Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title:	Advisory Committee on Reactor Safeguards 588th Meeting: Open Session
Docket Number:	(n/a)
Location:	Rockville, Maryland
Date:	Thursday, November 3, 2011

Work Order No.: NRC-1245 Pages 1-118

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

DISCLAIMER

UNITED STATES NUCLEAR REGULATORY COMMISSION'S

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

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

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

588th Meeting

+ + + + +

OPEN SESSION

+ + + + +

THURSDAY

NOVEMBER 3, 2011

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Committee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B1, 11545 Rockville Pike, at 8:30 a.m., Said Abdel-Khalik, Chairman, presiding.

COMMITTEE MEMBERS PRESENT:

SAID ABDEL-KHALIK, Chairman

J. SAM ARMIJO, Vice Chairman

JOHN STETKAR, Member-at-Large

SANJOY BANERJEE

DENNIS C. BLEY

CHARLES H. BROWN, JR.

MICHAEL CORRADINI

DANA A. POWERS

HAROLD B. RAY

JOY REMPE

MICHAEL T. RYAN

WILLIAM J. SHACK

JOHN D. SIEBER

GORDON R. SKILLMAN

NRC STAFF PRESENT:

PETER WEN, Designated Federal Official

RICH GUZMAN

IAN JUNG

GENE EAGLE

RICHARD STATTEL

PAUL PIERINGER

ALSO PRESENT:

SAM BELCHER

DALE GOODNEY

PHIL AMWAY

GEORGE INCH

PHILIP WENGLOSKI

RICHARD WOOD

I-N-D-E-X

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

8:27 a.m.

CHAIR ABDEL-KHALIK: The meeting will now come to order. This is the first day of the 588th meeting of the Advisory Committee on Reactor Safeguards. During today's meeting the Committee will consider the following. One, Nine Mile Point Unit 2 Extended Power Uprate application.

Two, Branch Technical Position 7-19, Guidance for the Evaluation of Diversity and Defense-in-Depth and Digital Computer Based Instrumentation and Control Systems.

Three, Preparation for Meeting with the Commission. And four, Preparation of ACRS Reports. This meeting is being conducted in accordance with the provisions of the Federal Advisory Committee Act. Mr. Peter Wen is the designated Federal Official for the initial portion of the meeting.

We have received no written comments or requests for time to make oral statements from members of the public regarding today's sessions. There will be a phone bridge-line. To preclude interruption of the meeting the phone will be placed in a listen in mode during the presentations and Committee discussions.

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.

At this point we will move to the first item on the agenda, Nine Mile Point Unit 2 Extended Power Uprate. Dr. Armijo will lead us through that discussion. Sam.

VICE CHAIR ARMIJO: Okay. Thank you Mr. Chairman. Our subcommittee on power uprates reviewed this application on October the 5th of 2011. Nine Mile Point Unit 2 is BWR/5 Mark II containment. And it, I believe, is the BWR/5 to apply for an extended power uprate.

The matters that we reviewed at the subcommittee are similar to the matters we reviewed in the past. There was one new technology that there was some discussion at the subcommittee meeting. It's a proprietary technology related to jet pump mixer coatings. I've asked the applicant and the staff to cover that information.

They have provided us a report at our request. And so they will cover that but that will be in a closed portion of the meeting, closed session.

With that I'd think I'd like to just turn it over to Rich Guzman of NRR to lead us through the presentation.

MR. GUZMAN: Thank you, Mr. Vice Chairman. And thank you, Chairman. Good morning, my name is Rich Guzman, I'm the senior project manager in the Office of NRR, assigned to the Nine Mile Point Nuclear Station. During today's full committee meeting you will hear from both the licensee and the NRC staff in providing you with the details of the EPU application.

The objective is to be able to present it to you in a clear concise way. And to do so we'd like to also present the staff's evaluation supporting our reasonable assurance determination that the proposed EPU will not endanger public health and safety.

Before I cover the agenda items for today's meeting I would like to provide some background information related to the proposed EPU.

On May 27th, 2009, the licensee submitted its License Amendment Request for Nine Mile Point Unit 2 for an EPU which would increase the maximum authorized thermal power limit from 3,467 megawatts thermal to 3,988 megawatts thermal, which represents and increase of approximately 15 percent from the current licensed thermal power.

And approximately 20 percent from its original licensed thermal power. The NRC staff's review effort involved several pre-application meetings with the licensee, starting as early as September 2008. The NRC staff also performed a detailed and extensive acceptance review before initiating its full review of the application.

During the course of the review the staff had frequent communications with the licensee, both public and closed meetings, as well as two staff audits. And numerous conference calls to discuss the EPU application and supplemental responses to several rounds of requests for additional information, or RAIs.

The RAIs covered multiple technical disciplines. Overall there were approximately 27 docketed supplemental responses from Nine Mile Point, which supported the staff's completion of its safety evaluation.

And finally, the staff projects completion of its review by December of 2011, which would support the licensee's scheduled implementation of its EPU which is projected for the second quarter of 2012.

This slide shows the topics for today's discussion. In the interest of time and staying within our two hour time block this morning Nine Mile Point will be taking the lead in presenting these six topics. And the staff will be supporting the dialogue as necessary as it pertains to our safety and technical review.

First the licensee will provide an overview of the proposed EPU, which will include a description of their proposed plant modifications and their power ascension testing.

The anticipated transient without scram and stability. Fuel methods topics will then be covered. And that will be followed by a materials presentation. And these four topics will be in open session, that is the intention.

At the conclusion of those four topics we can then switch to closed session to go over the remaining two items, which would be the steam dryer analysis as well as the open item that Mr. Armijo had mentioned and the jet pump mixer coating. And with that that concludes my presentation.

I would like to also mention on behalf of the Division Director, Michelle Evans, as well as Louise Lund, our Deputy Director in the Division of Operating Reactor Licensing, who is here today, and as well as the NRR staff members involved in this review we'd like to say a special thanks to the ACRS staff who helped in the preparation for the subcommittee and this full committee meeting. Particularly Mr. Peter Wen.

And I'm going to now turn over to Mr. Sam Belcher who will provide the opening remarks as well as a overview of the proposed EPU. He is the Senior Vice President for Site Operations at Constellation.

MR. BELCHER: As Rich mentioned I am Sam Belcher, the Senior VP of Site Operations for Constellation Energy Nuclear Group. I'll go through a brief overview and then turn it over to my staff for a more in-depth discussion on a number of topics.

Dale Goodney is the lead engineer on the project. Dale will walk us through plant modifications required for the extended power upgrade. Phil Amway is a senior reactor operator on the project and he will take us through discussion on power ascension testing as well as the anticipating transient without scram and stability methods discussion.

Phil Wengloski will talk us through our fuel methods discussion and then George Inch will take us through our materials, mechanical/civil discussion as well as the two closed session that were mentioned earlier regarding steam dryer as well as the jet pump inlet mixers.

As has been previously mentioned it is a BWR/5 technology with the Mark II containment. We are proposing a 15 percent power increase above existing current licensed power, but an overall 20 percent increase from the original licensed power that the plant was originally constructed to.

It is a constant pressure power uprate and there is no credit being taken for Containment Accident Pressure for ECCS suction pressure. As well as no new fuel introduction as a part of this. The core is currently all GE 14 fuel and will remain GE 14 fuel for the power upgrade cycle.

Also the alternative source term for the accidental radiological consequences was previously implemented using the EPU power level as the base assumption for that submittal. Nine Mile Point Unit 2 has implemented MELLLA as well as the New York State ISO has already received and approved the uprated power condition with no grid modifications necessary.

So at this point I will turn it over to Dale Goodney to walk us a through a discussion on plant modifications.

MR. GOODNEY: Thank you, Sam. As

mentioned earlier I'm Dale Goodney. I'm the lead engineer for the EPU project. And ths will be an overview of plant modifications related to the Nine Mile Point extended power uprate.

The balance of plant systems effected by the uprate were analyzed in accordance with the generic methodology outlined in the constant pressure power uprate Licensing Topical Report. This analysis included an assessment of the impact on design and operating margins at EPU conditions to identify modifications needed to support he uprate.

Based on these reviews over 20 modifications are identified and are described in the License Amendment Request. The primary objective of these modifications are to recover design and operating margins at EPU conditions. Restore material condition. And install instrumentation to support the engineering analysis as well the power ascension testing.

At Slide 3 we show the basic plant process parameters that changed due to the uprate. It compares the EPU to current licensed thermal power. As mentioned earlier, this is a 15 percent increase in core thermal power. In addition this will result in a 17 percent increase in nominal steam flow and feedwater flow. And 158 megawatt electric increase in generator output.

Slide 4 is the installation time line, this table lists the modifications that are described in detail in the License Amendment Request. Modifications in the two left-hand columns have been installed and the remaining modifications will be installed before startup in the 2012 refueling outage scheduled to begin next April.

Most of these modifications shown here directly support the increase in feedwater flow, steam flow and electrical output of the station. And I'd like to highlight some of the modifications on the next slide.

The feedwater system flow capacity is being increased by upgrading the existing feedwater pumps. This was accomplished by replacing the rotating elements and the step-up gears. In addition the heater drain pumps and motors were replaced in 2010 with higher capacity pumps to support the uprate.

In terms of steam path upgrades the high pressure turbine will be replaced to achieve higher steam flows. The six cross-around relief valves located on the piping between the high-pressure and the low-pressure turbines will be replaced with new valves to increase the steam relieving capacity.

Heat exchanger rerates include the moisture separated reheaters and the high pressure feedwater heaters. In addition the steam dryer will be modified to provide additional design margin at the higher steam flows. And we'll be providing additional details relative to the steam dryer modifications during the closed session.

MEMBER BANERJEE: Were there any other modifications between the steam dryer and the high-pressure turbines, in the piping?

MR. GOODNEY: With regard to the steam path?

MEMBER BANERJEE: Yes.

MR. GOODNEY: Well, as I indicated the --

MEMBER BANERJEE: So in the, yes you indicated between the high-pressure and the other stages. But in the piping itself? Does it go into the high-pressure?

MR. GOODNEY: No, physical plant modifications included just the high-pressure turbine. Thank you. There are two electrical modifications needed to support the increase in generator output. First of all the isolated phase bus between the main generator and the step-up transformers will be upgraded by installing a higher capacity plume system.

And in addition the coolers on the main transformers are being replaced with larger coolers to provide additional thermal margin to offset the higher loading under EPU conditions. Tech-spec related instruments affected by the power uprate include the APRM flow-biased scram and the main steam high-flow isolation.

New tech-spec allowable values for those two functions will be implemented as part of the EPU License Amendment. Also the balance of plant instruments affected by the uprate will be rescaled as required to accommodate the higher flows, pressures and temperatures at the uprated conditions.

Slide 6 covers the --

CHAIR ABDEL-KHALIK: The feedwater reg valves are not going to changed at all?

MR. GOODNEY: Excuse me?

CHAIR ABDEL-KHALIK: The feedwater reg valves?

MR. GOODNEY: The feedwater reg valves. We are upgrading the feedwater flow control valves with a new trim to provide additional, optimize the controllability and provide, you know, accommodate the additional flow.

CHAIR ABDEL-KHALIK: How far are you from fully open and when they are modified how far will they be from fully open?

MR. GOODNEY: Okay, Phil, can you address this? Thank you.

MR. AMWAY: Good morning, my name is Phil Amway. I am the operations lead for extended power uprate. Currently the valve positions, we normally have two feedwater pumps in service. Each one has their own feedwater reg valve and LV-10. And those valve positions right now are at about 48 percent open at 100 percent power.

With the new valve trim changes that we're doing we should expect a similar response to the valve in terms of where that valve position will be at extended power uprate.

CHAIR ABDEL-KHALIK: Forty-eight percent, is that typical for the industry?

VICE CHAIR ARMIJO: Yes.

MEMBER SIEBER: The real issue with those valves was electric turbine pumps tends to be flow control at low power levels. And that's where a lot of trim adjustments are made so that a little bit of valve movement does not give a large increase in flow. And so you try to get it as sort of a V-shape curve.

I presume that's the purpose of your modification.

MR. INCH: Yes, we redesigned the trim. My name is George Inch, I'm the principal engineer from mechanical. The trim was redesigned to maintain the flow gain on the system the same. So the full-open characteristics, C-V characteristics, were increased and then the trim adjusted to maintain the flow control characteristics the same as it was. And to be able to achieve the flow, rated power condition at the same point.

There's a small change in the first 15 percent open, there's a small slope change there, but that's in the start-up range.

MEMBER SIEBER: Yes, the ideal situation is to have valve position literally proportional to feedwater flow, which is what I think you're trying to do.

MR. INCH: Yes, we have maintained that.

CHAIR ABDEL-KHALIK: So if the valve were to fail fully open, what would be the increase in feedwater flow?

MR. INCH: The feed pumps are sized for approximately that the run out condition, that's around 115 percent for the run out scenario where, it's usually called the feedwater control to failure, which sets the minimum critical power ratio limits for the reload. And that assumes both valves go to full open conditions.

CHAIR ABDEL-KHALIK: Okay.

MEMBER SKILLMAN: I'm Dick Skillman and would like to ask a question, please, to Dale. In your list of modifications and in your explanation, the modifications really focus on secondary plant feedwater, drain pumps --

MR. GOODNEY: Primarily pumps, and plant, correct.

MEMBER SKILLMAN: -- bust up cooling, transformer cooling. Where have you addressed necessary changes in all of the systems that are required for decay heat removal. You've bumped this plant four percent and then 15, you're up 20 from your original design.

And my curiosity is what is your approach is decay generation rates that are accompanying this very large power increase?

MR. GOODNEY: Right. I understand you're asking where we analyzed or accommodated the additional decay heat removal required due to power upgrade.

MEMBER SKILLMAN: That is in the core, in the spent fuel pool. Anywhere the fuel is you've got an abundantly greater heat load.

MR. GOODNEY: Right. We did, again this uprate was analyzed in accordance with the LTR for constant pressure power uprates and that provided a generic methodology for evaluating those types of impacts. We did perform a series of technical evaluations that looked at the effected increase in decay heat removals.

And those are summarized in the License Amendment Request. And George could probably provide additional details to the specific changes and how those were accommodated. But, as I said, there were not physical modifications required as a result of those evaluations.

MEMBER SKILLMAN: Thank you. Thanks.

MR. GOODNEY: Ready to continue? Okay. So we're back on Slide 6, which shows other plant improvements. In addition to the EPU modifications described earlier, the station has implemented, or is planning to implement prior to the uprate, a number of other plant improvements to restore margin, improve equipment reliability and reduce risk.

Some examples include the 3rd Point Feedwater Heaters, which were replaced in 2010 to restore material condition. The standby liquid control system was upgraded to a higher pressure. And the relief valve set-point was raised. This provided additional margin between the pump discharge pressure and the relief valve set point.

Cooling tower upgrades are being implemented to optimize tower performance. In addition the station has also implemented several PRA related risk reduction improvements consisting of procedure changes and other plant modifications.

The feedwater pump seals are being upgraded in 2012, in conjunction with the feedwater pump upgrades I mentioned earlier. And all 20 jet pump inlet mixers will be replaced during the 2012 refueling outage to address inlet mixer fouling and restore the performance of the jet pumps to original design.

As mentioned earlier, as requested by the ACRS subcommittee, we will be providing additional information regarding the jet pump inlet mixer anti-fouling coating, that will be presented later in the closed session.

We also provided a detailed report on the coating process to the ACRS subcommittee in a separate submittal prior to this meeting. The main reason we're installing the jet pump mixers is to recover core flow operating margin. And to illustrate the effects that the new mixers have on core flow capability I'd like to turn this over to Phil Amway.

MR. AMWAY: Thank you, Dale.

VICE CHAIR ARMIJO: Before you go there, just one quick question. On the modifications to the steam dryer. When will those be completed, is that going to be in April of next year?

MR. GOODNEY: Yes, those will be during the 2012 refueling outages in April.

VICE CHAIR ARMIJO: Okay. I'll defer any further questions to the steam dryer.

MR. GOODNEY: Okay.

MR. AMWAY: Good morning. My name is Phil Amway and I am the operations lead for ascension power uprate. Before we get into the startup test program I'm going to lead off with a discussion of the plant's power flow operating map.

This first slide here is really just to show you the entire map. The region of interest for extended power uprate is in the upper-right corner. So the following slide shows that region that we want to talk about this morning.

The 87 percent line along the left axis

represents our current operating state, 100 percent of current licensed thermal power. And it shows our flow window between 80 percent and 105 percent core flow. If we were not going to replace the jet pump inlet mixers our maximum estimated core flow was 99 percent.

And, as Joel was showing with the mouse up there, that puts us with a single operating point at the 100 percent EPU power level at 99 percent core flow. That would be sufficient for periods of time if we wanted to come up in power and do our power ascension testing.

But it doesn't give any core flow window for the operators to effectively maintain 100 percent power operations with a normal cycle reactivity variations at the core throughout the site to length.

And that is why we made a decision to replace the jet pump inlet mixers is to restore that core flow margin. We anticipate through our analysis that that would regain a five percent core flow margin at 100 percent EPU, which is sufficient to operate the entire cycle at EPU conditions.

In our power ascension testing program the preparation, we have several test objectives. And those are to satisfy equipment performance that meets the design requirements and to ensure that we have a careful monitored approach to extended power uprate power levels. And we also want to make sure that we meet all established requirements.

We have defined roles and responsibilities and included that in our startup test program in the forms of procedure. And we have also included a number of industry benchmarking activities for plants that have already implemented EPU to make sure that our startup test program is consistent with other plants that have already done so.

We are currently working on our test procedure development. And our test plans have been established. And before we actually implement the test procedures we will make sure that the operators and technical staff are trained on those procedures prior to implementation.

In terms of schedule, we will ascend to the EPU power level in one percent intervals and we will perform data collection at each of those one percent intervals. At two and half percent intervals we will collect and evaluate data. And then our major testing plateaus occur every five percent.

During those five percent power intervals we will perform a combination of passive data collective and active control system stability dynamic testing. Those active control system dynamic tests include pressure regulator step testing and feedwater level control step testing.

As completion of the active and passive testing, data collection, we'll analyze that data. Review it by our Plant Operations Review Committee and forward that on to the NRC staff for review.

The next slide shows a pictorial analysis of all the testing that's required along the left column and the various power levels at which we'll perform that testing where Xs in the boxes show what tests are performed. And you can see some of those are repetitive at the various power levels.

The red shading across the top indicates those test plateaus where we will be forwarding test data reports to the NRC for review. Those highlighted in blue shading across the bottom indicate those tests, which is really just the data collection, that's done every one percent interval.

Moving on to the next topic, the long-term stability solution, Option III and ATWS stability events. Nine Mile Point Unit 2 installed and armed the NUMAC PRN OPRM system as an active RPS trip function in the year 2000. And it was done under Tech Spec Amendment 92.

In 2002, we implemented a plant-specific DIVOM curve to address the concerns of GE Safety Communication 01-01. And in 2003 we made additional changes to the filter frequency and period tolerance settings to address Safety Communication 03-20.

The effects of extended power uprate on a long-term stability solution includes no methods changes for extended power uprate. The maximum rod line remains the same, and that is the MELLLA boundary.

The OPRM arm region maintains the same level of stability protection. That was done by changing the Tech Spec Requirements from 30 percent. In which we armed the system at CLTP down to 26 percent, which is the same equivalent megawatt thermal value, so it provides that same level of protection.

We developed cycle-specific sub-point analysis to capture core design variations. And we are maintaining the Option III Long-Term Stability Solution, which is the period based detection algorithm.

The Option III OPRM set-points are developed based on plant-specific DIVOM curves for the EPU cycle-specific reload analysis.

Moving on to the ATWS mitigation design

features. Unit 2 has a redundant reactivity control system, which is designed to mitigate at loss events. That system is largely automated in terms of it is actuated on RPV high pressure.

And the immediate response of that system is to independently try to insert control rods using the Alternate Rod Insertion. And to perform an Automatic Reactor Recirculation Pump trip to slow speed.

The system allows those first two immediate responses to effect a reactor shutdown. If that is unsuccessful, after time delays, it will initiate an automatic feedwater runback, a trip of the reactor recirculation pumps to off.

And then, after a further time delay, if those actions are unsuccessful in bringing the plant to hot shutdown, we receive an automatic boron injection.

The effects of extended power uprate on ATWS mitigation strategies. NRR conducted a staff audit at Nine Mile 2 in 2009. And that audit confirmed that our existing procedures, operator action times and strategies are effective at mitigating ATWS and at loss instability transients.

The design feature of an automatic recirc pump trip results in a transient power level that's primarily based on the maximum control rod line, which is unchanged for extended power uprate. The automatic feedwater runback rapidly and effectively dampens thermohydraulic instability during the ATWS transient.

And again, we confirmed through the simulator demonstrations that operators can perform actions in a timely manner to bring the plant to safe shutdown.

MEMBER STETKAR: Phil, looking at your previous slide a lot of the ATWS responses are now automated, or all automated, what in particular operator actions does that last bullet on your Slide 22 pertain to?

MR. AMWAY: The operator actions primarily are one, to confirm that the redundant reactivity control system has indeed actuated as designed. And to confirm that the boron injection time occurs at the appropriate time.

Once those initial actions are done then we proceed on to our level control strategy and the automatic feedwater runback terminates high pressure feedwater injection. However, the operators have to take action to manually control feedwater to maintain RPV water level in the desired band after the runback is completed.

MEMBER STETKAR: Okay. Thank you.

MR. AMWAY: You're welcome.

MR. WENGLOSKI: Good morning. My name is Philip Wengloski, I'm the general supervisor for nuclear field services for Constellation Energy Nuclear Group. This morning I'll spend a few minutes talking about the fuel design and fuel methods utilized for the Unit 2 power uprate.

On my first slide you heard Sam mention earlier that we use GE14 fuel, we have a full core of GE14 fuel that was introduced in 2004. We only are using GE fuel types through EPU implementation. In particular they have Pellet Clad Interaction or the Barrier Liner Cladding and an integrated debris filter feature.

We don't have any test assemblies, test rods, lead use channels in Unit 2 core. The energy requirements for EPU have been met by changes to the bundle enrichments, bundle loadings and bundle loading patterns. Just as a figure of merit, prior to EPU we utilized batch advents enrichments of about 4.18 weight percent and 276 feed assemblies.

For the power uprate safe analysis report, 4.21 weight percent and 552 feed assemblies. And a cycle 14 which will start up in the spring of 2012. The first EPU cycle 4.23 weight percent and 332 feed assemblies. Of course as you make the --

CHAIR ABDEL-KHALIK: The middle number that you gave is 552?

MR. WENGLOSKI: Five hundred and fifty-two was used in the PUSAR, that's correct.

CHAIR ABDEL-KHALIK: In the what?

MR. WENGLOSKI: In the PUSAR, in the power uprate submittal.

CHAIR ABDEL-KHALIK: Okay. And the actual number of feed assemblies in the upcoming --

MR. WENGLOSKI: The actual number for the upcoming cycle is 332. So 20 feed assemblies less than what was analyzed as part of the equilibrium study.

MEMBER SIEBER: That's a pretty conservative fuel management strategy.

MR. WENGLOSKI: That's correct.

MEMBER SIEBER: In my opinion.

MR. WENGLOSKI: That's correct. I was just going to mention the core to zone limits that we use for Nine Mile Unit 2, with respect for design for minimum critical power ration, minimum heat generation rate we're maintaining the same margins pre-EPU to post-EPU and they're very conservative.

MEMBER SIEBER: Well it causes a greater balancing of enrichments across the core and therefore reactivity, because you are changing out a fairly large batch size with just a modest enrichment.

MR. WENGLOSKI: That's correct.

VICE CHAIR ARMIJO: Now, at EPU you're peak linear heat generation rate is going to be 12 kilowatts per foot?

MR. WENGLOSKI: Correct.

VICE CHAIR ARMIJO: Now, most BWRs operate at 13.4, has Nine Mile 2 been operating at 12 or 13.4 in their prior cycles?

MR. WENGLOSKI: It's been closer to 12.

VICE CHAIR ARMIJO: It has?

MR. WENGLOSKI: Yes, it has. We've been fairly conservative in our field management strategies.

VICE CHAIR ARMIJO: Okay. And so you basically distributed that extra power more uniformly throughout the core?

MR. WENGLOSKI: That's correct.

VICE CHAIR ARMIJO: In this design?

MR. WENGLOSKI: That's correct.

VICE CHAIR ARMIJO: Okay.

MEMBER SIEBER: I would say the bulk of your discharged fuel is twice burned.

MR. WENGLOSKI: For the EPU cycles?

MEMBER SIEBER: Yes.

MR. WENGLOSKI: That's correct. We'll have fairly large batch fraction that will be part of the feed assemblies.

MEMBER SIEBER: Okay.

VICE CHAIR ARMIJO: And your peak noble burn up, what will that be?

MR. WENGLOSKI: The peak noble exposure that we have for the EPU was around 52 gigawatt days for a short time.

MEMBER SIEBER: That's the thrice-burned assembly, right?

MR. WENGLOSKI: That's correct.

VICE CHAIR ARMIJO: Fifty-two --

MR. WENGLOSKI: That's correct, yes.

MEMBER SIEBER: Does that impact your fuel storage capability? Spent fuel storage capability?

MR. WENGLOSKI: For wet or for dry storage?

MEMBER SIEBER: Yes, the wet. Obviously this strategy is going to fill up your spent fuel pool faster.

MR. WENGLOSKI: Right.

MEMBER SIEBER: And force you into probably on-site storage outside the spent fuel pool, correct?

MR. WENGLOSKI: That's correct. The dry storage will be initiated at Nine Mile next year. And the additional loadings have been factored into that strategy to maintain full-core offload.

MEMBER SIEBER: How fast, how many assemblies per refueling would you expect you would need to move to dry cast storage per refueling cycle?

MR. WENGLOSKI: Well, for a full-core, to maintain full-core offload we need to balance obviously the 332 that come in. So 61 assemblies per dry storage can, we can do the math. And we would have to do those every two years to make sure we maintain a full core offload.

MEMBER SIEBER: Doesn't sound like you have a lot of margin right now. As far as empty space.

MR. WENGLOSKI: Both units, that is correct, both units do not have a lot of margin for full-core offload.

MEMBER SIEBER: Thank you.

MR. WENGLOSKI: I mentioned changes to

power distribution. Next presentation by George Inch will talk about how fluence changes in reactor vessel have been addressed in EPU.

CHAIR ABDEL-KHALIK: Did you just say that both units don't have much margin for a full-core offload? Are you required to do full-core offload for one unit?

MR. WENGLOSKI: This spring will a full-core offload for Unit 2 and we'll be able to obviously discharge the entire batch to the spent fuel pool.

CHAIR ABDEL-KHALIK: Okay. Would you be able to do a full-core offload while the other unit is in a refueling --

MR. WENGLOSKI: They're separate units.

CHAIR ABDEL-KHALIK: So they have separate pools?

MR. WENGLOSKI: They have separate pools, that's correct.

CHAIR ABDEL-KHALIK: All right.

MR. AMWAY: If I could add a clarification. Again, my name is Phil Amway. We plan to maintain a strategy such that we would maintain full-core offload capability at each unit.

CHAIR ABDEL-KHALIK: Okay.

MEMBER SIEBER: Aren't you required to do that? I mean you could end up getting stuck?

MR. AMWAY: That's correct. That's discussed in our safety analysis.

MEMBER SIEBER: If you have to do something with reactor internals you're finished.

MR. AMWAY: That's right.

MEMBER SIEBER: If you don't take that strategy.

MR. WENGLOSKI: With respect to methods. We utilized only NRC approved methods to do the core design and safe analysis. In particular the Topical Report on Applicability of the GE Methods to Expanded Operating Domains was implemented. The SER for that Topical Report imposed 24 limitations and conditions that we needed to evaluate as part of the EPU.

And all of those conditions that were relevant to the EPU were implemented and fully addressed. We also demonstrated that the fuel performance is consistent with the EPU plant experience database.

So in conclusion, only GE fuel types will be used throughout our EPU implementation. And cycle 14 with be the fifth consecutive GE14 reload. And we only utilized NRC approved methods for the core design and safety analysis. All of the applicable limitations and conditions from the Topical Report were addressed and fully implemented.

And our fuel performance is consistent with the plant experience database. And the analysis confirm safe operation of the fuel under EPU conditions.

Next George Inch will discuss the mechanical, civil and material aspects of the power uprate.

MR. INCH: Good morning. My name is George Inch, I'm the Principal Engineer on the EPU project for mechanical/structural. I'm going to summarize the evaluations that were done for the reactor vessel and the internals for the impact due to the power uprate.

One of the major things that are impacted with the core higher batch fractions and the additional power is that the neutron fluence that it exposes the core shroud and vessel is increased roughly 40 to 60 percent depending on where the peak locations are.

And those higher power bundles are not on the periphery but they're within two rows of the periphery. And the evaluations were done looked at what components might be exposed to a fluence level where irradiation assisted stress cracking risk may be increased because of those higher fluences.

And the evaluation concludes that the components that currently exceed that fluence remain the same. The top guide, core shroud and core plate. Those components are addressed by the AWR Vessel Internals Project Guidelines. The NRC approved guidelines for that.

To give you an idea the top-guide location is, you know, the highest fluence location in the core. At the end of 60 years the peak fluence is approximately 3.3 E22 n/cm^2. Did I say that right? E to the 22. The core shroud at the H-4 weld, which is about mid-height, is at 4.1 E21 n/cm ^{2}. And the core plate at 6.3 E20.

MEMBER BROWN: What is the core plate material?

MR. INCH: That's 304 now.

MEMBER BROWN: It's 304.

VICE CHAIR ARMIJO: Is that the same width for the top-guide and the shroud? Are they 304?

MR. INCH: Yes.

VICE CHAIR ARMIJO: Now you did, we asked a question at the subcommittee meeting about the piping. And that was fortunately a low carbon 316.

MR. INCH: That's correct.

VICE CHAIR ARMIJO: But, that did not get into the internals? You didn't use the same material in the internals?

MR. INCH: No, that's not in the internals.

VICE CHAIR ARMIJO: Okay.

MR. INCH: Our conclusion is that the program that is addressed in the VIP remains an effective way to identify any potential degradation due to fluence effects or degradation of the internals.

And the other conclusion we reached dis that hydrogen water chemical and noble metals process that we use to mitigate stress corrosion cracking will remain effective for 60 years for these components, even at the fluence level.

It is important to note the top-guide really isn't mitigated by those mechanisms. And the fluence level is above a threshold where you wouldn't expect that to be effective.

MEMBER SIEBER: In your in service inspection program for reactor vessel internals, have you found indications, so far, that would, or defects, you know, cracks or what have you, that would, well have you found any? And secondly have you done any remedial action for what you might have found?

MR. INCH: Yes, our internals inspections programs has identified cracking on the core shroud. It's not unusual, consistent with the OE on it.

MEMBER SIEBER: That's right.

MR. INCH: On the top-guide we have not identified any cracking. OUu inspection sampling is at the beginning, because of the age of the unit, we haven't achieved our full sample requirement of approximately five percent yet.

And the core plate, that inspection hasn't identified any issues. That inspection is currently in an update process, generically. As part of the VIP because it requires some inspection of core plate bolts.

For that one we are not really required to do any inspections until approximately 40 years. So we're --

MEMBER SIEBER: That could be a sensitive issue.

MR. INCH: The core plate bolting, for the core plate, our margins and stress relaxation for those bolts, analytically are shown to be remain effective even with potential cracking. Consistent with the generic guidance.

MEMBER SIEBER: Okay.

MR. INCH: So the core shroud cracking is on the OD, it's shallow on the H4 and H5 welds. And we've got an aggressive inspection program with ultrasonic. We've done a recent reinspection in 2008, which was a six-year interval since our last ultrasonic. And prior to that there was a four-year interval. So it's a very aggressive program.

And it's shown that the mitigation measures for hydrogen water and noble metals are very effective, the cracking is not --

VICE CHAIR ARMIJO: So as far as the length of the cracks and the depth of the cracks on your shroud. It's been many years since you've first detected them. And you've been operating with hydrogen and noble metals. And have you found that these cracks have grown either in length or in depth?

MR. INCH: Since the implementation of noble metals there has been no significant change. There is variation on ultrasonic measurement techniques, and we attribute the change to within the noise of the measurement.

VICE CHAIR ARMIJO: How about new cracks, maybe that hadn't been detected before?

MR. INCH: We don't believe there's any new cracking. Again, you have different coverage regions. So if you looked at a map it doesn't match up exactly. But there's placement errors. So essentially when you take the aggregate, our assessment is is that there's no significant change in the amount of cracking. It's approximately 70 percent of the circumference on the H4 weld.

And it's shallow, less than a half inch, it's a two-inch shroud. It's been stable since we implemented hydrogen water chemistry. When they were first identified in 1998 with UT. We went back in after two years, just prior to noble metals, and reinspected and it was a normal water chemistry.

We did observe what we considered growth at that time, under normal water chemistry. It was well bounded by the normal water chemistry crack growth rates of 2.2 E to the minus five inches per hour. And that was important information from our perspective.

And that's why we implemented a much more aggressive reinspection after noble metals to make sure we've stabilized it, because we were considering at that time other mitigation measures.

VICE CHAIR ARMIJO: So you didn't have to apply these clamping techniques or do that other people would have to do on the shrouds?

MR. INCH: Yes, we determined that the core shroud tie-rod modification was not warranted at this time. It is a contingency that we've looked into. But with the cracking stabilized at a half inch there's a large margin to allow.

VICE CHAIR ARMIJO: Thank you.

CHAIR ABDEL-KHALIK: What was the current fluence level for the top guide?

MR. INCH: The current fluence level for the top guide. I don't have that number at my fingertips, I can get back to you on that.

CHAIR ABDEL-KHALIK: But it is greater than 5 times 10 to the 20th?

MR. INCH: Yes. It's in the 21 range, high 21s.

CHAIR ABDEL-KHALIK: And you have not found any cracks in the top-guide, as far as you know?

MR. INCH: No we have not identified any cracking in the top-guide. We've done approximately six cells. We've inspected six of the control cells with enhanced visual techniques consistent with the new guidance. And in that sampling we have not identified any cracking conditions.

CHAIR ABDEL-KHALIK: Okay.

MR. INCH: Moving on to the bulk of the internals, looking at the, you know, the impact of the power uprate. There are two things we evaluate, flow induced vibration and the basic structural effects due to temperature and differential pressure changes. The evaluations performed by GE Hitachi apply scaling methods that are extrapolated from data from prototype plants and actual plant data.

And that scaling applies velocity squared for the internal components, such as the steam separator and other components. The results show that continuous operation at EPU conditions doesn't result in any detrimental effects on the safety related internal components.

Structural standpoint. The evaluation stress reconciliation was performed consistent with Design Basis Analysis. Load increases were evaluated by scaling the governing stresses and then compared to ASME code allowable limits. There's large margin on those internal components.

All stresses and fatigue usage are within the design ASME Code allowables. And the internal components have been demonstrated as structurally qualified for EPU conditions through the end of the license renewal term.

The fatigue monitoring program, fatigue is one of the things that is impacted through the power uprate because of the temperature changes. The current licensing basis for Nine Mile Unit 2 is cycle counting for fatigue monitoring for the design calculations.

And so for each event the maximum usage is accumulated. And for the stress based monitoring for the feedwater nozzle is planned for managing the feedwater nozzle location below 1.0 for the license renewal term.

EPU evaluations have concluded that cycle counting usage does remain below 1.0 for 40 years consistence with the current licensing basis. And that the current plans for stress based monitoring for the feedwater nozzle remains required for the license renewal term.

The Nine Mile Point 2 commitment is to implement stress based monitoring in accordance with the ASME Section II, NB-3200 and that's consistent with the RIS-2000-30 to make sure that we include all six stressed components, and stress based monitoring is implemented for the licensing basis.

That's all I had on the on the vessel on the internals. But the next subject was going to be the steam dryer.

VICE CHAIR ARMIJO: George, before you go there. I think it was a feedwater nozzle, or one of the nozzles it would be above the 1.0 accumulative usage factor at EPU conditions unless you do something different. What would it be, one point what?

MR. INCH: At the end of the 40-year term for EPU conditions the peak location is at a usage of 0.9. And the standard rule of thumb, if you, for scaling for license renewal is to multiple by 1.5. So approximately 1.4 or something.

VICE CHAIR ARMIJO: So you have to go to a different methodology or actually do a repair or replacement or something in order to stay within that limit?

MR. INCH: Right. Correct, if the usage were actually that high, corrective actions would have to be taken for the nozzle. And stress-based monitoring allows us to get accurate predictions of what the actual usage is for the nozzle and then take appropriate action. Long in advance of approaching usage of 1.0.

VICE CHAIR ARMIJO: Okay. And that's your final bullet on that chart, right?

MR. INCH: That's correct.

VICE CHAIR ARMIJO: Thank you.

CHAIR ABDEL-KHALIK: Well the first bullet says you conservatively assume the design base of stress for each event. How far are your from this design basis stress now, and how far will you be at the elevated feedwater flow conditions?

MR. INCH: I think you're asking me what the current usage is --

CHAIR ABDEL-KHALIK: Right.

MR. INCH: -- for the feedwater nozzle?

CHAIR ABDEL-KHALIK: No, no, no. The design basis stress level.

MR. INCH: Well for the fatigue usage it's really just the cumulative usage factor. Which will accumulate that usage, what we're referring to there is for each event, a maximum thermal event, the accumulated usage for each one. So off the top of my head I don't know what that actual stress is for each one of those events.

CHAIR ABDEL-KHALIK: But I'm just trying to talk this thing into meaning of the very first sub-bullet. And how conservative is that assumption. How close are you to the design basis stress? How close will you be to the design basis stress at elevated feedwater flow conditions?

MR. INCH: I think I understand the question. Is the severity of the design basis transient that we're assuming in accumulating the usage for the nozzle.

CHAIR ABDEL-KHALIK: Correct.

MR. INCH: How conservative is that compared to the actual events?

CHAIR ABDEL-KHALIK: What you expect to have. Correct.

MR. INCH: The limiting event for, example, a feedwater nozzle is actually one of the transient events that occurs during hot standby where they assume some rapid cycling. And that's a design basis assumption.

And the duration of how long that occurs. And that is, there is significant conservatism in that in that there's operating procedures that try and mitigate severity of the conditions.

So I don't have a exact number for you. But our evaluation and trending shows that there's significant conservatism in the assumptions that go into like the feedwater nozzle. Some of the events are just the normal startup and shutdown.

And there's not very much conservatism in that heat-up cycle. It's just the conservatism is in how many cycles you have.

But for the stress based monitoring condition there is quite a lot of conservatism, because it assumes the maximum possible and the actual event is procedurally mitigated by operations.

CHAIR ABDEL-KHALIK: Have you ever had a feedwater reg valve control failure?

MR. INCH: That's -- Phil?

MR. AMWAY: A feedwater, we've had some events. At the level valves have been very good operating performance in terms of failure. I mean we've had minor issues where, you know, it may not behave quite like we would expect it to. But not such that it resulted in a level excursion.

MEMBER SIEBER: You have electric-driven feed pumps, right?

MR. AMWAY: We have electric-driven feed pumps for all three, that's correct.

MEMBER SIEBER: So the plant stability depends far more on the operation of the feed reg valve than you would have if you had steam-driven feed pumps. Steam-driven feed pumps, feed reg valves pretty much stay at the same place.

MEMBER STETKAR: Do you have variable

speed feed pumps though?

MR. AMWAY: No, they are not variable speed.

MEMBER STETKAR: Right.

CHAIR ABDEL-KHALIK: Right.

CHAIR ABDEL-KHALIK: So you say you had a feed level reg valve controller failure, and yet it didn't result in a vessel level excursion, is that what you said?

MR. AMWAY: That's correct. What I'm talking about is we'll notice, because we monitor the motion of the feedwater reg valves and there's normally two in parallel at 100 percent.

So if you had a failure in one the other's going to try to compensate. Okay? So the failures that I'm talking about is you'll have some kind of LP10 will just fail on an as-is condition.

And you'll see that by when the operators do their rounds they're looking for that valve motor to be turning on some of a frequency to show that it's actually responding to the feedwater level control. So they have that.

And we also have alarm settings that will warn us of an actuator trouble, you know, so as long as we were at steady state operation we wouldn't see anything in the level control side of it. We would be looking at the actual LV10 performance, that detects --

MEMBER SIEBER: That's because they're reset controls?

MR. AMWAY: Yes.

MEMBER SIEBER: They will grind that until they get to the right point.

MR. AMWAY: Right.

MEMBER SIEBER: If one fails the other one will take up the --

MEMBER SKILLMAN: This is Dick Skillman and I understand you to say that with your current cycle counting program and for what you project in terms of future cycles, with the power uprate, your U will remain one or less. Your U session factor, the 1.0?

MR. INCH: That's correct.

MEMBER SKILLMAN: What changes have you made to your cycle counting program to ensure that you have accurate cycle count and an accurate cycle description? You've changed your feedwater about 15 degrees Fahrenheit. You've boosted feed flow and steam flow. It appears as though you've addressed the vibration and the other issues related to the higher mass flow rates.

But what have you done in your cycle counting program to make sure you're on the money for, if you will, the press towards your 1.0 U for the power uprate, please?

MR. INCH: That's a good question, because when we did the license renewal it was recognized that we were going to have to get much more accurate in managing the usage. At that point in time, in 2008, we did implement the FatiguePro Software, which was epi software that was developed.

What it allows us to do is it automatically records all the processed computed data an then has triggers for counting the cycles. So it doesn't rely on someone to go back and figure out what it was. So there's, actually all the data is recorded for the actual severity of the event.

And then each one of the locations is then sorted in the software as to which ones you're counting the cycles and which ones you want to also count with stress. So that program was implemented in 2008 and is currently being used to track the usage.

We're also double tracking the feedwater nozzles so we have a usage based on stress based and cycle counting.

MEMBER SKILLMAN: Thank you. I'd ask, please, if the individuals who are monitoring that program are sensitive to how important that program is to your utilization?

MR. INCH: Oh, yes. The program is managed through our Design Engineering Group, expressly because it's computationally intensive. You've got to understand the sensitive locations. And so that's well understood.

MEMBER SKILLMAN: Thank you.

CHAIR ABDEL-KHALIK: What would be the usage factor for 60 years of operation? Second bullet.

MR. INCH: For 60 years. Our usage is less than 1.0 for 60 years for all locations. And the location for the feedwater nozzle we expect to be able to maintain below 1.0 with a stress-based --

CHAIR ABDEL-KHALIK: Even for 60 years?

MR. INCH: Even for 60 years, yes.

CHAIR ABDEL-KHALIK: Okay. So why --

VICE CHAIR ARMIJO: But you'll be below one for 40 years without stress-based?

MR. INCH: That's correct.

VICE CHAIR ARMIJO: Okay. But not for 60?

MR. INCH: If you were to have all the

design events with the same design severity and then you simply did a projection with the 1.5, that's where you would predict you would be above 1.0. That's what mandates having to more accurately track that.

MEMBER STETKAR: George, I don't recall the license renewal. And I didn't look it up. Did you guys look at a trending on your cycle counts in a historical trending back through day one? Just to see how the slopes were heading.

You know, the questioning about extrapolating out through 60 years is a straight linear extrapolation, that depends on the shape of your operating history basically.

MR. INCH: Yes. What is showed is in the first five years of operation we accumulated a lot of usage. And there was a lot of startup, shutdowns and transients. And since then it's really plateaued and the usage has plateaued out. So there was a lot of usage in that first five years.

MEMBER STETKAR: Thanks.

MEMBER SIEBER: One thing you need to look out for though is that there is that there is a so called bathtub effect. Where when a unit first starts out, particularly if it's a first of a kind or the first for that particular licensee, the cycle rates are pretty high. Then operation becomes steadier, more experienced people, better repair programs. And so the cycles go down.

However, at the end when everything is wearing out your cycles go back up. So that's where you really have to pay attention. Is to watch your maintenance history and your failure rates. And as the plant gets older, some plants see that in a pronounced way. Other plants not so much. But you have to pay attention to it.

VICE CHAIR ARMIJO: I'd like to bring up a couple of items that came up during the subcommittee meeting that I think the full committee might appreciate. And, George, I'd like to ask you about the hydrogen water chemistry techniques that you'll use to compensate for the higher radiolysis rate in the core.

And the other question is what mitigation have you done for the indications of cracks that you found in your nozzle dissimilar metals weld so that the fatigue doesn't have to worry about some preexisting crack. So if you'd expand on those two points.

MR. INCH: Okay. I'll do the latter first. We've done for our feedwater nozzle dissimilar metal weld, there were indications identified in it, oh it must have been about six years ago, we did an overlay on that location. We have implemented the Performance Demonstration Initiative to properly inspect the dissimilar metal welds.

And there was one other indication that was originally identified back in '92. It was on a HPCS line that a mechanical stress improvement was done in that year. And it has been monitored since repeatedly and there's been no growth. So we've carried a contingency for an overlay on that location for many years, it's still on the books, but it looks like --

VICE CHAIR ARMIJO: How about the core spray nozzles?

MR. INCH: The core spray nozzles?

VICE CHAIR ARMIJO: Yes, the core spray lines. Did you have any --

MR. INCH: To my knowledge I don't believe there's any indications in the core spray nozzles.

MEMBER SHACK: Those are carbon steel on the BWR/5 aren't they?

MR. INCH: I would have to check that.

VICE CHAIR ARMIJO: And the hydrogen water chemistry. You're going to do something different I know that. You're going to, as far as you're going to increase the hydrogen, right?

MR. INCH: Oh, yes.

VICE CHAIR ARMIJO: Commensurate with the increase in --

MR. INCH: Yes. For noble, we perform noble metals with the online technique. So every year we reapply. And currently our hydrogen water chemistry program implements a molar ration of 4:1 for the upper shroud location on the OD. And that results in an injection rate of 15 SCFM.

For power uprate our plan is to maintain 4:1 at the upper shroud location and to implement 17 SCFM to maintain that same molar ratio. The required molar ratio for mitigation is 3:1 but we've implemented 4:1 because of some uncertainty associated with the radiolysis modeling predictions.

And we hadn't recognized any significant change in operating dose rates because of it. It is something that we might want to consider in the future to drop it to 3:1, if we're seeing any effect associated with the higher injection rate. But we don't anticipate that.

VICE CHAIR ARMIJO: What's the basis for that 3:1, where does that come from?

MR. INCH: That's a guideline that has been developed primarily by the industry and General Electric and NRC has endorsed as an acceptable molar ration for mitigation.

VICE CHAIR ARMIJO: Okay. Thank you.

VICE CHAIR ARMIJO: Okay. At this point I think we're, well we need the staff. So we're ready to go into closed session and address the steam dryer and the jet pump mixer coating or any other questions the committee may have that might deal with proprietary information. So let's just go ahead with that.

(Whereupon the meeting of the open session went off the record at 9:35 a.m. and went back on the record at 10:40 a.m.)

VICE CHAIR ARMIJO: We can now go back into open session. At this point I'd just like to get some feedback from the Committee members. Any closing remarks, observations, comments. And I'll just go around the table quickly. Jack, nothing?

MEMBER SIEBER: None.

VICE CHAIR ARMIJO: Dr. Banerjee. Pass. Harold, pass. David?

MEMBER BLEY: Nothing more.

VICE CHAIR ARMIJO: Dennis? Dr. Powers?

MEMBER POWERS: Compliment them on their conservatism and the care with which they've done this, it's quite impressive to me.

VICE CHAIR ARMIJO: Thank you.

MEMBER STETKAR: Nothing.

VICE CHAIR ARMIJO: Mike.

MEMBER RYAN: Nothing else, thank you.

VICE CHAIR ARMIJO: Bill. Well, I really have nothing else. We had a very good meeting today. I think you were very well prepared. The subcommittee meeting was thorough and you addressed all the questions we raised at the subcommittee meeting so I'm satisfied. I think it's now up to us to go into our session and prepare our letter on the subject.

We did not get the chance to hear from the staff here at this meeting in more detail. But we did get a lot of detailed review on the part of the staff at the subcommittee meeting and I'd like to compliment both the licensee and staff on their preparation for this application. And with that I turn it back to you, Mr. Chairman.

CHAIR ABDEL-KHALIK: Thank you. At this time we're scheduled for a 15 minute break. So we will reconvene at 11:00 a.m.

(Whereupon, the meeting went off the

record at 10:42 a.m. and went back on the record at 10:58 a.m.)

CHAIR ABDEL-KHALIK: We're back in session. At this time we will move to the next time on the agenda. Branch Technical Position 7-19. Guidance for the Evaluation of Diversity and Defense-in-Depth in Digital Computer-based Instrumentation and Control Systems.

And Charlie Brown will lead us through that discussion.

MEMBER BROWN: Okay, I'm not going to go through a big introduction. Just to let everyone know the staffs not really required to present the staff review plan. That we normally get after it's been issued but this one they gave us a heads up. We were interested in seeing it, so I appreciate that courtesy, I wanted to let the staff know that.

We had delayed a little it on coming to the full committee and they, again delayed issuance of this. Until after full committee to see if there were any other continents that would be good to put in. So I'm wanted to thank the staff for that and with that I will turn it over. Who's leading this, Gene?

MR. JUNG: Thank you, Charlie. Good morning. My name is Ian Jung, Chief of the

Instrumentation Controls and Electrical Engineering Branch to Digital Engineering. And thanks committee for taking time to go over this particularly important copy.

And this particular guidance is to implement the Commission Policy 93-087, regarding the software common-cause failures for digital systems, for of course safety systems.

And that we've gone through a sub-committee meeting in September, also ISG which is being incorporated into this particular revision, ACRS have retained that document earlier.

So the particular scope of change is to incorporate those currently what's in IGS-02 which will be added to Revision 5 forming a Revision 6.

With that I'll turn it over to Rich Stattel and Gene Eagle.

MEMBER SHACK: Let me just ask a quick question? What is the regulatory status of acceptance like 93-087, it's not a fuel but you all have followed the guidance in it.

MR. JUNG: It is not a regulatory requirement but SRM Commission set out as a policy, in general that is considered still the document. We considered that as a policy, I think applicants not addressing the policy should testify why the policy is not being addressed.

And Gene Eagle from Office of New Reactors. Both of them were, led this part of the effort, Gene.

MR. EAGLE: Okay, thank you. Today as we are approaching lunch we'll try to keep our presentation as short as possible. And some slides I'll only put up and not necessarily read everything on it and we'll try to hit the highlights or the key points.

The crux of the briefing today is to highlight and identify the key elements from incorporating ISG-02 Revision 2 into BTP 7-19 Revision 5 to form Revision 6, and the action items from the ACRS subcommittee presentation.

The current status is presented here, we would like to note that BTP 7-19 has received OMB concurrence as a non-major rule under the requirements of the Congressional Review Act. This is primarily, based on the fact that as we mentioned above the BTP 7-19 Revision 6 is the incorporation of the approved and issued ISG-02 Revision 2 into Revision 5 to create Revision 6.

Slide 3 presents the agenda for our

presentation today. First we'd like to review the purpose and general basis of BTP 7-19. BTP 7-19 applies to software Common Caused Failure and we will simply refer to it as CCF on the screen and often in this presentation.

The Interim Staff Guidance, ISG, documents were in an NRC method of rapidly getting further needed guidance on digital I&C to the staff and stakeholders in preparation for the new reactor designs.

The original concept was that all the ISG's would be incorporated into the appropriate standard review plan document. It forms the purpose in general, I'd like to read the summary notes in red.

In summary, while the NRC staff considers software Common Cause Failure in digital systems to be beyond design basis. Nuclear power plants should be protected against the effects of anticipated operational occurrences,, and postulated accidents with a concurrent Common Cause Failure in the digital protection system.

Slide 5 has our background. That's first we had Revision 2 which answered the initial comments that were presented by the ACRS during the presentation of Revision 1. And in particular the main thing was the idea of operator manual action to be able to be credited as part or some basis in the diverse means.

We then created, the decision was made to merge Rev 2 into the standard review plan, Rev 5 to create Rev 6. Seventy comments were received and the presentation was made to the subcommittee on September 7th.

As the result of several public comments on the paraphrasing of the NRC Four-Point Policy on D3 in Revision 5 the staff decided to quote the NRC Four-Point Policy directly as noticed on these slides.

Points 1 and 2 emphasis performing a D3 analysis on the proposed I&C system. The direct quotations of the four-points were followed by simple specific items or significant interpretations that the staff wanted to emphasize under concerning points.

One thing the four-points used the term best estimate methods. We thought a better term would be realistic assumptions. That then included a definition.

By the way the corresponding event here when we talk about zero power, this means that if the Chapter 15 covers any kind of thing that goes down to maybe a zero power that's included when we say corresponding to the event.

The Safety Analysis report id specified by .2 must be addressed. Concerning Point 3, if the analysis indicates a potential for Common Cause Failure, Point 3 directs the applicant to identify or add a diverse means to perform either the same function or a different function.

You also want to notice that the phrase "Safety Computer System" identified in Items 1 and 3 above, from Point 4 clearly indicates primary application is to the automated safety-related reactor trip system and the engineered safety features.

Point 3 also applies to manual initiated methods for the reactor protection system if subject to the Common Cause Failure

A diverse means may be accomplished by automated, manual, or a combination of these for initiating mitigating functions.

The staff wanted to emphasize that it is Point 3 that directs the identification or creation of a diverse means. If the D3 analysis identifies a Common Cause Failure.

The critical safety functions are more accurately defined as the plant critical safety functions and are the ones from the NUREG-0737, Supplement 1.

Also the safety parameter display system provides indicators and implementation to support these plant critical safety functions. They are listed in Revision 6.

Assume for a moment that a current nuclear power plant is upgrading with a digital I&C system. If certain panel alarms and instruments are retained but the input signals are derived from the new upgraded digital I&C system that is subject to a postulated Common Cause Failure. Then these retained I&C instruments would no longer qualify as independent and diverse point-four displays.

Public comments made a case that once manual activation from the main control room using point-four controls had achieved the initial objective, there may be, and I repeat, there may be a need later to use controls outside the main control room. An example might be actions needed in the long run beyond 72 hours.

However there may need to be in the short period use of these controls. An example might be the realignment and operation of manual valves to set up an alternate flow path to recover from failed or damaged equipment. The key point here is that it may be on a case or specific basis.

MEMBER BROWN: Before you flip off of that, don't forget the last line. "When supported by."

MR. EAGLE: Yes. Okay. Once manual action from Main Control Room, using point-four controls is completed, controls outside Main Control Room may be used for long-term and/or perhaps short-term management when supported. I like the last point, when supported by suitable Human Factor Analysis and Procedures.

At this time Rich Stattel will be presenting and discussing the independence of the diverse means.

MR. STATTEL: Yes, good morning everyone. Yes, I just wanted to say a few words regarding the independent means. Because although the primary objective of this revision to the BTP was to incorporate what the Working Group 2 had come up with, and the ISG-02. We also identified the need to clarify certain aspects of the guidance.

Regarding the independent requirements for the diverse actuations of the automatic diverse actuation system. This was an area that received quite a bit of feedback from the industry.

And we decided to add some clarifying language to the BTP to address allowances for both safety related and non-safety related diverse actuation systems.

Prior to this revision there was kind of an assumption that the diverse actuation would be non-safety-related and would be separated in that manner.

As you may know, there are basically different requirements for separation between divisions of safety and between safety and non-safety related systems.

And basically, we didn't want to change any of that guidance really, because that's something that they have to conform to the regulations that exist for those systems.

But the BTP also has to acknowledge that a licensee can choose to incorporate a diverse system within a safety related system. So for example if a plant chooses to have a diverse safety system. Like a four channel diverse safety system which several plants have done this.

Then it's really unrealistic to expect separation between the primary safety system and the diverse safety system.

So Channel A would be powered by the same

1E power source for example. But of course the divisional separation would still apply as it does for all safety systems.

For non-safety systems there's a different set of criteria, and those are defined in other standards, for example ISG-04. So as the slide states here the diverse means it could be safety related or could be non-safety related.

In the final analysis though, in either case regardless of how the licensee chooses to implement a diverse actuation. It should be independent of the safety system in the manner such that the Common Cause Failure of that primary safety system would not adversely effect the diverse system itself.

So that was really the goal, and I just wanted to explain that that was the reasoning for that clarification.

MEMBER BROWN: Just one point, the clarification I mean. If you look at BTP, trying to calibrate myself again here. That did not have as much explanation, well to get to this point. So there was a considerable amount of clarification to make these differentiation points which was a pretty good.

MR.. STATTEL: I was actually very

challenging to establish the criteria, knowing that plants are going to implement the diverse systems in different a different manner. But I think we came to an agreement and I think the language as it is in the new Revision, really addresses that issue.

MR. EAGLE: I also wanted to point out that, for instance, when they talk about the point-four displays and controls. They use the term independent and diverse and originally we had started using that.

And then during the industry comments they brought up some of these things and therefore we then addressed the independence with more detail.

Thank you Rich.

MR. STATTEL: Yes.

MR. EAGLE: The driving motivation for ISG-02 was the nuclear industries representatives presentation of a list of concerns and questions. ISG-02 addressed seven of these problem statements.

While we don't plan on going into all the details of each problem statement as we did in the sub-committee. We would like to look at the key issues and present some of these and discuss these.

The first one, was the automatic versus manual diverse means. Originally there was a hard limit that manual operator action could only be used if not required for at least 30 minutes. This was in line with guidance or regulations from other countries that were major generators of electrical power from nuclear power plants as learned in a major international meeting in this very room. Actually the room next door.

MEMBER STETKAR: Which were probably derived from very, very early, US NRC specifications of 30 minutes.

MR. EAGLE: I'm glad to see we're a leader.

MEMBER STETKAR: No, just don't rely on that survey of other international experience.

MR. EAGLE: As being independent.

MEMBER STETKAR: As being independent, or diverse. It's in fact derived from guidance from the US NRC in the '70's.

MR. EAGLE: I would hope the NRC is one of the key leaders in the world for power. Industry presented a strong dissent to not having an option to use manual operator action as all are part of the diverse means for actions required in a short period of time.

And the ACRS at the time agreed that it

should be considered. And the result is we went to a Revision 2 in which it was considered and was included as an option.

Now in the automated versus manual, first you perform a D3 analysis of the Reactor Protector System using realist assumptions. If subject to potential Common Cause Failure you need a diverse means to perform the safety function subject to the Common Cause Failure.

The diverse means may be automated or manual or actually even a combination. Now the automated diverse means is preferred. And it's stated in REV 6 that way and also in ISG-02.

If the manual means is selected as the diverse means, acceptability is based on Human Factors analysis.

MEMBER BROWN: That's reflected in 1.6 to Reg to 1.62 also isn't it?

MR. EAGLE: Yes, that's right.

MEMBER POWERS: Why is it human factors and not human reliability?

Mr Eagle: Well, Human Factors Engineering is, that's the term we usually use for it. Human Factors Engineering.

MR. JUNG: Charlie, just little

correction, it's the IGS-05.

MR. EAGLE: Well I know it's an ISG-05 but Reg Guide 1.62, maybe it was another one but I thought we also had this discussion available time required. Did I get it wrong?

MR. JUNG: Manually in ISG-05.

MR. EAGLE: Oh, I got it wrong.

MR. JUNG: Manually in ISG-05, which has been incorporated into Chapter 18, Appendix A.

MR. EAGLE: Oh, that's Appendix A, I'm sorry.

MR. JUNG: Subcommittee.

MR. STATTEL: We plan on talking about that in a little bit more detail in slide 14.

MEMBER BROWN: All right, lets go on then.

MEMBER POWERS: I mean doesn't the Human Factors, oh it's going to tell you that's it's physically possible to do this thing?

MR. STATTEL: That is the primary objective there, so it's basically a process that identifies what time is needed to perform an action. And it also establishes how much time it takes for the operators to accomplish that action.

And all the factors involved with that. And basically compares those two times and comes up with a reasonable assurance that the operator will be able to accomplish the required safety function. In that amount of time.

MEMBER POWERS: You mean it just tells you that it is physical possible to do within the required time?

MR. STATTEL: Right.

MEMBER POWERS: It doesn't tell you actually can happen.

MR. STATTEL: There was an aversion to actually establishing a firm time restriction on that, right? In other words, in the past, you know, if the operator had an extended period of time to perform an action it was just assumed that yes, he'll be able to do that.

And if it was shorter than another time he would not be able to do that. But unfortunately that's a very simplistic approach. That really doesn't work because the complexity of the action and the amount of analysis that the operator has to go through to take that action varies a lot, depending on the action.

So the action may be as simple as I get an alarm, I push a button. Or it may be as complicated as I look at ten different indicators. And if they align in a certain pattern then I will initiate a procedure that actuates 50 different components within the plant.

So those are two extreme examples. So with that in mind we felt, and we came to the conclusion that a Human Factors Analysis could support either of those cases.

And the amount of time whether it was 15 minutes or 72 hours was really not relevant to that. As long as that analysis took all of those factors into consideration.

MEMBER BLEY: I think, to Dr. Powers' original question, and I could be corrected on this. I know if Paul were, is Paul going to be here?

MR. STATTEL: He is here.

MEMBER BLEY: He is here?

MR. STATTEL: In the back of the room, yes.

MEMBER BLEY: He might correct me on this, but I think the traditional view of human factors aligns with what Dr. Powers said.

I believe in human factors engineering as it's been defined for design certification, it incorporates human reliability analysis as part of that whole discipline the way they've defined it.

MEMBER STETKAR: At least up to the point of, I think in terms of traditional human reliability analysis it does not include the actual quantification of the air raid. It includes everything up to that point, I believe.

MEMBER BLEY: That's not the way I read that.

MEMBER STETKAR: Okay, maybe Paul can --

MEMBER BLEY: It's on my HFE.

MEMBER STETKAR: -- help us.

MEMBER BLEY: But in any case, if it doesn't then I certainly agree with what Dana said in the beginnning. What you're talking about is human reliability analysis, and I think the way you've defined thing, that's part of --

MEMBER SHACK: Is it feasible, or is it feasible and reliable?

MEMBER BLEY: I think it's the latter. It's what it better be.

MR. EAGLE: Paul, do you want to comment on that? He's our human factors expert.

MR. PIERINGER: Paul Pieringer, Human Factors Technical Reviewer from DCIP. Feasible and reliable is the big picture and that's what we always go back to, and we do that by integrated system validation.

And I can stick to that more, we get into more details. It's my understanding that the way we interface with human reliability analysis right now is that the PRA group identifies risk-important human actions.

And there's criteria that they use to screen actions that are being taken by the operator that impact the PRA in a manner that makes those actions important.

And they use Fussell-Vesely and RAW scores to establish a criteria that selects those out. Those risk-important human actions go into the Chapter 18.

Now what I would tell you is that most, well, it depends on which design center you're working with, but many DAS Manual actions are not risk-important human actions.

So they would not necessarily get the full treatment of the Chapter 18 program. What we see currently is that most applicants are committing to manage their DAS Manual actions using the fundamental pieces of Chapter 18, the most critical piece being the integrated system validation.

And so a lot of the evaluation work that we do in HFE, we do an up-front review to make sure there's no fatal flaws, but we much prefer to see the proof demonstrated in the integrated system validation program.

MR. EAGLE: Thank you, Paul.

MEMBER POWERS: Well, now I'm confused.

PARTICIPANT: Yes, me too.

MEMBER POWERS: I mean it seems like, I mean I think what you told me is that we don't do this. We don't consider it an important action in the PRA.

MR. STATTEL: I think we're talking past each other in a little, what we use this for, this review plan guidance for is to perform safety evaluations on the acceptability of this instrumentation.

And when, for example, if a licensee has performed a D3 analysis and we're reviewing that it basically falls through, right?

So they assume a certain failure, a common cause failure mode and then they identify what the backup means for performing the safety actions are, right, and they relate that to each of the accidents that are considered in Chapter 15.

And if it falls through to a manual operator action, right, then we basically, you know, from a logistics point of view the NRR would basically turn that over to the HFE group and they would perform the human factors safety evaluation to support that.

MEMBER POWERS: So I got the impression that he'd come back and say it's not important to PRA so we're not going to look at it.

MR. STATTEL: Well, we issue our safety evaluations and we consider them to be risk informed, but not risk based.

MR. EAGLE: I think it's important to go back to the actual documents themselves starting with ISG-02 Rev 1, we have in there a hard line dimension.

If the response to an event with a common cause failure postulated, if the response would require, had to be done in less than 30 minutes, it had to be on automated diverse means.

If the response required in greater than 30 minutes, operation action was acceptable. That was Rev 1. In Rev 2, we went back and said diverse means can be automated, manual or a combination, but the automated means was preferred.

Now if it was manual chosen or even partial manual, justification by human factors analysis using ISG-05 Rev 1.

Now this was the document that would then, if you made a choice to use manual operation as part of this diverse means, then it would switch over and the ISG-05 Rev 1 would then provide the procedure or how you would go about analyzing if this was acceptable.

Now in BTP 7-19 it simply rolled the ISG in. At this point in time, remember we mentioned that also this ISG was in the process of being rolled into a new document. It was called Appendix 18A, which would cover the same thing that ISG-05 Rev 1.

So that would be the --

MEMBER POWERS: You're still not getting to my point. When do you do the human factors analysis, and is it perfunctory or is it something that I can chew on?

MR. EAGLE: If you had chosen --

MEMBER POWERS: I don't know anything about ISGs.

MR. STATTEL: We don't do that within our division, so basically we would create an activity for the HFE group and they would, for instance, for the Oconee application there were several short-term manual operator actions that were required for action at mitigation.

And the HFE group performed a safety

analysis that supported and it made a reasonable assurance conclusion that those actions could be performed in the required time.

And that was backed up by actual V&V tests that were done with operating crews at the plant. So they had demonstrated through simulations that the operators could reliably perform those actions within the required time.

But as far as the details of what go into that human factors and safety evaluation, I guess Paul would have to answer that because we don't perform those on our side.

MR. EAGLE: The point is, as soon as the decision is made, you've determined that you now need a diverse means because there is a postulated common cause failure of your automated system.

And once you make the choice to use manual action as part of the diverse means then you have to go to one of these, and it's completely procedurized as Appendix 18A or ISG-05.

Paul, can you comment on that any?

MR. PIERINGER: I'm confused to what the question is.

MEMBER SHACK: Let me just go, in ISG-05 there's a statement. "To credit operator actions, vendors/licensees should demonstrate that the manual actions in response to a BTP 7-19 software common cause failure are both feasible and reliable given the time available."

I don't find that feasible and reliable in the BTP except in the note, and there it's not sort of required to demonstrate it, it's kind of a, you should note that.

And I like the stronger language in the ISG-05 that says you demonstrate that it's feasible and reliable. And that to me was always the intent when you dealt with things that were less than 30 minutes, was to have both the feasible and reliable part in there, and somehow that seems to have slipped out of the current version of the Branch TP.

VICE CHAIR ARMIJO: Thanks for your comments. I think we are, I think the staff's not disagreeing with that, I think we'll work with the ISG folks and we'll try to incorporate to be consistent.

MR. JUNG: I don't think the intent of 7-19 was to have a disagreement with the HFP. I think fundamentally the Commission policy clearly stated that once you have a situation where it is subject to common cause failures and the potential consequence being not acceptable to meet on the Part 100 limit, that is, you know, applicants should have a means to be, you know, either automatic and manual if be feasible and reliable.

VICE CHAIR ARMIJO: We'll take that time and we'll provide the direct markup.

MR. STATTEL: I mean I believe the intent was to provide a hand-off. ISG-19 is guidance on performing diversity D3 analysis, not for performing a human factors analysis.

So it identifies that the manual operator actions are required and it identifies the need to perform an additional safety evaluation, but it doesn't give guidance on how to perform that evaluation.

So I'm not sure we're within the scope of the BTP 19.

MR. EAGLE: Correct. That is, once the decision's made to use manual then the justification of it has to come out of the procedures we mentioned, the Appendix 18A of the Standard Review Plan.

It was brought up in discussions that there were a number of manual functions in current plants that must be performed within a short period of time.

However, there are two important points to reiterate on this statement. First, the focus is on the automated protection system subject to postulated common cause failure, not just any operational function.

Second, if a protective function has normally performed by a manual action, then it was expected that that function or an alternate function would still be performed manually even in the presence of a common cause failure.

Further, I&C associated with the normal manual action is postulated to be subject to a common cause failure, then the manual action may have to be performed using different equipment.

We have a note that was added to describe special emphasis on being aware. For instance, as the difference between the time available and time required for operator action decreases, uncertainty in the estimates of both of these times must be evaluated carefully.

These uncertainties could invalidate or reduce the level of assurance of a conclusion that operators can perform the action reliably within the time available.

For actions within a limited margin of time to act, such as less than 30 minutes between the time available and the time required, additional staff review will be performed.

This statement was put in to put special emphasis as these uncertainties develop. I would also like to, I thank Mr. Stetkar's suggestion on how to correct that, to make a change. We had addressed that by making a change, and this is the latest version of this statement.

Another item that was brought up was the concern is that a potential common cause failure could result in the loss of measure of portions of the automated protection system, the operator's custom of depending on them at a time of crisis as an anticipated operating occurrence or an accident.

Now if one considers, however, that the staff expects a quality software development process for digital I&C systems and expects a quality verification and validation process, further considering that the digital I&C system goes through factory acceptance tests, site acceptance tests, start-up testing on the equipment, then the probability of a software common cause failure will be significantly reduced.

Further, the staff believes that because of this extensive testing, the trigger that causes a common cause failure and perhaps the results, will be something the operator is not expecting.

While not the CC type, there are already examples of the quote "unexpected" taking operator by surprise and then even scramming the plant.

Despite emergency operating procedures and abnormal operating procedures, which may include some common cause failure related actions, operators will likely be under significant pressure to respond appropriately to mitigate unanticipated plant events in coincidence with a common cause failure.

Good human factors dictate that this pressure to perform should be minimized, thus the inclusion of this warning note.

Some interested representatives advocated the use of component actuation versus system level or division level actuation. Actuation on a division level or a system level was retained.

Again, at the time when the operator may be under a lot of stress, actuation on a division level or a system level depending on the design, was retained to minimize the actions the operator would have to initiate in an emergency.

Another area of interest is spurious actuations. There are two types of spurious actuations to consider. One is caused by the common cause failure itself, and the second is caused by the diverse means.

The staff and industry representatives spent considerable time discussing this issue and came to a consensus as reflected in the next slide.

A spurious actuation is a lesser safety concern than failure to actuate because the challenges presented by spurious actuations are not considered to be as significant as failures to respond to AOOs and design based events.

MEMBER STETKAR: Okay, Gene, let's just stop here because there's a lot of words on this slide.

MR. EAGLE: Yes.

MEMBER STETKAR: Can you tell me the basis for that statement? That's a statement presented as if it's a fact and I'd like to understand why spurious, and I don't want to call it RPS, because that connotates shutting down the reactor.

I want to call it an integrated safeguards actuation system, which is what we're talking about here. Why is spurious actuation of an integrated safeguards actuation system always of lesser safety concern than failure to actuate?

MR. EAGLE: The basis is this is basically engineering judgment. And I can ask, you know, which --

MEMBER STETKAR: In my engineering judgment, here's another engineer, is that it's not. So now we have a difference of opinion.

MR. EAGLE: Different opinion. In other words, if you have a nuclear reaction that's running away with a positive period very rapidly, what is worse, for the failure to scram or a failure to -

MEMBER STETKAR: Let me pull you back. I'm not talking about the scram function, I'm talking about everything else that these systems do. For example, new integrated digital safeguards actuation systems automatically blowdown the plant.

They open up big holes in the plant creating LOCAs. Okay, a LOCA is a design basis accident. And in many cases they also blow open the secondary side of the plant simultaneously creating something that looks like oh, a fairly large steam line break.

There is no design basis event that looks at a simultaneous steam line break with a large LOCA. It is not looked at. It is not part of the design basis evaluation. It's not an AOO.

Although there may be systems, there may be common cause failure modes of these integrated safeguards actuation systems that could conceivably do that to you.

So now I'm concerned about why that is of lesser safety significance than an already analyzed design basis event or an already analyzed AOO.

MR. EAGLE: Here's one of the things, I think when we go into some of these other points we'll have to point this out. Further, spurious actuations are annunciated and thereby immediately detected.

MEMBER STETKAR: Okay, I am an operator in the plant and I know it's a really bad day.

MR. EAGLE: Yes.

MEMBER STETKAR: Because auto took over for me.

MR. EAGLE: Okay.

MR. JUNG: Gene, Ian Jung. And, I mean a couple of comments. It's for, we are beyond design basis space here, common cause failures.

So my response to Mr. Stetkar's comments is, the current safety system requirements and guidance for safety system software developments and digital systems development has been, that's where we've spent a lot of focus on.

So the goal for staff review and industry applicants, their main focus is really providing the high quality software that minimizes, and then hopefully to get completely eliminate the possibility of common cause failures.

And that's why the other day there was a, you know, the DAC procedure, the reason that we focus on those processes in life cycle for the element there's a reason for it.

Major common cause failure based on operating experience have shown that major cause has been development of requirements and translation to specific occasions.

So their current requirements, current staff guidance in other areas clearly try to re-achieve that goal. So I want to point that out.

But in terms of those multiple spurious actuations or possible scenarios, remember it goes back to the D3 analysis when so far most of the applicants coming in, when they use the same software for all scope of safety systems from RPS or ES effectuation, what they postulate so far has been completely, all safety systems that use the same software, all four divisions assume to have failed to perform the safety function.

So based on that assumption, when you come up with the diverse backup means, either manual or automatic, they provide an independent and diverse means.

Diverse means we'll have a completely different way of looking at symptom based app approach. There we'll see different parameters are being measured by different software, different analog system or digital systems.

(Crosstalk)

MR. JUNG: I think there's a defense in place, but in terms of postulating different spurious actuation causing it, staff and industry significantly discussed, and we couldn't come up with the situations where current overall D3 guidance we have would not be sufficient to cover the type of scenarios there would be represented as part of spurious actuations.

MEMBER BLEY: It's a nice speech and I appreciate what you guys have done.

When you go back to that first bullet which is a reflection of the text, it's the same text, it doesn't say that spurious actuations is less frequent, therefore we're not as concerned with it, it says the challenges are not considered to be as significant.

And I think that example that John gave points out that, you know, if you don't look for the challenges you don't know.

The idea that the worst thing that could happen is it doesn't do what it ought to do, doesn't acknowledge that maybe the worst thing it does is something that wasn't supposed to do. And that's the point that's being made.

And I don't think, I understand all the other things you're saying. You could also say, well, it's not in the design basis so we're not going to look as hard, which is kind of what you're saying. But just the statement I don't think has any basis.

MR. EAGLE: Well, I think that I'd have to disagree with you on that. For instance, and we talked about the scramming, you know, that if you have a runaway nuclear reaction versus, that is worse than --

MEMBER BLEY: There are certainly examples on each side. I don't think you're acknowledging each side.

MR. EAGLE: Okay, well, we were looking at, during this process we went through a lot of these and we didn't see places where that the failure to be able to actuate when it was really needed, you know, for instance, the water is dropping in the boiling water reactor. It's coming down and getting ready to uncover the fuel, something needs to be done.

MEMBER BLEY: Nobody disagrees with you on that one.

MR. EAGLE: Okay, if that is worse than suddenly the failed common cause failure and electronics suddenly deciding to throw extra water in there, and we looked at a lot of these, and basically the key point is that it's annunciated and the operator can now take action.

In other words, if something is spuriously turned on or is starting then he has a warning about it, and that's because even with common cause failure taking out the automated systems you still have your diverse systems.

And you remember the Point 4 displays are independent, and the controls and displays are independent of the automated protection system. So he's going to have an indication if we've had a common cause failure in this automatic system, he's going to have a clear indication.

And at that point in time you're depending on the operator to take action.

MEMBER STETKAR: Gene?

MR. EAGLE: Yes.

MEMBER STETKAR: Let me try something else. This is guidance for reviews and by implication, performance of a D3 analysis, Diversity and Defense-in-depth analysis.

If a person, an applicant who performs that Diversity and Defense-in-depth analysis doesn't look for these types of complex spurious actuations that, you know, I mentioned, they then don't have the opportunity to install either automatic or manual diverse mitigation systems.

In other words, you know, my example about blowing open a hole in the primary side and blowing open a hole in the secondary side, if someone hasn't identified that vulnerability they may not have installed a diverse way that the operators can somehow mitigate that, you know, manually closed valves that may have been opened if they weren't squib valves or something like that.

So that's my whole point about if people, and I think Dennis raised it also, if people don't look for these things, they don't have the opportunity to identify a potential vulnerability and perhaps design into their system a diverse way of dealing with that as they are doing now for the failure to acuate either manual or automatic failures, you know, capabilities.

The other point, getting back to a little bit of what Ian said, is that there are some analogies for other guidance for beyond design basis events that do require explicit evaluation of multiple spurious actuations, and in particular for fire events.

Both deterministic and probabilistic guidance don't have any limits on the number of multiple spurious actuations as they're characterized there that need to be considered.

In other words, that there's no limit on the number. And it's absolutely required that applicants do that evaluation and that the staff review those evaluations.

So there's kind of precedent, you know, legal precedent, if you will, for beyond design basis events to address this issue of multiple spurious actuations.

If it's considered to be important enough from the fire perspective, why isn't it considered to be important enough from the software perspective?

MR. STATTEL: If I may, I was a member of the working group and we had extensive discussions on this.

This language basically resulted from a discussion regarding the consequences of a spurious actuation, and a much better example is the depressurization system in boiling water reactors obviously.

The consequences being worse and have a higher probability of occurring than the common cause failure that we're all about here in this BTP that we're trying to avert.

And an argument was being used by industry at that time to basically use this as an argument for not putting in a diverse system or not incorporating diversity because it would have a down effect of increasing the probability of a spurious actuation.

It's really not the intent of the guidance in the BTP to downplay those consequences, and it's really not the intent to imply that a licensee not consider the effects of spurious actuations.

In actuality that they have always done that. In the boiling water reactors, as you know, there are significant design features that are added in to prevent spurious depressurization signals from occurring because they realize that those cause LOCAs, basically the spurious actuation would cause the LOCA that you're trying to prevent.

Those need to be considered, and the current position is that as before, as the design guidance that we had prior to this BTP and its existence, the licensee would consider those eventualities.

The other thing I'll point out is that this was language that was approved in ISG-2 and really our effort was to incorporate that guidance into BTP 19, and not to rehash or question what the working group's conclusions were, because those had already been presented to the Committee.

MEMBER STETKAR: Yes, and I think we had the same comments when we talked to the working group on ISG-2.

MR. STATTEL: Yes, it's a stretch to say that we have total consensus on these.

MEMBER STETKAR: It would be a stretch.

MR. EAGLE: By the way, talking about fires, this is partly attributed to the fact that fires have a proven record of destroying cables, creating short circuits and disrupting operator and automated controls as at the Browns Ferry fire event.

Thus, four physical and often widely separated divisions are used as part of the defense-in-depth.

Further, in modern digital data communications and networks using fiber-optic cables, the cable may melt, the path of logic may be lost, the division logic may be destroyed, but unless the signal is simply an on/off signal, it is unlikely the fire damage would cause a legitimate recognizable but false message frame that would cause the further down systems receiving this to react.

Anyway, this is one of the reasons that we looked at the idea of fires, but the main thing is it comes back to the bottom line that we looked at in making these various statements. And the consensus was is the fact that it will be self-announcing and the operators then can take action.

For example, in Chapter 15 you have an inadvertent opening of a safety relief valve is one of the things that I think, and if the software, a common cause failure caused the software to suddenly said open up these safety relief valves, that is an item that is handled or taken care of in the Chapter 15.

But the big thing about it is, for instance, in an ESFAS if the water level is dropping and the operator recognizes it and the automatic safety systems of ESFAS don't start putting water in, he's going to be able to recognize it and then take action.

And that's a worse condition than being able to, suddenly water starts pouring into the reactor from suddenly the common cause failure, on effect on instrumentations suddenly making a false assumption and starting to put water in, maybe too much water in.

Anyway, I think we probably have a disagreement on that but I think on that, a lot of my experience has been with the BWR and if more simplified areas there, when that water level starts dropping something has to be done.

MEMBER STETKAR: I think we need to move on.

MR. EAGLE: Okay. There is a second type of spurious actuation that we -

MEMBER BROWN: Before you do, have you gotten at least the interchange you want in the dialogue?

MR. EAGLE: Yes.

MEMBER BROWN: Okay, Dennis?

MEMBER BLEY: Yes.

MEMBER BROWN: Okay.

MEMBER BLEY: I understand.

MEMBER BROWN: Okay, all right. We do have some time and there's not a whole lot of slides, you know, left. So I wanted to make sure you all had adequate time to -

MEMBER STETKAR: I think we understand it.

MEMBER BROWN: Okay, all right. Go ahead, Gene.

MR. EAGLE: Thank you. Charlie said his lunch bill goes off somewhere -

(Crosstalk)

MEMBER BROWN: Theoretically we've got until 12:45, but it's not, if we finish before that that's perfectly satisfactory as long as we get everything covered.

MR. EAGLE: The second spurious actuation is that actually caused by the diverse means. And remember we went back to talk about how that industry's, one of the objections they had to some adding diverse means was the fact that there could be a higher probability of a safety concern than it would be if you didn't have the diverse means, and we talked about that for a moment.

So the way this was handled is the design of diverse automated or diverse manual means should address how to minimize the potential for spurious actuation of the reactor protection system caused by the diverse means. In other words, quality of design.

Another item that came up of interest was the combining of two manual initiations. There's two manual initiation systems that may be needed. First, there's a requirement in IEEE 603-1991, that there has to be a safety related manual ability to initiate the automatic protection systems.

One independent and diverse safety or non-safety is then needed per BTP 7-19, if the reactor protection systems manual initiation safety system would be subject to the postulated common cause failure.

So in other words, there would have to be two manual initiation methods. Now how do you get this down just to one? These two can be combined under the following conditions.

The reactor protection system manual initiation of the automated reactor protection system is independent and diverse from the automated protection system.

It has to be safety related and it has to be not subject to the same potential common cause failure as the automated reactor protection system. In that case then you can have one.

In case this may sound confusing this diagram should help make it clear. Notice on the one on the left you have a manual trip system that goes directly into the reactor protection system, into the electronics.

Both of these are a safety system, but you notice that if the, on the left if you have a common cause failure you won't be able trip the reactor with a manual trip.

You have to then have our requirements BTP 7-19 Rev 6, you have to have a diverse manual system as represented in the green. It can be non-safety.

On the right hand side, you notice that now is a completely independent and diverse manual trip that is safety related and comes down and blow and is not part of the common cause failure electronics.

MEMBER BROWN: Are you all going to put the picture in 7-19?

MR. EAGLE: No, we never did. That might be an interesting idea.

MEMBER BROWN: Can I request that?

MEMBER STETKAR: It might be a good annex or something, you know.

MEMBER BROWN: Go ahead.

MR. EAGLE: BTP 7-19 Rev 6 was sent out for public comments and there were something like 70 comments and there were a lot of the, were received from four sources.

Now NEI provided 90 percent of these comments, each with their basis and a suggested rewording. The public comments and the task working group response to each comment was documented in the spreadsheet and included in materials provided to the ACRS in advance.

Each comment was given careful consideration, a response was prepared to each comment and documented, and some of the notable comments are in this slide.

One of the things that got brought out, the staff agreed that not all reactor protection system safety functions may be disabled by a common cause failure, but pointed out that assuming that all reactor protection system functions are disabled is considered a worst case bounding condition.

The staff accepted the comment, expressing concern that after a actuation of the engineering safety feature functions from the main control room, the need may exist, and I repeat, may exist, for some use of local controls later.

And we discussed this a little bit earlier, like the realignment of equipment or perhaps after 72 hours before the action has to be taken in the passive plants.

There were many other items, but just to keep things short I just want to throw up a few examples. We also included some notable clarifications and a considerable amount of rewording to improve the English and improve the presentation and clarification.

A couple of interesting points was that the system level was changed to system or division level depending on the design.

Since single failures concurred with a common cause failure not required to be postulated, a normal equipment alignment is assumed, diverse actuation of one division is sufficient provided that that division will be in service.

Diverse design may need more than one division. Also, the use of the term "diverse backup method" was replaced with the words "diverse means" to match with the four-point D3 policy and because some current nuclear power plants portions termed primary and backup even in the main system.

A CCF that affects normal displays or

controls should not prevent an operator from manually initiating safety functions.

In summary, once again would like to mention that the guidance of ISG-02 Rev 2 was merged into the Standard Review Plan by incorporating ISG Rev 2 guidance into BTP 7-19 Rev 5 to create Rev 6.

This Rev is an extensive revision providing significant specific guidance for a number of stakeholder concerns. It addressed the seven questions and concerns that were presented.

It's hoped that we can issue this by November 30, and any additional advice, like Charlie said on the diagram, would be welcomed. I thank you for your attention today. Are there any questions?

MEMBER BROWN: I'm just going to look around. Are there any questions before, we have one other public comment that we were going to get to for a few minutes.

CHAIR ABDEL-KHALIK: Could you go to Slide 14, please?

MR. EAGLE: Okay.

CHAIR ABDEL-KHALIK: This 30 minutes deals with the margin, not the total time available, correct?

MR. EAGLE: It's the difference between

time available and time required.

CHAIR ABDEL-KHALIK: Right.

MR. EAGLE: I have a diagram. I wish I'd put that in here.

CHAIR ABDEL-KHALIK: I understand this. But isn't this a little too restrictive?

MR. STATTEL: It's just an example. It's just intended as an example, it's not really providing the direct guidance. The direct guidance is in the previous statement.

CHAIR ABDEL-KHALIK: So this particular 30 minutes statement is not going to be included?

MR. STATTEL: It is, this is a quote out of the BTP, the new revision.

CHAIR ABDEL-KHALIK: Right, so I mean it's there. I mean the fact that 30 minutes is used for a lot of other things.

(Crosstalk)

MR. STATTEL: Originally we had a 30-minute as a rule. Basically if it's less than 30 minutes do this, if it's more than 30 minutes do that.

CHAIR ABDEL-KHALIK: But that's related to the total time, not to the difference between the available and the time required.

MR. STATTEL: Yes.

MR. EAGLE: But once again, when we said 30 minutes, basically it's the time available. In other words, you're supposed to have an action take place.

So water levels dropping the BWR, all of sudden the automatic system detects it, said level 3, and it's supposed to start some kind of action. It doesn't happen because there's been a common cause failure.

Now something has got to be done. The clock is measured usually from the time that action should have taken by the automated system and now something has got to be done. That water level's dropping.

Something has to take care of that safety function or you're going to uncover the fuel. That's that time period that we looked at when we said the 30 minutes originally. But actually the difference is the real thing, it's being used here.

MR. PIERINGER: This is Paul Pieringer, Human Factors Reviewer. We use that 30 minutes only as a guideline, and that is because if the time between event initiation and the first manual action is less than 30 minutes that's a very critical period where diagnostics have to be evaluated, and we always provide a very detailed assessment of whether those actions are really feasible and whether they are reliable.

However, that doesn't address all of the critical actions. You could have a remote action that brings in a lot more variables that could be outside of the 30-minute window, and you would certainly want to look at those remote actions to make sure that communications and environmental factors, accessibility and all those other variables are addressed.

And then there's another category that deals with when the criteria are established for initiating the action occur versus when the operators take the action.

So example, here's safety injection. You don't get safety injections, tight conditions for safety injection until usually later in a scenario. Well, so the operator's working in there looking at many other things.

What we are sensitive to is, once he reaches those conditions and the alarms and controls indicate that they're there, then you have to look at whether the operator can still reliably take those actions regardless of whether it's 30 minutes or not from initiation time.

CHAIR ABDEL-KHALIK: All I'm saying is that if you read this statement, the available time is one hour and the operator is able to do this function in 30 minutes, you still are going to consider that something that needs further review.

MR. STATTEL: That's right.

MEMBER RAY: Let me ask before he steps away, supposing the diverse actuation has the horrendous consequences that John described awhile ago.

In fact, if you look at the stress levels on core support structure, for example, they're even more horrendous than that in my opinion. When you look at the reliability, the operator action, do you reflect on the reluctance that an operator might have to take that action?

MR. PIERINGER: Yes, sir.

MEMBER RAY: Okay.

MR. PIERINGER: In fact, a key consideration in some recent proposals that had operator reaction within two minutes of an event initiation, and it was presuming they were responding to a prompting alarm.

And my experience is that operators want to validate an alarm. They don't want to just react to the alarm coming in. And that reluctance to initiate the action was a key part of the logic in asking the applicant to redesign that particular part of the task.

MEMBER RAY: Yes, because, you know, the blowdown stresses in some of the core support structures, for example, says if I push this button I'm going to replace the core support structures, and that's a big event, bigger even than blowing off the steam generators. Okay.

MR. EAGLE: I think one of the key things about this is it's a warning. I think if you, any of you think of it, we talked about actions taking place and just in your imagination you imagine that, you know, if some action takes place and you have a difference of about 30 minutes here, that's a lot of time for maybe making decisions.

And part of this, by the way, in terming out the time required by the operator, includes in case he has to analyze it, he also, if he makes a mistake it has to recover from it.

So this is to give you a warning. As that narrows down, I think we're all concerned about, you know, what could be done and to the operator's actions, so the main thing this was put in for is to give a warning.

Whereas before, we did have a hard limit now we have a, basically this is just a warning. And also it gives an area that'll be more review if this difference is less than 30 minutes.

MEMBER BROWN: This was a fallout of a previous ACRS letter that we wrote back in September of 2007, and then was amplified in the ISG-5 review.

And so that the things that were changed, at John's request, was to make sure we reflected the uncertainty in the time available as opposed to appear to be just time required in the way they had initially written the thing.

CHAIR ABDEL-KHALIK: In the past, the 30 minutes pertained to the total time available.

MR. STATTEL: That's correct.

CHAIR ABDEL-KHALIK: And now this is put in as --

(Crosstalk)

MEMBER STETKAR: This is margin and uncertainty. I mean -

(Crosstalk)

MR. STATTEL: There's really not a direct correlation between the past rule and the, well, I shouldn't say rule, but the past requirement and this 30 minute mentioned.

I also want to put this into context. This is a direct quote out of the BTP, however, it is contained in a separate note under a subsection. And the subsection actually provides the guidance which is not shown on this slide here.

It is really just a note and it's only intended to be an example.

MEMBER BROWN: Well, it's there to kind of reflect what we had in ISG-5. I mean fundamentally, I mean it's to get that concept in.

MEMBER RAY: Well, Charlie, I just think that, I do, I'm, you know, a skeptic that somebody isn't going to want to pause and think a good long time before they take some of these -

MEMBER BROWN: I agree with you. I was hard over on even doing this, okay. I was beat to death. I come from the rule the 30 minutes was the minimum you had and you ought to make sure that larger times weren't required before you allowed this kind of stuff to go on.

MEMBER RAY: Between all the agonizing and -

MEMBER BROWN: Absolutely.

MEMBER RAY: -- is this really, really, really what I want to do.

MEMBER BROWN: That the committee made the statement, you know, four years ago that we really need to be more practical and that there are some operator actions that you can do in 30 seconds.

And as long as they're simple and straightforward we ought to allow those, okay, as opposed to limiting it to 30 minutes and whatever else you had to do. So I'll stop right there.

John, did you have anything else? Mike? Bill?

MEMBER REMPE: No.

MEMBER BROWN: I'd like to take a couple of minutes. Is Richard Wood still here? He's from O&R, excuse me, Oak Ridge National Labs. I apologize.

He's been the NUREG, originally 6306 involvement, 6303, I'm sorry, on diversity analyses and I guess there was a follow on NUREG 70, 70?

MR. WOOD: 7007.

MEMBER BROWN: 7007. And he wanted to make a couple of comments on the new NUREG. It's not out yet, I think.

MR. WOOD: No, it's my understanding it has been -

MEMBER BROWN: Oh, it has been issued?

MR. STATTEL: Yes, it is issued.

MEMBER BROWN: Okay.

MR. STATTEL: Okay, correct.

MR. WOOD: I'm Richard Wood from the Oak Ridge National Laboratory. And I had some brief observations and that I think lead to some questions that I trust that the Committee will consider as they finalize their evaluation of this document.

One of the key objectives of the Working Group 2 was to resolve the issue of what constitutes adequate diversity with the implied context that the need for diversity has been established through the Diversity and Defense-in-depth analysis.

And so that was discussed at length in the activities of the working group. And also concurrently, there was a research program that the Office of Nuclear Regulatory Research engaged in which led to NUREG-7007, which was released after the issuance of ISG-02.

So I understand that the purpose of Revision 6 of BTP 7-19 is to incorporate the positions embodied in ISG-02 and that appears to have been accomplished.

But I will note that subsequent to the

development of that document, there were these technical bases that were developed through the research program that are not addressed in the revision, specifically the diversity strategies that are embodied in Section 6 of NUREG/CR-7007, which identified means of resolving the vulnerabilities, postulated vulnerabilities of common cause failure.

And so the question that I think comes up is, is there a plan for Rev 7 of BTP 7-19 that will address the issue of what constitutes adequate diversity, and if the strategies that are identified in NUREG/CR-7007 are not quite adequate in the minds of the staff, are there activities planned to take those forward or a different approach so that the objective of TWG-2 can be completely resolved and those positions can be put in the branch technical position to address the issue of what constitutes adequate diversity?

And so that's all I had to say.

MR. JUNG: This is Ian Jung, and an issue came up during last year to development as well as the Subcommittee briefly, to establish that I think there's some value.

Anybody can use that. I mean the industry is given a document that can supplement the ISG-2 and

BTP Revision 6 that's coming out.

But NRR and licensing staff looked at that, and even the assumptions made and the data set that was used, essentially one of the key is to come up with a numerical value that says, oh, this is, one may, you know, degree of, you know, diversity is if you have certain numerical value based on a sample set of applications that's been used in nuclear power plants and the whole work in other industry.

I think there's value to it, yet the staff did not feel fully comfortable putting that out as one of the acceptable guidelines until we validate the methodology for one or two actual applications and see how it works out.

So we, right now the staff has decided to defer the endorsement of 7007 NUREG until we validate that through one of the applications or two applications.

If in the future as the applicant actually chooses to use that because it's going to be additional burden in addition to BTP 7 Version 19. So that's where we are and we'll evaluate that in the future to see whether that's a acceptable methodology to demonstrate adequate diversity.

In terms of adequate diversity, the way

that it was handled is all that the remaining guidelines in 14 in terms of just manual methods, the quality requirements, expectations in the Generic Letter 85-06, their quality provisions and degree of diversity in NUREG-6303, as a total staff felt that we have a viable method right now.

It's not easy, but viable method that's been done. So I think adequate diversity, we are using those guidance and use some engineering judgments to reach a safety findings right now. So I think more to come on that subject.

MR. WOOD: If I may, I just wanted to clarify that NUREG/CR-6707, the primary information in that deals with diversity strategies. And there's frequently a misconception that the tool which Ian refers to is the product.

The tool is a comparative analysis tool that's in an appendix, is the strategies that are identified in Chapter 6 that define a conservative basis for establishing adequate diversity.

And I would recommend that there be a new look at 7007 to look at the strategies rather than looking at the tool. And I do agree, the tool needs considerable more work to assess some of the subtleties that might not be accounted in the tool, but the strategies themselves are based on a very detailed analysis of the cause of common cause, the nature of common cause failure.

They deal with the purpose of an I&C system, the process for developing an I&C system, the product, which is the I&C system itself, and the performance of the I&C system.

So with the first two, the purpose and the product, you deal with the sources of common cause failure. With the product itself, you deal with the location of that vulnerability within the architecture of the system.

And with the third, the performance, you deal with the influences that trigger common cause failure from those vulnerabilities. So you're dealing with environmental influences, human interaction, internal states and the trajectory of signals that are introduced from the plant.

So it was a very thorough assessment and it was supplemented by a review of the techniques that are applied in other industries for addressing the issue of common cause failure, along with recent examples in the nuclear industry and international plants.

So there's a very solid technical basis

for those strategies. And I'm afraid we got so wrapped up in the tool that we lost sight of the strategies that are there that provide a very good basis for determining, is there adequate diversity in this proposal or not?

And so I am recommending that the Committee consider asking for a fresh look at those, and if they prove to be insufficient there should be additional work conducted to take them to the level that this goal can be achieved of defining what constitutes adequate diversity when diversity is required based on the Diversity and Defense-in-depth analysis.

So I agree with what Ian said, I just don't want us to lose, to throw the baby out with the bath. We don't need to wait until the tool, which is a comparative tool, is rigorously validated when we've got a very solid technical basis that's embodied in that document itself, in the main part of the document.

MEMBER BROWN: Okay.

MR. WOOD: Thank you.

MR. STATTEL: I would like to mention that the team that worked on this revision was very cognizant of the 7007 development and the guidance it provides.

We did consider it and we had considerable discussion on whether to incorporate that within this guide. As Ian stated, the staff decision was not to incorporate that here or to endorse it.

However, I'd also like to mention that we're not just keeping it on the shelf. In several of our reviews we have used the guidance from 7007, and made the determinations of how diverse the systems were.

We've used this for the Wolf Creek application, we've applied the methods for Oconee application, so we are gaining experience as we go forward with our reviews.

And I would hope that in a future revision of BTP 19 we would, in fact, endorse that NUREG.

MEMBER BROWN: Okay, if there's no more comments I want to thank you all for a lively Subcommittee meeting we had as well as a lively full Committee meeting, and thought you were presented a good case and thoughtful comments.

Thank you very much.

MR. STATTEL: Thank you.

MEMBER BROWN: I'm complete, pass it back to you, Mr. Chairman.

CHAIR ABDEL-KHALIK: Thank you. We are off the record at this time.

(Whereupon, the foregoing matter was concluded at 12:19 p.m.)

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

Presentation to ACRS
Standard Review Plan
Branch Technical Position 7-19 Revision 6

November 3, 2011

Richard Stattel, NRR/DE/EICB
Gene Eagle, NRO/DE/ICE2
Ian Jung, NRO/DE/ICE2
Russell Sydnor, RES/DE/DICB
Paul Pieringer, NRO/DCIP/COLP

BRANCH TECHNICAL POSITION (BTP) 7-19 Revision 6,
"GUIDANCE FOR EVALUATION OF DIVERSITY AND DEFENSE-IN-DEPTH IN DIGITAL COMPUTER-BASED INSTRUMENTATION AND CONTROL SYSTEMS"

PURPOSE OF THIS BRIEFING:

Highlight and identify the key elements from incorporating DI&C-ISG-02 Revision 2 into BTP 7-19 Revision 5 to form Revision 6, and the action items from the ACRS I&C subcommittee presentation

Current Status of BTP 7-19, Revision 6:

-Received OMB approval as "non-major rule" , (Congressional Review Act)

-Presented to ACRS I&C Subcommittee Sept. 07, 2011

- Expected to be issued by November 30, 2011

Agenda

1. Purpose and General Basis of BTP 7-19 Revision 6
2. Background
3. NRC Four-Point Policy on Defense-in-Depth and Diversity (D3)
4. Comments on NRC Four-Point Policy on D3
5. Independence of the Diverse Means
6. Automated verses Manual Diverse Means
7. Component verses System Level Actuation
8. Spurious Actuation
9. Combining Two Manual Initiation Systems
10. Public Comments and Staff Response
11. Notable Clarifications in BTP 7-19 Revision 6
12. Summary and Questions

<u>Purpose and General Basis for BTP 7-19</u>

- Purpose: Assure adequate D3 and provide guidance for evaluating applicant's D3 assessment and D3 design
- Software-based digital systems are considered susceptible to the same software error appearing in identical copies of the software-based logic or architecture that are present in redundant divisions of safety-related systems
- Therefore, software-based or software-logic-based digital system development errors are a credible source for a potential common-cause failure (CCF)
  - ****
- ***In summary, while the NRC staff considers (software) CCF in digital systems to be beyond design basis, nuclear power plants should be protected against the effects of anticipated operational occurrences (AOOs) and postulated accidents with a concurrent CCF in the digital protection system***

Background

- DI&C-ISG-02 Revision 2 (currently effective) was issued in June 2009 considering ACRS comments as:
  - ISG will help licensing review
  - The staff should determine the conditions under which operator manual actions can be credited as a diverse protective function
  - The issue of spurious actuation needed to be examined further
- Decision made to merge DI&C-ISG-02 Revision 2 into NUREG -0800 (the Standard Review Plan) by incorporating DI&C-ISG-02 Revision 2 into BTP 7-19 Revision 5 to create **BTP 7-19 Revision 6** (main reason for Revision 6)
- 70 public comments received and addressed
- Presentation to ACRS Digital I&C Systems Subcommittee Sept. 07, 2011
  - Minor revision to “Note” using Mr. Stetkar’s (ACRS) suggestion

<u>NRC Four-Point Policy on D3</u>

[from SRM on SECY-93-087 in Item 18, II.Q]

1. “The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed.”

2. “In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) <u>using best-estimate methods</u>. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.”

<u>NRC Four-Point Policy on D3 (cont)</u>

[from SRM on SECY-93-087 in Item 18, II.Q]

3. "If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. <u>The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions</u>"

4. "A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above."

<u>Comments on NRC Four-Point Policy on D3</u>

Concerning Point 2

- The term “best-estimate methods” is more accurately referred to as <u>“realistic assumptions”</u> – defined as normal plant conditions corresponding to the event:
  - Power levels, temperatures, pressures, flows, and equipment alignment
  - This revision only clarified intended existing scope
  - It was not intended to expand or re-define scope
- The “corresponding to the event” phrase was added to emphasize that some analyzed events at worst conditions may occur at power levels other than the power range (i.e. zero power; see BTP 7-19 Revision 6, Section B.1.4)
- Events from Safety Analysis Report (Chapter 15) as specified by **<u>Point 2</u>** must be addressed

Comments on NRC Four-Point Policy on D3

Concerning Point 3:

- If D3 analysis indicates potential for CCF, Point 3 directs applicant to identify or add a diverse means to perform either the same function or a different function
- The phrase “Safety Computer System identified in items 1 and 3 above” from Point 4 clearly indicates primary application is to the automated safety–related reactor trip system (RTS) and the engineered safety features actuation system (ESFAS)
- Point 3 also applies to manual initiation methods for the reactor protection system (RPS) if subject to the CCF [Note: RPS includes RTS and ESFAS]
- Diverse means may be accomplished by automated, manual, or a combination of these for initiating mitigating function

Comments on NRC Four-Point Policy on D3

Concerning Point 4

- Directs providing <u>a set of displays and controls </u>(safety or non-safety) in main control room (MCR) independent and diverse from any CCF vulnerability in RTS or ESFAS and at division/system level
- For control and management of "(plant) critical safety functions" [From NUREG-0737, Supplement 1] Reactivity Control, Reactor core cooling and heat removal from primary system, Reactor coolant system integrity, Radioactivity control, Containment conditions
- If not subject to CCF, some of these displays and manual controls may be credited as all or part of diverse means directed by Point 3
- For digital modifications in operating plants, retention of existing controls in MCR <u>may</u> help satisfy Point 4
- Once manual actuation from MCR using Point 4 controls is completed, controls outside MCR may be used for long-term (and/or perhaps short-term situations) management when supported by suitable HFE analysis and procedures

Independence of the Diverse Means

- Independence requirements of diverse means from safety protection system (i.e., physical and electrical) are defined in IEEE Std. 603 and communication separation in DI&C-ISG-04
- Diverse means could be safety-related and part of a safety division, and would be subject to meeting divisional independence requirements
- Diverse means could be non-safety-related; then the IEEE Std. 603 requirement to separate safety from non-safety equipment would still apply and would require independence of the two systems
- In either case, the diverse means should be independent of the safety system such that a CCF of the safety system would not affect the diverse system

Automated vs. Manual Diverse Means

Clarification when operator action is acceptable as a diverse means to address a potential CCF

•Perform a D3 analysis of RPS using realistic assumptions

•If subject to potential CCF, need a *diverse* means to perform the safety function subject to the CCF

•Diverse means may be *automated or manual*

•Automated diverse means is preferred

•If manual means is selected as diverse means, acceptability is based on HFE analysis

Special Note on Manual Action in Diverse Means

"As the difference between Time Available and Time Required for operator action decreases, uncertainty in the estimate of both of these times must be evaluated carefully. These uncertainties could invalidate or reduce the level of assurance of a conclusion that operators can perform the action reliably within the time available. For actions with a limited margin of time to act, such as less than 30 minutes between the Time Available and the Time Required, additional staff review will be performed."

Component vs. System Level Actuation

- Diverse means performed on a *system-level* basis for *each division* in accordance with the policy in SECY 93-087 SRM
- Does not prohibit use of manual controls to operate individual safety system components after the safety system function actuates
  - Depends on type of function and specific design objective
  - Some actuations go to completion (e.g. reactor trip or containment isolation)
  - Some actuations start safety function and may then need manual action to complete (e.g. controlling vessel levels)
- Potential for CCF in digital safety systems should be considered in new plants and in upgrades to existing plants (backfit of current NPP equipment is not intended)

Spurious Actuation

- Two types of CCF associated spurious activation
  - I. Caused by CCF in automated RPS
  - II. Caused by the Diverse Means

Spurious Actuation

- (I) Spurious actuation caused by CCF in automated RPS
  - Spurious RPS actuation is a lesser safety concern than failure to actuate because challenges presented by spurious actuations are not considered to be as significant as failures to respond to AOOs and DBEs
  - Further, spurious actuations are annunciated and thereby immediately detected
  - Assuming a postulated CCF in automated RPS and related displays, operators still have the (diverse and independent) Point 4 displays and controls and/or Point 3 diverse means that can be expected to detect the spurious actuation
  - Spurious actuations that could challenge barriers to release of radioactivity typically are addressed in the plant licensing basis (e.g., over-pressurization of PWR primary coolant system caused by spurious actuation of high pressure safety injection system)
  - Therefore, spurious actuations of safety-related digital protection system resulting from CCF do not need to be addressed beyond what is already set forth in plant design basis evaluations

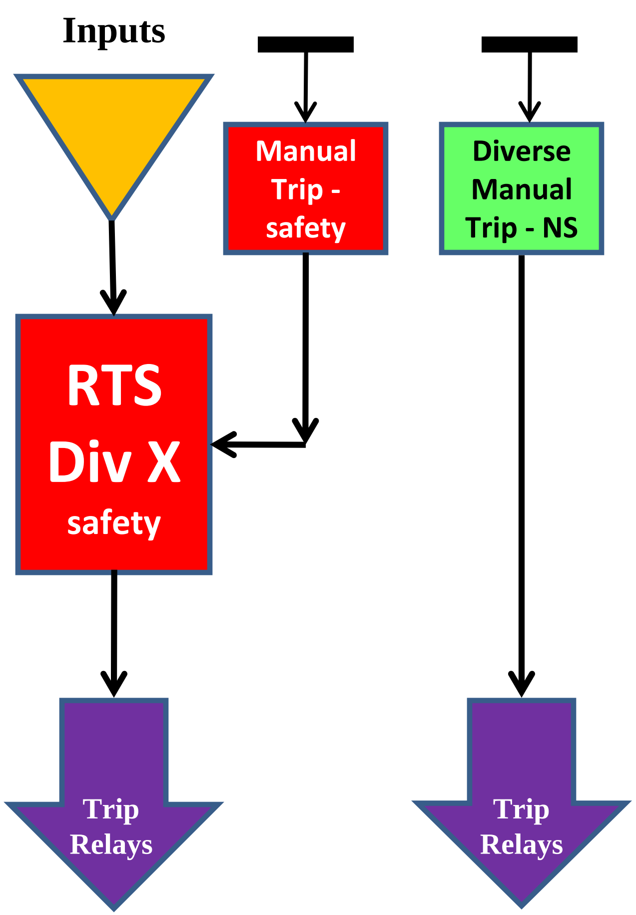
Spurious Actuation

- (II) Spurious actuation caused by the Diverse Means
  - Design of diverse automated or diverse manual means should address how to minimize the potential for spurious actuation of the RPS caused by the diverse means

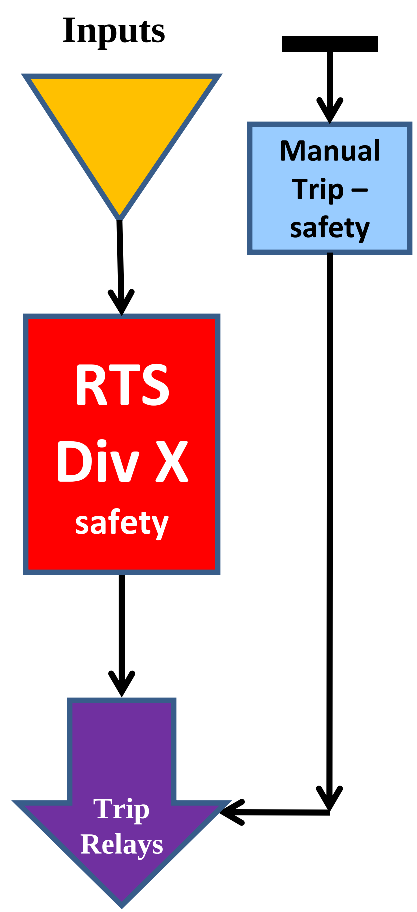
Combining two Manual Initiations

- Two manual initiation systems may be needed
  - One ***required*** by IEEE Std. 603-1991 (safety-related)
  - One independent and diverse (safety or non-safety) needed per BTP 7-19, ***IF*** RPS manual initiation safety system subject to the postulated CCF
- Two manual actuation systems may be combined if:
  - RPS manual initiation of the automated RPS is independent and diverse from automated RPS
  - Safety-related
  - Not subject to same potential CCF as automated RPS

Two Manual Initiations Means Needed



Only One Manual Initiation Means Needed



Notable Public Comments and Staff Response

- In some instances comments led to additional clarification for clearer understanding and improved explanation
- Staff agreed with some comments in principle , but not with the specific rewording recommendations. Staff addressed theses comments based on principle or accepted portion
- Staff agreed that not all RPS safety functions may be disabled by a CCF, but pointed out that assuming all RPS functions are disabled is considered a worst case bounding condition
- Staff accepted a comment expressing concern that after actuation of ESF functions from the MCR, the need may exist for some use of local controls later (e.g., re-align equipment , manual override failures, 72+ hours after event)

Notable Clarifications in BTP 7-19 Rev 6

- Based on ACRS letter on RG 1.62, *Manual Initiation of Protective Actions*, “system level" was changed to "system or division level (depending on the design)”
- Since single failures concurrent with a CCF are not required to be postulated and normal equipment alignment is assumed, diverse actuation of one division is sufficient provided that division will be in service, i.e. diverse design may need more than one division
- The use of the term “diverse backup method” was replaced with “diverse means” to match with the Four-Point D3 Policy and because some current NPP RPS portions termed “primary” and “backup”
- A CCF that affects normal displays or controls should not prevent an operator from manually initiating safety functions

BTP 7-19 Revision 6

Summary

- Again, the current interim staff guidance in DI&C-ISG-02, Revision 2 was merged into the Standard Review Plan by incorporating DI&C-ISG-02, Revision 2, guidance into BTP 7-19 Revision 5 as Revision 6
- Revision 6 of BTP 7-19 is an extensive revision providing significant specific guidance for a number of stakeholder concerns
- Revision 6 of BTP 7-19 is expected to be issued by November 30, 2011
- ACRS review and advice of this revision are appreciated

Questions?

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

ACRS Full Committee
Power Uprates

NRC Staff Review
Nine Mile Point, Unit 2
Extended Power Uprate

November 3, 2011

Introduction

Rich Guzman

Senior Project Manager

Division of Operating Reactor Licensing

Office of Nuclear Reactor Regulation

Introduction

- Objective
- Background
    - NMPNS EPU Application – May 27, 2009
    - 3467 to 3988 MWt, 15 % increase (521 MWt)
    - 20 % increase above original licensed thermal power
- NRC staff effort
    - Pre-application review and public meetings
    - Acceptance Review
    - Requests for additional information
- EPU Implementation

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

Topics for Full Committee

- NMPNS EPU Overview
- Anticipated Transient without Scram and Stability
- Fuel Methods - IMLTR
- Materials and Mechanical & Civil Engineering
- Steam Dryer Analysis
- Review of open items / Conclusions