



UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

September 30, 2008

MEMORANDUM TO: ACRS Members

FROM: Christina Antonescu, Senior Staff Engineer/**RA**
Reactor Safety Branch B, ACRS

SUBJECT: CERTIFICATION OF THE MINUTES OF THE MEETING OF THE ACRS
SUBCOMMITTEE ON DIGITAL INSTRUMENTATION AND CONTROL
SYSTEMS, MARCH 20, 2008—ROCKVILLE, MARYLAND

The minutes of the subject meeting were certified on September 16, 2008, as the official record of the proceedings of that meeting. A copy of the certified minutes is attached.

Attachment: As stated (Draft)

cc w/o att.: E. Hackett
A. Dias
C. Santos
S. Duraiswamy

cc: w/att.: J. Delgado
N. Mitchell-Funderburk

MEETING MINUTES
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
MEETING OF THE ACRS SUBCOMMITTEE ON
DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS
MARCH 20, 2008—ROCKVILLE, MARYLAND

INTRODUCTION

The Advisory Committee on Reactor Safeguards (ACRS) Subcommittee on Digital Instrumentation and Control (I&C) Systems held a meeting on March 20, 2008, at the headquarters of the U.S. Nuclear Regulatory Commission (NRC) in the Commission Hearing Room, 11545 Rockville Pike, Rockville, MD. The purpose of this meeting was to review issues related to DI&C Systems used in nuclear power plants. Mr. Girija Shukla was the designated federal official for this meeting. The subcommittee received no written statements or requests for time to make oral statements from the public. The subcommittee chairman convened the meeting at 8:30 a.m. on March 20, 2008, and adjourned at 4:30 p.m.

ATTENDEES

ACRS Members

G. Apostolakis, Subcommittee Chairman	J. Sieber, Member
D. Bley, Member	J. Stetkar, Member
M. Hecht, Consultant	

ACRS Staff

G. Shukla, Designated Federal Official
C. Antonescu, Cognizant Engineer

Principal NRC Speakers and Consultants

M. Waterman, RES	S. Arndt, NRR	C. Doutt, NRR
J. Grobe, NRR	W. Kemper, NRR	G. Kelly, NRR
S. Bailey, NRR	P. Loeser, NRR	M. Gareri, NRO

Principal Industry Speakers

R. Torok, EPRI	B. Geddes, Southern Engineering Service	
G. Clefton, NEI	W. Bowers, Exelon	D. Blanchard, AREI

Other members of the public attended this meeting. A complete list of attendees is in the ACRS office file and is available upon request. The presentation slides and handouts used during the meeting are attached to the office copy of these minutes.

OPENING REMARKS BY CHAIRMAN APOSTOLAKIS

Dr. George E. Apostolakis, Chairman of the ACRS Subcommittee on DI&C Systems, convened the meeting at 8:30 a.m. Chairman Apostolakis stated that the purpose of this meeting was to discuss NRC staff and industry activities for DI&C systems. Specifically, the subcommittee was to discuss three new interim staff guidance (ISG) documents issued by the NRC staff to address issues on cyber-security, on the review of new reactor DI&C probabilistic risk assessments (PRA), and on the DI&C licensing process. The staff also was to discuss progress associated with the operational experience review and digital categorization update. In addition, the staff was to make a presentation on the assessment of operating experience in nuclear and other industries to obtain insights regarding potential failure modes to be used for inventory and classification of Digital Instrumentation and Control (DI&C) in nuclear power plants.

DISCUSSION OF AGENDA ITEMS

NRC Staff Activities Regarding Digital Instrumentation and Control Systems

Presentation on Digital Instrumentation and Control Steering Committee Activities

Stew Bailey, the new chair of the Digital I&C Steering Committee, made a brief presentation on the structure of the steering committee and the task working groups (TWGs). In early 2007, the steering committee was generated along with six task working groups. These working groups were set up to address areas that have been identified as needing prompt attention to address issues related to DI&C.

The steering committee has had a lot of support from industry in addressing technical issues in preparation for new reactors that will be using DI&C extensively and for existing reactors seeking to do retrofits because of obsolescence. As a result, technical issues were identified and task working groups were set up to address these technical issues.

Since 2007, the staff has had 15 public meetings of the TWGs to address various technical and process issues. They also had three (3) public steering committee meetings.

In addition, a new TWG was generated for the fuel cycle facilities.

The staff has issued three ISGs on cyber-security, on the review of new reactor DI&C probabilistic risk assessments which are in concurrence, and on the DI&C licensing process.

The steering committee is still working to finalize several ISGs that will be completed in the near term, including an ISG on the licensing process and one on operator actions. In October 2008, the staff will issue the ISG on fuel cycle facilities. In February 2009, the staff will revise the licensing process ISG to include issues related to cyber-security. Also, there may be other subsequent revisions to the licensing process as these other TWGs finish up the results of those task groups. These revisions could affect licensing and other documentation. The NRC's staff review would be factored into the licensing process ISG.

The staff has been getting industry feedback at many levels, and has incorporated and revised the ISGs as appropriate so that everything is to be incorporated into the regulatory infrastructure. Overall the staff is planning to retire direction provided in ISGs by putting it into the regulatory infrastructure and using the standard processes.

In addition, the staff is currently working on a **tracking system** to make sure that everything is done correctly, as some of these actions will likely still be on-going when the staff retires the steering committee. Thus the staff wants to make sure that they have the appropriate tracking mechanisms for that.

Chairman Apostolakis wanted to know what is meant by "interim," and how long was that supposed to be. The staff responded that the ISG is a vehicle to allow the staff to quickly get out positions on important technical issues to the industry. The staff is considering updates to the Standard Review Plan (SRP), NUREGs, and other agency documents within the next couple of years. At that point the staff will be retiring the ISGs.

In addition, the ISG was created and used in a number of different offices for different purposes. In some cases, the agency depended on interim guidance for an extended period of time, maybe as long as a decade. Again, after a while, the staff will be integrating this guidance into the normal infrastructure and will eliminate the ISG. Specifically the ISGs will be rolled into either a revision to the SRP issuance or updated in a regulatory guide, or, in other cases, ISGs will be incorporated into revisions to industry standards, e.g., IEEE standards. This will be accomplished over the next several years. But the goal is to get the ISGs into the formal infrastructure as rapidly as possible.

Chairman Apostolakis also wanted to know what kinds of reviews ISG documents get (e.g., by the ACRS, CRGR, and industry). The staff answered that externally these ISGs have gone through at least two review drafts. ISGs are discussed publicly with the industry and comments have been obtained from them. Internally these documents are concurred with by all the TWG members, which represent multiple offices. At a minimum, the Office of Reactor Regulation (NRO), the Office of Research (RES), and the Office of Nuclear Reactor Regulation (NRR) concur on ISG before issue. During their review, the staff incorporate and consider industry comments, some in writing, before issuing ISGs. Also, there is substantial value gained from dialogues with the DI&C Subcommittee of the ACRS regarding these ISGs. The industry has provided the NRC staff with four (4) reports on topical areas, including minimum inventory of human system interfaces, computerized procedures and implementation guidance for those procedures, and guidance on manual operation actors and common-cause failure applicability, which assisted in the NRC's decision-making in developing ISGs and ultimately assisted with updates to other NRC documentation. In some cases the staff gets extensive interaction with vendors of new reactor designs, such as Mitsubishi, and with the reactor operators. So, typically, a public steering committee meeting might have 25 or 30 representatives of the various different industries. The TWG meetings are on a more technical level. The challenge is to get an industry position, because different components of industry have different needs and perspectives, and many of them compete with each other.

Member Bley asked if the staff is getting participation also from operators, engineering and maintenance personnel. Mr. Grobe answered that currently they have under review two (2) fairly substantial operating reactor license amendments, one for Oconee and another for Wolf Creek. Oconee is in-house, and the staff just started their review of an extensive application to retrofit the reactor protection system (RPS) and the engineered safety features actuation (ESFA) system with digital. Wolf Creek also has an application in-house to replace the main steam feed isolation system (SFIS) with a digital upgrade. Thus the staff has interactions with the engineering organizations and has input on the issues that affect the operators.

Member Stetkar followed up with a question on how much interaction the staff had with the international community on their operating experience in I&C systems. Mr. Grobe responded that the NRC had an extensive variety of international interactions, including specific topic focus meetings and site visits. Other members of the staff have attended professional meetings or international professional meetings. About six or eight months ago, the staff provided the ACRS with a compendium of such interactions. Also, in recent months, there has been an additional level of interaction. One of the interactions is the multinational design evaluation program (MDEP) on AP1000 reactors and on the EPR. The staff is looking at leveraging international engineering activities so that they can be more efficient in the review of

those two designs, which include digital controls. Also, about six months ago, the staff hosted a meeting on common cause failure, at which seven countries participated.

Member Sieber asked if the staff was making an attempt to have an international consensus standard for computers, data processing, or DI&C. He argued that since there are so many branches in the standard-setting organizations, achieving some kind of consensus could be helpful when buying designs that originate outside the United States.

Mr. Grobe responded that as part of the MDEP initiative, the staff is going try to get the international standard-setting organizations, whether ASME, different organizations in Europe and Japan, or other standard-setting organizations, to try to define a standard for a certain particular attribute, identify the differences, and try to see if a consensus could be developed, which might take many years. This particularly affects component manufacturers. United States reactors require ASME code compliance, whereas French reactors and Japanese reactors use a different code. Now that component manufacturing has become global, it would be much more efficient to have an international set of standards. The challenges that the staff is going to have are whether designs used in operating reactors in the United States meet our standards.

However, the immediate goal of the DI&C Steering Committee does not include international standardization. That is a long-term project and a long-term activity. Another staff member added that the NRC actively participates in both U.S. and international standard-setting bodies like the IEC, which has NRC representation. The IEC has a special section for nuclear I&C. The NRC staff also occasionally participates in the OECD and IAEA bodies. These bodies do not set standards, but set criteria and try and bring things into standardization. As part of Chairman Diaz's vision to integrate standards internationally, the staff started this effort a decade ago and prepared to have international standards for the new reactors that they are hoping to build over the next several years. The standards could be part of the MDEP for the next generation of reactors. The staff does not anticipate that standards will be in place for this generation of reactors.

Member Sieber asked if the staff anticipates any required rulemaking. Mr. Bailey responded that at least one rulemaking is going to be needed related to cyber-security.

Presentation on Interim Staff Guidance on Cyber-Security

Mr. Gareri, Office of Nuclear Material Safety and Safeguard (NMSS) (supporting NSIR), from the staff gave a presentation on the background regarding what actually occurred before the ISG on cyber-security was issued, the actual ISG and the status. This ISG was developed to provide clarification on cyber-security guidance as it relates specifically to DI&C safety systems. It was not intended as guidance to cover the entire cyber-security program such as the staff is trying to develop right now during the rulemaking. The specific task for the TWG was to address issues and concerns relating to possible inconsistencies and conflicts within two specific documents: Regulatory Guide 1.152 Rev. 2 and NEI 04-04 Rev. 1.

The staff continued with the presentation on how the staff developed a gap analysis to determine what the possible inconsistencies and conflicts may have been between the two documents, RG 1.152 and NEI 04-04. Through that gap analysis, the staff found that there were no real inconsistency conflicts because each document served a different purpose. The two documents were actually complimentary to one another. The industry committed to revising NEI 04-04 Rev. 1 to fill some of those gaps and differences that the staff found from an examination of Regulatory Guide 1.152 so that they could actually cover the same criteria in NEI 04-04 Rev. 2 and use that in lieu of the regulatory guide itself.

Also the staff went over an example of how the cross-correlation table is structured so that it maps the criteria from the regulatory guide to the NEI 04-04 Rev. 2 document. The staff can find a specific section in the Regulatory Guide and then find the matching section within NEI 04-04, Rev. 2. The reviewer will be able to see if the provided direction is consistent and complete.

Chairman Apostolakis asked what kinds of threats the staff was talking about. Mr. Gareri responded that the issue is not directed at threats or cyber-security as a threat assessment. The industry felt that the two documents, Regulatory Guide 1.152, Rev. 2, which has cyber-security criteria in it for safety systems, and the industry guidance document, NEI 04-04, Rev. 1, which was endorsed by the NRC and which addresses cyber-security as a programmatic approach, had inconsistencies and conflicts. Chairman Apostolakis followed up asking what sort of threat the staff is trying to protect I&C system from. Mr. Gareri answered that from a design aspect, the staff is trying to prevent possible bugs while software is developed. From a programmatic approach, the staff is trying to prevent attackers from the outside getting into the systems through a cyber attack, the Internet.

Consultant Hecht followed up that a definition of cyber-security would be very useful and that there is need for a definition of what cyber-security is. Consultant Hecht feels that a threat assessment and a vulnerability assessment is needed in a cyber-security guide. Also, consultant Hecht commented that it appears that the staff is dealing primarily with access control, not with authentication and not with logging and other aspects in auditing, which are the other aspects of general computer security.

Consultant Hecht's opinion was that coming up with good guidance on the structured process and access control needs to be covered, and it might not be a public threat assessment—it might be classified. The staff answered that a threat assessment has been developed in a NUREG and its sought security-related information. It is also addressed in the NEI 04-04 document, because the scope of this TWG was very limited, it was not to address cyber-security as a whole.

In addition, the draft guide DG-5022 that is being developed now in the Office of Nuclear Security & Incident Response (NSIR) and the Office of Research (RES) will cover other threats that are addressed in other documents. In particular, the staff is going to develop a specific ISG for cyber-security licensing criteria. But that information will be put into the ISG for the licensing guidelines. Mr. Hecht also pointed out that staff needs to be clear regarding what the differences between these two documents are and how they fit together.

Member Bley wanted to know how the regulatory guide or ISG would fit within that regulatory framework. The staff answered that the ISG basically gives background on cyber-security as a whole. The two documents will provide clarification on how exactly these documents are to be used. It has a correlation table attached to it so that if you use NEI 04-04, Rev. 2, in lieu of Regulatory Guide 1.152, you can look at this correlation table and discover where the criteria from the Regulatory Guide are found in the NEI document. So it makes it easier to review or to be able to make a determination if it is actually covered in that document. Basically, the industry revised NEI 04-04, Rev. 1, to capture the criteria within Regulatory Guide 1.152. The staff worked together with the various offices and with industry, had a lot of public meetings and interaction, and comments were considered and incorporated when possible.

The cross-correlation table itself was developed mainly to be able to map the criteria from RG 1.152 to NEI 04-04, Rev. 2. Training was provided to the staff in an ISG workshop. The ISG is basically to clarify the cyber-security guidance as it relates specifically to the safety systems.

Another staff member, **Mr. Kemper**, stated that Regulatory Guide 1.152 is a licensing document, and the staff uses it to license new digital processes from a security standpoint. NEI

04-04, Rev. 2, is a programmatic document, but it did not necessarily cover all of the licensing aspects for new or modified systems. So the task was to compare the two documents and then embed the licensing aspects of information within NEI 04-04. So now the industry can in fact use the NEI 04-04 document to make submittals for all aspects of cyber-security.

Mr. Bowers has been involved as an industry representative with the TWG on cyber-security. He answered a couple of the questions related to NEI 04-04, Rev. 2, that cover nuclear-significant systems, which include safety related, important to safety, security, and emergency response. The safety systems which include safety support systems or auxiliary supporting features are all those under 10 CFR 50 Appendix B, QA program. Cybersecurity in NEI 04-04, Rev. 2, is much broader than the limited scope of safety-system equipment.

Mr. Bowers continued to address member Bley's comment that the programmatic things in NEI 04-04, Rev. 2, are much broader than the limited scope of what is in Regulatory Guide 1.152. Regulatory Guide 1.152 endorses IEEE 7.4.3.2, which is only for applications of digital equipment to safety systems.

Member Stetkar pointed out that in NEI 04-04, Rev. 2, there is a reliance on the Probabilistic Risk Assessment (PRA) to identify systems important to safety, important functions, and so forth. One thing to keep in mind is to identify those systems important to safety from the perspective of the instrumentation and control (I&C) systems. Also another thing to keep in mind is that traditionally I&C systems in PRAs have been modeled at a very high and simplistic level. When one does a detailed fire analysis where one is worried about fires either failing particular signals or initiating other, spurious signals, one often needs to add a lot of detail to the PRA to capture those impacts. Thus if you rely solely on existing, simplified PRAs to identify important interactions between I&C signals and other systems, you may not capture the full range of things, because the PRA is probably not developed to a sufficient level of detail. On the one hand, the PRA should be relied on because it is useful. On the other hand, if you go through the details, there is a lack of sensitivity to interfaces between DI&C systems and support systems.

Consultant Hecht discussed one technique which is used to diagnose dependencies among plant infrastructure services. NEI 04-04, Rev. 2, speaks about a concept called the critical digital asset (CDA) that is related to controlling, in this case, safety systems. Also those CDAs depend on the infrastructure, depend on power, HVAC, a number of other things, and maintenance. These types of things can be identified through this dependency analysis as a technique. And perhaps that should be more closely reflected in staff guidance.

Chairman Apostolakis asked if this ISG on cyber-security will come before the full committee and the Committee will write a letter. Mr. Grobe answered that it will be coming before the ACRS in probably the context of the regulatory guide necessary to implement the proposed 10 CFR 73.55 (m) rule. Specifically, there is a regulatory guide being developed that is a companion to the new proposed rule 10 CFR 73.55 (m) that will come to the ACRS in the development of the regulatory guide, which is scheduled for June 2008.

Chairman Apostolakis wanted to know if the ISGs were part of the regulatory guide infrastructure. The staff answered that the ISGs do not come before the full committee. The ISGs will be incorporated into some form of formal regulatory infrastructure, whether an RG, SRP, or a NUREG, which will come to the full Committee for consideration. However, the Committee wrote a letter that said that they looked at three ISGs that the staff had previously briefed the Committee on and they were comfortable with the issuance and use of those ISGs. The arrangement was that the staff would brief the Committee on a regular basis on the status of various things that either had recently been finished or would recently be available, and the Committee would provide input on the acceptability of that guidance and any additional recommendations for future work. Also, in a letter that the Committee wrote in November 2007,

they endorsed the issuance of the three ISGs and provided additional guidance on areas that the staff might want to look at before they made them a formal document. The Committee will be expected to continue to do this. However, the ACRS's procedures do not require a letter for ISG.

Mr. Scott Morris, the Deputy Director for Reactor Security and a member of the I&C steering committee, offered further insight on the cyber-security ISG. The staff does not anticipate this ISG will have a lifespan beyond the end of this year, because the separate regulatory guide that they are writing to support the proposed rulemaking in Part 73, which is the new programmatic requirements for cyber-security, has been developed and has been through several levels of staff review. By the end of March 2008, it should be out on the street for the stakeholders to comment. It will capture the whole range of cyber-security from a programmatic standpoint, and it will include some of these specific issues from the standpoint of licensing safety-related systems.

Chairman Apostolakis also wanted to know when would be a good time for ACRS to review the document. The staff is planning to put the draft guide out for a 45-day comment period. They are going to meet with the industry at least once and fold-in the industry comments probably by the end of May through June 2008. However, the regulatory guide itself will not go final probably until the rule is in effect early next year in 2009. Another staff member, Mr. Kemper, commented that ACRS would have the opportunity to review the draft regulatory guide before it goes out for public comments. Typically however, ACRS declines and waits until the public comments are received and incorporated. In addition, Mr. Morris added that this will be the NRC's own guidance, but the industry has also asked if the staff would include an endorsement of the latest version of NEI 04-04 as part of the guidance. So rather than just one option, which would be the staff methodology, the industry has asked about putting two options in the Regulatory Guide to also include NEI 04-04, Rev. 2.

Presentation Interim Staff Guidance on the Digital I&C Licensing Process

The staff made a presentation on the process for licensing of digital systems and on what documentation needs to be issued and needs to be submitted by the licensees or the vendors. The Standard Review Plan (SRP), Chapter 7 (NUREG-0800), provides the review procedures for the staff when reviewing any DI&C and the branch technical position, BTP-14 that goes specifically into software. In addition, when the staff does these reviews, they not only depend on testing, but they also depend on a well-defined life cycle and a high-quality process. The reason for this is the end product of a digital system is very complex, and the staff cannot just review the code and see if it is good, because it is too much to review. The staff depends upon the licensee and the V&V team to do the detailed review, and the staff will sample this.

Generally the staff takes a look at a typical waterfall life cycle as defined in IEEE-1074-1997 Software Life Cycle. They look at the concepts, the requirements, the design, the implementation, the tests, and they check out the installation, acceptance testing, the various inputs that go into these life cycles, the outputs, and the processes. In a typical review, the staff will look at the system specification and at how that system's specification is translated into a hardware and software specification. Also, they look at the design procedures and the V&V program that are used to verify and validate those design procedures. The staff reviews any information that may be available on hardware and software history. Under specific plant applications, they do a thread audit where they sample various plant parameters or select various plant parameters and also walk through the development process of how that particular parameter works. They look at the coding standards that were used. Then they also look at the hardware/software systems, they look for interfaces and timing problems, etc. During thread

audits, they may pick out (looking at a very small sample, looking at the process that was used for the licensee to do it) half a dozen out of 8,000 different specifications.

The real problem is that the review takes a significant amount of documentation. The question is, does the staff really need all of this? The licensees would prefer to submit less. So the TWG looked at several different things. One is level of detail. How much detail do they need? What is the application of the SRP, Chapter 7 (NUREG-0800), in digital reviews? The staff needs some clear protocols for developing this application and clear guidance for licensing on cyber-security.

The aim is to look to see that the process does these things. The method of review asks the following four (4) questions:

- 1) What's going to be done? They look at the various plans that are going to be used. What planning documents are being used for the configuration management? What's being done for software quality assurance? How is V&V being handled?
- 2) How will it be done? What method will be used? The staff reviews how the plans and procedures are implemented.
- 3) Was it done correctly? This they do in two steps: (a) They look at the procedures, the methods that are going to be used, and they see if using those procedures will actually accomplish the concepts within the plan. (b) During the thread audit, they look at what was actually done, then they take these sample parameters and go through them and see that the various processes were actually used and used correctly.
- 4) And what were the results? They look at the final results such as test results and the V&V report to assure themselves that the overall specification items have in fact been met.

The working group tried to come up with a listing and a reason for the documentation that needs to be delivered to the staff. Considerations include the phase at which this licensee documentation is needed, and the question of which documentation needs to be on the docket and which does not, but should instead be available for the staff during an audit visit.

The staff had considerable input from industry. They have come up with a draft version of the ISG. This staff guidance is based, so far, on the most complex review. That is a new platform and a new application and at the moment is only applicable to existing plants. The staff is planning to expand this later to cover new plants. But the process is somewhat different.

These guidelines do not modify or exceed the existing regulations. The staff has been using the branch technical position, BTP-14. The staff has divided up the review into licensing and operational issues; software maintenance planning and the software training planning that are considered operational issues.

Some of the basic approaches the staff assumed is that by the time they get a license amendment request, the planning stage of the modifications have already been done. The specification V&V plan has already been written. Also, the software quality assurance (QA) plan has already been written too, and all of these planning documents will be available at the time of submittal.

They may not have finished the final design yet, may not have finished all of their V&V, and they may not have done any of the detailed design yet at this point, but the staff expects that the design documentation should be available sometime in the neighborhood of six months after they do the acceptance review, and this is somewhat negotiable, depending on the review schedule.

The staff does not need some of the detailed design documents, for example individual code listings and individual schematics, as long as they are available onsite when they go to the vendor site to do the thread audit. And of course some of them, like installation testing, cannot be done prior to the staff review. The staff cannot possibly complete the installation testing

before their approval. That has to be available for the regional staff review for startup testing or whatever the regional staff looks at.

The ISG also specifically looks at the information needed for an acceptance review. And when the staff does an acceptance review, they have to see that there is enough information available, that the system is planned well enough, and that they see a clear path to success and acceptance. For example, if they are not planning on doing V&V, the staff cannot accept that, so they will not even accept it for review. If there are other problems, they may not accept it either for review.

Generally they look at the system specifications, the system requirements, the system description down to a block diagram level, hardware and software, dedication, whether they are using commercial parts or commercial systems, and the commercial grade dedication plan. Then, the V&V planning, quality assurance, and defense-in-depth are all quite important. The staff expects to see those up front.

Member Bley wanted to know when the staff is doing the V&V, do they look to make sure that the systems perform the way they ought to and, if there is any testing to look for, what happens with these systems if inputs drift outside of the normally expected range? The staff answered not only do they look outside of normal range, but if communications between one software unit passing of parameters goes out of whack for some reason, they make sure that the various units are compatible and look at the timing analysis that was done on the hardware, and also they may trace things through the schematics. They are doing this on a very small percentage of the overall system. They are taking five or maybe ten individual specification items out of thousands. They are looking at a sample to make sure that they have reasonable assurance that the V&V team and the plant and the vendor did all of these things. If they start finding problems with it, then of course they would go into much deeper detail and potentially turn down the application. What they are really looking for is the process that was used by the V&V people and by the licensee to assure them that they did this on everything, because they do not have time to do it all unless they had lots of reviewers for years.

Member Bley was concerned how the process works after the initial approval such that if software patches and software changes are made, do they get a thorough V&V and how is that change monitored after the initial installation?

What the staff is looking at during the initial review is what the configuration control process will be, the vendor who is likely to be doing the software changes, what level of regression testing is required, what level of V&V is required, how do they control their configuration at the plant, how do they know that what they are receiving as a change is in fact appropriate and has been appropriately tested as part of their approval. Also, the changes that are made at a later date are no longer in the licensing process, are now in the maintenance phase, and are handled by the Regions. The staff makes sure the planning is correct, but the Region and local inspectors make sure the performance is correct. Most of these changes are done under 10 CFR 50.59. If a change were such that it invalidated the assumptions by which the Safety Evaluation Report (SER) was approved in, then that would require a re-submittal to the NRC to be re-reviewed.

Member Bley was concerned that when software upgrades come out, they will be applied across the board or are they likely to be plant specific or even plant-system specific?

At this time the staff thinks that software upgrades are very likely to be plant specific when individual plants are making individual changes. For example, Oconee is replacing their entire RPS and ESF systems. Wolf Creek is only replacing their main steam isolation system. Thus somebody may use the same platform that Oconee is using, the TELEPERM XS, but have different kinds of changes they are making, apply them to different safety functions, fewer or more, and therefore a code change may not be appropriate. Only if the change were in the

operating system would it probably be applicable to everyone. But if the change were in the application specifically, it would be by plant unless there happened to be two plants that were sufficiently identical and they were using the same application code.

Chairman Apostolakis commented that there has been quite a lot of work that the agency has sponsored at Brookhaven National Lab (BNL) and Ohio State University under the umbrella of developing PRA methods for software. He believes staff effort has been spent on developing methods for identifying failure modes. Also the drawbacks of these methods are that they are very labor intensive, because they model specific systems and a lot of time is invested to develop a particular model that will allow identifying failure modes. Also, Chairman Apostolakis asked if the staff finds these methods useful to them.

As far as the staff is concerned the methods are useful for general information to make them more aware of problems and things to look for. But with the specificity needed for specific plant or vendor reviews, it has not gotten to the point yet where the staff can actually incorporate these lessons into their review guidance. Also, there are some efforts going on at the University of Virginia and the University of Maryland for things like fault injection and classification that the staff hopes to use. However, it has not gotten to the point yet where they can actually use the results of these efforts. In addition, the staff in the Office of Research (RES) has acquired some of the systems which the staff has also approved, a Tricon system, for example, or a TELEPERM to investigate the design details, how it works and how specifically software works to try to develop better models. The staff explained that the fault injection project is on-going down at the University of Virginia, which RES is still managing. NRR and NRO are looking forward to RES useful results to use in licensing new applications and to identify reliability and to be able to assess empirically rather than just estimating.

Chairman Apostolakis clarified that there are two parts to it. One is the identification of failure modes and the other is the reliability. Some members of this Committee have had serious doubts about the reliability part. But the failure modes work is very useful and ultimately Dr. Apostolakis thinks that the staff will have a number of tools.

Consultant Hecht was not clear as to what the scope of the staff's activities is. One part is verifying if the process (i.e., the plan) is in conformance with IEEE-1074. Another part is how they might do their plan, and the last part was testing oriented toward failure modes. In particular, he wanted to know if the scope of the staff's activities says not only that they did testing, but also what techniques were used and whether those techniques were adequate. The staff answered that they have to make sure that the testing is adequate. For example, there is a different level of testing. There is a unit testing where they start putting the software together. Also, there is integration testing where they integrate it in with the hardware. Then there is the factory acceptance test where you are looking if the system overall meets specifications. Thus different levels of tests are trying to perform different things. However, first they look at the test plan to make sure that they are planning to do all the things they say they would. Then they look at the procedures to see if these procedures prove what the plan says it is supposed to do. Then during the thread audit they look at how it was tested, what were the test results, the particular test sequence, and what was done and who signed it off. In some cases, if the equipment is still there, they may ask them to repeat one of the tests. Also, they have to tailor it each time in accordance with what the system is, what it is supposed to do and what the testing philosophy of the plant is. Are they doing all this manually? Are they using a software tool to do all the testing? Does the software tool actually perform the testing that they want it to? These are all decisions that have to be made. This is not an easy thing for a staff reviewer to do. It takes a lot of experience and knowledge.

Consultant Hecht clarified his question. If a licensee were to present the staff with a plan that they were going to do fault injection or that did not have fault injection testing in the

plan and the staff felt on the basis of the results and work done by Research that fault injection testing should be in there, does NRR staff have the authority to say we think that you should do this and include that?

The staff further confirmed that they are not allowed to tell the licensee exactly what they ought to be doing. The staff judges what the licensee is doing. The staff is telling them their overall expectations and what the end result needs to be and then they look at what the licensee does to see if they have reached that end result. The staff cannot be prescriptive on exactly what tests they want them to do. Further, the testing techniques are not prescribed by the staff, but are recommended, and it is really at the discretion of the licensee.

Also if the licensee follows a particular standard and the staff thinks that the standard is good enough, then the staff will propose a method. But the staff cannot tell the licensee that if they do not use this standard, they will not approve it. The staff has to look at whatever the licensee did do and then determine if they reached an equivalent level of safety, an equivalent level of protection. And if they did, the staff will approve it. If for some reason they did not, then the staff has to look at what possible compensating measures were done, then reach this determination.

And the goal of this ISG is to provide a predictable level of review consistent with the standards of the RGs and the SRP and of what documentation the staff expects to review and how they expect to perform audits. The component that has not yet been defined well is the inspection piece in the field once the equipment has begun to be installed and before it goes into operation.

What the staff is planning to do is use this draft ISG in the Oconee review and later come back to the subcommittee and describe how that is going and what the staff is finding and develop reasonable assurance.

Member Sieber asked if the staff has given any thoughts to certified designs. The staff responded that they have reviewed three of them so far: Triconex PLC triple redundant, TELEPERM XS, and Westinghouse Common Q have been approved. When the staff does a review now, they would only look at the plant specific application and anything that may have been changed in the design. As an example, the TELEPERM XS is using a different microprocessor than the one they originally reviewed, which is a different board. So the staff would have to look at the temperature, humidity, and EMI qualifications if it changed, if they have used the same design process, and if they have used the same V&V process. Also, the staff would not go back to review something that has already been reviewed. They do not have the time or the people. In addition, the design team will also look at all the interfaces, make sure that any timing changes have been accounted for any differences in signal trajectory have been taken care of.

Member Bley also wanted to know if the RGs, the SRPs, the BTs distinguish between initial V&V and V&V on upgrades. The staff answered that they did not account for this presently.

Consultant Hecht wanted to know more about a document entitled "Documents Needed for Reviews of Different Complexities," and how it is used.

The staff answered that Table 1 shows the review criteria, where they show the applicable SRP sections, what the requirements or the standards that are associated with these particular documents are and how the requirements are met or referenced in the license amendment request. And then columns 4 through 7 show at what stage the staff expects to have this document—whether it is with the original review—with the original submittal, whether it is supplied later on during the process of the review, whether it is available for audit, or available onsite for the region. The document has actually three (3) tables. One of them shows a digital platform that was previously reviewed and is being used in the same format as was reviewed.

There have not been any changes to the basic platform, but the application that it is being used in is new. So it is plant specific, in which case the staff would not look at any, just the application and the manner in which the application software was developed. Attachment 2 shows where the staff has a previously reviewed an application, but they have made some changes to it. An example of this is the Oconee review that the staff is doing at the moment where they have made some changes. Only the items that have changed will require a review. The things that are still the same, like the process documentation, does not have to be re-reviewed. Attachment 3 shows a new application with a new platform. They have not seen any of it before so they basically have to review everything.

Also the staff has a pilot project going on where the staff is trying to look at the possibility of having fewer things initially docketed. The pilot is being used now with Oconee.

Member Bley wanted to know what criteria would lead the staff to decide what goes on the docket and what does not. Does it affect the requirements of what people have to do, to make the change if the document is on the docket? The staff has talked about documentation that they need to review to reach a determination of reasonable confidence. They do not need all the design details. They probably need some of the procedures and some of the tests and are still working their way through it. The staff has gotten about eight or ten of the major documents on the docket so far from Oconee. Also, there are going to be things that they do not initially ask for that they are going to need. The list may be very different for different reviews of different complexities and different scope.

Member Stetkar wanted to know if the staff had any interaction with international regulatory agencies to see what types of reviews and audits they have been doing or have done since they have already implemented some.

The staff response is that there is a difference between the review strategies and the final results between the Finn's review of the TSX and the French review of TSX where the Finns were significantly more strict. The staff got a briefing a couple of days ago or last week from the Germans on what they consider are some of the requirements for safety systems, and it is quite different from the NRC's.

Also the staff found that the difference in the regulatory infrastructure that exists between the various countries' regulatory processes lends itself to quite a bit of variability in what they actually reviewed and the level of reviews. For example, Electricity de France (EDF) serves the French regulatory agency, and GRS advises the German regulatory agency. The NRC does most of that stuff themselves and the NRC uses their own internal Office of Research for some of those things. So it really makes for a complex issue trying to read some kind of continuity into what is reviewed and the timing for the reviews and the level of detail that the staff needs.

Presentation on New Reactor Digital I&C PRAs

The staff presented the background on the Task 3 Working Group "New Reactor Digital I&C PRAs". The NRC and industry currently are using a deterministic approach for handling the review of DI&C systems to determine if they are acceptable. This has turned out to be very resource intensive. Also the Commission has indicated that it wanted the staff to evaluate to what extent it can risk-inform the process. Thus the staff is seeking to provide early on better guidance for how to perform risk assessments for new reactors in the area of DI&C. The staff has been told following the June 7, 2007, Commission meeting with the ACRS and the Staff Requirements Memorandum (SRM) dated June 22, 2007, that they should be looking at operating experience and taking that into account in what they have been doing.

In looking at risk-informing DI&C, there are a number of significant challenges that the staff looked forward to overcoming over time. One of them is the lack of consensus about how to perform modeling of DI&C systems, in particular the common-cause failures.

There is a lack of robust data from the staff's standpoint about DI&C systems faults and common cause failures (CCFs). Part of this is due to the fact that software keeps changing and so you do not have a long track record. Also, we have a lot of different applications being used, and with each different application we have the potential for different CCFs. Therefore, it is not clear that we can lump together lots of different applications and say this provides us with a good data source about common cause failures.

Thus the staff has uncertainties associated with modeling of reliability of the systems. There are some issues once we perform the additional I&C risk assessment to include it with the rest of the PRA and determine what to do with it.

Also the Commission wants the staff to use the process of risk-informed decision that is laid out in Regulatory Guide 1.174, the five principles, and some of the other guidance.

The purpose of the working group was to evaluate the feasibility of risk-informing digital system evaluation with the intent of improving the effectiveness and efficiency of digital system review by taking into account those five principles of risk-informed decision-making, including adequate defense-in-depth and diversity when implementing a digital system either as a retrofit or a new reactor installation, from Regulatory Guide 1.174. The staff clarified that the purpose of the working group was to evaluate the feasibility, given where the staff is with modeling and data, that we can evaluate at a high level the DI&C systems and get a general overall appreciation of the level of risk that is associated with it, given the assumptions that are made about the data failure rates.

The staff had quite a few public meetings. They have worked with industry attempting to really deal with this issue. The industry provided the staff with white papers and the staff had a lot of different discussions on things that the staff can do.

The TWG identified three (3) major issues and these became problem statements 1, 2, and 3. The **first problem statement** is to clarify how to do the reviews of new reactor DI&C PRAs by using previous NRC licensing experience. Specifically, it clarifies how to use current methods to model DI&C for Part 52 PRAs. The issues include addressing CCF modeling and uncertainty analysis associated with DI&C. The **second problem statement** states where possible, use risk-insights to improve operating reactor DI&C review. And the **third problem statement** issue is to see if you need to enhance the state-of-the-art so that a comprehensive, risk-informed decision-making process for licensing DI&C systems can be performed.

The scope of problem statement #1 is to provide ISG on how the NRC should review future DI&C PRAs including software and CCF for new reactors by not substituting the NRC regulations and by not modifying the deterministic review performed under SRP Chapter 7. The ISG outlines various attributes and risk insights to help a reviewer identify, at high level, any potential risk-significant problems in a DI&C implementation. Also it provides guidelines for DI&C PRA review for situations where either detailed or limited review is required.

In conclusion of the staff presentation, the DI&C PRAs can provide some risk insights with significant modeling and data uncertainty because of lack of robust data. All this reinforces the need for independence, defense-in-depth, diversity, and redundancy. The risk-informed regulation decision to reduce or eliminate plant prevention and mitigation features such as Diverse Actuation System (DAS) is a concern for the staff.

Member Stetkar asked the staff to identify the fundamental differences between the DI&C system and a traditional analog I&C system, and how the approach for modeling those things would differ in a PRA. In particular, having modeled analog I&C systems for 25 years, most of the problems in digital are precisely analogous in the analog system-modeling world.

The staff answered that the challenges are that the failure modes are potentially significantly different; for the software, which has different kinds of failure modes, the challenges are associated with identifying failure modes; issues associated with hardware/software interface; and both internal and external timing issues on how to interface with the different systems. Also from a reliability modeling standpoint for analog systems there is a fairly well established theoretical basis in reliability analysis. However in terms of software-driven systems, there is a significant amount of debate as to whether or not we can even analyze digital systems in a way that we can decompose software and hardware, and that the hardware/software interfaces can be separated into components, whether or not it makes sense to do that, or if we have to do a more system-based analytical process.

Member Stekar clarified that what is unique to DI&C systems is software and its failure modes, in particular about the problems in DI&C PRA. What is not known is how to do a reliability assessment of software that is equally split with the hardware part of it, which can be wired together and can face the same problems that analog systems do and that are not modeled very well.

Also **Member Stetkar** pointed out that without a detailed review of the models, if somebody presents to us a PRA that includes DI&C systems and it has not addressed a comprehensive treatment of the possible failure modes, it is deficient because there are interactions between hardware and software.

Chairman Apostolakis recommendation to the staff on this ISG is that in order to ensure risk contributions from DI&C, including software that are reflected adequately in the overall plant risk results, the staff should rearrange and delete some of the 14 review guide steps.

Presentation on Industry Comments on ISGs

The overview slide summarized what was already covered in a number of the topics on the TWGs earlier. The position of the industry on this ISG is to work closely with the NRC. There was cooperation between the interface of the industry and the staff members at TWG meetings, telephone conferences, webcasts, and other associated methods.

The industry benefitted by having the NRC come to NEI to work together. There are seven **(7)** TWGs. The industry is pleased to see the nuclear fuel cycle one added to the list. The steering committee has been very effective. In the short term they are looking at the ISG and they expect those to finish out this year. In the long term, they are hoping that they will have quality final staff guidance out there. The expectation is that the ISGs will be revised and enhanced as they go along. Lessons learned with the pilot projects is that more information needs to be gathered by reports and white papers so that ISGs are in as a good form as they can be before they roll into the final guidance documents, Standard Review Plan (SRP), the regulatory guides (RGs), etc.

Also, the industry would like the NRC to endorse some of their industry guidance documents that would allow the industry to have more details as technology improves. For example, the new plan for TWG, ISG #5 on human factors, is to have some details into the industry documents, as happened with NEI 04-04, Rev. 2, which was enhanced to match up with the RG 1.152 and fill in the gaps. The industry would like to encourage that in the future as well.

Gordon Clepton, NEI ran through the seven ISGs, that is, the TWG items starting with the cyber-security one discussed earlier in the day. This ISG #1 was issued in December 2007. In general the industry did not have any issues, and they are looking forward to the support and review comments on the documents that are coming out.

The defense-in-depth ISG #2 was issued initially in September 2007. Industry has been working closely with the staff to enhance that. They have recently submitted white papers and they have some points that they are still working with the staff on in clarifying their joint understanding of the BTP 7-19, Point 4 (system-level vs. component-level). The diverse actuation system is an issue that is heavily under discussion, too. The industry and the NRC have TWG meetings almost every week. They also have scheduled a combined effort of TWG # 2 and # 3, which is their D3 group and their risk reliability, risk-informing organization. The communication ISG # 4 that was issued in September 2007 has some minor editorial issues of consistency, which are in progress. The ISG # 5 is the human factors. It was issued in September 2007. The issue resolutions are in progress. The industry and the NRC had recently an all-day public meeting at NEI with industry working on minimum inventory and computerized procedures, and on the methods for acceptable evaluations to determine manual operator actions and the time periods associated with it. The number of people supporting it, including the industry, is a list of 150 people that includes everybody from operators to managers and vendors from Westinghouse, Areva, and General Electric. The ISG # 6 is the licensing process. It was issued in April 2008. The issue resolutions are in progress that will have a pilot plant benchmarking. But it also wraps in communications and in cyber-security. The one it does not do currently is the risk or the ISG # 7, which is for fuel aspects.

Chairman Apostolakis wanted to know what combined operating licenses (COLs) means. The industry spokesperson answered that they are focusing on the 10 CFR 52 type plant applications rather than existing plants right now.

Member Stetkar wanted to know more about a pilot plant project, a risk application. The industry spokesperson answered that the Duke Oconee pilot project is principally to support the ISG supporting TWG ISG #6 for licensing process.

The ISG #6 is where they have the pilot project. The License Amendment Request (LAR) from Oconee was submitted on the 31st of January. The industry thinks they had good success with the steering committee members from the industry side as well as the NRC side, and are working together. Because the regulatory uncertainty has been significant in the past and it still exists, the industry wants to see that this is handled as professionally as possible.

The ISG # 7 on nuclear fuel facilities is a late start. The industry is working with Dave Rahn, NMSS staff, to refine the problem statements. The meetings are also bringing in the vendors. They are anxious to put digital applications into the fuel cycle with the safety aspects. NEI is working actively to ensure that those steps are made with the input of the major vendors and our fuel supply channels. In cooperation with industry and the NRC, they are putting together identified issues that occurred. They started with an inventory of over 500 issues. And what EPRI and supporting contracting companies, and TWGs have done is to refine the analysis and the evaluation of the operating experience.

Industry Review of Operational Experience (OE)

The industry presented their on-going project looking at operating experience of digital systems in U.S. nuclear plants. The main industry presenter was R. Torok, EPRI, and co-presenters were Bruce Geddes from Southern Engineering Services, who is the principal investigator for this EPRI project, and Dave Blanchard from AREI, who has been a consultant for the industry in dealing with the evaluations.

The industry briefly explained the basis of the investigation they did and what they did with the data to bin the various events. Also the basic findings and conclusions were discussed along with some interesting observations that are useful in terms of generating insights. This is industry's first attempt to answer the simple question: What is the OE trying to tell us? The

industry has looked and has evaluated 322 “digital events” over a period of about 20 years, both safety and non-safety, by evaluating NRC and INPO databases. Now, of these 322, about half of them were also on a list that was developed by Office of Research staff over a number of years.

The focus today is on defense-in-depth and diversity (D3) and specifically on actual and potential common-cause failures (CCFs) and safety functions (Class 1E systems). This work is important as the ACRS asked in their May 18, 2007, ACRS letter:

- “The staff should evaluate the operating experience ... to obtain insights regarding potential failure modes.”
- “The information ... should be used in the development of regulatory guidance on defense in depth and diversity for DI&C systems.”

There were no actual CCF events that disabled a safety function, and non-software issues dominated potential CCF events. Out of six system-level potential CCFs, one involved a software design defect. Lifecycle management and human performance issues were more prevalent, e.g., incorrect setpoints and parameters.

Current methods for protecting against software CCFs have proven effective by the use of software codes and standards, and design and process features and characteristics that preclude, avoid, or limit CCFs (defensive measures).

Industry’s current methods have been effective in keeping software a minor contributor to potential CCFs. The recommendations were to encourage additional OE investigations with other countries and industries (to confirm U.S. results) and to analyze for risk significance and other insights. Secondly, refocus D3 guidance by endorsing methods that have proven effective in protecting against software CCFs and establish more balanced treatment of software and non-software CCF sources. Additional insights and lessons learned by the industry are:

- Non-software issues made up the majority of both 1E and non-1E digital system events.
- In non-1E systems, software changes were commonly used as corrective actions for non-software problems.
- Discovered events that confirmed effectiveness of signal and functional diversity in protecting against CCF.
- Discovered no events that indicated platform diversity would be effective in improving CCF protection.
- Discovered many events where defensive measures were deployed to prevent recurrence, and there were no repeat occurrences.
- None of the potential CCF events were safety significant.

Presentation on Operational Experience Review and Digital Categorization Update

The staff presentation was on the review of operational experience (OpE) to obtain insights regarding potential failure modes, how they are developing an inventory, and how they are doing the classification of digital systems and using the assessment to develop diversity strategies.

The staff started developing their diversity strategies in September of 2006, and then, on the basis of a Commission meeting and some other recommendations, they formed a steering committee in 2007. The steering committee then formed a TWG to develop, among other things, diversity and defense-in-depth strategies. In the summer of 2007, the staff presented the approach that they were going to take. After the staff discussions with ACRS DI&C subcommittee, they wanted to develop some diversity strategies so they could answer the question of how much diversity is enough. The staff has seven issues in the TWG ISG # 2, six

of which are related to the need for diversity. Thus the staff research was supposed to answer the question about what is meant by diversity.

During this meeting, **Chairman Apostolakis** pointed out if the staff is going to develop diversity strategies, they also ought to know what the failures are so that the strategies address the most common failures that the staff agrees with.

Furthermore when you have a diversity strategy, you must be sure that it is going to work with the type of system that you are going to apply it to. So you have to go out and classify your systems somehow.

Thus the staff went out and looked at a lot of different sources of data. There are some sources of data that they have yet to acquire. The staff has looked at the NRC operating event report database. They have looked at a common cause failure database and analysis system, the one that was developed by Idaho National Lab. This database used to be called the NPRDS. Also, the staff gathered the Institute for Nuclear Power Operations Equipment Performance Information Exchange (INPO EPIX) data. The Organization for Economic Co-Operation and Development (OECD) out of Halden has the COMPSIS Project, the Computer-Based Systems Important to Safety, gathering all kinds of data from various countries, because no one country has a lot of digital failure data, so the staff is trying to gather it from all over the world and put that into a database. The staff talked a little bit about the quality of those databases.

The staff also has the INPO Equipment Performance Information Exchange database. It is part of developing diversity strategies, and it is part of their emerging technologies program. Oak Ridge National Laboratory (ORNL) is also taking a look at the various operating experience of nuclear and non-nuclear sources. Also the staff has gotten the NEI/EPRI review that will come out sometime later this year. The staff looked at other sources of data with the Department of Defense (DOD), which was very reluctant to talk about failures in their defense systems. The staff is trying to figure out a way to get that. In addition, the staff was trying to acquire some more detailed NASA data. Consultant Hecht also pointed out that NASA has a publicly available lessons-learned information website: NASA.PBMA.

Specifically, the staff found during the assessment that detailed root cause information on DI&C failures is difficult to obtain because of the unwillingness of end users to participate in a data collection effort, which impeded gathering sufficiently detailed information, and because the failure reports do not note specific software failure and are insufficient for developing diversity strategies. Also the failures were reported at high level as "Software failed" or "System reset." Few details on cause of failures like design or function errors were available. In addition, the short lifetime of each generation of digital equipment limits the base of experience available for diagnosing model-specific failures and can lead to systems consisting of different generations of equipment and software. Thus, the staff assessment of DI&C failure data and operating experience indicates that available, high-quality data are limited.

The staff future activities are to obtain more detailed information from OpE reviews to obtain more detailed information on the NUREG/CR-6303, "Method for Performing Diversity and Defense- Depth Analysis of Reactor Protection Systems," diversity attributes and associated attribute criteria to be addressed in proposed diversity. By March 31, 2008, develop an inventory of existing and new digital systems and structure to align with the system classification method. In addition the staff will identify diversity strategies consistent with failure modes and system classification.

Additional Information was provided to the Subcommittee by the Staff (after the meeting as follow-Up):

- (1) Industry White Paper on Common Cause Failure Applicability (ML080700390)
- (2) System Inventory and Classification Structure (ML080590383)
- (3) Assessment of Digital System Operating Experience Data and System Inventory and Classification Structure (ML080590323)
- (4) Industry paper on operating experience (to be provided when available by the industry)
- (5) ORNL diversity NUREG/CR report titled "Technical Review Guidance and Acceptance Criteria: Diversity Strategies for Avoiding Common-Cause Failures in Instrumentation and Control Systems at Nuclear Power Plants." (This ORNL research effort is to establish technical review guidance and associated acceptance criteria for use by regulatory staff in confirming that appropriate mitigating diversity strategies are employed to adequately address potential common-cause failure vulnerabilities in I&C systems. This report will be available to ACRS sometime this summer).

SUBCOMMITTEE DECISIONS AND ACTIONS

Overall, the subcommittee was pleased with the staff's progress on the ISGs to review anticipated near-term licensing actions on DI&C. The members were also encouraged by the degree of collaboration between the staff and industry regarding the ISGs.

In particular, the ISG on cyber-security will clarify the staff's guidance regarding the implementation of cyber-security requirements and will facilitate the licensing process when NEI 04-04, Revision 2, "Cyber Security Program for Power Reactors," is used in lieu of Regulatory Guide (RG) 1.152. The committee and consultants offered comments to the staff's deliberations in developing additional guidance:

- A threat assessment should be performed to ensure that the defensive measures address the right cyber-security threats. This assessment should include both internal and external threats.
- Dependency analysis is necessary to identify plant infrastructure services (power, heating, ventilation, and air conditioning, etc.) that support Critical Digital Assets (CDAs). The cyber-security program should protect the CDAs and ensure that their support systems and any interfacing data systems are also protected.
- The process for the identification of CDAs is expected to use insights from the plant PRA.

The draft ISG on the DI&C licensing will clarify what documentation is required, and when, as well as provide guidance on the scope and content of a license amendment request to address the regulatory requirements. The committee's opinion is that these clarifications will help streamline the licensing process.

Also, the draft ISG on the Review of New Reactor DI&C PRAs should be revised to emphasize the importance of the identification of failure modes, de-emphasize sensitivity studies that deal

with probabilities, and discuss the current limitations in DI&C PRAs. The staff has indicated that this ISG will be revised, taking the subcommittee comments into consideration.

Some specific conclusions and comments from different members:

Member Stekar was encouraged by a lot of the staff's work on difficult topics: the importance of defining the failure modes, defining the scope and the interfaces, and defining component boundaries (i.e., defining boundaries of the hardware and software parts that were analyzed) that the staff and the industry are doing. He was a little bit cautious with regards to how things are coming together from a practitioner's point of view in a way that will help to evaluate the contribution from DI&C to risk. He would like to see a little bit more in this area in terms of the vision forward, in terms of how all of this information will be combined in terms of a practitioner's view of the applications.

Member Bley was pleased with the quality of the presentations and the depth of the answers the staff gave. Specifically he was rather encouraged on the work on failure modes in getting a handle on what to do to link to the PRA. He thinks once the staffs knows how to categorize these failure modes and come up with categories of their effects, it might be possible to move to quantification with higher hope. Also the efforts to get data from other industries on similar processors and pull the similar parts together will help to be able to move ahead with the quantification.

Member Sieber was also encouraged by the presentations. He thinks that by moving out of the theoretical speculations down to practical matters, the staff is going to ultimately reach a conclusion. His impression is that of the few systems that have been approved by NRR for application in power plants, he does not see how the staff is going to get operating experience to help them out. The staff needs to look out into other industries like chemical industry, chemical and petroleum, to get better event data. He is also encouraged that the staff is looking further at databases outside the nuclear industry in the United States and even activities overseas. Also, there are so many possibilities for system architecture that affect the diversity and defense-in-depth (i.e., D3) process to whether it is advisable to run a pipeline on one CPU since computers do not last more than five or six years. In addition, Member Sieber would like the staff to think about architectural concepts like that with regard to how they fit into diversity and defense-in-depth.

Consultant Hecht commented that the conceptual framework for gathering the data is the key issue. And if the conceptual framework is proper, then the data can be incorporated from multiple disciplines. One has to distinguish between events, that is, the actual incidents and the causes. Within the causes, one has to distinguish between process causes and other types of causes. And one has to be able to isolate what is common from other systems to the nuclear world so that one can actually incorporate those experiences. And that it relates to the digital system boundary, not necessarily the sensors and actuators, but whatever it is that lives between there and the actual CPU that is relevant. Also he thinks it is important that as one looks at operating experience, one should look at successes, not failures. There is no hypothesis that is unstated which is that digital systems have common cause failures that will eventually cause something terrible to happen.

In addition, consultant Hecht thinks it is incumbent on the people gathering the data to either approve or disprove that hypothesis to whatever level of confidence they can. Also, in the process of looking at that, try to get specific lessons learned so that one can speak about what the D3 guidelines are.

Chairman Apostolakis added that the most important thing that came out of the meeting is the idea of having someone pull together all these efforts on failure mode

identification and try to come up with a comprehensive approach, maybe supported by computerized guides that the staff can use to identify failure modes, because he thinks the state-of-the-art right now can support something like this. It will evolve over the years, but it can be supported. Although this is not a subject of this meeting, Dr. Apostolakis is really pessimistic about any probabilities coming out anytime soon. But he feels the failure mode work that is being done in various research efforts of the agency is very good and very useful.

Mr. Bowers (from Exelon) made an overall observation that came out of the morning staff presentation about what the effect in a regulatory process is in reviewing the Oconee amendments. The challenge to the industry, the staff, and to the Committee is to make sure that as they go through all of these reviews and get probability numbers, and get failure data, it gets translated into very clear criteria so that the industry knows what the criteria are and knows how to satisfy those criteria, and the staff specifically knows what the criteria is, how they are going to satisfy it, what they are going to look at in the amount of documents, and what they are going to do in the review so that there can be closure in the licensing process.

BACKGROUND MATERIALS PROVIDED TO THE SUBCOMMITTEE

1. DI&C-ISG-01, "Cyber Security," including the following:
 - Appendix A, "RG 1.152 (Rev. 2) and Draft NEI 04-04 (Rev. 2) Cross-Correlation Table"
 - Appendix B, "NEI 04-04 (Rev. 2), "Cybersecurity Program for Power Reactors" (please note that Appendices A and B are restricted documents, "need to know")
2. Draft DI&C-ISG-06, "Digital I&C Licensing Process," including the following:
 - "Documents Needed for Review of Different Complexities"
3. Draft DI&C-ISG-03, "Review of New Reactor Digital I&C PRA"
4. Draft White Paper "Assessment of Digital Systems Operating Experience Data & System Inventory and Classification Structure"