Hansen/r&t

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

PUBLIC MEETING

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

SUBCOMMITTEE ON PLANT FEATURES IMPORTANT TO SAFETY

- - -

Nuclear Regulatory Commission
Room 1167
1717 H Street, N.W.
Washington, D.C.

Tuesday, February 3, 1981

The subcommittee met, pursuant to notice, at 1 p.m.

BEFORE:

DAVID A. WARD, Chairman

M. BENDER, Member

E. EPLER, ARCS Consultant

ALSO PRESENT:

RICHARD K. MAJOR, ACRS Staff

- - -

8102050608

P R O C E E D I N G S

MR. WARD: This meeting of of an Advisory Committee on Reactor Safeguards, ad hoc Subcommittee on Plant Features Important to Safety, will come to order.

I am David Ward, I am the subcommittee chairman. We also have present Mr. Epler, who is an ACRS Consultant, and Mr. Bender will be here shortly, another member of the committee.

The purpose of the meeting is to discuss the NRC definitions of the terms "safety grade", "safety related," and "important to safety," as developed during the testimony for TMI I restart. In addition to the definitions, we would like to review the generic implications of their use in the licensing process.

This meeting is being conducted in accordance with the provisions of the Federal Advisory Committee Act and the Government in the Sunshine Act. Mr. Richard Major, at my right, is the Designated Federal Employee for the meeting.

The rules for participation in today's meeting have been announced as part of the notice of this meeting previously published in the Federal Register on January 19, 1981.

A transcript of the meeting is being kept and we request that each speaker first identify himself or herself and speak with sufficient clarity and volume so that he or she can be readily heard.

We have received no written statements nor requests for time to make oral statements from any member of the public.

I would like to make a couple of comments before we get on. In the TMI I restart hearings there were contentions that the NRC had been inconsistent in the quality requirements placed on plant systems and components which could impact reactor safety.

To deal with those questions and to organize its own thinking, the staff attempted to develop concise definitions for three particular terms, "important to safety," "safety grade" and "safety related."

The "important to safety" definition derived from 10 CFR 50, Appendix A, the general design requirements, with reference to Appendix B which gave QA requirements.

Generally, "important to safety" was taken to mean to assure no undue risk to the public. "Safety grade" is defined in 10 CFR 100, Appendix A, or derived from definitions there which had to do with seismic design and safe shutdown earthquake criteria. It dealt with those items deemed important to safety, but particularly related to the primary pressure boundary integrity of safe shutdown systems and systems which provided for prevention and mitigation of releases exceeding those prescribed in 10 CFR 100.

The term "safety related" was not defined in the testimony but was defined in a Ross letter to DIS personnel, and was defined to be approximately the same as the term "important to safety," but I understand there has been some rethinking of that as an acceptable definition.

I think from what I have read and seen of what the staff has written and how things have been interpreted, it is generally agreed that "safety grade" is a subset of "important to safety" dealing with the three particular systems.

The remainder of the subset has not been defined and that may be part of the problem.

I see as a parallel issue, and perhaps it is really the same issue, the question of graded quality assurance. The staff has expressed, I believe, some unhappiness in the past with industry's "all or nothing" approach to QA. QA philosophers in general would like to see QA applied commensurate with risk, and in general this has been done, as I said, in an "either-or" category.

This sort of suggests that the definition of another subset of "important to safety" or perhaps more than one subset might be the one way to get degraded QA, which is desired. So, I think there is a tie-in here.

The sorts of things that might be considered as separate classes - and there are probably others - are systems that could be used to mitigate an accident if the first-line safety system became unavailable or inoperative or, for example, systems failure or misuse could challenge the safety system, require its operation.

In the letter from the staff to the ACRS from Rubinstein to Freily(?), a letter of last November 17, the staff asked for ACRC's opinion on these definitions as developed in the testimony and also in the Ross letter. After hearing the staff's presentations this afterncon, I think we need to consider whether we should concur with some better though-out semantics as proposed by the staff, or whether we believe that development of more comprehensive nature, a more complete set of definitions that could have some impact on how systems are designed and evaluated in the future. I guess there is a spectrum in-between those two things that we need to look at.

Before going on, I understand from Mr. Conran that the staff is happy with the tentative agenda as published. Before getting on with that, I would like to ask Mr. Bender or Mr. Epler if they have any comments to make.

MR. EPLER: This is entirely new to me, and I have been listening for about ten minutes now, but I feel the need for a little bit of clarification.

I see this as a part of a very large, long-range problem, and I believe our assignment is very likely to be to concentrate on difficulties in interpretation in the short range.

Therefore, I suppose that we should draw our attention to short-range aspects but, at the same time, keep an eye open to long-range implications.

MR. WARD: All right. I think Mr. Conran will serve as the escort through the agenda from the staff. So, go ahead, Jim.

MR. CONRAN: I think the first comment, our immediate goal for the meeting is very consistent with what Mr. Epler said. Whenever one gets into a discussion that involves various safety terminologies, one tends to rely on examples and experience to help define the terms and express the concepts to each other.

Our experience has been over the last few months that there is a very fundamental difficulty, this lack of consistency in the various terms that are used.

Just in conversation we tend to use them interchangeably a great deal. They do have considerably different meanings in the regulations and regulatory guidance. So, our objective at this meeting is to discuss the two terms that we have settled on a definiticn for, that is "safety grade" and "important to safety" and ask for the committee's comments if they have any, or concurrence if they see nothing wrong with the way we defined and explained it.

The third term, "safety related," as you pointed out, we have some difficulty in arriving at a single definition of that term that would embrace all the different ways in which I can see that is being used in reviewing regulations and regulatory guidance, and as it was applied just conversationally by the staff.

I simply did not have time to run down and try to develop a single definition in time for the TMI hearing. So. we left it undefined at that point and made a real attempt to confine our discussions of the contentions in the TMI hearing to use of just "safety grade" and "important to safety." It was not altogether successful because in NRR, our safety process, we use the term "safety related" as very nearly the equivalent if not identical to the "safety grade." It was possible to do that.

So, again, at this meeting we are looking for your comments, if there are any critical comments, or concurrence if you have no objections to the definitions that the staff has established, to settle on "safety grade" and "important to safety," and then we will combine with that a discussion of the term "safety related" and its interrelationship with the other two terms; and a bit more discussion on some of the recent difficulties that we have encountered in trying to define those terms.

MR. BENDER: Before you go on, I wanted to make a point that possibly would help in the discussion. Everything is safety related. If we look at a very broad interpretation of the word, anything from roads and streets to reactor fuel has some safety relationship. It is the type of relationship that we need to be addressing.

I think when you make your presentation that somewhere along the way what we need to do is to establish how we discriminate between safety relationships that require certain kinds of engineering provisions, special design treatment, or maybe operational treatment that is different from what we would have if we just allowed normal and conventional practice to persist.

I think it is that discrimination at least that should come out of this discussion. I did want to make that point.

MR. CONRAN: I tried to do that, and I hope that it satisfies your comments.

Just to reiterate the background a bit more specifically, the background for this meeting is really two tracks of the staff's effort and activity over the last several months. The first one, the Division of Systems Integration was given the assignment to respond to certain contentions in the TMI I re-start.

UCS contention No. 14 was the one that was of particular interest. It stated all systems and components which can either cause or aggravate an accident or can be called upon to mitigate an accident must be identified and classified as components "important to safety" and required to meet all safety-grade design criteria.

Naturally, depending on what the definition of "important to safety" and "safety grade" is, that could have some pretty far-reaching implications.

It reads as though UCS thought that "important to safety" was the equivalent to "safety grade." In fact, that is the way it developed in the hearing. If that is true and one accepts the premise of the intention, then the result is that very nearly all major plant control heat transfer systems should be "safety grade."

This contention was addressed in testimony that I developed and has been provided to the committee. Incidentally, that is the general form of a contention that has expression in two other contentions that address specific components, specifically pressurizer heaters and the PORV --

The contention UCS 3 said basically that pressurizer heaters should be "safety graded." And UCS contention No. 8 said that the PORV and block valves should be made "safety graded."

So, this is the general form of several contentions that were directed towards specific components.

The second major trend that I referred to, track of activity of the staff, really grew out of a finding by the Pogovin Study regarding deficiencies that they perceived in the quality assurance program.

One of the findings in that section of the study pointed out that NRC lacks definitions for safety related to assure that Appendix B quality assurance standards are implemented consistently. And much like the other terms above, the consequences in an ad hoc uncontrolled application of safety-related requirements to equipment outside the reactor protection system and the engineered safety features systems.

Now, that statement in itself implies that the Pogovin people thought that the term "safety related" applied only to basically safety systems, safety-engineered safety systems, reactor protections systems and engineered safety systems.

This problem was addressed in the action plan, Item 1-F and the Quality Assurance Branch has the lead, along with Standards, in correcting the problems that were brought to light.

Basically, the approach is to expand what is called the "Q" List, which is requested of all applicants along with applications to cover all equipment important to safety - not just component systems that are involved in accident litigation.

The second task was to rank equipment in order of its importance to safety. There should be a third item on there, really. These are both done as preliminary steps to developing a graded quality assurance program.

In developing testimony for the hearing, and in trying to develop a graded quality assurance program our experience was that of course these terms kept recurring - "important to safety," "safety grade," and "safety related." It soon became apparent that the staff and the industry all have been rather careless, or inconsistent, in the use of these terms. Very often, as I said, conversationally they are used interchangeably.

But the definitions that we finally settled on so that we could address the underlying issues in the hearing, and in the development of the QA program were these, just briefly:

"Important to safety" is actually defined in the regulations, the Preamble to the General Design Criteria, 10 CFR 50, Appendix A.

The specific definition was cited there, "Those structures, systems, and components that provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public."

Because of the context in which it is defined, it refers to all of the structurs, systems, and components, the plant features that are covered by the general design criteria. When I said "covered by that," not necessarily explicitly because the staff considers that a number of the plant features component systems are in fact covered by the general design criteria and must meet the requirements of the general design criteria, even though they are not spelled out specifically in the general design criteria.

Evidence of that is in our Standard Review Plans that are used as guidance by our safety reviewers. A very large number of them address plant features not considered "safety grade."

MR. WARD: Does that leave you with a terribly open-ended situation?

MR. CONRAN: I am not sure that I understand what you mean. The definition, typical of regulations, is rather broadly drawn so as to leave flexibility in implementing it.

It is typical that additional detailed guidance has to be prepared to interpret and apply the raw language of the regulations.

The way that we have applied the intent of the general design criteria is to write regulatory guides and standard review plans. So, it is not really surprising that in that sense, at the bottom line, a number of plant features not identified specifically in the general design criteria are in fact covered by them and are subject to the requirements.

Well, "important to safety" then is a broad class of plant features that contribute in important ways to safe operation and protection of the public in all phases and aspects of facility operation. That includes normal operations, normal plant control systems, heat transfer systems, as well as components and systems used for transient control and accident mitigation.

So, the term "important to safety" includes "safety grade" or safety systems as a subset.

MR. WARD: OK, you have a little trouble with definitions, then, It seems to be clear in what I have read that it includes "safety grade" as a subset. Now you are saying here that "safety related" is a subset, and that seems to be not very well agreed upon.

MR. CONRAN: That is maybe a bit premature. From our viewpoint right now that is a true statement.

MR. WARD: You are going to get to that?

MR. CONRAN: The quality assurance people take some exception to that because they define "safety related" a little bit differently than we do, as you will see when we get down to law.

But whether or not they are equivalent, it is true that "important to safety" includes "safety grade" as we understand it, as a subset, and "safety related" even as QAB used it as a subset. We consider them equivalent. There is a little bit of a problem in the quality assurance program area.

Well, the term "safety grade" is not used anywhere in the regulations explicitly. It does not appear in the regulations, at least I could not find it and I read a lot of sections of the regulations.

It is widely used and applied by both the staff and industry in the safety review process. So, even though the term itself does not appear in the regulations, the definition staff us using is derived from Part 100, Appendix A, the seismic and geologic siting criterion.

The specific language comes from a section in which the safe shutdown earthquake is defined. What we call "safety grade" systems are those structures, and systems, and components which are designed to remain functional for the SSE, and they are those features necessary to do these three vital safety functions. To assure the integrity of the reactor coolant pressure boundary; to assure that we can achieve and maintain safe shut-down; and to assure the capability to prevent or mitigate the consequences of accidents where the offsite exposures could exceed the Part 100 guidelines.

The final comment is, they are therefore a subset of "important to safety." Again, we consider them equivalent to "safety related."

Now, the problem that I spoke of with "safety related." "Safety related" is defined in the regulations themselves only in the context of QA program requirements. The term is defined in Appendix B, Part 50, quality assurance criteria; and the definition is, "Structure a system with components that prevent or mitigate consequences of postulated accidents that could cause undue risk to public health and safety."

That definition contains elements of both "important to safety" and "safety grade." The mitigating consequences of postulated accidents sounds very much like subitem 3 under "safety grade," mitigate consequences of accidents that could result in undue risk to public health and safety.

Structure systems and components that are important to safety provide assurance that the facility can be operated without undue risk to the public health and safety.

So, the definition in the regulations themselves sounds like a mixture of both. As applied by the Quality Assurance Branch, "safety related" as a class or subset, "safety related" includes plant features identified in Reg Guide 129, which gives a rather detailed listing of the plant features that must be "safety grade," that must be seismic category 1, actually.

As we will show on the later slide, everything that is "safety grade" is seismic category 1; so, it is a congruent set. But that is not all it is. If that was all that it was, it would be identically equal to "safety grade" obviously. The staff position is that the staff wrote Reg Guide 129 to identify what should be "safety grade."

I got off the track. As applied by QAB the "safety related' includes all the plant features identified in Reg Guide 129, but sometimes some others. The way that the QA requirement is implemented, the staff requests that the licensee has what is called a "Q List," that is, structure systems and components that the licensees believe are necessary for safe operation of the facility.

I am told by the Quality Assurance Branch people that at times items other than those listed in Reg Guide 129 show up on the Q List, and one typical example was rad waste systems, as I recall.

Now, that is as the term is defined in the regulations and used in the QA program, as defined and used in many other safety review contexts by the rest of the NRR staff; and the way it is applied in those other contexts, or reflected in a number of r g guides in the Standard Review Plan. A good example is Standard Review Plan 7.4 on instrumentation and control systems.

In those contexts the term is equivalent to "safety grade.' In other words, it does not contain any systems that do not have to be "safety grade" that don't have to be seismic category 1.

So, there is a slight difference between the term "safety related" in the quality assurance program context and in all other safety review plans.

MR. BENDER: Jim, are we locked into this hierarchy that you showed up there?

MR. CONRAN: We are locked in insofar as regulations are or practice is; that is the way we have done things for years. That is the way that we interpreted and applied regulations - the staff, I am talking about.

Our understanding of those terms is reflected in, rather consistently, regulatory guides and SRPs. If we were to change this terminology it would require some considerable amount of effort just editorially changing the reg guides and SRPs in which these terms are used.

MR. BENDER: If I heard you right, only one of these terms is in the regulations.

MR. CONRAN: Two of them are, "important to safety" is defined in the Preamble to the General Design Criteria, that is Appendix A. "Safety related" is defined in Appendix B, the introduction to Appendix B.

Well, this is a kind of convenient or short-hand way of showing it.

MR. WARD: Jim, excuse me, can I go back? Is "safety grade" really defined in Appendix B, literally?

MR. CONRAN: "Safety grade?"

MR. WARD: Yes, is that not what you just said?

MR. CONRAN: No, "safety related." Yes, it is. It is in the introduction to Appendix B.

MR. HAASS: Let me interject here, Walt Haass is my name, Quality Assurance Branch.

It is not a definition per se. If you read the introduction, I think, you can derive the definition of "safety related." You just have to read it in context. To most people, I think, it is clear it says that "safety related" structures, systems and components are those needed to prevent or mitigate the effects of an accident. That is what we read out of Appendix B.

MR. WARD: The reason I asked is because of your comment that if you were to change definitions, you do not consider yourself locked into the definitions, that there would be need for a lot of editorial changes in the regulations, seems to be somewhat at odds with the problem, which is that the terms are not defined very well in the regulations.

MR. CONRAN: Maybe I spoke too generally there. We have proposed a change to the regulations that we think would involve minimum effort in getting complete consistency among those terms in the way that they are used by the bigger, the greater part of our safety regulations.

That, in fact, would not involve much change. But depending on how you changed it, it could involve a considerable amount of change. For example, if you decided that you were going to equate "important to safety" and "safety grade", or "important to safety" and "safety related," that would involve a pretty considerable amount of work.

MR. BENDER: Well, I guess I was trying to lead into a thought I was trying to express earlier, namely, we might as well accept right away that every part of the plant has some "safety related" function, and the "safety grade" is going to be keyed to that safety relationship.

What we probably ought to try to do is decide what "safety grade" means in terms of that "safety related" function. Now, the question of the term "important to safety," which seems to be the thing which comes up, seems to be synonymous with the term "safety related function."

If you use those two terms interchangeably, then you only have to define one of them. To be perfectly honest about it, I think it would help if we did decide to define one.

MR. CONRAN: Well, I had intended to touch on that point later, but since you brought it up now -- in fact, in talking to the old "heads" around the organization, that is exactly true. From the beginning, when the two appendixes were written, the intention was that "safety related" be equivalent to "important to safety."

Unfortunately, it did not work out that way. For whatever the reasons, NRR or whatever its progenitors were called, restricted its scope and applied it to the plant features that basically are used to respond to design basis accident or events. That has been the way it has been applied for a number of years.

Now, we have indication that is the way the industry thinks of it in a very consistent way. I have an example to show you, an excerpt, in fact, of a licensee's manual. So, you are right, just the way you used the term conversationally, that is certainly a good definition to put on it.

Our problem is that by practice it has been applied in such a different way so consistently, and it appears in so much of our regulatory guidance meaning something other than "important to safety." That is a change that I am talking about if we actually set about right now trying to change the language of the regulations and all the implementing guidance documents, reg guides and standard review plans, that that in itself would be very considerable, just editorially.

MR. BENDER: I see.

MR. CONRAN: As I said, we have a proposal that we are going to try out on you today, which involves eliminating one of the terms from the regulations. If they mean the same thing, why not say the same thing? That is the idea. Simplify it to that extent.

These diagrams reflect what I have been saying previously, safety classifications, and I have shown the way that NRC/NRR defines the term, and have comparative the way that I understand the IAEA.

Again, to reiterate NRR, if the entire circle is important to safety, then a subset of it is "safety grade" or "safety related." Those two terms are used interchangeably by NRR. That is the smaller sector.

QAB adds a small increment for other structure systems and components that licensees identify as necessary for safe operations.

MR. WARD: The example there was a rad waste system; is that true?

MR. CONRAN: I though rad waste was the example that you gave.

MR. HAASS: That may be not the correct impression to be giving here. We asked the technical branch of NRR to review the Q List because they understand the functions of each item that is on the list. So, we have given the guidance, we tell them that we are looking for structures, systems and components that prevent or mitigate the effects of an accident, safety-related items.

There is additional guidance in Reg Guide 129, which gives somewhat of a list.

So, they reviewed the list and they tell us that in the area of review the list is complete or things should be added to it. On occasion they come up with items that one would say are not "safety grade," i.e., they are not seismic category 1; they don't meet the single failure criterion, they are not environmentally qualified, those kinds of things.

Yet, they have significance to safety at such a level that the QA program, the Appendix B program, should apply to them.

MR. WARD: But this is kind of on a case-by-case basis, I take it.

MR. HAASS: Yes, case-by-case basis.

MR. CONRAN: Is this the staff or the licensee that does this, Walt?

MR. HAASS: The staff is reviewing it.

MR. CONRAN: Is it not the licensee that puts the item on the list?

MR. HAASS: Well, he originally creates the list and then we review it for acceptability. We may ask him a question and say, "Why isn't this on the list? It ought to be on it." Then he either puts it on, or disagrees with us.

MR. CONRAN: But for example, if a licensee in addition to the Reg Guide 129, structures, systems or components, added something that the staff does not think of as "safety grade," there is no requirement that in their review the technical branches take off anything that is not "safety grade."

MR. HAASS: That's right.

MR. CONRAN: So, basically it is the licensee who is responsible for it.

MR. HAASS: There are two items I can think of at the moment, there are rad waste systems and fire protection that the staff has decided are not safety related. Yet, they are of such importance to safety that we have created special requirements for those areas. We have branch technical positions on those that describe a less complex QA program, as an example, than would be called for by Appendix B.

So, we asked the applicants to describe their programs to us or, as an alternative, they can include the item on the Q List and have the Appendix B program apply to it. And that is the genesis for why those items appear on the Q List. We don't require it, but they take the easy way out by saying that, "We are not going to create a special program, we will include it under our existing Appendix B program."

So, therefore, it appears on the list sometimes, but it is not "safety related."

MR. CONRAN: I think the way I understand that IAEA used the term may be closer to what you are saying. In other words, it harks back to the comments Mr. Ward made in his opening comments that part of the problem is not having an expression for the part of the "important to safety" pie that is not "safety grade."

Over here, for example, we are stuck with calling that "nonsafety" or "nonsafety grade" structures, systems or components. Still, they are important to safety. So some people have difficulty using the terms that way.

Certainly, since this sector is "safety related" it would also proper to call the rest of it "nonsafety related," but that grates on the ears too much. If it is important to safety, how can it be not related to safety at all?

MR. WARD: Exactly. What does the SSC stand for, over there?

MR. CONRAN: Structures, systems and components. The IAEA identifies a subgroup or subset of what they call safety features or safety systems, and they include explicitly the reactor coolant pressure boundary. They also call out specifically the three barriers to fission products, the fuel planning, the reactor coolant pressure boundary, containment, and they also have a reactor protection system, what we call a reactor protection system and ingeneered safety system.

So, the subset that we call "safety grade" they call "safety features," and "safety systems." All the rest of their "important to safety" pie is called "safety related."

So, that is one possible approach to your suggestion that some specific language that does not have "non" in it, I suppose, applies to the rest of that pie.

MR. WARD: But I guess, further, whether that hunk of the pie should be subdivided.

MR. CONRAN: Oh, yes.

MR. WARD: You know, a hand-rail in the visitors' center is not safety.

MR. CONRAN: We will touch on that consideration later on. I did not want to show it on here, but we have in subsequent slides some ideas or approaches to that.

Well, I think those slides and that discussion cover the background discussion, all subtopics, unless there are some other questions.

MR. BENDER: Let me try one more time to make a point. Since right now we are in the throes of trying to decide how much of the plant has to be dealt with in these categories that we are tossing up here, I am inclined to a view that says eventually we are going to have to determine what is it that makes every piece of the plant "safety grade." For some parts of the plant it may be its seismic qualifications, and for others it may be its ability to perform certain functions that only occur under normal circumstances.

Now, that involves a more comprehensive examination of what is in the plant. If you do it that way, you won't have to worry about whether Part A necessarily has to have the same kinds of qualities to be classified "safety grade" as Part B. You can decide that the containment structure needs one kind of quality to become "safety grade" and the turbine building requires another.

Well, in my mind that would be a better way of getting away from the dilemma. Just decide to put the "safety grade" qualifications on everything. That makes people go down through the list and say, "What is it, what properties am I assigning to this in order to let it perform in safety-related functions?".

If we could do that, I think we would solve most of our problems. But the way you have it now, it almost seems like when you say something is "safety grade," if it is a structure at all, it automatically says it is seismically qualified.

MR. CONRAN: That is true.

MR. BENDER: We know in some cases that doesn't buy anything. Sometimes you don't have any other qualification on it except that, so you miss some important things.

MR. CONRAN: Let me put up this slide which I was going to use later, and see if it is the sort of thing that you are talking about.

Right now, we do something like that. This is safety classification versus applicable quality standards. Right now the things that we call "safety grade" even within that subset, there are gradations of quality.

This is a comparison of the characteristics of "safety grade" and "not safety grade" systems. Just examples. In the design fabrication area, for example, everything that is in the "safety grade" category that is required for those Part 100 critical safety functions is either Class 1, 2 or 3. Things like the reactor coolant pressure boundary, DCCS systems. Something like the rad waste system has presumably a lesser standard of quality for the materials in the plant.

With regard to redundancy and diversity, everything in the "safety grade" category has to meet the single failure criterion with the exception of reactor coolant pressure boundary itseslf. They are not double walled, in other words. There we substituted a very high quality level to depend on that for reliability.

But certainly all the active components in the "safety grade" category have to meet the single failure criterion.

Those plant features not "safety grade" generally do not have to do that. With regard to seismic design classification, according to the regulations the requirements of Par 100, Appendix A, all systems that perform those critical safety functions do have to be seismically qualified.

I put these in parentheses over here because NRC does not, to my knowledge, define Seismic 2 or 3; but one of the architect-engineers has, or at least had that sort of scheme.

For Seismic 2, for example, we have components like major plant features, heat transfer systems, plant control systems; and three was items of lesser importance. But they had some sort of a scheme for gradations even within the "important for safety" category.

Similarly, power source. All the "safety grade" systems gave a Class 1-E, and again there is a gradation from the viewpoint that, for example, if the reactor protection system is powered from the critical power bus which is uninterruptable, other "safety grade" features have Class 1 in power supply, but they don't have to be noninterruptable, they are not battery types.

Again, "important to safety", that degree of quality is not required.

To date the practice has been for the requirements of Part 50, Appendix B, the 18 QA program elements all had to be present and were rigorously applied, although I guess there was perhaps some gradation within the QA program. But at least there had to be all 18 elements present.

"Important to safety," I guess we don't really know because it has not been the staff's practice to review the QA program, apply it to "important to safety" components that were not "safety related."

That does not mean there has not been a QA program. It is a safe bet that licensees want power generation facilities that are reliable. So, to the extent that you need a turbine and a condenser, and that sort of thing, to have an available plant, there are undoubtedly quality assurance measures, programs, applied. But we don't know that because we have not been reviewing it.

That is the area which will be covered under the graded QA program.

MR. BENDER: Let me just explore this thing for a minute before you go on.

If I were to take the steam turbine and say, is it important to safety, what answer would I get?

MR. CONRAN: It is important to safety, yes, to the extent that its failure could cause or contribute to an accident.

MR. BENDER: Let's pretend that it is. Then I will go up there and say, "If it's important to safety, how many characteristics listed up there fit the steam turbine?" What would I find?

MR. CONRAN: I probably could not address that question very much.

MR. BENDER: I am just trying to illustrate it.

MR. CONRAN: I would say this, we don't have to speculate about it. There is an SRP section on the turbine and condenser. It lists the characteristics the staff is to review for, and it references applicable general design criteria.

I guess the way to say it is, components or plant features that the staff considers important to safety they have identified as important to safety, and they are covered by SRP sections or reg guides in some way or another.

MR. BENDER: And that is where the "safety grade" is established.

MR. CONRAN: I would say "quality" to stay away from the term "safety." That is where the quality level is established, right.

So, we already have something of this kind of a scheme and, as a matter of fact, this is nothing new. You may quarrel with the facts placed on this hierarchy that one system or another applies, but what I am trying to show here is that we already recognize explicitly in our standard review plans and in our review criteria that there are varying degrees of importance of components in the plant, both in the safety grade subclass and in what is left over.

Just starting up with the top up there, the reactor pressure vessel has to meet the requirements of Section 3, Class 1. As to all the other reactor coolant pressure boundaries, I don't think there would be too much quarrel over the fact that maybe the RPV is listed first because we don't have any design features whatever to accomodate a failure of a reactor pressure vessel.

The reactor coolant pressure boundary has to meet the same quality standards, but there are design provisions for coping with failures in the reactor coolant pressure boundary. Those are both Quality Group A.

The reactor protection system -- well, again I say, you can quarrel with individual locations in this hierarchy, but generally the next item that I come to that the staff has already identified as being recognizably a specific lower quality level is the ECCS, RHR containment piping. Some of that piping, at least, would be Class 2, which is Quality Group B.

The AFW system, one of the engineered safeguards, its piping has to meet Class 3 standards, that is Quality Group C.

All the way down to rad waste systems, which we mentioned before, there are specific quality standards applicable that must be mer for rad waste system piping. That is a Section 8 level of quality and it is called Quality Group D in Reg Guide 126.

We already have the rudiments of a ranking like this. Then, within the part of "important to safety" that is not "safety grade," that is this part down here, our experience at TMI certainly highlighted the importance of some of the components that are closer to the top of that hierarchy, the PORV and pressurizer heaters, reactor coolant pumps.

Generally, what I have done here is tried to rank them in order of how directly, or how violently they might affect reactivity, or how seriously they might cause or contribute to an accident, that sort of thing.

MR. STOLZ: John Stolz. The "safety grade" category, though, is narrowly defined in the regulations, although it is not explicitly called out. It is defined within the three criteria defined in Appendix A and also spelled out in front of Reg Guide 129 as a precursor to what is required -- if you read those requirements you need to have that piece of equipment or that system designed to seismic category standards.

So, basically we are saying, everything above that line is shown in "safety grade," and they essentially provide the basic reactor coolant pressure boundary and all of the protection systems, and all of the backup systems needed to mitigate the consequences of an accident.

MR. CONRAN: And able to shut down.

MR. STOLZ: Right. Heat emoval systems, and the single failure requirements are quite specifically called out in the regulations. They are specifically called out for the protection system, the engineered safety features, and the heat removal system, very clearly.

So, anything outside of that category is really not "safety grade." It may be "important to safety," and it may have some impact on safety systems if they fail, but nonetheless, the other systems outside of that line, although they are included in "important to safety" are not needed in accordance with the requirements of Appendix A.

MR. WARD: May I ask you a couple of questions? What is it you are defining across there?

MR. CONRAN: It is degree of "importance to safety," increasing in this direction, versus quality standard or quality level increasing in this direction. This is supposed to reflect the "quality level."

MR. WARD: I see.

MR. CONRAN: It is hard to qualify, but there are some points that are already quantified.

MR. WARD: A, B, C and D.

MR. CONRAN: Right, roughly in our reg guides.

MR. WARD: I mean, is that part of the problem that you see? I mean, you don't have quality grades for a lot of the items there. I do not see, for example, the containment system on the list.

MR. HAASS: That would be in the first group.

MR. CONRAN: I tried to indicate that many, if not all, the items that are below the "safety grade" line are addressed by standard review plans or reg guides, and some very specific quality standards are applied.

It is not as refined or as fine structured as I think it is going to get. One of the reasons is that in our safety analysis we have not typically taken into account the effects of nonsafety component failure. We have a program for addressing that question now.

But really, the gradations of degree of "important to safety" almost inevitably are going to fall out of the risk analysis and the systems interaction analysis that is going on.

MR. BENDER: Well, you are suggesting something here that I need to think about a little bit. You are saying that the level of quality can be reduced to some degree as the importance to safety is reduced.

I am not sure that that kind of criterion can make any sense. I think you can have, "No, you don't need anything," and, "Yes, you need something."

MR. CONRAN: The reason that you have not come to any final resolution on that before is that many of these things you have never considered explicitly in your analyses. But now we have programs that are trying to do that.

MR. BENDER: All I am saying is, they are more likely just to be defined in a different way, promptly, as you might specify, are not the same ones, depending on how that safety function is safisfied. But the term, the degree of importance, just does not have any meaning.

MR. CONRAN: It may be that I am trying to be too specific about "degree of importance." The general design criteria is where the language comes from. The quality standards apply to structures, systems and components. The safety is to be commensurate with their importance to safety, the degree of importance to safety. That is a concept that is introduced and a requirement that is stated even in the general design criteria.

Of course, it is stated very generally, and here we are trying to get more specific.

MR. BENDER: The term "commensurate" is a different matter than degree, I think. I don't know that I am making the right point, but if I looked down here and saw the things that are listed, like you have coolant pumps, they are also built to Section 3 of the Code. The structural requirements are the same as the primary coolant system, the whole primary coolant system.

MR. STOLZ: I think he was talking about the pump motors, Mr. Bender, not the casing for the pump itself.

MR. CONRAN: The reactor coolant pump is a part of it, the reactor pressure coolant pump.

MR. BENDER: Let's talk about the pump shaft if I can just use a piece of hardware. What kind of quality do I put on it? The primary boundary has a certain requirement that has to do with structure. But the equipment that circulates the coolant has a requirement that is equally important. You have to make sure that the pump can close down; that is important to safety. That means dealing with the ability of the motor not to cease; the ability of the pump shaft not to break. You have the ability of the pump not to run away if you have a primary coolant system break.

Those are, in their way, of the same importance. If they would violate the ability to control a raiodnuclide release, there would be a problem.

MR. WARD: Could you give us an example, or maybe Mr. Haass could, of a quality standard at Grade A, and one at Grade C, and one at Grade D. I mean, what in practice is the difference?

MR. HAASS: For example, the pressure vessel, that is the highest quality. Take rad waste management. I don't think it has the same level of quality requirement as the vessel does. I am not saying it is not important, it is an item important to safety, but not to the same degree as a reactor vessel.

MR. WARD: This is evidenced in what way, there is more complete ultrasonic testing of the vessel, of the main pressure vessel? There would be no UT testing of a rad waste system vessel, for example?

MR. HAASS: Whatever Section A requires.

MR. CONRAN: That is the problem, we need someone who is familiar with the requirements of those codes.

MR. WARD: OK, but there is a difference in the codes.

MR. CONRAN: Oh, yes, sur, and very exclusively for those items. Those are ones that I could identify because they have already been spelled out in the reg guide.

MR. BENDER: Let me point out the real difference between Section A and Section B, it has to do with the way in which they address the service conditions.

Section A is the simplest kind of design approach that requires a vessel which may be covered by the Code, be analyzed for stresses and nozzle loadings, and be tested to one and-a-half times the working pressure, and have a factor of safety of four between working stress or design stress and ultimate stress.

If you go to Section 3, you find that that factor of safety is three, but there is a greater requirement to analyze the structure. There are more working conditions imposed on it. That is mainly because the service conditions that we have to deal with are of a different sort.

When the Code developed these criteria it was with that thought in mind. Now we kind of flip-flop. The fact that the requirements are different has to do maintly with the kind of service conditions that have been imposed.

That is also true of the single failure criterion. You put the single failure criterion on some things because you have no other way of assuring its reliability except to say that two is more likely to work than one. Lately we have found out that is not a very good basis.

So, you are going to have to go back and look at it in a different way than what you are presenting now, that is the argument I am making, at least.

MR. CONRAN: Yes, I perhaps should have been more emphatic about the fact that this was just a particular way that I ranked them for illustrative purposes here. I surely did not mean to imply that this was the staff's position.

I am sure there are a lot of considerations that go to the requirements of the ASME Code, for example, that I don't understand.

MR. EPLER: Please, could I interrupt?

I am interested in the last comment that there might be another way to look at this, and I have been struggling with that. I feel that we have built something pretty complex here, and we are a little bogged down in terminology and in various concepts that don't seem to have any future.

I notice in this RRPM on the board here you have one system that you call a reactor protection system, which I prefer to call reactor shutdown system - the same thing. If you examine that in comparison to all the others on that sheet, you find an interesting difference.

First, the design objective of the reactor shutdown system is to be able to shut down the reactor on the occurrence of any conceivable failure of a control system. We have been fairly successful in accomplishing that.

We have not been successful against protecting against some idiot turning it off and then initiating a transient, but we have been pretty successful in protecting the core against any malfunction of any control systems that would initiate a transient.

It has another important feature, it can fail-safe such that if you lose power to it that by and large - not always but by and large - the mission will be accomplished in spite of the failure. That is not always true, but it is in large measure true.

Then there is the most important aspect of all, that the other items on this page do not have, that the reactor in operation can by action of the reactor shutdown system create, then, another mode of operation which is safe shutdown.

Now, if you look at the other items on the page, and particularly the items relating to heat removal, there "ain't" no place to go. You have to sit in there and get the heat out. You can't go to another safe place.

Now, what that means is, to me, that in the case of a reactor shutdown system you don't have to exhaustively review or quality assure, or do a lot of good things to prevent failure of the controls because you can accept the failure. What you do is to watch the system and if it fails too frequently and challenges the shutdown system too frequently, you observe this and do something about it.

But you don't have to prohibit this failure or to take any extraordinary means to prevent the failure because the failure can be mitigated by shutting the reactor down.

Now, if you look at heat removal, there is not a safe place to go, you have to make the stuff work. You have to do everything that you can think of. You put your entire effort into prevention, and it is a big deal, and it brings up all these questions of near safety, and safety related, and all sorts of things because by and large all the emphasis has been put on prevention and we don't have a way to mitigate the failure.

Now, this creates a problem that is unique. I don't know what to do with it except to suggest, I wish we had a system that worked, but we are not going to have it.

I think that in looking at all these activities to prevent failure you can say in the case of the pressure vessel, as you did, you have to prevent it.

On these other things there should be a ability to tolerate failure, but we just don't have it. We could have it. So, all of this activity, then, appears to me to be in an area where we have elected to concentrate on prevention because we have not elected to put in some measures for mitigation. That is going to be a problem.

MR. WARD: Jim, let's go on.

MR. CONRAN: Let's see, we seem to have skipped on to Item 3C. Was there any desire to go back and pick up A and B before I go any further?

MR. WARD: Yes, I think you should I would like to hear what you have to say.

MR. CONRAN: I had these slides available and I showed them as a kind of opening for what Walt might have to say about developing a graded approach.

What I was trying to show is that when you develop a graded approach there are two things that are involved. One is, to the extent that you can determine it, if you can determine that you can get by with a lesser quality level, you can determine the degree of importance to safety, then you might be able to rely on a lesser quality standard.

The other part of the equation is, of the specific 18 elements identified in Appendix B that should constitute a QA program, it may also be viewed with decreasing importance to safety where you can perhaps not have all of those elements in your program or be less stringent in the application of one or more of those elements.

MR. BENDER: I think what I am trying to do is discourage you from this rated approach if this rating means a curve of importance versus level of quality. I think it would be better to say that safety grade quality is what we need to prevent radionucli releases. Then say what qualities are represented by safety grade to this. That would be different for every piece of hardware, but it is not a graded kind of thing, it is just some assigned properties.

MR. HAASS: Isn't that more a question of semantics? I mean, if you go through the standard review plans, we do have requirements for each of these items, and they are different.

MR. BENDER: Well, it is not semantics, it is just that there is no grading associated with it. These are properties and that is what you need.

MR. HAASS: But if you did set them up that way it would come out to some kind of a curve, maybe it would not make sense to do that.

MR. BENDER: It would not come out to a curve, it would come out to different kinds of equipment and different kinds of hardware, and different kinds of structures, needing different kinds of capabilities because that is the way they function.

MR. HAASS: You are talking about categorizing all the items, saying all the items within a category are treated similarly.

MR. BENDER: I am saying, you deal with the items in terms of their service conditions.

MR. WARD: The service conditions, Mike, or the service requirements, the requirements of service?

MR. BENDER: Well, a combination, I guess. What they are required to do, and the conditions under which they have to do it. I think that really is what we have to deal with. But, I am digressing.

MR. CONRAN: We are thinking of what we are already stuck with. I would agree with you to that point. But it strikes me that we are already hung with the notion that there are some systems or components that contribute to safety in a more important way than others in the plant, and therefore they have highe. quality levels applied to them.

MR. HAASS: I have to go along with that, that is a fact.

MR. CONRAN: That is the system we operate under now.

MR. HAASS: Yes.

MR. WARD: Well, it is a fact, and it is also reflected in Appendix B.

MR. HAASS: Yes. We are not talking about that now.

MR. CONRAN: We have Criterion 1, and the fact that we have something that we call safety grade features which are associated with very vital functions, another sub-class.

I don't think there is any other way to say it, the quality standards are just not that stringent, the requirements. I tried to show on that one slide, taking specific characteristics like seismic design classification or design classification standards, or redundancy and diversity, that some systems are required to be Grade A top-notch in all respects. Then there are other systems -- maybe we are wrong about it, but so far you consider them of lesser importance.

MR. BENDER: But it is not because they are less or more important, it is because the conditions under which they are required to operate are described differently.

You need the feedwater system most of the time. There is no need to have an auxiliary feedwater system if the feedwater system is not working. But we have decided that we will let the feedwater system - I don't know if we do or not - but we could say, "We will let it be nonseismic resistant and just have the auxiliary feedwater seismic resistant."

Now, that is not necessarily a gradation, it just says, here is a service which I am assigning to one of these things and I am not assigning to the other; but they are both important under certain circumstances.

MR. CONRAN: I am having trouble with terms, I guess. To me it is just inherent in the notion that something cannot fail, by God. That makes it more important than something that can fail, and, no big deal, we can accomodate that.

But if my expression of that or the way I give expression to that idea bothers you, that is where we are hung up.

MR. BENDER: I am using up a lot of time. If my chairman is not getting impatient, he ought to be.

MR. WARD: I guess I am coming around to believe what Mr. Haass expressed, that it is probably more semantics here than anything else.

MR. HAASS: I think the bottom line is the same.

MR. WARD: Yes.

MR. ROSSI: Can I say just one thing? I am Ernie Rossi from the Instrumentation and Control Systems Branch.

I would just like to say one thing on this level of importance to safety of components, and that is that if you have very severe consequences when something fails, a particular component fails, then it seems to me that you have to do a lot to that particular component to make sure that you have a very low probability of it failing.

If you have less severe consequences if a component should fail, then you can live with a somewhat higher probability that it might fail, and perhaps you do less in terms of what you put into it to assure that it won't fail.

I wonder if that is not the kind of thing that we are talking about when we talk about levels of importance to safety.

MR. BENDER: For sure.

MR. ROSSI: That something with severe consequences has a high level of importance to safety, and with zero consequences, if it fails as far as safety is concerned, then it has no importance to safety, then.

MR. BENDER: I don't think that fits.

MR. CONRAN: I would readily admit that the hierarchy of the order that I chose may very well not stand up under much more complete analysis. I was just trying to illustrate a point.

With regard to the question of your topic III-A, is the list of items confined to safety grade given in Reg Guide 129 an adequate list; does it require additions or deletions.

The general answer to that question is, we have not identified, to my knowledge within the last year, any system or component that has to be made safety grade that was not already safety grade.

We have not moved any components from the lower part of my chart up into the safety grade subset. We have upgraded the reliability of certain components, such as PORV and power supply pressurizer heaters; position indication of the PORV and that sort of thing, but we have not required that they be made safety grade.

As a matter of fact, it can be said stronger than that and was in the testimony in the TMI I hearing. The presusurizer heaters, the PORV valve are not required to perform any of the critical safety functions that we had identified in return to safety grade.

Now, that general situation is complicated a little but by rulemaking proceedings that are going on. For example, in hydrogen control features that have been required on the NTOLs, hydrogen igniters, I really don't know whether it has been determined that it has to be safety grade.

I guess as a general statement I would say, if we added that requirement, if we added to the design bases the requirement that we have to be able to accomodate a lot more hydrogen than we used to and it is critical to do that - and it sounds like it is - well, then as a first cut I would say, whatever it takes to do that it probably would have to be qualified. There would have to be a quality level that you would identify in terms of safety grade.

But I simply do not know whether that determination has been made in that language, or what the quality standards are, whether it has been, in fact, added to the design basis.

MR. BENDER: I would like to get back to the point that was made where it says, "Importance to safety is determined by the consequence of failure."

That would not be a bad measure.

MR. CONRAN: I think that determination would be made on the basis of risk. If the probability was low enough, the determination might still be made. That is why I don't know what is happening.

MR. STOLZ: That still would give you a so-called rated approach which you find objectionable. But it still is a measure of the risk involved, associated with the failure of any of the equipment in the so-called "important to safety," it is outside the "safety grade" classification.

MR. BENDER: It has just been measured in a different way.

MR. CONRAN: They quantified it.

MR. WARD: Yes, sir?

MR. GALLAGHER: I am John Gallagher. I am the chairman of the Joint Working Group between the IEEE - it is an ad hoc task force - and members of the NRC to try and come up with a graded approach to instrumentation control and electrical systems and equipment important to safety.

What Mr. Rossi referred to here, he has been on this group, is the approach that we are taking. Later on, if you would like, I could give you a very brief view of the progress we have made on this.

MR. WARD: All right, why don't we plan on that?

Before we leave the 129 question, if I was to take - this is the Q List, I guess - if I was to take a Q List from similar reactors but, let's say, owned by different utilities, how much difference would I find among them?

MR. HAASS: For similar plants there would be very little. I am talking about recent reviewed plants. We have changed our process for reviewing the Q List relative to what we had before that. So, we have more confidence in the listing we are coming up with now.

But if you compare the recent ones we are doing, take North Ana, Salem, the list would be roughly similar. You go to Sequoyah, it is a little bit different. Then you go to LeSalle, which is a BWR, that is going to be different. But for some of the plants we have similar lists.

MR. CONRAN: Question B, NRC argues in testimony that improper operator action towards safety systems resulted in reliance on nonsafety system at TMI 2. What is the implication of this line of reasoning concerning such topics as operator action before or after ten minutes into an incident, to mitigate or in the transient?

I think the answer to that is the same as it was with respect to the question of, what is the implication of taking credit for operator action to perform some accident response functions, not just in the transient but to recover from an accident.

Our analyses of TMI 2 have indicated that the most serious, or the most fundemental problem was operator error in operators defeating installed safety systems which otherwise would have worked properly and could have mitigated the consequences of the event without core damage.

So, the biggest part of the regulatory effort over the last year has been directed towards improving that situation.

Another involves better procedures, providing better procedures to operators based on more realistic analyses, and results are reflected in improved operator training, including the requirement for simulator training to control, sort of, transients or accidents that are referred to.

By doing those things, I think it is a legitimate question whether or not it is acceptable to depend on operator action, particularly after an event like TMI 2, or operator error which led to core damage.

But our answer to that is, we have confidence that we have improved this situation by doing the things that I mentioned to the point where you can in fact rely on the operator not just to control transients --

MR. WARD: Are there any more questions of Mr. Conran?

MR. EPLER: Maybe I would like to pursue this last part a little bit because I don't like to see it left quite like that.

Going back a little further,in designing systems we ask ourselves, can we fix the system so the operator doesn't have to respond; that would be much better because if he does respond he might make it better, or he might make it worse. So, it would be better if he just didn't have to be called on.

Now, important to that concept is the importance of never lying to the operator. Don't give him misinformation because if you do, he might decide quite unnecessarily, spontaneously, to go ahead and make something worse when there is nothing really wrong. We had that at TMI. We lied to the operator.

I was amazed to see that practice persist this late in the industry. I thought we had that problem solved 30 years ago. Now it is still out there.

Now, since you raised the question, I feel it is worth-while to insert into the record that the lessons learned did not recognize that we must not lie to the operator. So, we are training the operator to respond better to misinformation - there is no future in that.

The lesson learned says that now for the safety and release valves you must do either of two things. Tell the operator the true position of the valve, or tell him whether there is any fluid going through it.

Well, if you tell him there is no fluid going through it, he can legitimately ask, is that because the valve is closed, or because it is open and the block valve is closed. So, he has to make a judgment based on information that could be completely misleading, the valve may be open, but this information says it is closed.

Now, I think one of the things we have to learn either way is, don't give the operator misinformation or he will make the situation bad when it really is not bad. So, I think the emphasis on operator training is a little bit out of proportion to getting systems that won't invite operator error.

MR. CONRAN: It is possible we could have done a better job, but maybe you didn't catch the first part of my comments. There are three things that we have done.

MR. EPLER: I did.

MR. CONRAN: To try to improve the situation after Three Mile Island. Basic was improved procedures based on better analyses. And I should have mentioned, improvements in instrumentation. We recognize the fact that he was fooled by indications, and we did address that.

MR. EPLER: That is serious.

MR. CONRAN: I was seriously delinquent in leaving that out, you are correct. That is an important element. We did not miss it. It may be that we could have done a better job in improving instrumentation, but at least two of the lessons learned, the early recommendations, had to do with direct indication of PORV and blocked valve.

MR. EPLER: To finish my comment, if I can pursue it. Identified in this discussion are two important points. One is that in prevention, which has to be emphasized because of lack of adequate mitigation, we have to go to great lengths to prevent failure of plant elements, and for the same reason we have to put a dependence - we would prefer not to - on the operator.

So, there are two areas there that have added complexity to this whole picture, the inability to free ourselves from those dependencies.

MR. CONRAN: I guess the only answer that I know of is when I have heard the question discussed before, some people pointed out that if you tried to do away with dependence on the operator at all, it would require confidence that you could identify every possible accident sequence so that the equipment could respond automatically.

MR. EPLER: I don't think that is true because I have seen it done. You do have systems that do that.

MR. CONRAN: I guess there is a question of whether to be in a system that complex; maybe it is a matter of complexity.

MR. WARD: Jim, does that complete your part, or will you get into the QA next?

MR. CONRAN: With regard to the terms "safety grade" and "important to safety" I am not sure whether the status of things was threatened or not by Mr. Epler's concern. What we are trying to do, in this meeting at least, up front, is to define terms that we can talk to each other about the underlying problems and the fundamental concerns involved.

I think it is entirely appropriate to talk about it, but I am not sure -- well, we need an established set of terminology so we can talk to each other about those things and know that we are being understood.

MR. BENDER: Well, I am a little unhappy with the definition, I am trying to write down something myself: Importance to safety is a measure of the consequence of failure. Safety grade is a measure of the quality needed to serve a safety function. And safety related refers to the conditions under which the safety function is to be performed.

I can deal with definitions like that. I am not sure they are the same things that you define, but I don't find any definition in what you have told me so far.

I do know that when you say "safety grade" I have to think about what qualities are related to it. That is why I said it is a definition of the qualities that serve the safety function.

When you say safety related, then thing that I do is say, what is it that I am relating to, and then I have to think, "Well, in a primary coolant system its ability to survive under very high pressure and temperature." And in the radioactive effluent system it is the ability to deal with very low pressure fluid that has some radionuclides associated with it.

Then I can deal with the importance of safety just in terms of, "Well, what are those consequences when I have a safety grade system performing some safety-related functions, what can I tolerate?"

Then, if you want to use that as a measure of the degree of importance I can say, "Well, the importance of safety is a function of what I would do if it failed." That is a set of definitions that I offer just because you have to have some food for thought. You may want to have some different ones, but I have not heard any definitions yet from you that I could re te to the things that are up there.

Now, I will just leave it.

MR. CONRAN: I don't have a problem with any thought processes or classification schemes, or ways of determining what quality level ought to be.

What I am wondering is, are you suggesting that when I say "safety grade," that is a term that means something to the staff and to the industry, people who have been involved in the licensing process. And it is related to or associated with a certain section of the regulations.

I have not, in fact, tried to describe a scheme for classifying with any fine degree of resolution what the safety classification or the level of safety, or quality standard ought to be. That has already been done, as a matter of fact. That is not something that we have to do starting from scratch.

MR. BENDER: The thing I am trying to point out, in some cases you said something was safety grade, and you add certain properties to it - seismic resistance.

When you do not say it is safety grade, you imply certain qualities. The quality you imply is the normal thing you would get if you did not do anything special. But there is still something there.

MR. CONRAN: Nothing that I have said runs counter to that.

MR. BENDER: No, it does not, but I think it commits you to accept the designation as something being safety grade by saying, "I have fully defined the problem." If I do not designate it as safety grade I am saying that its ordinary properties are acceptable for safety purposes.

MR. CONRAN: That is asically the same degree category and the rest of the whole set of importance, say. That is not safety grade. That's really the breakdown that we have right now.

MR. BENDER: I don't want to go into it any further.

MR. WARD: You know, it really seems to me that the definitions, a little more meat on the bones, will come in the QA discussion where we have the categories and the definition of those classifications and classes. Why not go on to that and then return to this?

MR. CONRAN: I guess I would want to talk a bit more about the relationship.

MR. WARD: OK, Item C is the relationship between the definition of safety terms and QA requirements. That is the next item.

MR. HAASS: I thought I would take a few minutes to just explain how we handled this kind of a problem in the QA area, that perhaps throws a little sand into the grease, but we think we have it straight.

We basically divide things, provide structure, systems, and components into two major groupings, and we rely on the definitions given in Appendix B and in Appendix A of Part 50.

The first grouping is "safety related," and there we draw on the definition of safety-related items in Appendix B which says that they are the items needed to prevent and mitigate the consequences of accidents. We rely on Reg Guide 129 to give further guidance regarding what kinds of items those are.

As far as QA controls are concerned, they satisfy Appendix B, and we require that they be applied to these items consistent with the items "importance to safety" as stated in Criterion 2 of Appendix B.

We have developed detailed requirements for such a program. It is given in our standard review plan and we rely on the reg guides and the endorsed standards to define what that program is.

Now, as we already discussed this afternoon, there is a second grouping of items, items we call "important to safety." We say those are the remaining structures, systems and components in the plant that have some effect on safety. They fall under General Design Criterion 1 of Appendix A, which alls for a QA program for items important to safety.

One of the differences, now, between "safety related" and "important to safety" as far as QA is concerned is, we have not gone as far as to develop the specific criteria that would satisfy GEC-1. We have only done that for Appendix B.

We are proposing for the future, and we have a rule-making process under way, to clarify the applicability of Appendix B to all items that affect safety. In other words, it would apply to all the items important to safety. This can be derived from Appendix A to Part 50. We do not have a list at this point, but we feel that would include practically everything in the plant with the exception of perhaps water coolers and "Johns." Everything else has some effect on safety and therefore a QA program which is consistent with that item "important to safety" should be applied.

MR. EPLER: Let me ask a question to test your statement. If the roof caves in, then all of the items in the first category will likely be inoperable - cables will burn up and things would not work in general. That would make the fire extinguisher equipment of safety; wouldn't it? But you don't expect to gold plate it.

MR. HAASS: I missed your last statement.

MR. EPLER: You would not gold plate a fire extinguisher. In other words, you would leave it in this category; all the columns supporting the roof, the fire extinguisher and all those things would have to be just good enginerring.

MR. HAASS: Yes.

MR. EPLER: But they could destroy everything in the other category.

MR. HAASS: We have a positioning in Reg Guide 129, that is Postion 2, that calls for consideration of items that can fail that are not generally safety related, but whose failure can affect safety-related items. Those would have to be analyzed to determine what is the effect that they can incur on safety-related items, and then appropriate measures would have to be undertaken to assure that that would not happen.

MR. EPLER: Then you have to make a deliberate assumption that conventional engineering techni ues are as reported for the building structure because when it fails, the game is over.

MR. HAASS: Yes, sir.

MR. CONRAN: There is something wrong here. There are requirements, design provisions, to assure with high confidence that the roof is not going to fall in on the first category. The structure that those safety-related systems and components are housed in must be designed --

MR. EPLER: I am making an assumption here that if the roof caves in it is catastrophic; the operators are out of the building, nothing works.

MR. CONRAN: But you are obviously beyond the design basis. You can design to accomodate a safe shutdown earthquake and other natural phenomena, whatever is appropriate.

If it is located in proximity to a firing range, I think so. If it is located next to an airport --

MR. EPLER: I don't think you will send your grand-children to college on that one.

MR. CONRAN: What I am saying is, safety-related systems by definition are housed in structures whose design basis is to accomodate these extreme natural phenomena and every likely occurrence.

MR. EPLER: This is endless, there is no end to this.

MR. WARD: Why don't we let Mr. Haass proceed?

MR. HAASS: Well, I think the situation at each plant site has to be considered. As Jim was saying, if there is a firing range nearby, that aspect is going to be considered. Whatever impact it can have on the plant design has to be considered.

MR. EPLER: If you know about it.

MR. HAASS: Yes, if you know about it. That forms part of the design basis.

Under plan, under the TMI Action Plan, is to expand the listing of items, structures, systems and components, to which Appendix B applies by including all items important to safety. In fact, we have initiated that position on several plants, as noted in the bottom paragraph. We have applied it to Zion, Indian Points 2 and 3, and also to TMI 1. They have been particularly selected for this.

But the position will also be applied to all plants once the rule is promulgated.

MR. EPLER: Well, then this tells me that in the case of the Browns Ferry fire where we found the design and the preventive techniques to be inadequate, that we should go back, back to Browns Ferry, put one cable-spreading room above the control room and one below the control room so that we can stand the next fire because we can't prevent it.

MR. HAASS: No, not at all.

MR. EPLER: I would not want to, either.

MR. HAASS: I am talking quality assurance, and the stipulation is that the QA is forward fit. We are talking about activities, future activities would be under the Quality Assurance program.

Now, you are raising a question of design requirements, I am not going to address that point. That is a different point. I am talking about quality assurance. I don't know of any plan to go back to other items because we stick them under the QA program to change their design requirements. I do not think that is in the cards.

2:55
Minson
fls

MR. BENDER: The thought that crosses my mind, listening to what you are saying, is that with this approach you would be imposing a burden on the staff, because you will wind up having to check everything, and the things that you can do may not be very meaningful.

MR. HAAS: When you say checking, what do you mean by checking?

MR. BENDER: To be able to look at documents, being to see the fabrication, construction, and design processes.

MR. HAAS: You are talking about the I & E f nctions?

MR. BENDER: Yes. That is what your emphasis is on, the I&E functions, as I see it.

MR. HAAS: That is where a good bit of the effort would eventually reside. Again I would assume, just as is being done now, the inspections have to be selective. We inspect on an audit basis. We have to select those that we think are more significant to safety than others.

I am not really in a position to say what would be done, but I would think that this is the kind of approach that would be taken.

MR. BENDER: But you have a narrower list to deal with now.

MR. HAASS: Yes.

MR. WARD: But, Mike, isn't that the point of the graded system, whether you want to use those terms or not. The systems whose failure would have the most significant consequences are going to be given more intensive I&E inspection, more intensive auditing. You spread that effort where it will do the most good.

MR. BENDER: I keep worrying about the term "graded."

MR. WARD: Yes, I hate that term.

MR. CONRAN: May I raise a point?

I think what has happened here is another example of the same sort of thing that happens, say, in the context of the TMI case. We are being careless, I think, with terminology here. It sounds like you are saying, if I could refer to a pie-chart diagram, it sounds like you are saying, they are safety related, and everything else in here, this is important to safety. That is not consistent with the language in Appendix A. Appendix A says that all of these things, taken together, are important.

MR. HAASS: I understand what you are saying, and I can clarify that. The way you described it before is correct. All items important to safety would include the safety related items. We have taken them aside as a subset. I am just being consistent with your prior discussion, I think.

MR. CONRAN: What you mean, that is all other important to safety SSCs.

MR. HAASS: Yes. All other SSCs needed to provide reasonable assurance. I think that it is consistent.

MR. BENDER: I am trying to encourage you not to be so broadsweeping in the amount of stuff that you are going to have to maintain quality assurance surveillance over, because it will get out of hand. You will not be able to cover it. You will wind up getting an inundation of documentation that you can't deal with.

MR. CONRAN: Doesn't it depend on the stringency with which you apply --

MR. HAASS: We don't plant to get inundated with documents. I don't know how that would happen.

MR. WARD: May I ask you this. Would it be fair to say that on the pie diagrams there, in the second group, much of that is going to be covered by what you might call standard industrial practice?

MR. HAASS: I would say that that is pretty much true, yes. We have talked to a lot of utilities, and queried them regarding what kind of QA they are applying to this second group of items. The answers ranged pretty broadly from commercial practice to some items we feel have some importance to safety, or they are necessary for the reliability of the plant, so we apply additional QA controls on them, but they are not on the QA list, so the I&E inspector is not involved in those, but under this proposed scheme, of course, he would be.

Again, let me explain that the grading or the applicability of QA controls to particular items is going to be determined by the applicant. It is not something we do. It is the applicant who does this. We stress that it should be a combination of the engineering people, who understand what the function of the item is, to identify the important characteristics, the important aspects of that item, and the QA people deciding what controls are appropriate to assure that those characteristics are, indeed, provided.

So it is that combination that should decide what is the extent of the QA requirements to be applied to a particular item, and it will vary.

MR. CONRAN: Is it inevitable, or is it required, to address Mr. Bender's concern, that NRC inspectors would have to involve themselves in auditing the QA program for the rest of this?

There are really two aspects to this. One, the staff has never reviewed what the applicant does in that area, and that Walt it is proposing to do. Then the second part of that is, if necessary or if desired, have the I&E inspector audit to verify that the licensee is doing what it says it is.

Is that last step necessary; maybe that is the answer to your question.

MR. BENDER: The auditor has to have something to audit. He cannot audit commercial practice, because commercial practice is generally not written down. That is what I am trying to ask you to think about.

MR. HAASS: I think that this gets into some of the remaining questions. That is, the plans for classifying items, our action plan under 1(f)(1) calls for developing a Reg Guide that will assist in categorizing and determining the extent of QA controls appropriate to a particular category. That has not been done yet, but that is the kind of thinking that we are doing. We plan on that in the future.

To get back to your other question about the extent of IE involvement, obviously there are more things that I&E would be looking at that may involve additional inspectors. We have not gone into that yet.

MR. BENDER: You are going to get it into the regulatory format before you have determined what your capabilities are. I really think you have to think very hard about that. Once you get it into the format, you can't back away from it because the Congress did not let you have another 100 inspectors. You will have to do with whatever resources you have got. I believe somewhere you are going to have to restrict how much coverage there is going to be. I doubt if you could find 100 inspectors that were qualified anyway.

MR. HAASS: I can't add anymore to item d, unless you have more questions.

The plan is to categorize items, and determine roughly the kind of QA program that is appropriate for this category.

MR. WARD: Let's, Walt, item d, I guess I did expect you to give us a little more meat. How, for example, do your classifications a, b, c, and d, fit in with these definitions? Is there some correspondence at the present time, or isn't there?

The QA classifications a, b, c, and d, do they correspond with this? Are they subsets of the second important to safety group in some logical way?

MR. HAASS: You are talking about the class of systems?

MR. CONRAN: I can answer. a, b, and c belong to the safety related grouping. d belongs -- I am sorry, the safety related, the way that we talk about it, a, b, c, and d are all in the safety related the way that you have defined it.

MR. HAASS: d is rad waste systems, that is not safety related.

MR. BENDER: That only applies to pressure containment components. There is a whole category of other stuff that is outside of that category that is all safety related, or has a safety associated with it.

MR. CONRAN: That is right.

MR. HAASS: I really had not thought in terms of that. Our approach is that the technical people establish the technical requirements, the quality standards that an item must meet. Then our relationship with that is to apply the QA program consistent with that item's importance to safety.

As I have mentioned, up to now we have divided it into two groups: safety related, and other items. The safety related comes under the QA program, and those are generally the upper-tier items, the items needed to prevent or mitigate the effects of an accident. Those have been treated extensively under the Appendix B program. Others fall under GDC-1, and we have no detailed guidance for what applies to those items QA-wise.

MR. BENDER: If the solution is to have a Reg Guide, I am opposed to it.

(General laughter.)

MR. BENDER: Life is not long enough to go through that Reg Guide.

MR. HAASS: Question e is, "How would the creation of a quantitative safety goal affect the distinction between various plant systems?"

I guess I can speculate at this point that if the quantitative safety goal is developed, at the same time there would be assigned a contribution to safety that individual items would provide toward meeting that safety goal. I could visualize that that contribution to safety would serve as a means of categorizing items.

In other words, you would again categorize items consistent with their importance to safety QA-wise, and then apply the appropriate QA controls consistent with each category. That is the general scheme I see at this point, and we are not close to that.

MR. WARD: Are there any questions on this point?

MR. BENDER: One point, and maybe it is going to come up later. There is a very heavy emphasis here on what I would term design and construction, and a very low level of emphasis on use and inspection. This may be the way in which this has to go, but when we are dealing with this business, end use is the crucial issue, and I don't know where that comes into the picture. Where is that?

MR. HAASS: I may have not conveyed the correct impression.

We are considering this philosophy for operating plants as well as design and construction. In operating plants, we are talking about activities involving maintenance and repair, replacement, inspection, testing, any activity that might take place subsequent to initiation of operation, and the same principles would apply. No distinction is made.

MR. WARD: We are down to the last item on our agenda. We do want to give Mr. Gallagher an opportunity. Why don't we take a 10 minute break, and then we will come back, and we would like to hear what you have to say. Then we will have our wrap up.

We will come back at 3:15.

(A short recess was taken.)

MR. WARD: Mr. Gallagher.

MR. GALLAGHER: What I would like to show you, as I said earlier, work that has been going on in an ad hoc group that was established through joint agreement with the NRC Office of Standards Development and the IEEE, to attempt to prepare a document that sets forth criteria for determining the level of importance to safety of the instrumentation, control, and electrical portions of nuclear plants, and to specifically work up methods for then guiding the design of these systems.

It says, "The purpose of this document is to present a uniform classification approach for determining the applicability of design criteria and design requirements based on the level of their importance to safety."

The basic thought here was, if one could get some graded approach, then you look back at the requirements that were already there, and find out how applicable they were, or how one might relax on some of the rules that are already there based upon the fact that their safety function was not as important with respect to the consequences.

So this was our general approach. We had some interesting numbers. This effort is not easy. They were people from NSSS vendors, utilities, equipment manufacturers, and the NRC. We have had four meetings, each meeting running from noon Monday till noon Friday in the basement of the NRC offices in southern Rockville. We have spent about 1300 manhours, split as you see, of people from the industry and the NRC.

We are on our fourth document, which will be issued at the end of this week for review and comment, for review and then action by the IEEE-NPEC, the power engineering group, early in March.

That is sort of an overview.

In order to do this, to get this goal, we have three major sections. First of all, you have to identify what these systems are. We have worked up sort of a structure thought process that one can go through, and by going through this identify the systems in the plant, with respect to the functions they perform, that are important to safety, or their failure modes that have an adverse impact on safety.

Hopefully, they are written in a way that the average engineer working in the field can go through and say, "Yes, this is one of these, and these are its characteristics," and establish adequately enough to be able to go through the process in Section 4 which allows one then, to judge the level of importance to safety by coming up with a characteristic number for the system.

The numbers run from minus all the way -- Although if it is less than a zero, it says that maybe you ought to go back and look at what you did in Section 3. If it is a low number, it says that it is not really that important to safety. If it is a large number, it says it is important to safety. These numbers run from like zero to six.

MR. WARD: Can you tell us a little bit more about it?

MR. GALLAGHER: I am just giving you an overview of what is in the document.

Then Section 5 gives you general requirements in the mid-range of importance to safety. These cover the areas of QA, qualification, maintenance, testing, calibration, and the general area of system configuration, which talks about diversity, physical and electrical separation, and things like that.

The identification looks, as I said, first of all at systems provided to assure the safety of the nuclear reactor, and to maintain the radioactive releases within specified limits. This would be the safety grade plus things like the coolant system for the spent fuel pit, which now isn't covered by our present documents.

It would also include systems whose failure could cause the design basis of an event to be worse than that analyzed for. Then there are the normal systems that are there for the operation of the plant, so that it can generate the thermal energy and turn it to power. Then there are other systems for the administrative operation, such as the security system.

So this, then, covers the systems, and this is a further of that. You can see that these are the systems that I think you people cover by safety grade. These are systems that also do safety functions that are not covered. These are systems whose failure could, as I said, lead to situations worse than in the design basis event.

For instance, the interlock that prevents the crane from carrying the cast over the spent fuel pit, that interlock would be in that system. It is there, and people put that in, so now since that is there I can limit the accident to this damage.

Then there is the one that we always seem to talk about, and that is systems whose failure could either impair systems that are there for safety, or could challenge the safety systems. For instance, those systems which control the reactivity, if they fail, pull the rods out, and they challenge the safety systems.

MR. CONRAN: In your scheme for ranking, do you attach quantitative values, generally decreasing to these?

MR. GALLAGHER: These are the systems as they are identified. Then we will go into the step with the numbers.

MR. ROSSI: That is not a ranking there.

MR. GALLAGHER: This is not a ranking.

MR. ROSSI: That is just the listing of systems.

MR. GALLAGHER: Our purpose was to realize that everything in the plant has to be looked at to decide whether or not it is important to safety. Hopefully, from this looking, you will be able to put them into categories, or into groups where you can then take some appropriate action on them.

The model for determining the systems' importance to safety is based upon risk. The basic argument is that for these systems, our ranking process only ra [illegible] the systems that are outside of the normally class 1[illegible] systems, since we felt that part of the process is to look at the failure of the system to function.

We all know that if you look at the failure reaction trip system, that is an issue that people have been spending quite a bit of time on, ATWS, and here we felt that we wanted to give a way of dealing with the systems that had not yet been given requirements. So we put those outside of this ranking process.

MR. WARD: You are saying this whole discussion, or this task P827 is all for non-1-E systems.

MR. GALLAGHER: It is for systems that are not now considered as class 1-E systems, right. We have already said that those systems have already been given rules.

MR. WARD: Right.

MR. GALLAGHER: If you look at this chart here, risk is a function of the probability of event, and the consequences resulting from the event. So here we say that risk is the frequency. Then it is the probability of the system that is there to do the function, or an alternate system that could do an equivalent function, or manual actions one might take to get these systems back into operation, or provide another alternate fail, and then what are the consequences, then, in this failure.

The solution that you are after here is the value that the system has to have. In other words, what should its failure probability be to satisfy the risk.

Part of our thought process is that it is unlikely that a failure in these systems, which are those that were not grouped with the safety system, that a failure in these other systems would result in a failure of all three barriers to prevention of release. That is, the fission product, the fuel cladding barrier, the reactor, the primary pressure barrier, and the containment barrier. However, the failure of this system can be a cause or a contributory cause to the failure of one of those.

Then we further say that the failure will have to cause a direct measurable harm to one or more persons because of the radioactivity release. In order to do that, we have to look at the value for risk, and we set the value of risk as 10 to the minus 6 early deaths per event, which is a number that was taken from -- It is very similar to the number, I think, that was in the (inaudible) that was five times 10 to the minus 7. That is a number that I believe is used in the UK. That gives us the basic value for risk.

MR. WARD: So your bottom line here, the consequence of failure, is the number of early deaths from the event; is that what you are saying?

MR. GALLAGHER: Yes.

MR. WARD: And your acceptable risk level is 10 to the minus 6.

MR. GALLAGHER: Yes.

We also know that the overall consequences, and these pretty well are pretty based upon to 10 to the minus 6 values per demand, and a rate of one per year.

If one say, that is the total, then you can allocate this total to the different barriers. Here we put most emphasis on the integrity of the fuel cladding. That is really the first barrier, and if you protect that barrier then you are in reasonable shape. So we want the highest confidence associated with the protection of this barrier.

If you go down to the next one, the loss of primary pressure boundary, it isn't as strong, unless you also do damage to the fuel.

We are not talking in this about LOCA accidents, or accidents of that type. They are already covered by those other systems. These are systems that are not now graded with respect to their importance to safety.

With this methodology, we are able then to --

MR. WARD: Let me see if I follow this. You are saying that the propability of failure is 10 to the minus 6, and you are kind of arbitrarily dividing that up among the three barriers.

MR. GALLAGHER: Yes.

MR. WARD: Then assigning qualities to your ICE systems in each of those areas to meet those goals..

MR. GALLAGHER: Right. This lets you get a number for the consequence which is six minus whatever this value is. For instance, the consequence of this is larger than the consequence of a failure in this area.

When you solve the equation, if I had realized the earlier discussion, I could have made these slides differently, and shown you that when you solve for this value it is basically the ratio of the risk to these other factors. The more important a system is to safety, the larger this value is. It is basically everything that has been put into logs, so that the numbers are all like numbers from one to five range.

We give curves for all of these. You can go through and look at these systems. You can look at the frequency of the initiating event. You can look at the alternate systems. We have curves for the probability of the alternate systems. You can look at the remedial actions in terms of the time to take the action versus the time available for the action. You can look at the function to see exactly which barrier it is you are providing protection for. Then that ratio then gives you a number for this.

If the number is less than 0.5, we say that it is not important to safety. If it is greater than about 3.5, we say that it is very important to safety. If it gets up around five or six, there is even a question of why wasn't this in the 1-E.

If it is in the middle range, we say that we think we can identify reasonably clearly what one may do with those systems in terms of QA, and qualifications, and other factors.

Basically, what we are asking to be done in those areas -- First, assume QA, we spent a lot of time on the QA in one of our meetings, and about the best that we could come up with is that there shall be a QA program. The QA program shall be based upon the factors identified in Appendix B, the applicable factors.

However, the burden of proof for an adequate QA program is placed upon the person who either procures the equipment or who uses the equipment. It is his job to make sure that what he is buying is going to do the job it is supposed to, or that the user keeps it in a way that it will do the job it is supposed to.

He does not have to pass these on down to other people. For instance, he can go into a manufacturer's shop, look at the QA program there, satisfy himself as to how applicable that is to the QA he sees has to be met. If necessary, he may buy some additional steps in that shop, or may do some testing on his own. But we are trying to prevent him from having to go to that person and saying, "You have to meet a QCS 1," or whatever. He picks up that burden.

Assume the person using that, before he makes a modification, he should know the level of importance to safety, so that he assures that the modification is properly done.

We feel that both the people who are responsible for the procurement, as well as the operation, already know most of the rules for the 1-E stuff, because they have been living in that atmosphere.

What we are trying to do is to not have them have to pass this on down to people who normally don't live in this climate, but who do very good commercial practices. They are out to sell the product, and if they want to make money on it, they have to meet certain guarantees.

MR. HAASS: You are talking primarily about commercial kind of items, where the purchaser really can't impose additional requirements on the supplier.

MR. GALLAGHER: That is right.

MR. HAASS: It is really not practical to do that.

MR. GALLAGHER: If he would go, a lot of these people would tell him, "Why don't you buy from somebody else."

MR. HAASS: So the purchaser, the burden is on him.

MR. GALLAGHER: It is on the guy who either purchases it, or who uses it.

MR. HAASS: Yes.

MR. GALLAGHER: The burden obviously has to be on the person who would use it, because he has to make sure it gets put in right, and maintained properly.

Similarly, in the area of qualification, the rules as they have been written by industry say that you can do a qualification by testing, experience, or analyzing. In reality, testing has been where all the emphasis is.

We feel that we could relax these to allow more use of related experience, in both the nuclear industry and in other industries, by extrapolation or interpolation of their experiences through means like analyzing the situation.

For instance, if one can show that the stress the equipment was placed in, when somebody else used it, is equivalent to the stress that is going it is going to be placed in for this use -- Once you are able to use that as a justification, it will do its function when called on. For instance, there is a lot of work in instruments in the geothermal area, and things like that.

MR. WARD: Do you think that the experience is well enough documented and expressed quantitatively enough to be used in this way?

MR. GALLAGHER: Part of the analysis would have to include that. It would have to show the basis for this, and one would have to make sure that the documentation is on a reasonable basis. That way, when somebody says, "I have good experience," you have to find out where it was actually used, and what he did with it when it failed. Did he fail because nobody told him that it failed, but just kept it operating.

Here again the emphasis is to make more use of what is already available. Then to put it through some special program which in the long-run may not give us much confidence as to get the other way.

We have similarly set up rules in the area for the configuration, and of the other items that I mentioned.

That is a summary. This has been a very controversial matter. We get a lot of comments, very much like those that Mr. Bender raised -- what does this mean with respect to the amount of the plant that has to be looked at. You could end up with very large and difficult burden, unless it is properly implemented, and the responsibilities for having it done are properly placed.

This document will most likely, if it gets issued, and it has to be voted on to issue, be issued as a trial use guide. We have found this to be of value to let people talk to each other, so they can talk on a common basis as to whether or not something is important to safety, arelatively how important is it.

A lot more work has to be done, I think, and a lot more experience has to be gained before one would dare issue this as a statement.

MR. HAASS: John, what prompted this?

MR. GALLAGHER: Two things. One, I have been working on a similar item with the IAEA, I am one of the working group there. The IAEA had to come up with a document that dealt with instrumentation and control systems.

Prior to that, up at Westinghouse they had been putting a lot of effort to get a classification system into the industry. In addition to the 1-E, we wanted 2-E. They have given up on that. But after Three Mile Island and all the things that came out in the action plan, to us it was obvious that a lot of things were not 1's, but they had to have some rules.

So based upon the work that was done at the IAEA, which Ed Windsor had also been doing -- he on the group that locks over this -- we felt that it was worth an effort to try it in this country once more with a group from the IEEE, and the NRC.

MR. BENDER: Could you take and illustrate a piece of hardware, and show how you might apply the analysis to a piece of hardware?

MR. GALLAGHER: Yes.

For instance, the system that we built to drive the rods has some circuitry in it that is there to maintain the maximum speed of the rods within a certain value. We do our design basis study based on that speed. In order to violate that speed, this system now has to go through a double failure.

So one could say, we are going to look at the frequency of a rod withdrawal accident, asset it, and anticipate its operational occurrence would be on the order of once per year. So frequency would be one per year.

MR. BENDER: All rods, or each rod?

MR. GALLAGHER: Our rods move in groups, so this is a group of rods.

So it would be that frequency. Alternative system, there really isn't one now. Based upon the fact that we have built this to a fairly quality, there isn't enough time for the operator to take any action, and when this thing goes up, it comes out.

The consequences of failure of this, if you go and look, are somewhere in the range more like a threat to the fuel cladding. Most of the consequences of this would be to reduce the d and b ratio from 1.3 down to 1.1 or 1.0.

So it is difficult to say that there is loss, but it puts you in this range of either a threat or a loss, and when one then goes and works through the numbers, this would come out to be in the range of somewhere between 1.5 to 2.5.

This, by the way, turns out to be the values, since both the risk and the failures per demand that we were given here are equal. If they were not equal, it would be different.

MR. CONRAN: Is that the tolerable probability of failure in order to meet the 10 to the minus 6?

MR. GALLAGHER: For overall.

This would say, then, that the system is an intermediate level of importance to safety. Going in and looking at the rules, it should meet the single failure. We had said that we had better put it in so that more than one failure has to occur before you get this.

That is sort of an easy one. We have looked at it for things like, what about the reading on the level of oil in the diesel tank --

MR. BENDER: Let me just go back to this illustration, and I will arbitrarily change the conditions to see what happens.

Let's say that the probability of threat to the fuel cladding integrity remain the same, but the loss of the primary pressure boundary instead of being one times 10 to the 2 is now 1. There are some reactor systems where you can't scram.

MR. EPLEP: You have not scrammed yet.

MR. GALLAGHER: This one I gave was when the event was an inadvertent rod with a draw that was bounded, that was held to a certain speed of insertion of reactivity, not the loss of a scram capability.

MR. BENDER: I am just trying to find out what happens when you change it. I don't really care because it is not an accident.

If I were to take the condition which said the primary pressure boundary is 1, what would happen to the valuation process; that is all I am trying to find out.

MR. GALLAGHER: Our process does not deal with the accidents that are presently done under the 603, or the 1-F studies. In other words, the way this process works, it can deal with things which make those situations worse, but not in order of magnitude.

MR. BENDER: So this is a grading.

MR. GALLAGHER: Yes, this is a grading. We did not want to put this in, and have to always go back and try to numerical solve the anticipated transients, or without scram. So if you look at the boundary, this is a perturbation to that boundary. It does not deal with failing the clad, failing the primary system boundary, and failing the containment. It deals mainly with one or the other, or maybe some combinations like failure here, and threat there. It is a perturbation.

MR. WARD: For example, in the actual analysis of a LOCA, you assume the starting conditions are here, and those systems are those that assure you are in that range of starting conditions. Is that what you mean?

MR. GALLAGHER: Yes, and that you are outside of that range, and how much might you be out, and if you are out, you are going to have a little more energy in the fuel, so you will make the situticn somewhat worse.

I think the value of this is that it does allow you to address the kind of things that you are counting on, and to keep things for the basis for the design of the other systems.

It is also interesting that if you lock at the effect of an increase in the frequency of challenge, we showed that the frequency of a challenge has to go up by several factors before it really becomes important. But the most important aspect of these other systems is if they make the situation worse, if they make the situation worse than that which it was analyzed for. This clearly shows that.

MR. WARD: Are there any other questions of Mr. Gallagher?

Did you say that there had been some reports issued from your working group?

MR. GALLAGHER: We have issued three drafts, and we are working on the fourth draft now. Members of the NRC get those.

MR. WARD: Could you see that Mr. Majors would get a copy of those, or access to them?

MR. GALLAGHER: I would only want to give him the fourth one, since the changes --

MR. WARD: You mean that the first ones are only drafts?

MR. GALLAGHER: The fourth one also. This is a draft until it gets approved by the IEEE at the next meeting.

MR. WARD: So you don't want it circulated outside of the working group, is that what you are saying?

MR. GALLAGHER: I give them to members of the NRC to comment on, and what they do with them --

MR. HAASS: The thing is that there is no point in you getting the first three drafts, because the fourth one is a revision of those drafts.

MR. GALLAGHER: There was a major change.

MR. WARD: Thank you, Mr. Gallagher. You, IEEE fellows, always seem to come up with some neat ways of looking at thing that the mechanical guys never quite get caught up with.

(General laughter.)

MR. WARD: Mr. Madeiros wanted to add something.

MR. MADEIROS: Thank you, Mr. Chairman.

My name is Manning Madeiros, first of all, and I am from the Office of Standards Development. I have got a little different perspective on what two of these gentlemen have said, Mr. Conran, and now Mr. Gallagher and I thought that it was worth you folks hearing it. I will try to be short.

I just learned about the meeting yesterday, so I don't have any fancy slides like Mr. Gallagher. I made some quick notes this morning, and some others through the meeting here.

I particularly want to address the early point of Mr. Bender. He said that everything is safety related, and it is the type of relationship that we should be addressing. We have to discriminate in how we design, and what engineering we bring to bear. Those are almost his exact words. I would like to spend five minutes on it.

By way of quick background, I have spent many hours with Mr. Conran, and several others, on the testimony for the TMI-I restart. I was also the first NRC member on Mr. Gallagher's group. I signed the agreement between the NRC and the IEEE. I was a member until recently. I am taking over full-time the work on degraded coolant activities, and that is why I am not on it now.

MR. WARD: We are sure glad you are here.

MR. MADEIROS: I am kind of glad that I am here, too, because I am disturbed by some of the things I am hearing.

First of all, I don't share Mr. Gallagher's optimism on the value of the work that his group has done to date. Basically, there is a prime need for a very practical document that ranks the importance of control instrumentation and equipment in relation to safety.

These fellows, as hard working for 1300 manhours, and as well intentioned as they are, are using a surgeon's scapel to cut a cord of wood, when instead they ought to be using an axe.

I stated this publicly. I stated it in writing. All the comments I want to make here now are all going to be very terse, but I can support them all in detailed written justification if you so desire.

I will get to Mr. Gallagher's business a minute later, but I wanted to mention this background so that you would know that I had more than just a superficial interest here. I have some knowledge of the subject.

Because of the way that pie was cut up on the screen a little while ago, the way those portions are handled, mediocrity abounds in the instrumentation in the control area.

That is the one I am talking. You could start with the well mentioned standard review plan 7.7. It is technically repulsive. It talks about instrumentation control equipment which are very strong systems that can cause an accident, or make worse; can preclude an accident, or mitigate its effects, and relegates them to non-safety related. Of course, we know how non-safety related equipment is reviewed.

It is not reviewed. It is well stated in Commission publications that have been published in the Federal Register recently, and several documents, and I can provide those if you wish.

A recent one, for example, said this, "With regard to Standard Review Plan, Section 7.7, it calls for staff reviews to assure that failures of control systems will not impair the capability of protection systems in any significant manner or cause plant conditions more severe than those for which plant safety systems are designed."

These words, now, the staff has not pursued these reviews other than to assure that electrical interconnection between protections system and control systems are implemented, so that failure in system equipment cannot impair the operation of system equipment. It is not a very thorough review at all. This happens to be in a memo from Ross to Denton. I could quote something similar in some of these others.

Another example of mediocrity might be the TMI control room, and I doubt that I need to recite all of that. You can go and pick up some of the Kemeny Commission reports and see the numerous deficiencies. Fifteen hundred alarms in the control room, one silencing switch, no rhyme or reason to the colors that are used for alarms and indicators. Some indicators are behind the panel with switches on the front that you can't see. Just beyond design deficiencies, they are actually out and out stupidities, yet this control room has never been considered safety related, safety grade. That is an example that I can give you of that.

Another point I would like to make. When we base our standards, our reviews, and our designs on this kind of mentality that you see in that pie chart up there, you end up with mediocre equipment, it does stupid things.

The Crystal River recent incident, last June, I believe it was, it merely wanted the plant to shut down, and it automatically pulled the control rods. You needed water for cooling, but they automatically shut it off. These are fundamental things that should not happen in systems if they were built to high standards.

Now to get back to Mr. Gallagher's presentation here a little earlier. I will try to be brief, but I can go into great detail if you wish.

There still seems to be a lack of understanding in the agency and in the industry, in particular in Mr. Gallagher's group of which I have been a part, to technical excellent in the control area.

You need not look any further than a letter issued a couple of weeks ago, for example, whereby a member of Mr. Gallagher's group - this was issued on January 19 - he characterized some of what we just saw on the board, and I will quote, "A rehash of an outmoded approach to the design of control systems. It leaves virtually all of the nuclear power plants' major systems outside the ranking process, and outside the process of applying greater requirements, an obsolete idea that was complete debunked by such events as that of the TMI accident." That is an excellent letter from the gentleman that you ought to read in connection with this work, that I think characterizes a good deal of this.

MR. GALLAGHER: Why don't you also say that was on the previous draft.

MR. MADEIROS: Yes, but as early as last week, when we were all in meetings, Mr. Gallagher and his group still did not consider control systems.

MR. GALLAGHER: That is not true. Have you looked at our last draft?

MR. MADEIROS: Not in detail.

MR. GALLAGHER: So you are not making an accurate statement.

MR. MADEIROS: I am bringing you up to date --

MR. GALLAGHER: Be careful of the accuracy of your statements.

MR. MADEIROS: May I finish please, I did not interrupt you.

The next point I want to make. I have not reviewed this group's work beyond last Monday morning. They met last Monday for a week in the Nicholson Lane building. I have not caught with it in the last week. However, I have listened to enough here today to support the general view of the scapel versus the axe, for example. That is not the kind of thing we need in this work.

MR. BENDER: Do you plan to tell us what the axe is?

MR. MADEIROS: I had some early suggestions, but mine are not sacred either. I was willing to work with the group, and still am, to come at some practical ones. Yes, I would be willing to do that with you, certainly.

MR. BENDER: Give us one or two. I am trying to get the flavor of what you are proposing as an alternative.

MR. MADEIROS: I don't have a proposal here. I just made these notes in the last minutes. My idea would run something like this:

Certainly, all the control instrumentation equipment, the major control instrumentation, rold control systems, rod position indication systems, reactor plant alarm systems, all of those are very important to safety and should be considered as part of this work. Do you include them today in your standards?

MR. GALLAGHER: Most of those that you have mentioned are already in.

MR. MADEIROS: That is not so. I have been working with it, and I know.

First of all, I would make sure that it included all the important instrumentation. Secondly, I would try to find some practical way to rank them without all of this risk assessment business, perhaps in relation to coolant, perhaps in relation to inventory, perhaps in relation to reactivity addition, major functions like that. Then simply come up with something that a good engineer could apply without benefit of legal advice, and a manyear of effort to decide whether this system was important to safety.

MR. BENDER: Let's agree that probably an engineer will have a great deal of trouble finding what the mortality is in the event of failure of the instrument. There is still a need to make a judgment about risk, and if it is some other kind of risk that we want to address instead.

If it is coolant system failure, then the tolerance for that failure will have to be dealt with in terms of all that instrumentation. Is that the general idea?

MR. MADEIROS: I am not sure I followed you completely to answer yes or no.

MR. BENDER: Suppose I said, I need a pressure sensor on the ECCS system -- I don't know whether I do or not, I just picked that. I would have to judge whether I need redundant sensors or not. I can judge it by deciding what the reliability of the sensor is, if I only have one, and I can also judge it on the basis of, what if I don't have any, which is tolerance for failure.

Now, would you envision that you would make those kinds of judgments?

MR. MADEIROS: Yes, but a more important one than either of those two -- I will make another one from the standpoint that the most important contribution that you can make to reactor protection is that which you can give the operator in the way of simplicity. The basic line of protection for your reactor is the operator. So besides good training, like everybody was talking about, good procedures and all of that kind of stuff, the next most important thing you can do for your operator is to give him good equipment that is simple, that he can understand, that he can operate correctly. I would factor that kind of mentality into my judgment of importance to safety.

MR. BENDER: It is probably another point just to say, design the system so that I don't have to depend on the operator.

MR. MADEIROS: I don't buy that. That is what is wrong with computer control ideas, there is nobody smart enough to understand all accidents ahead of time, or all ineptness ahead of time. Whether it be just casualties, or maloperations, or accidents, you can't forecast them ahead of time. If you could, you would correct the design defects.

MR. BENDER: But you anticipate the operator will be smart enough to diagnose the accident.

MR. MADEIROS: What you hope is to train him to such a high level that when need be his excellence in relationship to a machine will come to bear, and he will use his ingenuity based on his training, and his imagination based on his training, to do the right thing, where a machine can't do it. That is what I say.

MR. BENDER: Thank you.

MR. MADEIROS: I will finish real quickly, if I still have time, with a couple of other quick observations here.

The qualification particularly bothered me. I hope Mr. Gallagher has a new line on the qualification, because I would like to read out of one of the official reports of one of these working group meetings what qualification meant to that group.

"Some working group members would accept as qualification a vendors pamphlet. Others would accept a letter signed by a vendor's registered professional engineer. Others would accept a certified letter, and still others, simply a signed letter. In discussion, I established a threshold to qualification something more substantial than a vendor's telephone call." At least no one was willing to accept a telephone call as an acceptable form of equipment qualification.

What I am saying, what Mr. Gallagher has been recommending here today is not qualification, gentlemen, it is certification, which may be okay for certain levels of equipment that are not so important to safety.

When you have equipment that is important to safety, and you say that it should be qualified, then, By Golly, it ought to be qualified, and not certified by somebody's pamphlet, some analysis based on somebody's calculation. It ought to be a test. This is what qualification has meant traditional, and I would not corrupt it.

You don't agree that traditionally this is what qualification has meant, I see you shaking your head.

MR. WARD: No, go ahead.

MR. MADEIROS: I would not corrupt it with calculations, or analyses, or some of the things that Mr. Gallagher was suggesting a little bit ago.

MR. WARD: The problem is that if we can't satisfy ourselves with something less than full qualification, we are into the problem that Mr. Bender is quoting, and that we are overwhelmed by trying to have an elaborate qualification program for every little item in the plant.

MR. MADEIROS: I don't recommend that.

MR. WARD: I think the effort here is to come up with a graded qualification program, a graded approach.

MR. MADEIROS: In relation to safety.

MR. WARD: Right.

MR. MADEIROS: But only those important ones would be qualified. But don't tout that you are qualifying all these others, you are just certifying those.

MR. WARD: Okay. Qualification in lower case letters, let us say.

MR. MADEIROS: It is corruption to call some of this stuff qualification.

The last point I would make here is a quote that I took from an AEOD report. AEOD is a new office, I am sure you all know, that has been set up in the last year to analyze operational events. I was one of the fellows who set that office up. They are doing some very excellent work.

I read this out of one of their reports a little earlier: "Alternate safety grade instrumentation, independent of the non-nuclear instrumentation in the ICS single and vertical failures, should be installed at Crystal River and other BNW plants in order to provide information to operators in case of repetitive events."

I think that this is a very serious endictment of the kind, and I will go back to my word, mediocre approach to instrumentation control and design review that was characterized by this pie that is up on the board here.

With that, I will be quiet, except I offer to provide you further details to substantiate many of the views that I voiced here today, and I will do it promptly if you ask.

MR. WARD: Thank you, Mr. Madeiros, for your points of view.

I guess I would like to offer Mr. Gallagher a chance to -- I don't feel you have to refute or rebut every contention made, because Mr. Madeiros was just speaking quickly, and he made a lot of contentions.

MR. GALLAGHER: I will not go back on all of them. I will just go back on the last statement that he made in reference to our letter.

He used the term "official document" from the working group. The working group has issued no official document. It has issued drafts, which I did not realize were looked at as official documents.

Be that as it may, we did, based upon your concerns, change that section in the second draft, when you were still a member of the group, to meet equipment performance verification requirements, realizing maybe with some reason that qualification had come to mean something. That the bottom line of qualification is to verify that the equipment can do the performance. So we have already answered that one for you, and the document is written with that as the title.

MR. MADEIROS: I will check on that.

MR. GALLAGHER: All you have to do is look at the draft No. 3 which you have, and draft No. 2 which you have.

I think that one of the basic differences that some of the working group members had with the views presented here --

Let me go back to the statement of simplicity. I think that many of the working group members had experiences that came from large, land-based, commercial nuclear power plants, and our experience may be somewhat different than experiences that one might have from the Navy nuclear program. Things are somewhat different.

As I think back upon a lot of the differences of views that Manning brought up versus other people's, this was probably the kernel of a lot of those differences, when tried to write that dealt with large land-based, commercial nuclear plants.

MR. MADEIROS: I agree with that.

MR. WARD: I think, as Mr. Bender advised me earlier, we are probably not going to come to any wrap up subject at this meeting, and I think that it is true.

I think we have revealed that it is a little more than a semantic issue of coming up with some useful and consistent definitions. So I think we will have to go back and do some thinking on what we have heard here today, and we will be asking to hear from you. Particularly Mr. Madeiras, we will be asking you for further information.

Mr. Bender, Mr. Epler, do you have any particular comments?

MR. EPLER: I have a whole lot, and I don't think I can cover them in just a few minutes.

I think what I am worried about is an opportunity to go over this information, and discuss it further.

MR. BENDER: Did you have something that you were going to say?

MR. EPLER: I think maybe where we go from here from my understanding. I don't know how you want to handle that.

MR. WARD: You can ask the staff where they are going from here. We will have another meeting, and I will be in touch with you between now and then.

MR. EPLER: Fine.

MR. BENDER: Jim, I heard your discussion, and I think we got some kind of what I will call weak perceptions of how the QA part of I&E sees this thing, and some interesting views from other people, as well as the industry activity.

What is your idea of how you can put this thing together? I think you have partially showed us how difficult the problem is.

MR. CONRAN: My overall impression is that the discussion kind of got out of hand with regard to what I was trying to accomplish this afternoon. I don't resent having you discuss it.

It is natural that when we start talking about the concepts, that I am trying to put tags on, just names on them. I am not trying to specify acceptable methods or anything like that, I am just trying to come to a consistent terminology, so that we can talk about the real problem in a coherent fashion.

I was worried, or I was a little bit uneasy about what I thought was your reaction to a definition of safety grade. After hearing your comments, I gather that maybe it is the wrong term. Safety grade maybe implies to you the quality level. If I called that safety feature, or safety system, and then said that the safety grade or the quality level was determined in a fashion that has either yet to be agreed upon, or some -- In other words, it is a separate consideration from what I call that chunk of the pie right there.

Really what I would like to get away with this afternoon is this. Having looked at our regulatory process, the documents we use, and the terminology to be used, I contend, as a matter of fact Ross contends, that this is what we call things in order to do our business. Now it may seem strange, and it kind of took me aback, too, but everybody doesn't agree with it.

What we are trying to do is establish that as the terminology used. If the implications of the particular words that I have used are so offensive, or if you think they are misleading, let's say, we are amenable to a suggestion that we change the language.

Basically what we are asking is, look, after my review of our process, and the terms we use, that I contend is the way that we do business, and we want everybody to use the terms that way.

From your involvement in the process, perhaps when these regulations were drawn, you recognize an error in the way I have applied terms.

MR. BENDER: I think what has happened -- I am not saying that what you have up there is wrong, but what has happened is the legal process has created an aura about these terms that may have meaning for the purpose of a regulatory process, but has no real meaning for the people who are trying to define the requirements for these things.

What I tried to suggest to you was that in order to have terms that can be segregated, there has to be some hierarchy of meaningful, or separation of meaning, on or the other, and I see neither one up there. There is no order to it, and there is no separation of them.

MR. CONRAN: Let me address that. There is in the regulations a section that says, plant features that are provided to do these critical safety functions, this is in Part 100, that you have to provide systems to do that, and that they have to be seismically qualified, they should be seismic category 1. They don't apply a term to that.

So, just so that we can work with each other, and express things in kind of a shorthand form, the tag that we apply to that set of components without regard to what quality standards apply, we just call that group safety grade.

MR. BENDER: You can call them Sam, and you have avoided all the problems.

MR. CONRAN: Maybe when I said, safety grade, it implied to you that somehow in one word I was trying to define all the quality standards, or all the characteristics. That is not really true. Those are specified completely separately, and in great detail in various Reg Guides, SRPs, and codes, and standards, and that sort of thing.

MR. BENDER: What I am saying is that the terms mean nothing to me the way you have expressed them. They may mean something to a lawyer, because lawyers can just look at these papers and say, "In case X this is the way we used it, and as far as I am concerned that establishes a precedent. Therefore,, every time I deal with something, I go to the precedent that was established by case X."

But if you want people to have something physical, analytical, or functional to relate those things to, then you have got to provide more than just a pie chart. You have got to give them some attributes, and I missed that in this particular discussion.

I think the people on the Industry Committee, Manning's remarks notwithstanding, have tried harder to give the matter of how you define these things some qualities, and to that degree I think they are farther along than you are.

MR. CONRAN: Let me try something else, and it will only take me a couple of minutes.

I got talked out of using a little more complicated slide, which said, in the definition of importance to safety, it encompasses a broad class of plant features that contribute in important to safe operation, in all phases and aspects of the operation, including systems and components provided for normal operation of the plant whose failure could directly cause or aggravate an accident, or could be called upon to help mitigate the consequences of an accident. Examples, main steam, condensate, feedwater reactivity control, primary pressure control.

It also includes major casualty control systems, fire protection, emergency lighting, emergency communications. It also includes systems and components provided and control radioactive waste effluents, and we name the radioactive management system. In addition to those, it also includes vital safety systems, and interim safety features.

Would that have made you feel better?

MR. BENDER: You are doing exactly what I said was going to happen. Every part of the plant has some function that is important to safety, including the roads and streets, and including the role of the NRC in operating the plant during an emergency.

So you have got something that is so encompassing that you can't get the job done.

MR. CONRAN: It is pretty broad, I will admit, but there are some components I believe, probably, that are not important to safety.

MR. BENDER: If your effort is to define some terms, then say, "The job is done," that is what I wanted to know. We ought to go further than that. Who is doing it, and who is carrying the ball from there.

MR. CONRAN: To go a little bit further, the reason it is important to make a definition, or put a tag on the concept of the importance of safety, is that these terms have been so ill-defined, and so interchangeably used in the past, as a matter of fact there are some licensees that treat as equivalent all of the terms, safety related, safety grade, important to safety. It seems to me to be an unten-- e situation if you are going to even communicate with [illegible] other, especially when you are trying to embark upon thi [illegible]terprise, to determine degree of importance to safety.

MR. BENDER: Is this any better than that?

MR. WARD: I don't see anything wrong with the pie being divided up in some way to define categories, but some people seem to have a problem with that. The problem, as I see it, first of all, you have divided it very coarsely.

You have identified one type of thing as safety grade, and I might have a problem with that. You could name it "banana," or anything else.

The rest of it is ill-defined. Not only is it ill-defined, but it has the worse name that you can think of, non-safety. That is a terrible thing to name it.

MR. CONRAN: I understood that. They are not all that ill-defined.

MR. WARD: I have not heard any nice, crisp definitions, or even attempts at it. The chart you had up earlier with sort of the hierarchy, that certainly had the potential for defining things in the two, three or four slices, but you didn't do that. It seems to me that that can be done.

You don't have to get to the scapel approach, which maybe someday we will, and that would be great, but maybe with an axe I can cut this chart up into four slices, and give them some reasonable names. I don't see why we can't do that.

MR. CONRAN: That is a future activity. I have heard and understood, and we will respond to the comments that I have heard with regard to what we are going to do in the future. But even in order to embark upon that task, having wallowed around in these kinds of undeterminate discussions for several months, one major factor is that we don't use terms consistently.

To begin the enterprise, we want to agree on a set of terminologies that everybody will use.

MR. WARD: We can't agree on that. That is a place to start, we can't agree on that.

MR. CONRAN: Then, I suppose we would be open to suggestions.

MR. BENDER: Suppose we could agree, what would you do next?

MR. CONRAN: You understand that the burden of safety is already defined in the regulation.

MR. WARD: We agree with part of it. I can't agree with non-safety as a category, let's put it that way.

MR. CONRAN: That term, I don't like it much either. What about safety grade, that is not used in the regulations, but whatever that term applies to is defined fairly explicitly in the regulations.

MR. BENDER: Let me just make sure I understand what you are saying.

MR. WARD: I think that a lot of these folks have to catch a bus; is that right?

MR. BENDER: Do these words mean the same thing?

MR. CONRAN: By practice they are interchangeable, and this term covers the whole circle, and this means the same as that. Importance to safety covers the whole thing, and this is a subcategory.

MR. WARD: That is where the contradiction is.

MR. CONRAN: I commented on that when I went through. We generally don't tag a name on the components that fall in that area.

MR. STOLZ: Mr. Chairman, take the Crystal River example, obviously the 24-volt non-nuclear instrument power supply was the initiating thing. That was termed clearly a non-safety system, only because it did not fit into that safety grade classification.

We could have called it anything else, but clearly we are tuned up in systems interactions, and all of the things we are going to lay emphasis on in looking at the interfaces between the so-called safety grade systems, and the so-called non-safety interfaces, be they control systems or power supplies, because I think most of the surprises we are going to see in terms of things that can affect our ability any kind of a safety goal, be they deterministic or be they quantitative, as you said before, are probably going to come out of the so-called non-safety that we have not heretofore examined, and that are going to give us fits.

There will probably be a common cause failure, because you can assume anything can fail a non-safety system. You can take an earthquake, and that can knock out all of them. So we see an area there that we are going to emphasize clearly in the systems interaction program that we are developing. As we mentioned at the electrical meeting, we plan to lay that on Indian Point as part of their systems interactions.

I think I sense a lot of the concerns on the part of people here that we talk about non-safety systems, and that we are not planning to do anything about them. I think the fact is that we are recognizing that we have not done anything about them before, but we sure as heck plan to do it now.

There has been a lot of emphasis, both from Congress, yourselves, and the realization among the staff, even among the sornero people in their risk studies, that that is the area where most of the surprises are going to be. So it is a matter of semantics.

We had two issues to cover here today. One was the grade QA, which was kind of distinct. The other one was the terminology, and we were hoping to at least get passed the terminology, but apparently we are not successful.

But the fact is that safety grade is a sharply defined segment. The non-safety, admittedly, isn't. The best I can do on that would be to say, if I had to define the so-called non-safety, or the rest of the importance to safety circle, I would rather phrase it in that terminology.

MR. WARD: It is a better name. It still is not very good, but it is a better name.

MR. STOLZ: I would rather give it some other name, but I would say, outside of the importance to safety, outside of the safety grade segment, that would be everything that is listed now in the Standard Review Plan, which lists condensors, turbine, feedwater line, steam lines, demineralizers, all of the things that we call the non-safety systems, but the fact is that these are items whose failure somehow may be able to affect safety systems, and the staff looks at them from that point of view.

MR. WARD: What we are looking for is a good name for that, and perhaps a subdivision or two of that, as we get more and more sophisticated.

MR. STOLZ: I guess what we used there was common terminology as presently used, and if we want to have a prize for some kind of game for coming up with names --

MR. CONRAN: I think the scheme is pretty reasonable as far as just common usage goes. You understand that until we get that done, in order to do that, if you say, "We don't give a damn for the terminology," you are going to have to change it before we will even be able to talk to each other. What I am saying is, we have to establish some kind of a reference point.

I think for the future you are right. One step that I mentioned in trying to help get a handle on this problem, we have proposed a change to Appendix B. It involves nothing more than every place the term "safety related" appears in Appendix B, stick "important to safety," because that is the intention.

MR. WARD: That is the more general term.

MR. CONRAN: Don't use two terms for one concept.

MR. BENDER: Don't let my statements be misinterpreted. I do agree with the philosophy that "A rose by any other name is still a rose." If you want to call it Sam, I really don't give a damn. I am more concerned about distinguishing certain properties.

MR. CONRAN: Right, and I understand your concern, and I may have given the wrong impression. I was giving some examples in the area about graded approaches, and I should have been more careful to explain that that was not meant to be comprehensive, or even very well done. It was just a list of things, and really what we are worried about right now is terminology.

MR. WARD: Mr. Epler has one more comment.

MR. EPLER: I have said this once every hour, and I will say this again. On this chart there is nothing to describe the system that will take charge of the situation, in spite a catastrophic failure, and you are going to have from time to time catastrophic failure of non-safety related systems, but we have elected not to do anything about it, except to review it.

MR. CONRAN: As a matter of fact, we are starting to analyze it, and we are starting to do things about it.

MR. EPLER: When are you going to start talking about a system that is dedicated to the removal of residual heat, when the general purpose plant systems will not work anymore?

MR. CONRAN: I think there is an action in the specific action plan.

MR. EPLER: What is it?

MR. CONRAN: I am not doing anything on it.

MR. STOLZ: That is one of the unresolved safety issue items.

MR. WARD: I think that it is certainly an important issue, but I am not sure where it fits in.

MR. EPLER: This problem will disappear when that one is implemented.

MR. CONRAN: But that would be catastrophic failure of a non-safety systems that would influence the residual heat removal?

MR. EPLER: You must isolate them so that they will not. It has not been done, but it must be done.

MR. WARD: Mr. Gallagher wanted to add one thing.

MR. GALLAGHER: I would like to add thing on this

IAEA. I have worked on that group, and my assignment was to work in that area. We tried very hard to have three levels of safety related.

MR. CONRAN: Three subdivisions of that?

MR. GALLAGHER: Yes, low, medium, and high.

The problem we came up with, without some way to quantify that, it was very difficult, other than being arbitrary, to say where those levels were.

Manning mentioned cooling, and when you look at cooling, you have to look at whether the failure of the cooling going to be a bad, a medium, or a not so bad consequence.

We also found that not all the rules can be graded to these three levels. That is why in the IEEE effort that we are working on with the NRC, we went to a different way, but it is not a scapel. We realize that in reality you have to group things in fairly large sections, otherwise nobody could deal with it.

I think we have to be careful that without some quantification, it is going to be very difficult to group things.

MR. WARD: Thank you.

Thank you everybody.

(Whereupon, at 4:40 p.m., the meeting was adjourned.)

NUCLEAR REGULATORY COMMISSION

This is to certify that the attached proceedings before the

____

in the matter of: ACRS/Subcommittee on Plant Features Important to Safety

Date of Proceeding: Washington, D. C.

Docket Number: ______________________

Place of Proceeding: February 3, 1981

were held as herein appears, and that this is the original transcript thereof for the file of the Commission.

M. E. Hansen

Official Reporter (Typed)

M.E. Hansen

Official Reporter (Signature)

NUCLEAR REGULATORY COMMISSION

This is to certify that the attached proceedings before the

____

in the matter of: ACRS/Subcommitte on Plant Features Important to Safety

Date of Proceeding: February 3, 1981

Docket Number: ______________________

Place of Proceeding: Washington, D. C.

were held as herein appears, and that this is the original transcript thereof for the file of the Commission.

Patricia A. Minson

Official Reporter (Typed)

Patricia A. Minson

Official Reporter (Signature)