From:	Jain, Bhagwat
To:	tgurdziel@twcny.rr.com
Cc:	Screnci, Diane; Chairman Resource; John.Esberg@constellation.com; "Fellows, David E:(Exelon Nuclear)"; Bridget Frymire; Tim Echols; Johnston, Jeanne; Umana, Jessica; Marshall, Michael
Subject:	RE: Digital I & C: February 15, 2022 Meeting Comments
Date:	Monday, March 14, 2022 6:44:34 AM

Dear Mr. Gurdziel,

The USNRC staff would like to thank you for your interest and participation in potential expansion of Common Cause Failure policy to allow risk-informed alternatives. We regret you had trouble in un-muting your telephone during the public meeting. The staff value your participation and is considering your feedback in the development of its SECY paper.

Thank you,

Bhagwat Jain
Senior Project Manager

Plant Licensing Branch IV
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation
US Nuclear Regulatory Commission

301-415-6303

From: tgurdziel@twcny.rr.com <tgurdziel@twcny.rr.com>
Sent: Tuesday, February 15, 2022 10:39 PM
To: Jain, Bhagwat <Bhagwat.Jain@nrc.gov>; Marshall, Michael <Michael.Marshall@nrc.gov>
Cc: Screnci, Diane <Diane.Screnci@nrc.gov>; Chairman Resource <Chairman.Resource@nrc.gov>; John.Esberg@constellation.com; 'Fellows, David E:(Exelon Nuclear)' <David.Fellows@constellation.com>; Bridget Frymire <bridget.frymire@dps.ny.gov>; Tim Echols <techols@psc.ga.gov>
Subject: [External_Sender] Digital I & C: February 15, 2022 Meeting Comments

Hello,

I took the afternoon off from work to attend this meeting. Since I do not have a microphone or a camera hooked up to the computer, I used my telephone so that I would have the capability to ask questions or make comments (I thought.) Initially I was told that my telephone was put on mute but that I could take it off mute by pushing “pound” “ 6 “. At 2:25 pm Eastern time, I attempted to ask a question about the Consequence Calculation which was on Slide 5 of the INL presentation. I tried a few times but could not get through.

Ten or more years ago, during a meeting, the NRC would have a telephone operator who would ask if anyone on the line wanted to speak, then take their name and then announce them and connect them. Could we try doing something like that that did work in the past instead of doing something to save money but doesn't work?

OK, now let's make some comments.

One

First off, I appreciate that this meeting was held AND, as best I could determine, it was held with an open mind on the part of the NRC staff participants. (I hope that is the case.) And it was very helpful to me to have an explanation of what is a "SECY" and what is a "SRM".

Two

Although I have heard it said, (in Commission meetings over the past few years on digital I & C), that the original digital I & C guidance provided from way back in the 1990s does not need to be changed, I think it does need to be changed. Think about it, where are we today with usable digital I & C for existing, commercial, nuclear plants? We are just about no place. Take a look at my non-analog heart monitor. Do you think it would be here in service if the manufacturer was held to 1990s-established requirements? I don't.

So I think the comment here is that we cannot predict what is necessary or, perhaps, what is most effective in the future. In other words, the use of rigid Rules in a fast-changing environment guarantees failure (in my opinion.) I heard you say the same thing with these (approximate) words: "new risk tools don't meet old requirements".

Three

I don't like the way you, (the US NRC), work today. Everything is "consensus"

this and “consensus” that. This method DOES NOT work when you are in a hurry, (which you should be in). You need ONE person in charge and that person must be held accountable for necessary decisions and progress or must be replaced. There is not another way. And this brings me to the mentioned IAP or the “Integrated Action Plan”. Isn’t this the Victor McCree-clearly-thought-out-process to rejuvenate the digital I & C effort that the designated participants decided to stop doing?

Four

I think Slide 17 was mentioned with low probability – high consequence events. But, aside from hearing those particular words at the meeting, I do not recall any explanation of how such events are to be handled. So let me give a little explanation of how low probability – high consequence evens were handled while doing PRAs in the 1990s. (I worked on PRAs for two plants. Both are still operating today, but certainly not because I worked on their PRAs.) If an event was expected to happen very infrequently, it was just discarded. But, being nuclear, we didn’t say we threw it out. No, we said that it was “screened out”. And this, in my recollection, was the widespread industry practice.

So, if we want to be consistent in treating digital I & C studies with PRA studies (from years ago), we would not worry about anything less than about 1 times 10 to the minus 7.

Incidentally, I recall Dr. George Apostolakis giving a RIC presentation when he was an NRC Commissioner, saying that the occurrence of a tsunami should have been able to have been identified for the Tokyo Electric Power Company Fukushima Dai ichi plants. I do not recall him mentioning what that probability was, though.

As I think about it today, isn’t accepting some disastrous event up to a selected chance of occurrence actually accepting risk? And this was even before anybody started taking about accepting more risk!

Five

Probably this is a good time to reference Kenny Scarlotta's comment, made at 1:48 pm Eastern time, that establishing bounds on your software reliability to use with your risk model does not seem likely in his opinion. Why not? There is, in my opinion, a great need to do this because, if the number established is lower than the value above (in Four), then it could be "screened out" and that would be the end of what to me appears to be the biggest barrier to digital I & C progress that we have right now.

Oh. And let me tell you how that could be done. As a last resort, assemble a group of experts in the field in question and have them decide. Use that until you get something better. I believe this is an old PRA trick.

Six

This is just a little out of order. How are you going to use the wealth of experience and knowledge available on the ACRS? Here is how they are used right now. You get to a certain point and feel obligated to bring it to the ACRS. They make comments. You don't accept any of them. Life goes on.

You need to think about getting their thoughts earlier in the process. Then see how you might be able to satisfy their concerns and yours as well. But, still, in the end, you are responsible for choosing what to keep and what to delete.

Seven

I wanted to get more information about slide 25 of the staff presentation but it was not shown by them. However, it was included on Slide 5 of the INL presentation. This is when I wanted to unmute my telephone and talk, but could not. Anyway, as I see it, the Accept Category with a dose increase at the site boundary, (I expect), means reactor core meltdown. This means we are finally accepting risk, not just talking about it. I don't see why you don't just specify a probability of occurrence of a core melt down (that would be acceptable)?

In my opinion, if the core starts to melt, you had better just expect that it is all going to melt. So that 10% dose increase will only be with you for a short period of time as it continues to go up.

Eight

At about 2:54 pm Eastern time there was a question about the need for reliability goals. This is an excellent question. How long do we need these systems to work? If the reactor trip system is necessary for, say, 15 seconds at most, should we even bother to worry about its reliability? How about the other systems, how long do we need them? I would expect there is a lot of cost associated with these studies of reliability that probably are not needed if we discover single failures ahead of time and have alternate systems that will get the same desired result, not to mention human, licensed, knowledgeable operators and their licensed supervisors.

To be clear, I am saying that it does not seem necessary to have reliability goals or reliability studies if we have redundancy and defense in depth already.

Nine

If the V & V cost of a software system is 8 times the cost of building the software, why do I care? Why do you care? That, in aggregate, is the cost of your control system for that plant. It is a cost of building an operable plant. Why is it necessary to spread out the cost over multiple plants? Do you think any cost savings is going to be passed onto the purchaser by the designer?

The financial cost accounting I heard during the meeting on this topic is, in my mind, completely wrong and a barrier to progress.

Ten

Finally, it was appropriate to hear an industry veteran state a clear fact: in 30 years we have gotten nowhere.

Thank you,

Tom Gurdziel