorry, NRR. For those members who don't know, I had Christina's job about 25 years ago.

MEMBER REMPE: And we worked together.

DR. ARNDT: Yeah. We will get that revisions based on comments from the Subcommittee cleaned up, finished and concurred on by the various players, and then we'll forward a courtesy copy over to you, so that you understand, along with our comment resolution letter, what we've done to address your comments.

MS. ANTONESCU: Before they're issued, right?

DR. ARNDT: Yes.

CHAIRMAN ARMIJO: Okay.

MEMBER SKILLMAN: Hey Charlie, I do have a question. I'm thinking about how often we update computers. It seems that once every 36 months there's a need to update. What's the required update frequency for these Reg Guides?

MEMBER BROWN: I think they didn't use to have one, and now they're trying to do it on a five year review cycle, is what, that's what -- if I'm correct, that's what you said at the earlier part of the presentation.

MEMBER POWERS: What we found was when we didn't have a regular review of it, that when it became inevitable we had to, it was a horrific process.

MEMBER BROWN: Yeah, that's what it appears to be.

MEMBER POWERS: And so now a more regular process, at least the magnitude of the changes is trackable.

PARTICIPANT: So once each five years or once 60 months?

MEMBER BROWN: Yeah. That's what their, I think the NRC plan now is, right? That's part of the overarching --

MEMBER BLEY: But they've still got a third of them to revise.

(Simultaneous speaking.)

MEMBER BROWN: It's a big job.

MEMBER POWERS: Right. But at least we're not letting it accumulate for a decade or so.

MEMBER BROWN: For 25 years. Twenty-five years in some circumstances.

(Simultaneous speaking.)

MEMBER POWERS: I think that's the -- I mean the single biggest thing is the commitment to do a fairly regular update, without having to have somebody sitting there changing it day by day, you know like an odometer changing.

MEMBER BROWN: I want to make one other comment. Just trying to coordinate six Reg Guides with all the changes in the IEEE standards was just a huge job, and the staff, Karl and the folks that he dealt with, and I know he had assistance from others in wrapping some stuff up.

My personal opinion is they did an outstanding job of putting this together, and then

mapping it, such that we had some idea of where pieces from the old ones went and what was added in new. Without that, the review of these and the identification of the changes would have been just --

MEMBER POWERS: The problem is that you look at any one, mostly you look at the IEEE standard. Just look at one of them and you get totally confused. You have to have a very much more integrated view on things.

MEMBER BROWN: And these are all intertwined, and that's the problem. These six Reg Guides are very much intertwined.

MEMBER BLEY: But there's charts you put together, Karl, for us to show that mapping were very helpful.

MEMBER BROWN: Anyway, I wanted to thank you very much. I thought you did an outstanding job on that, your staff and your supervisors and whole thing. Unfortunately, they let you loose to do your thing, and job done very well.

(Laughter.)

CHAIRMAN ARMIJO: We're going to get a copy of the transcript and preserve that. It will get written down.

(Laughter.)

MEMBER BROWN: Sam, I turn the meeting back over to you. Thank you, with some time on your hands.

CHAIRMAN ARMIJO: Yes.

MEMBER BROWN: Definitely ahead of schedule. That was very well done. Thank you. That's management. That's time management, Sam.

CHAIRMAN ARMIJO: That's outstanding. I think you'll definitely get a bonus this year.

(Simultaneous speaking.)

(Laughter.)

CHAIRMAN ARMIJO: Well, I also want to thank Karl. It was a lot of work, and you made it easy for us to follow. It took a while to figure out the code in your color-coded stuff, but actually even I could figure it out, so that's good.

What I'd like to do now is recess for lunch, but since we're going to take advantage of the time that you've saved us and we're going to reconvene at one o'clock. Okay.

(Whereupon, at 11:45 a.m., the meeting in the above-entitled matter was adjourned.)

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

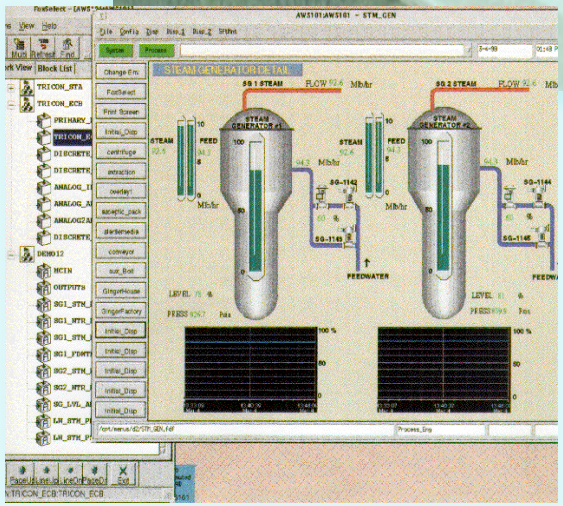
Software Regulatory Guidance

US Nuclear Regulatory Commission
Advisory Committee on Reactor Safeguards
June 5, 2013

Karl Sturzebecher
Office of Nuclear Reactor Regulation
Division of Engineering

Purpose of Meeting

- Background
- Review 6 Regulatory Guides (RGs)
  - RG 1.173 Project Management
  - RG 1.172 Software Requirements Specs
  - RG 1.171 Unit Testing
  - RG 1.170 Test Documentation
  - RG 1.169 Configuration Management
  - RG 1.168 V&V Review Audits
- Conclusion



Background

- What was goal for these RGs?
- How did we go about this effort?
- What was overall result?
  - Change in emphasis
  - Approach refinement
  - Common cross cutting topics: security, integrity, tools, and release management & delivery

Background

Regulatory Guides & Associated IEEE Standards

Planning Activities → Requirement Activities → Design Activities → Implementation Activities → Integration Activities → Validation Activities → Installation Activities → Operation & Maintenance Activities

SOFTWARE PROJECT LIFE CYCLE PROCESS – RG 1.173
IEEE Std. 1074-2006

SOFTWARE REQUIREMENTS SPECIFICATIONS – RG 1.172
IEEE Std. 830-1998

UNIT TESTING – RG 1.172
IEEE Std. 830-1987 (R2002)

SOFTWARE TEST DOCUMENTATION – RG 1.170
IEEE Std. 829-2008

CONFIGURATION MANAGEMENT PLAN – RG 1.169
IEEE Std. 828-2005

VERIFICATION AND VALIDATION PROCESSES – RG 1.168
IEEE Std. 1012-2004
IEEE Std. 1028-2008

Background

Regulatory Guide change matrix

- Demonstrates the IEEE updates (Left to Right) per RG
- Level of complexity of the RG and IEEE changes
- Natural flow of the RGs on developing software

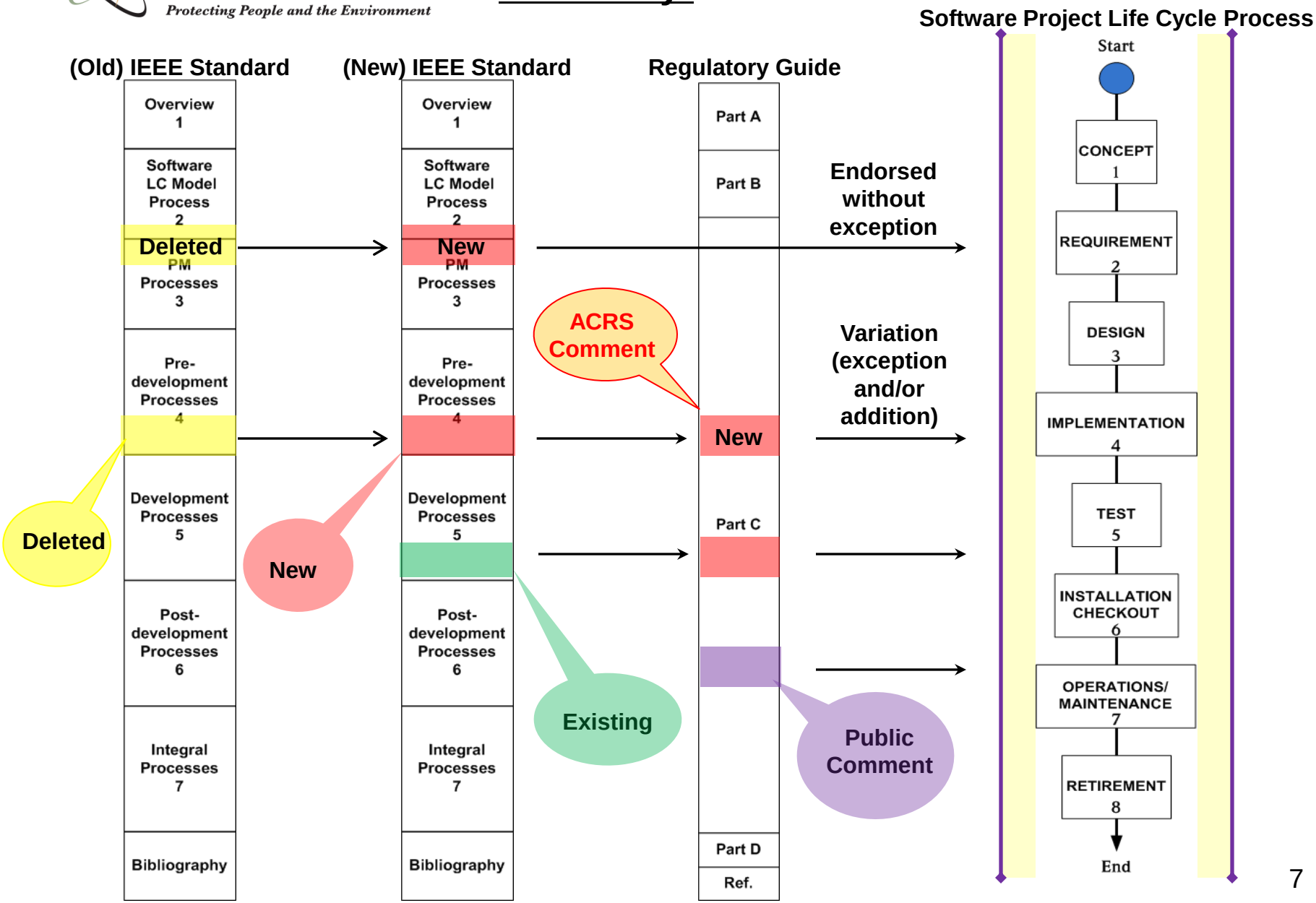
Regulatory Guides	IEEE Standards: Previous	Interim	Update	Future	Change Complexity
RG 1.173	1074-1995	1074-1997	1074-2006		2nd Highest
RG 1.172	830-1993	→	830-1998	IEC 29148	Low
RG 1.171	1008-1987	→	1008-1987(2002)		Reaffirmed
RG 1.170	829-1983	829-1998	829-2008		Highest
RG 1.169	828-1990	828-1998	828-2005	828-2012	Medium
RG 1.168	1012-1998	→	1012-2004	1012-2012	Medium
	1028-1997	→	1028-2008		Medium

Review 6 RGs

<u>Suggested revisions by the ACRS Subcommittee:</u>

1. Coverage of RGs to include more than safety grade systems
2. RG 1.173 make cyber security language consistent in Part B and regulatory position (RP) 3, as compared to RG 1.152
3. RG 1.170 remove “likely to cause” sentence in RP 6 (also found in RG 1.168)
4. RG 1.170 add failure recovery software testing in RP 4
5. RG 1.169 add “test cases” and “test documentation” to RP 6
6. RG 1.168 realign paragraph contradiction on independence in RP 3

Review 6 RGs


Color Key:
Software Project Life Cycle Process
(Old) IEEE Standard
(New) IEEE Standard
Regulatory Guide
Overview 1
Software LC Model Process 2
Deleted
PM Processes 3
Pre-development Processes 4
Development Processes 5
Post-development Processes 6
Integral Processes 7
Bibliography
Deleted
New
Overview 1
Software LC Model Process 2
New
PM Processes 3
Pre-development Processes 4
Development Processes 5
Post-development Processes 6
Integral Processes 7
Bibliography
ACRS Comment
Existing
Part A
Part B
New
Part C
Part D
Ref.
Public Comment
Endorsed without exception
Variation (exception and/or addition)
Start
CONCEPT 1
REQUIREMENT 2
DESIGN 3
IMPLEMENTATION 4
TEST 5
INSTALLATION CHECKOUT 6
OPERATIONS/ MAINTENANCE 7
RETIREMENT 8
End

RG 1.173

Developing Software Life-Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants

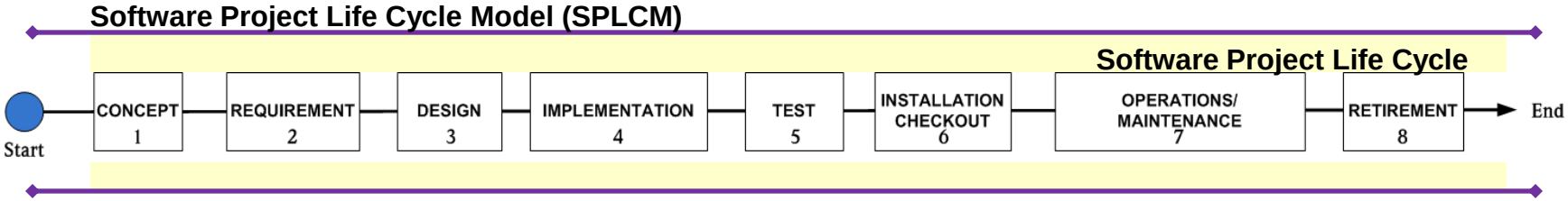
- Background
- Review 6 Regulatory Guides (RGs):
  - RG 1.173 Project Management
  - RG 1.172 Software Requirements Specs
  - RG 1.171 Unit Testing
  - RG 1.170 Test Documentation
  - RG 1.169 Configuration Management
  - RG 1.168 V&V Review Audits
- Conclusion

RG 1.173

Developing Software Life-Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants

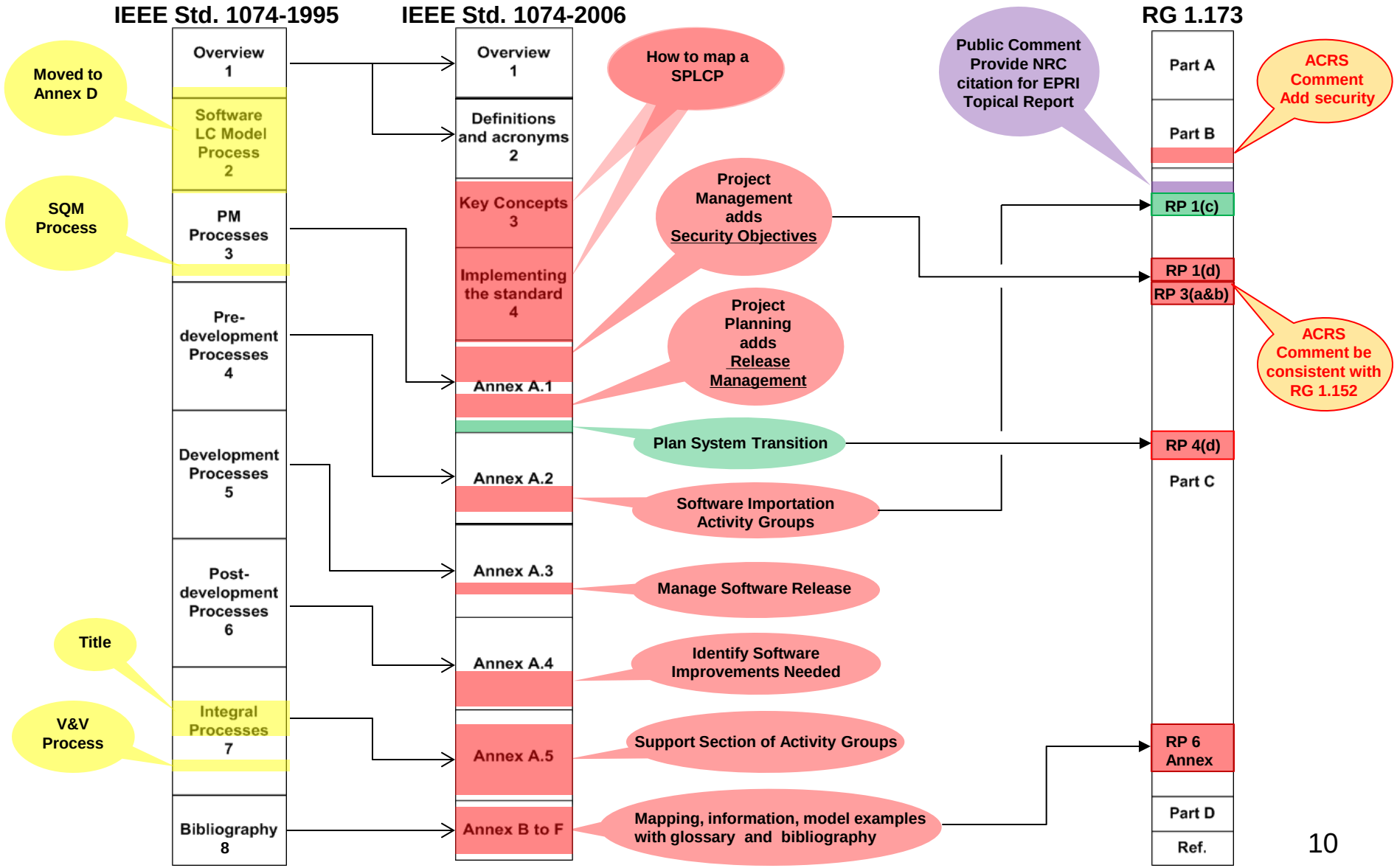
What does this RG do?

- Follows IEEE 1074-2006 directly
- Overview regulatory guidance
- Objective: Create a Software Project Life Cycle Process (SPLCP)
  - Establish requirements
  - Select a Software Project Life Cycle Model (SPLCM)
  - Develop Software Project Life Cycle (SPLC)
  - Establish SPLCP
  - Validate the process



Software Project Life Cycle Process

RG 1.173


IEEE Std. 1074-1995
IEEE Std. 1074-2006
RG 1.173
Overview 1
Software LC Model Process 2
PM Processes 3
Pre-development Processes 4
Development Processes 5
Post-development Processes 6
Integral Processes 7
Bibliography 8
Overview 1
Definitions and acronyms 2
Key Concepts 3
Implementing the standard 4
Annex A.1
Annex A.2
Annex A.3
Annex A.4
Annex A.5
Annex B to F
Part A
Part B
RP 1(c)
RP 1(d)
RP 3(a&b)
RP 4(d)
Part C
RP 6 Annex
Part D
Ref.
Moved to Annex D
SQM Process
Title
V&V Process
How to map a SPLCP
Project Management adds Security Objectives
Project Planning adds Release Management
Plan System Transition
Software Importation Activity Groups
Manage Software Release
Identify Software Improvements Needed
Support Section of Activity Groups
Mapping, information, model examples with glossary and bibliography
Public Comment Provide NRC citation for EPRI Topical Report
ACRS Comment Add security
ACRS Comment be consistent with RG 1.152

RG 1.172

Software Requirement Specifications for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

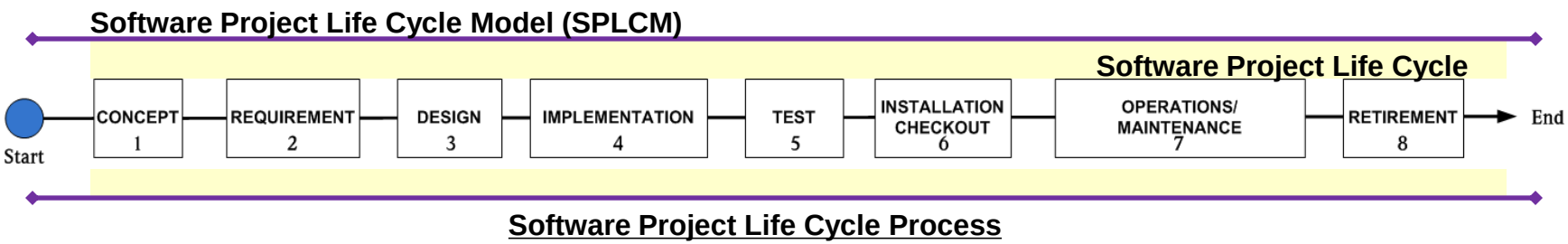
- Background
- Review 6 Regulatory Guides (RGs):
  - RG 1.173 Project Management
  - RG 1.172 Software Requirements Specifications
  - RG 1.171 Unit Testing
  - RG 1.170 Test Documentation
  - RG 1.169 Configuration Management
  - RG 1.168 V&V Review Audits
- Conclusion

RG 1.172

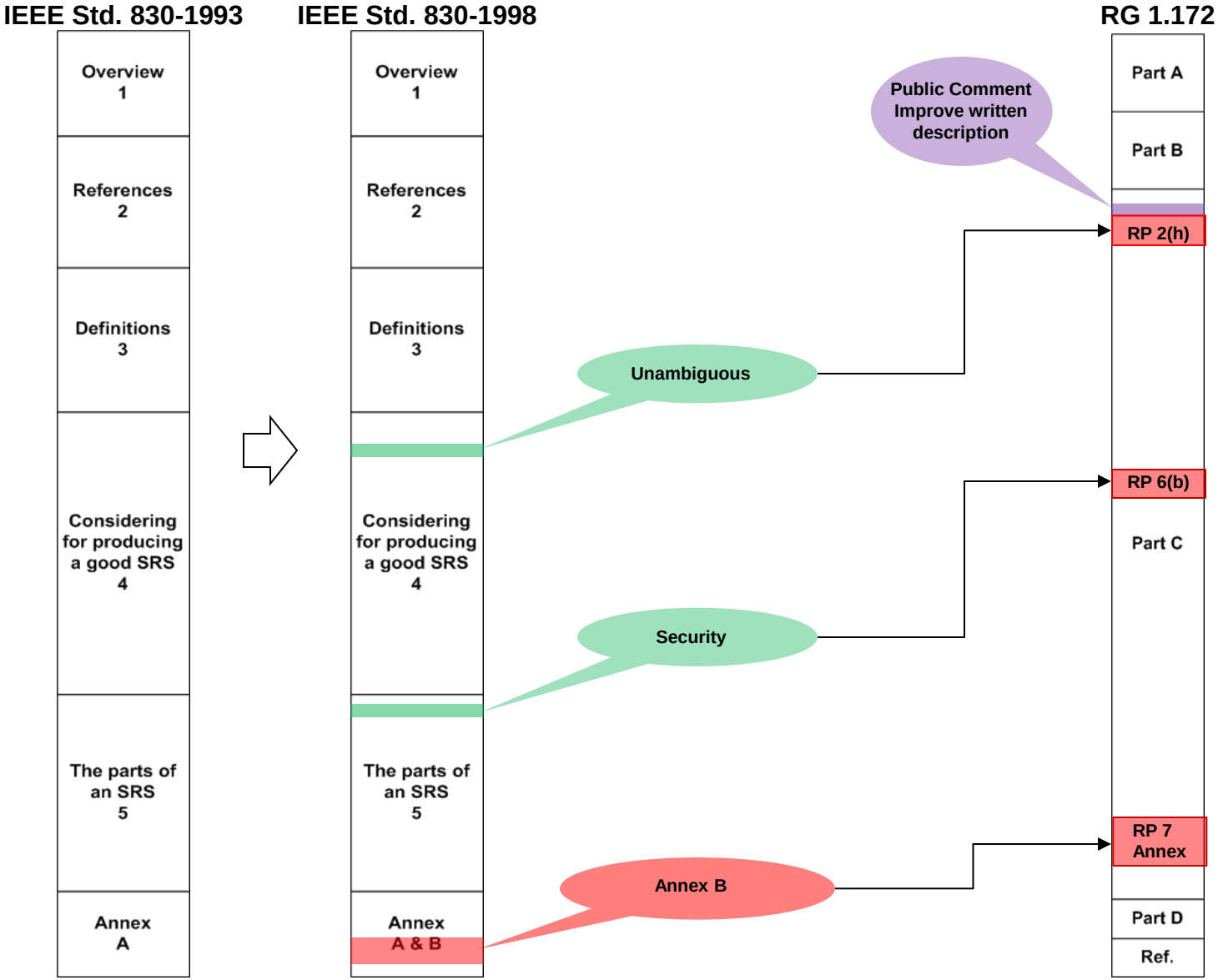
Software Requirement Specifications for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

What does this RG do?

- Follows IEEE 830-1998 directly
- Objective: Create a Software Requirements Specification that delineates the function accurately without added constraints
- Traceability for both original baseline and future development
- Supports the SPLCP



RG 1.172


IEEE Std. 830-1993
IEEE Std. 830-1998
RG 1.172
Overview 1
References 2
Definitions 3
Considering for producing a good SRS 4
The parts of an SRS 5
Annex A
Overview 1
References 2
Definitions 3
Considering for producing a good SRS 4
The parts of an SRS 5
Annex A & B
Public Comment Improve written description
Unambiguous
Security
Annex B
Part A
Part B
RP 2(h)
RP 6(b)
Part C
RP 7 Annex
Part D
Ref.

RG 1.171

Software Unit Testing for Digital Computer Software used in Safety Systems of Nuclear Power Plants

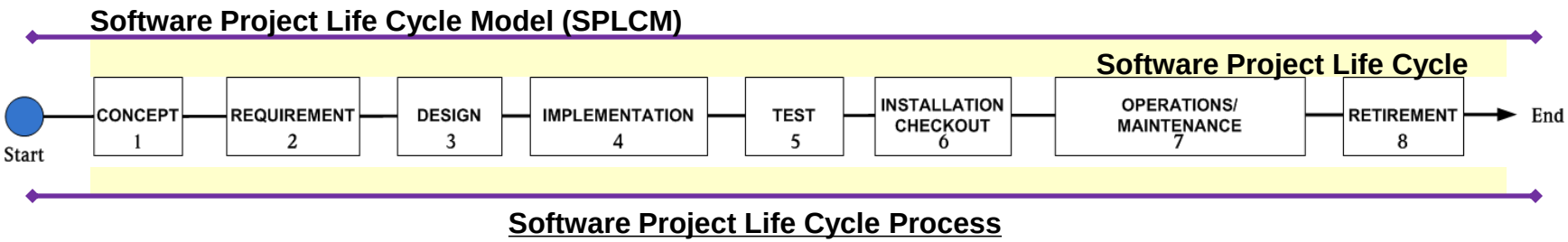
- Background
- Review 6 Regulatory Guides (RGs):
  - RG 1.173 Project Management
  - RG 1.172 Software Requirements Specs
  - RG 1.171 Unit Testing
  - RG 1.170 Test Documentation
  - RG 1.169 Configuration Management
  - RG 1.168 V&V Review Audits
- Conclusion

RG 1.171

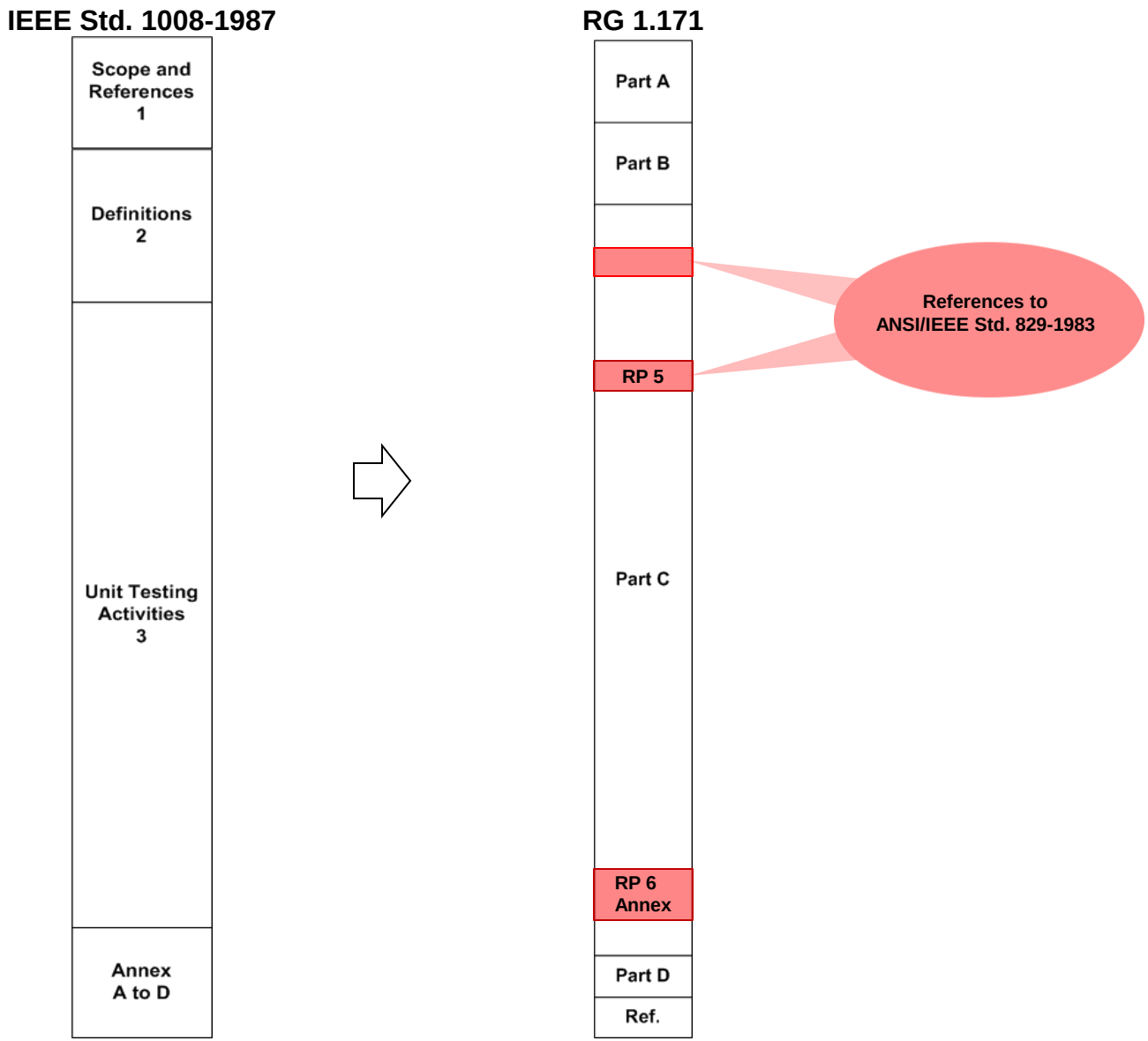
Software Unit Testing for Digital Computer Software used in Safety Systems of Nuclear Power Plants

What does this RG do?

- Follows IEEE 1008-1987 directly
- Objective: Provides emphasis on unit testing for software safety systems
- Smallest piece of software that can be independently tested



RG 1.171


IEEE Std. 1008-1987
Scope and References 1
Definitions 2
Unit Testing Activities 3
Annex A to D
RG 1.171
Part A
Part B
RP 5
Part C
RP 6 Annex
Part D
Ref.
References to ANSI/IEEE Std. 829-1983

RG 1.170

Test Documentation for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

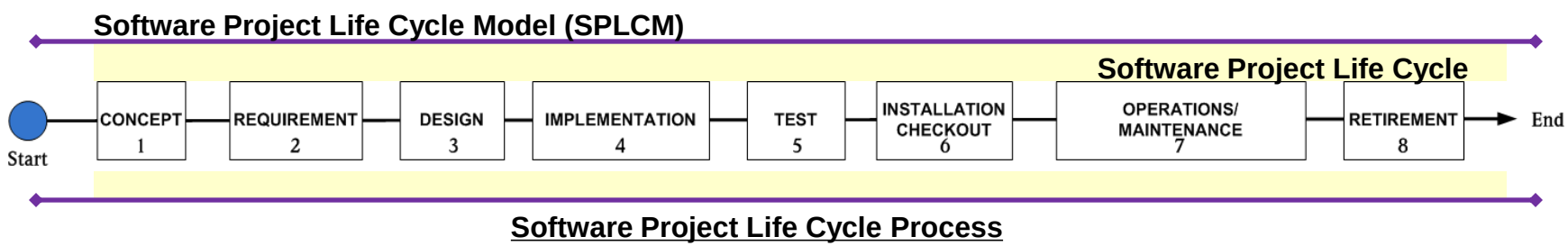
- Background
- Review 6 Regulatory Guides (RGs):
  - RG 1.173 Project Management
  - RG 1.172 Software Requirements Specs
  - RG 1.171 Unit Testing
  - RG 1.170 Test Documentation
  - RG 1.169 Configuration Management
  - RG 1.168 V&V Review Audits
- Conclusion

RG 1.170

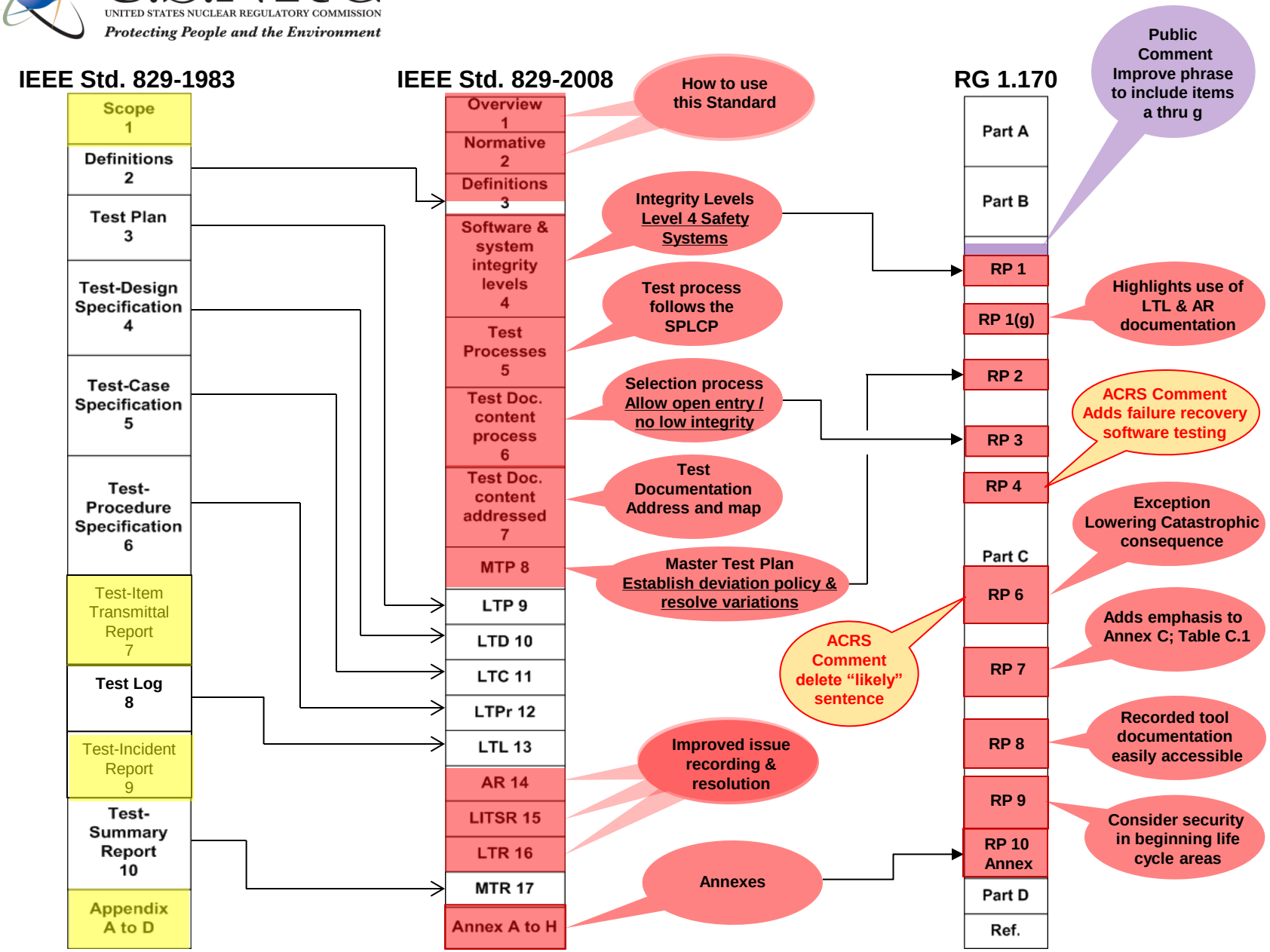
Test Documentation for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

What does this RG do?

- Follows IEEE 829-2008 directly
- Objective: Create a software test plan that methodically documents the software requirements with a reportable demonstration of the unit, component, system and acceptance testing
- Follows a common framework with life cycle processes
- Applies to developing software in the life cycle and/or preexisting or pre-developed software
- Uses Software Integrity Level 4 with traceability, when reporting anomalies



RG 1.170


IEEE Std. 829-1983
Scope 1
Definitions 2
Test Plan 3
Test-Design Specification 4
Test-Case Specification 5
Test-Procedure Specification 6
Test-Item Transmittal Report 7
Test Log 8
Test-Incident Report 9
Test-Summary Report 10
Appendix A to D
IEEE Std. 829-2008
Overview 1
Normative 2
Definitions 3
Software & system integrity levels 4
Test Processes 5
Test Doc. content process 6
Test Doc. content addressed 7
MTP 8
LTP 9
LTD 10
LTC 11
LTPr 12
LTL 13
AR 14
LITSR 15
LTR 16
MTR 17
Annex A to H
How to use this Standard
Integrity Levels Level 4 Safety Systems
Test process follows the SPLCP
Selection process Allow open entry / no low integrity
Test Documentation Address and map
Master Test Plan Establish deviation policy & resolve variations
Improved issue recording & resolution
Annexes
RG 1.170
Part A
Part B
RP 1
RP 1(g)
RP 2
RP 3
RP 4
Part C
RP 6
RP 7
RP 8
RP 9
RP 10 Annex
Part D
Ref.
Public Comment Improve phrase to include items a thru g
Highlights use of LTL & AR documentation
ACRS Comment Adds failure recovery software testing
Exception Lowering Catastrophic consequence
Adds emphasis to Annex C; Table C.1
ACRS Comment delete "likely" sentence
Recorded tool documentation easily accessible
Consider security in beginning life cycle areas

RG 1.169

Configuration Management Plans for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

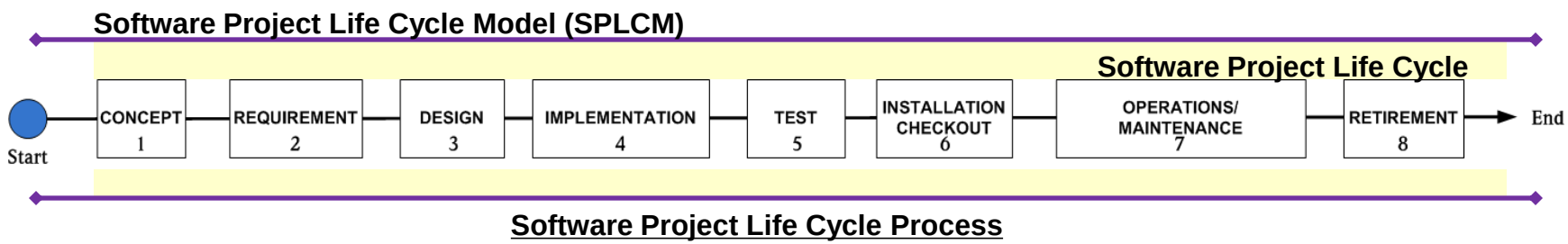
- Background
- Review 6 Regulatory Guides (RGs):
  - RG 1.173 Project Management
  - RG 1.172 Software Requirements Specs
  - RG 1.171 Unit Testing
  - RG 1.170 Test Documentation
  - RG 1.169 Configuration Management
  - RG 1.168 V&V Review Audits
- Conclusion

RG 1.169

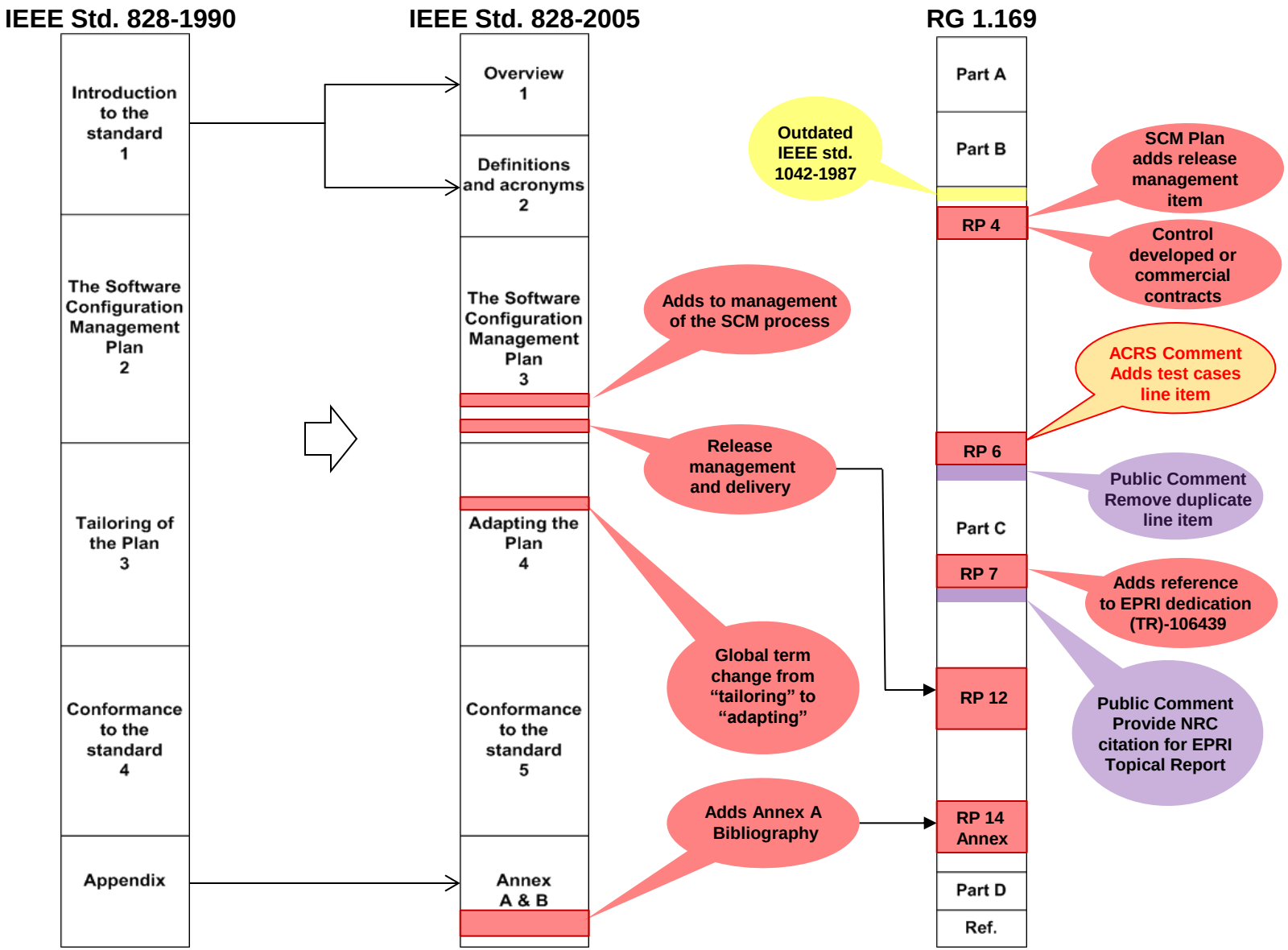
Configuration Management Plans for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

What does this RG do?

- Follows IEEE 828-2005 directly
- Objective: Addresses an integral SPLCP need for Software Configuration Management (SCM) plan with activities for tracking and reporting software safety system history from baseline to final use
- Enables sustainability of software development with release management and delivery
- Monitors and records version iterations and extends this discipline to preexisting software



RG 1.169


IEEE Std. 828-1990
IEEE Std. 828-2005
RG 1.169
Introduction to the standard 1
The Software Configuration Management Plan 2
Tailoring of the Plan 3
Conformance to the standard 4
Appendix
Overview 1
Definitions and acronyms 2
The Software Configuration Management Plan 3
Adapting the Plan 4
Conformance to the standard 5
Annex A & B
Part A
Part B
RP 4
RP 6
Part C
RP 7
RP 12
RP 14 Annex
Part D
Ref.
Outdated IEEE std. 1042-1987
SCM Plan adds release management item
Control developed or commercial contracts
Adds to management of the SCM process
ACRS Comment Adds test cases line item
Release management and delivery
Public Comment Remove duplicate line item
Adds reference to EPRI dedication (TR)-106439
Global term change from "tailoring" to "adapting"
Public Comment Provide NRC citation for EPRI Topical Report
Adds Annex A Bibliography

RG 1.168

Verification, Validation, Reviews, and Audits for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

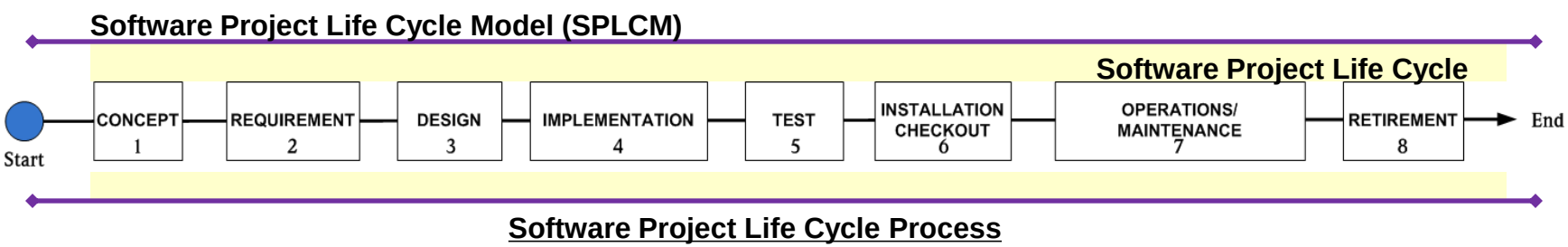
- Background
- Review 6 Regulatory Guides (RGs):
  - RG 1.173 Project Management
  - RG 1.172 Software Requirements Specs
  - RG 1.171 Unit Testing
  - RG 1.170 Test Documentation
  - RG 1.169 Configuration Management
  - RG 1.168 V&V Review Audits
- Conclusion

RG 1.168

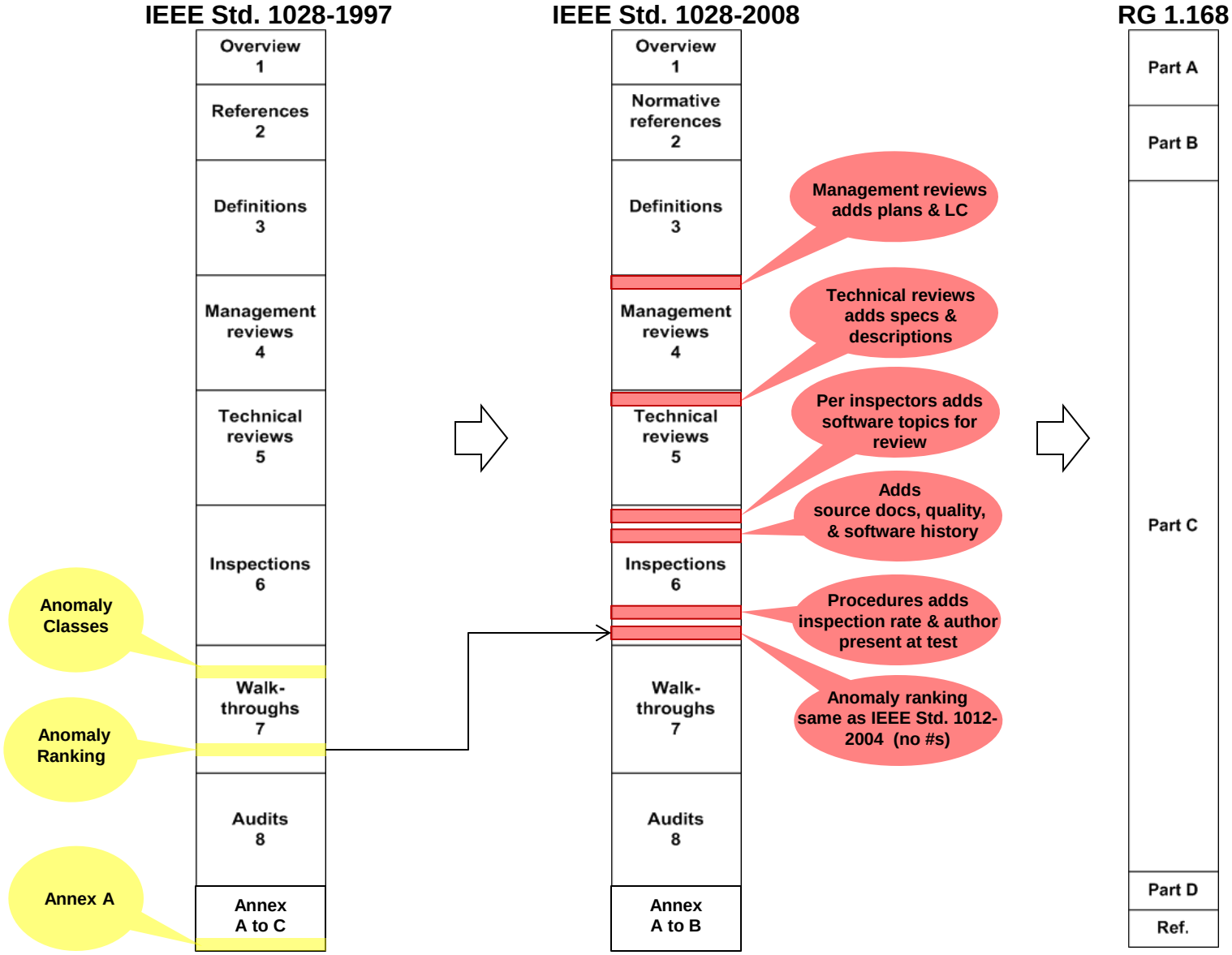
Verification, Validation, Reviews, and Audits for Digital Computer Software and Complex Electronics used in Safety Systems of Nuclear Power Plants

What does this RG do?

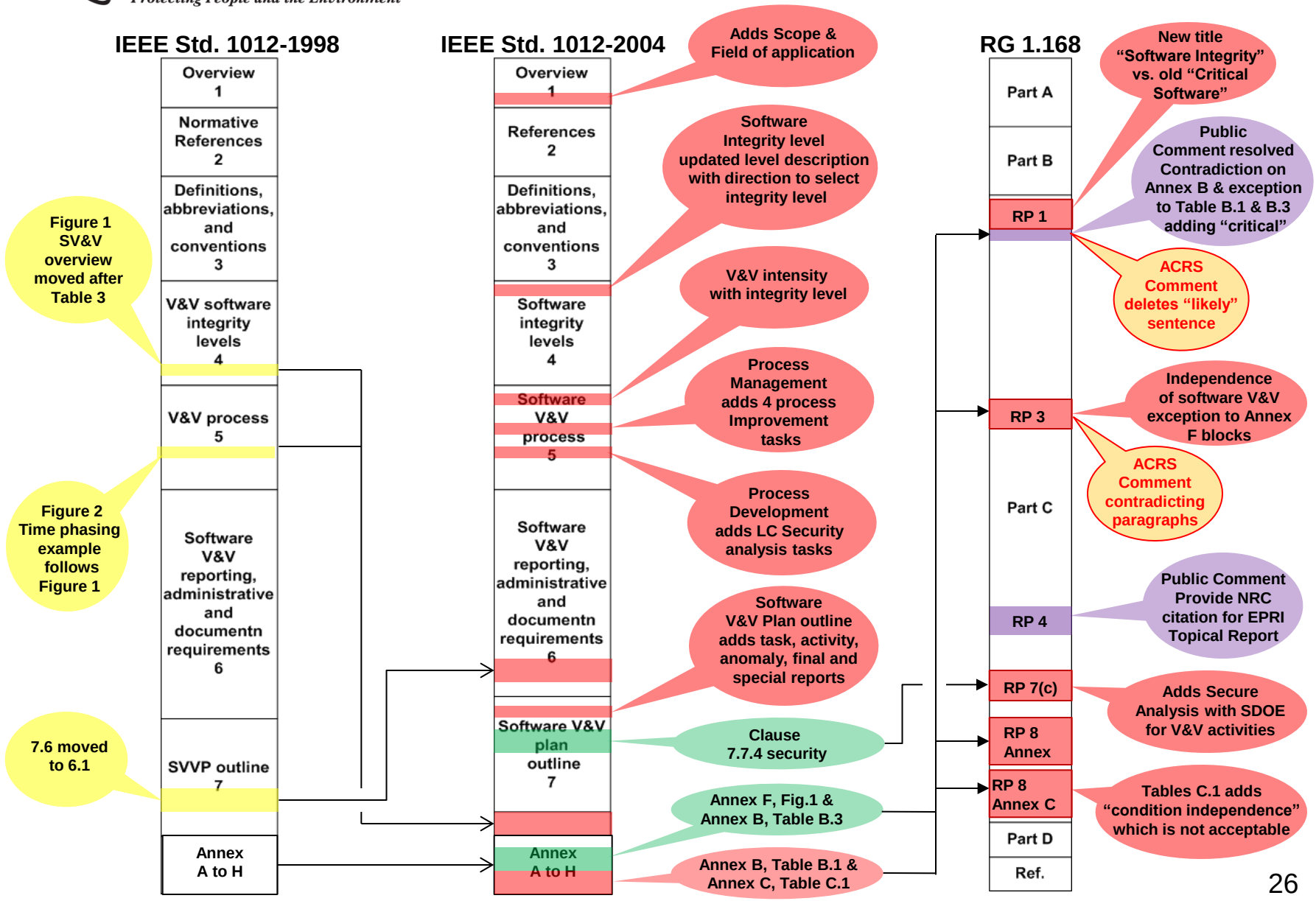
- Follows IEEE 1012-2004 and 1028-2008 directly
- Objectives:
  - Engage in verification and validation plans that follows the SPLCP to ensure objective assessments of software safety systems
  - Provide expectations for inspectors performing walk-throughs, reviews and audits
- Follows a common framework with life cycle processes and integrity level
- Applies to developing software in the life cycle and/or preexisting or pre-developed software



RG 1.168


IEEE Std. 1028-1997
Overview 1
References 2
Definitions 3
Management reviews 4
Technical reviews 5
Inspections 6
Walk-throughs 7
Audits 8
Annex A to C
Anomaly Classes
Anomaly Ranking
Annex A
IEEE Std. 1028-2008
Overview 1
Normative references 2
Definitions 3
Management reviews 4
Technical reviews 5
Inspections 6
Walk-throughs 7
Audits 8
Annex A to B
Management reviews adds plans & LC
Technical reviews adds specs & descriptions
Per inspectors adds software topics for review
Adds source docs, quality, & software history
Procedures adds inspection rate & author present at test
Anomaly ranking same as IEEE Std. 1012-2004 (no #s)
RG 1.168
Part A
Part B
Part C
Part D
Ref.

RG 1.168

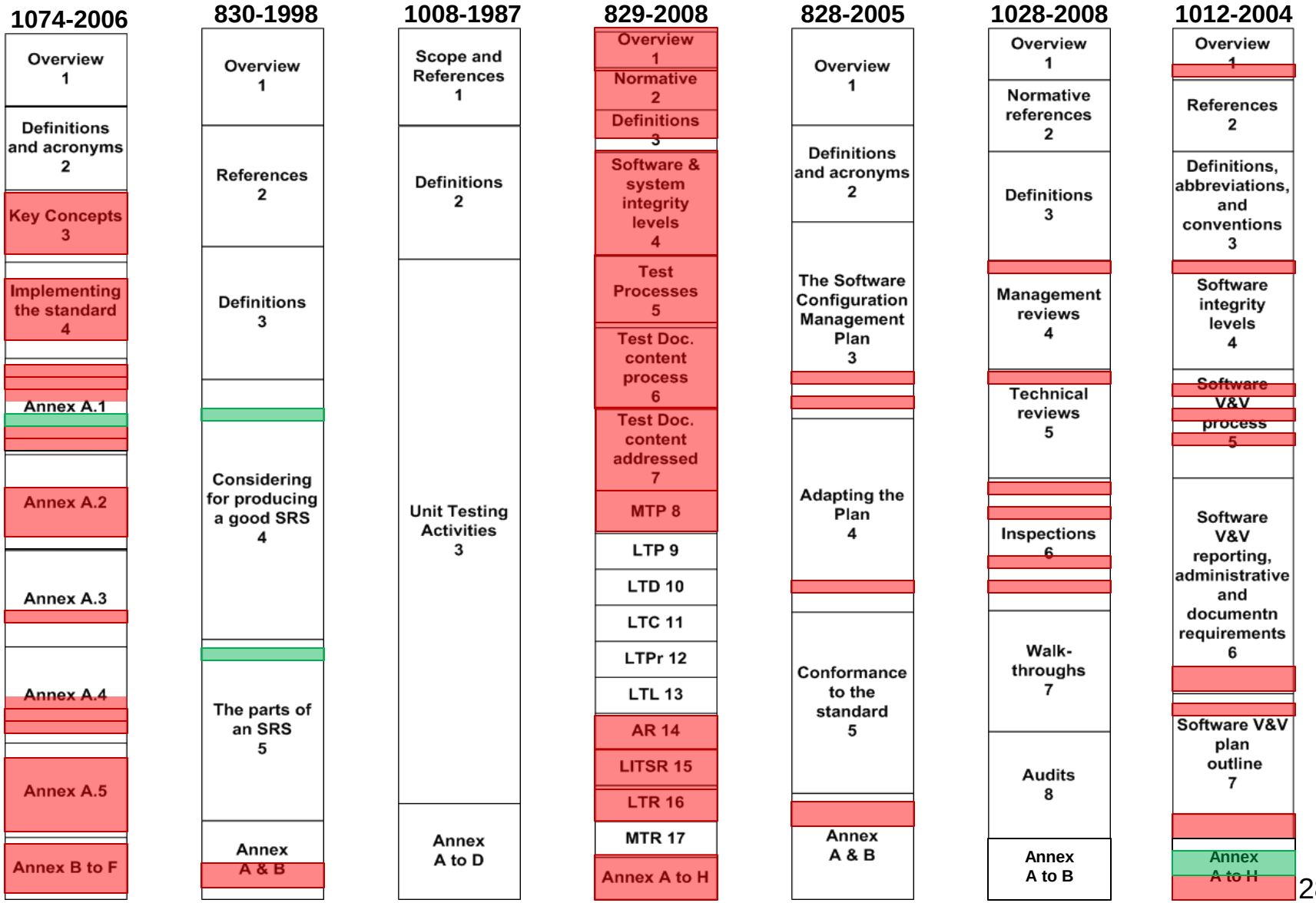

IEEE Std. 1012-1998
Overview 1
Normative References 2
Definitions, abbreviations, and conventions 3
V&V software integrity levels 4
V&V process 5
Software V&V reporting, administrative and documentn requirements 6
SVVP outline 7
Annex A to H
Figure 1 SV&V overview moved after Table 3
Figure 2 Time phasing example follows Figure 1
7.6 moved to 6.1
IEEE Std. 1012-2004
Overview 1
References 2
Definitions, abbreviations, and conventions 3
Software integrity levels 4
Software V&V process 5
Software V&V reporting, administrative and documentn requirements 6
Software V&V plan outline 7
Annex A to H
Adds Scope & Field of application
Software Integrity level updated level description with direction to select integrity level
V&V intensity with integrity level
Process Management adds 4 process Improvement tasks
Process Development adds LC Security analysis tasks
Software V&V Plan outline adds task, activity, anomaly, final and special reports
Clause 7.7.4 security
Annex F, Fig.1 & Annex B, Table B.3
Annex B, Table B.1 & Annex C, Table C.1
RG 1.168
Part A
Part B
RP 1
RP 3
Part C
RP 4
RP 7(c)
RP 8 Annex
RP 8 Annex C
Part D
Ref.
New title "Software Integrity" vs. old "Critical Software"
Public Comment resolved Contradiction on Annex B & exception to Table B.1 & B.3 adding "critical"
ACRS Comment deletes "likely" sentence
Independence of software V&V exception to Annex F blocks
ACRS Comment contradicting paragraphs
Public Comment Provide NRC citation for EPRI Topical Report
Adds Secure Analysis with SDOE for V&V activities
Tables C.1 adds "condition independence" which is not acceptable

Conclusion

- RGs updated
- RGs and IEEE Standards provide cohesive approach
- Common topics contemplated
- Key public comments addressed
- RGs ready for publication

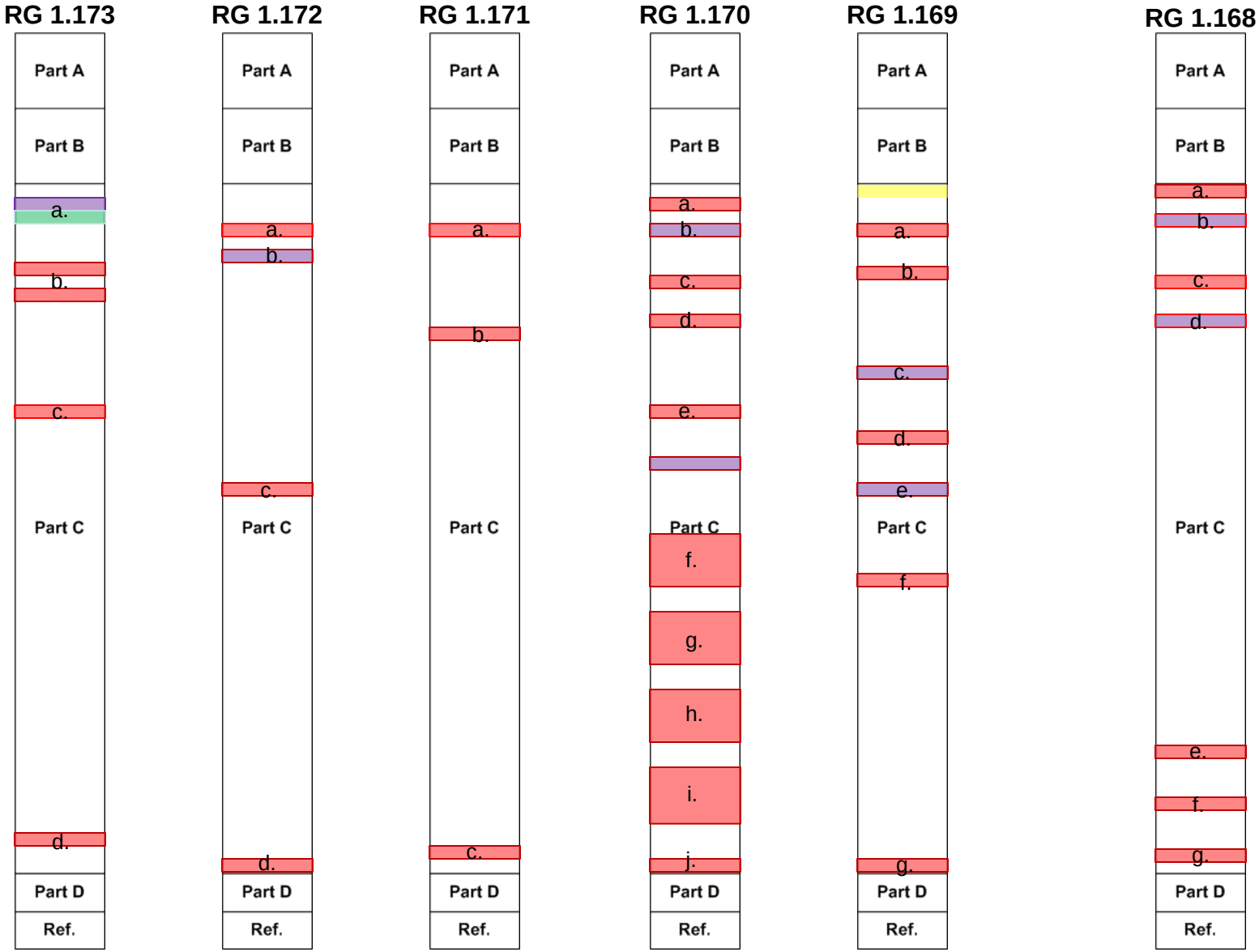
Backup

Change Comparison between Standards



Backup

Change Comparison between Regulatory Guides



Backup

Acronyms

- **ACRS – Advisory Committee on Reactor Safeguards**
- **ADAMS – Agencywide Documents Access and Management System**
- **ANSI – American National Standards Institute**
- **AR – Anomaly Report**
- **CFR – Code of Federal Regulations**
- **DI&C – Digital Instrumentation and Control**
- **eDF – Électricité de France**
- **EPRI – Electric Power Research Institute**
- **IEC – International Electrotechnical Commission**
- **IEEE – Institute of Electrical and Electronics Engineers**
- **RG – Regulatory Guidance**
- **ISG – Interim Staff Guidance**
- **JPL – Jet Propulsion Lab**
- **LC – Life Cycle**
- **LER – Licensee Event Report**
- **LITSR – Level Interim Test Status Report**
- **LTC – Level Test Case**
- **LTD – Level Test Design**
- **LTL – Level Test Log**
- **LTP – Level Test Plan**
- **LTPr – Level Test Procedure**
- **LTR – Level Test Report**
- **MTP – Mast Test Plan**
- **MOU – Memorandum Of Understanding**

Backup

Acronyms (Cont'd)

- **NASA – National Aeronautics and Space Administration**
- **NEA – Nuclear Energy Agency**
- **NRC – U.S. Nuclear Regulatory Commission**
- **NRR – Office of Nuclear Reactor Regulation**
- **NRO – Office of New Reactors**
- **NSIR – Nuclear Security and Incident Response**
- **NPP – Nuclear Power Plant**
- **OpE – Operational Experience**
- **QA – Quality Assurance**
- **RES – Office of Nuclear Regulatory Research**
- **RP – Regulatory Position**
- **SCM – Software Configuration Management**
- **SDOE – Secure Development and Operational Environment**
- **SPLC – Software Project Life Cycle**
- **SPLCP – Software Project Life Cycle Process**
- **SPLCM – Software Project Life Cycle Model**
- **SRM – Staff Requirement Memoranda**
- **SRS – Software Requirements Specification**
- **SwA – Software Assurance**
- **TR – Topical Report**
- **SVVP – Software Verification and Validation Plan**
- **V&V – Verification and Validation**

Backup

References

Beizer, B., Software Testing Techniques, Van Nostrand Reinhold, New York, NY, 1990.

Code of Federal Regulations (CFR), *Title 10, Energy*, Part 50, "Domestic Licensing of Production and Utilization Facilities."

Electric Power Research Institute (EPRI) Topical Report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," EPRI, Palo Alto, CA, October 1996. (ADAMS Accession No. ML092190664)

IEEE Std. 1074-2006, "IEEE Standard for Developing a Software Project Life Cycle Process," IEEE, Piscataway, NJ, 2006.

IEEE Std. 830-1998, "IEEE Recommended Practice for Software Requirements Specifications," IEEE, Piscataway, NJ, 1998.

IEEE Std. 1008-1987, "IEEE Standard for Software Unit of Testing," IEEE, Piscataway, NJ, 1987.

IEEE, Std. 829-2008, "IEEE Standard for Software and System Test Documentation," IEEE, Piscataway, NJ, 2008.

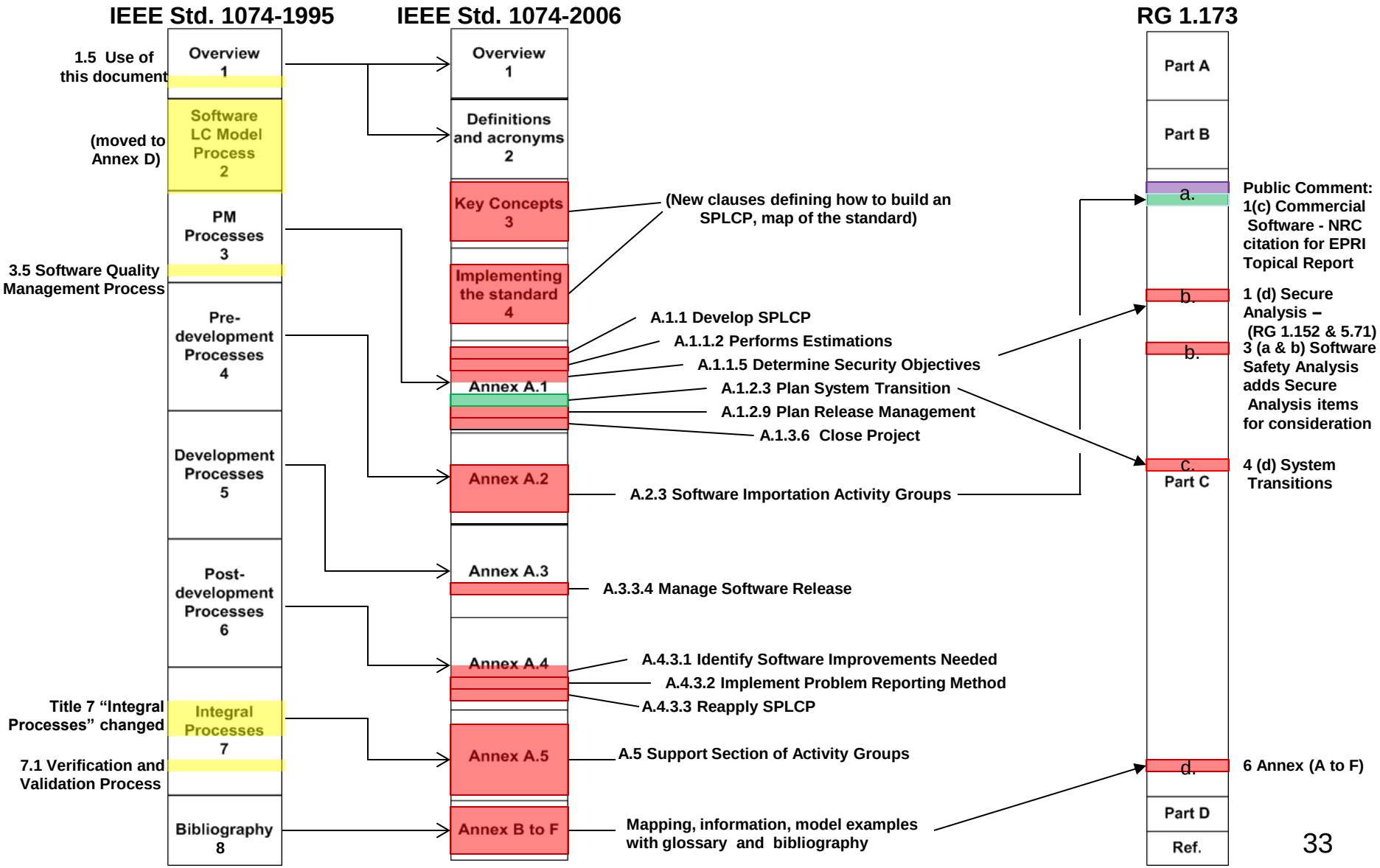
IEEE Std. 828-2005, "IEEE Standard for Software Configuration Management Plans," IEEE, Piscataway, NJ, 2005.

IEEE, Std. 1012-2004, "IEEE Standard for Software Verification and Validation," IEEE, Piscataway, NJ, 2004.

IEEE, Std. 1028-2008, "IEEE Standard for Software Reviews and Audits," IEEE, Piscataway, NJ, 2008.

Backup – RG 1.173

Example from ACRS Subcommittee May 21, 2013



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Station Blackout Mitigation Strategies Rulemaking

Advisory Committee on Reactor Safeguards

Full Committee

June 5, 2013

Purpose

- Discuss with the ACRS full committee the draft regulatory basis for the Station Blackout Mitigation Strategies rulemaking in conjunction with the status of the implementation of EA-12-049 (mitigating strategies order):
  - Basis for moving forward with rulemaking
  - Current thoughts on draft rule concepts (appendix)
- Obtain ACRS feedback to inform our regulatory efforts going forward

Background

- Previously briefed the Regulatory Policy and Practices Subcommittee on December 5, 2012 and on April 23, 2013

- COMSECY-13-0002 (dated 1/25/2013) revised the scope and schedule for the rulemaking recognizing the scope of EA-12-049 and the fact that it is addressing safety issues

- Revised scope and major schedule milestones:
  - Scope includes regulatory actions stemming from NTTF Recommendation 4 and 7
  - SBOMS Regulatory Basis: CA Note to the Commission - 7/8/2013
  - SBOMS Proposed Rule (with guidance): June 30, 2014 to the Commission
  - SBOMS Final Rule (with guidance): December 2016 to the Commission

- Issued SBOMS draft regulatory basis for 45 day comment period
  - Held a public meeting on May 13, 2013
  - Comment period ended May 28, 2013 and currently reviewing comments

Basis for SBOMS Rulemaking

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Mitigating strategies requirements issued in EA-12-049 were issued to a all licensed power reactors

- The Order requirements need to be made generically-applicable

- Current station blackout requirements (sec. 50.63) do not provide for:
  - Station blackouts involving damage to both the onsite and offsite ac power sources from beyond design basis external events (including unavailability of alternate ac power)
  - Site-wide events (i.e., multiple power reactors in a station blackout)
  - Station blackouts that extend indefinitely
  - Spent fuel pool cooling
  - Not applicable in all modes of operation

ELAP Definition

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Conceptually an ELAP definition is an “SBO” that extends indefinitely
- Since this can involve severe external events the ELAP definition would assume that ac power sources (both the 1E sources and the SBO alternate ac source) are not available and can not be readily recovered in the near term
- Specifically the current concept would include:
  - Complete loss of ac power to the essential and nonessential switchgear busses
  - Loss of offsite power that results in a reactor trip and concurrent turbine trip
  - Unavailability and non-recoverability of onsite emergency ac power sources and offsite ac power sources continuing beyond the duration determined by the licensee per sec. 50.63
  - Unavailability and non-recoverability of a sec. 50.63 alternate ac power source (if relied upon to meet sec. 50.63 requirements)
  - ac power is available from inverters fed by safety-related batteries
  - If requirements are put in place by this rulemaking to allow for a “supplemental ac power source” – then this source would be available to restore power
  - Portable mitigating strategies equipment can be used to maintain/restore functions

Mitigating Strategies

- Mitigating strategies requirements would follow an approach similar to EA-12-049:
  - Develop, implement, and maintain guidance and strategies to maintain/restore core cooling, containment, and SFP cooling capabilities
  - Guidance and strategies would be required to be adapted for all modes
  - Equipment would be required to be of sufficient design and capacity considering the nominal conditions expected
  - Mitigating strategies must be required to consider contingencies
  - The strategies would be required to be integrated into existing station blackout procedures
  - The strategies would be required to accommodate the use of offsite assistance and resources including consideration of damage to transportation infrastructure
  - The regulatory framework would integrate with NTTF Recommendation 8 rulemaking requirements

Design Requirements

- Design requirements for equipment:
  - Equipment must be design to perform functions relied upon for ELAP mitigation
  - Portable equipment would be independent of installed SSCs
  - Portable equipment must be designed, stored, and protected to minimize common mode and common cause failure
  - Portable equipment would need to be protected from the effects of beyond design basis external events
  - Portable equipment would be designed, staged, and deployed to minimize potential damage or impairment to installed safety-related equipment
  - There needs to be sufficient sets of portable equipment to enable maintenance and testing
  - Design should enable periodic testing and inspection
  - A test program needs to be established to provide assurance of continued functionality

Supplemental AC Power Source

- Supplemental ac power source is a potential new design flexibility – in concept it would be:
  - Electrically independence from emergency ac power sources
  - Potentially diverse in design from current emergency ac power sources
  - Physically located to minimize common cause failure from external events
  - Capacity and capability to operate equipment necessary to maintain or restore core cooling, containment, and spent fuel pool cooling following a beyond design basis external event, for all units on a site
  - Supply power through physically and electrically separate pathways to multiple distribution systems or motor control centers
  - Designed to for external events to a margin ≥ supplied equipment (at least one train of equipment)
  - Designed to interact with connected SSCs

Additional Concepts

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Change Control
  - Change control appears needed to control the configuration of the strategies, guidance and equipment relied upon over time
  - Current sec. 50.59 would typically not be effective for changes to the strategies, guidance, and equipment
  - The concept: ensure that changes continue to meet the new requirements or otherwise follow the sec. 50.90 amendment process to obtain prior NRC review and approval

- Link with 10 CFR 50.63
  - Mitigation of ELAP is linked into the current plant procedures in the emergency operating procedures (i.e., the station blackout EOP)
  - This links mitigating strategies with current station blackout procedures
  - Linking these requirements (sec. 50.63 and the new sec. 50.xxx) aligns the regulatory framework with implementation
  - Current concept is to amend sec. 50.63 to indicate that if a station blackout exceeds the specified duration (including the failure of an alternate ac power source) then the mitigating strategies are to be implemented

Next Steps

- Staff is currently considering the feedback and revising the regulatory basis accordingly
- We are required to provide a Commissioner Assistants (CA) Note on the regulatory basis in early July
  - We would appreciate ACRS feedback (if practical) to support the CA note
- We plan to proceed forward to proposed rule stage
- We plan to interact with ACRS on the proposed rule (2014) and final rule (2016)