

ORIGINAL - ACRST-3105

**OFFICIAL TRANSCRIPT OF PROCEEDINGS
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS**

**Title: MEETING: ACRS/ACNW JOINT
SUBCOMMITTEE**

TRO4 (ACRS)
RETURN ORIGINAL
TO BJWHITE
M/S T-2E26
415-7130
THANKS!

Work Order No.: ASB-300-1087

LOCATION: Rockville, MD

DATE: Thursday, January 13, 2000

PAGES: 1 - 302

**ANN RILEY & ASSOCIATES, LTD.
1025 Connecticut Ave., NW, Suite 1014
Washington, D.C. 20036
(202) 842-0034**

**ACRS Office Copy Retain
for the Life of the Committee**

DISCLAIMER

UNITED STATES NUCLEAR REGULATORY COMMISSION'S
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

JANUARY 13, 2000

The contents of this transcript of the proceeding of the United States Nuclear Regulatory Commission Advisory Committee on Reactor Safeguards, taken on January 13, 2000, as reported herein, is a record of the discussions recorded at the meeting held on the above date.

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

1 UNITED STATES OF AMERICA
2 NUCLEAR REGULATORY COMMISSION
3 ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

4 ***

5 MEETING: ACRS/ACNW JOINT SUBCOMMITTEE
6

7
8
9
10 USNRC, ACRS/ACNW

11 11545 Rockville Pike, Room T-2B3

12 Rockville, Maryland

13 Thursday, January 13, 2000
14

15 The subcommittee met pursuant to notice, at 8:30
16 a.m.
17

18 MEMBERS PRESENT:

19 THOMAS KRESS, ACRS, Co-chairman

20 JOHN GARRICK, ACNW, Co-chairman

21 GEORGE APOSTOLAKIS, ACRS, Member

22 RAYMOND WYMER, ACNW, Member
23
24
25

ANN RILEY & ASSOCIATES, LTD.
Court Reporters
1025 Connecticut Avenue, NW, Suite 1014
Washington, D.C. 20036
(202) 842-0034

P R O C E E D I N G S

[8:30 a.m.]

MR. KRESS: Could we please come to order?

This is a meeting of the Joint Subcommittee of the Advisory Committee on Reactor Safeguards and the Advisory Committee on Nuclear Waste.

I am Thomas Kress. I'm co-chairing this joint subcommittee, and on my right is Dr. John Garrick, who is the other co-chair of the joint subcommittee.

I guess I'll be mostly in charge of this particular meeting.

Other joint subcommittee members in attendance are Dr. George Apostolakis of the ACRS, Dr. Ray Wymer of the ACNW, and also present is Dr. Milt Levenson, who is a consultant to the ACNW.

The purpose of this meeting is for the joint subcommittee to discuss the defense-in-depth philosophy in the regulatory process, including its role in the licensing of a high-level waste repository, its role in revising the regulatory structure for nuclear reactors, and how the two applications should be related to each other.

The discussion will also include the role of defense-in-depth in the regulation of nuclear materials applications and other related matters.

The subcommittee will gather information, analyze

1 relevant issues and facts, and formulate proposed positions
2 and actions, as appropriate, for deliberation by the full
3 committees.

4 Michael Markley is the designated Federal official
5 for the initial portion of this meeting.

6 The rules for participation in today's meeting
7 have been announced as part of the notice of this meeting
8 previously published in the Federal Register on December 21,
9 1999.

10 A transcript of the meeting is being kept, so it's
11 requested that speakers identify themselves, speak clearly
12 and plainly and into the microphone, so that the
13 transcriber can get you on tape.

14 This promises to be a very exciting meeting to me.
15 We have some very distinguished people here.

16 We have the staff, who's willing to come and share
17 some of their views with us, and we have three invited
18 experts with us this morning, all of them former office
19 directors of the Nuclear Regulatory Commission and now
20 highly-regarded consultants.

21 Our three invited experts are Bob Bernero, Bob
22 Budnitz, and Tom Murley.

23 I have some introductory comments that talk about
24 these people. I guess I'll just read them.

25 Mr. Bernero spent 13 years in naval and space

1 nuclear work at GE and then served for 23 years, from 1972
2 to 1995, with the AEC and NRC regulatory staff.

3 After five years in reactor and fuel cycle
4 licensing, Bob began work in regulatory development,
5 including decommissioning standards and spent fuel
6 licensing.

7 After investigating the TMI accident, Bob formed
8 the Division of Risk Analysis in the Office of Research,
9 served later in NRR licensing divisions, and then went back
10 to NMSS until he retired as director in 1995.

11 Dr. Budnitz worked at the University of California
12 Lawrence Berkeley laboratory from '67 to '78 and held the
13 position of associate director and head of the Energy and
14 Environmental Division.

15 In 1978, he joined the Nuclear Regulatory
16 Commission as Deputy Director of the Office of Research and
17 was appointed Director of that office in '79.

18 In 1980, Bob left the NRC to found the Future
19 Resources Associates, a consulting firm working mostly in
20 risk analysis.

21 His current consulting activities include PRA,
22 emphasizing external hazards, upgrading the safety of older
23 reactors, and using risk in safety regulation, including
24 performance analysis of waste disposal systems.

25 Dr. Murley was the Director of NRC's Office of

1 Nuclear Reactor Regulation from 1987 to 1994. Prior to
2 that, he was the Regional Administrator of NRC's Region I
3 office, beginning in 1983.

4 Dr. Murley retired from NRC in 1994 after 25
5 meritorious years of service. He is presently a consultant
6 on nuclear management and safety matters in the U.S. and
7 foreign countries.

8 In addition to all this brain power and good
9 thoughts, you're going to be treated early on this morning
10 with some thoughts on this subject from me and Dr. Garrick
11 and from Dr. Apostolakis, and by virtue of this awesome
12 power I have as chairing this committee, I've decided I'll
13 go first and get things started and then turn it over to
14 John for his comments and then let George run the sprint lap
15 and make up for all the time we've overrun.

16 So, I do have view-graphs, so I'm going to do this
17 and move up to the front.

18 I am going to give you some thoughts I have on
19 this subject, to put it in somewhat of perspective. These
20 thoughts are my own, by the way, and may or may not
21 represent any of the views of the ACRS or the ACNW. For
22 that matter, I don't even know what the ACRS views are on
23 this topic, or even if they have any.

24 So, they are my own.

25 That disclaimer said, I do have a couple of

1 concerns that I hope we can at least address in this
2 meeting.

3 The first concern I have is there are a number of
4 definitions to defense-in-depth that vary slightly from one
5 to the other that I've seen.

6 Most of these definitions have a component of
7 defense-in-depth is there to compensate for uncertainties in
8 our risk numbers.

9 Well, I think we can all agree on that, but the
10 problem I have with that is I can't use that. That's not
11 enough. That's not a definition. It's a sort of a
12 description, and I have no way to implement that in that
13 regulations or to use it when I design some sort of system
14 to deal with the risk.

15 So, that's the first problem. I don't know how to
16 design to that, and we need a better definition.

17 The second problem is what definitions I have seen
18 don't lend themselves in any way that I can tell, except in
19 an arbitrary sense, of determining necessary and sufficiency
20 conditions on defense-in-depth.

21 We've had a number of instances where there's been
22 arbitrary appeals to defense-in-depth to disallow some
23 change or some regulation, and if we're going to reap the
24 benefits of risk-based or risk-informed regulation, we have
25 to have a way to put rational limits.

1 We have to know what defense-in-depth is, we have
2 to be able to identify it, and we have to be able to say how
3 much of it is enough, and I hope -- I don't think we'll
4 resolve those two things at this meeting, but I hope we at
5 least make some headway in addressing it.

6 MR. APOSTOLAKIS: Tom?

7 MR. KRESS: Yes, sir.

8 MR. APOSTOLAKIS: I think language is extremely
9 important here. So, I would change a little bit something
10 you said earlier.

11 You said "arbitrary appeals to defense-in-depth."
12 The appeals do not have to be arbitrary, because
13 defense-in-depth itself is arbitrary.

14 MR. KRESS: Yes. Good point, George, and I agree
15 with that.

16 As a way to approach the subject matter, I hope
17 today we can -- if you notice, in my title, I had the word
18 "design" defense-in-depth. I hope we can focus on that, as
19 opposed to operational.

20 I don't want us to get sidetracked into things
21 like inspection, procedures, quality assurance, management,
22 and even emergency response.

23 While those things are considered components of
24 defense-in-depth, I think if we're going to address a true
25 definition of defense-in-depth that has ways to put limits

1 on designing facilities to deal with risk, we ought to focus
2 on design aspects, and in addition to that, we have a
3 tendency to lapse into barriers and nuclear reactor
4 defense-in-depth as it's traditionally been covered or been
5 looked at, and I think we need to generalize the concept,
6 generalize it in the sense that it applies to any hazardous
7 activity, and in order to do that, I've put together what I
8 call four design defense-in-depth principles that I think
9 are general and would apply to just any hazardous activity.

10 The first one is do what you can to prevent
11 accidents from starting in the first place. That's, I call,
12 initiation or paying attention to initiating events.

13 Second is do what you can to stop accidents at
14 very early stages before they progress to unacceptable
15 consequences. I call that one intervention.

16 The third is do what you can to provide for
17 mitigating the release of the hazard vector. The hazard
18 vector in nuclear power reactors are the fission products,
19 but it could be toxic gases or fire and smoke or heat or
20 whatever the hazard is you're dealing with. I call that one
21 mitigation.

22 And fourth, provide sufficient instrumentation to
23 diagnose the type and progress of any accident. Call that,
24 of course, diagnosis.

25 And I've categories these, the first two, as

1 prevention and, with some overlap, the second and third one
2 as mitigation and the fourth one as belonging in both
3 categories.

4 So, I've categorized defense-in-depth principles
5 in terms of prevention and mitigation.

6 Now, with those as sort of principles of
7 defense-in-depth, I think one could arrive at a definition
8 of defense-in-depth, and I think we may hear several of
9 those today.

10 I have one that I prefer, so I'm going to propose
11 it right now, based on these kind of principles.

12 A generalized risk-related definition of
13 defense-in-depth could be -- and I'll just read it -- design
14 defense-in-depth as a strategy of providing design features
15 to achieve acceptable risk, in view of the uncertainties, by
16 the appropriate allocation of the risk reduction to both
17 prevention and mitigation.

18 I like this definition for a number of reasons.

19 One, it, I think, captures the essence of what we
20 traditionally think of as defense-in-depth, and number two,
21 it is linked explicitly to risk analysis and risk concepts,
22 and number three, I think it lends itself to being able to
23 provide limits to defense-in-depth, and you may ask how can
24 I work from this definition to arrive at limits? Well, the
25 key words are "appropriate allocation."

1 In order to arrive at limits on defense-in-depth
2 with a definition like this, first off, you do have to have
3 risk and acceptance criteria for the activity you're dealing
4 with.

5 These are things like, in nuclear reactors, early
6 death, latent fatalities, land interdiction, could be
7 frequency of fission product release or could even be LERF
8 as a surrogate for all of those, but you have to have an
9 overall risk acceptance criteria, and not only that, you
10 have to express these risk acceptance criteria in terms of
11 the uncertainty.

12 If we're going to deal with uncertainty by
13 defense-in-depth, we have to have some quantification of
14 what that uncertainty consists of.

15 Now, you may hear that there are two kinds of
16 uncertainties, those that you can quantify and those that
17 you can't.

18 I maintain that if we're actually going to put
19 limits on defense-in-depth, you cannot have un-quantified
20 uncertainties; you have to quantify the whole thing.

21 What we normally call quantifiable uncertainties
22 can come right out of the PRA.

23 What we normally call un-quantifiable
24 uncertainties, I think, would have to have some estimate of
25 what those are, and we'll probably have to get that from

1 expert opinion, for this activity-specific and maybe even
2 facility-specific activity, and the acceptance criteria that
3 I'm talking about in terms of uncertainties have to include
4 both of these.

5 Now, once you have that risk acceptance criteria,
6 the next question is you have to allocate it among those
7 four areas of prevention and mitigation, because that's what
8 defense-in-depth basically is. It's an allocation of risk.
9 And how do you do that allocation?

10 Well, there's no differential equation or no
11 technical basis for doing it. Allocation is a matter of
12 policy, and we have to have a policy statement of some kind
13 that says how much we value prevention over mitigation.

14 Now, that's policy, and I can't say how to do
15 that, but we could provide guidance.

16 For example, such an allocation or such a value
17 judgement could depend on the level of the inherent hazard.
18 The more hazardous an activity, the more we probably should
19 value prevention.

20 It could depend on how big the uncertainties are.
21 The more uncertainty you have, you probably want to put
22 equal balance on things.

23 It could depend on how much of this uncertainty is
24 un-quantifiable, as opposed to how much is quantifiable.

25 You may want to minimize the uncertainty. That

1 would be a classic optimization problem.

2 You might have noticed in my title I had "beating
3 a dead horse with a red herring." The dead horse is
4 defense-in-depth as we traditionally think of it. This
5 minimization is what I threw in as a red herring, just to
6 confuse the issue.

7 It also -- some allocation rationally could be
8 based on what's called the loss function and decision
9 theory. That's how one normally allocates things. You ask
10 yourself am I willing to suffer this loss if I don't
11 prevent? What are the consequences of that? And you can
12 work from that towards a probability that you want to accept
13 for that occurring.

14 With that as my introductory thoughts on the
15 subject, I guess I'll either ask if there are any questions
16 or turn it over to John Garrick for his thoughts.

17 I guess I confused everyone.

18 MR. BERNERO: Bob Bernero.

19 Are we going to reserve dialogue for the general
20 discussion period rather than take one paper at a time?

21 MR. KRESS: It probably would be a good idea to do
22 it that way. I think I prefer it that way.

23 MR. GARRICK: I think we're already in trouble
24 schedule-wise.

25 MR. BERNERO: So, I won't slap my forehead now.

1 MR. BUDNITZ: Bob Budnitz from Berkeley,
2 California.

3 I have one very specific but, I think, important
4 comment.

5 If you put a dangerous reactor 100 miles from the
6 nearest off-site person, then you have kept, as best I can
7 tell from the technology and what I understand it -- you've
8 kept off-site fatalities to zero, and that's a piece of
9 defense-in-depth called siting and mitigation, protective
10 actions.

11 By the way, if you could do protective actions
12 perfectly, it's another piece, and you don't have that here.
13 You only had the piece about keeping the source term --
14 understanding it or keeping it low.

15 MR. KRESS: Bob, I agree.

16 MR. BUDNITZ: I think that's a crucial leg of
17 this.

18 MR. KRESS: Yes, I agree with you that that is
19 crucial defense-in-depth.

20 My reason for not discussing it, or even excluding
21 it, was there are lots of reactors out there that don't have
22 that characteristic, and we're talking about revising the
23 regulations, and we're talking about a lot of the NMSS
24 activities in hospitals and dispersed areas.

25 So, I was trying to say what would it be in terms

1 of design?

2 I agree with you that that is a good
3 defense-in-depth.

4 MR. BUDNITZ: But more to the point, if I have two
5 identical facilities that might be NMSS hospital licensees
6 and one of them is in the middle of nowhere and the other
7 one's in the middle of New York City, you might require
8 different engineering at the facility, depending on the
9 site.

10 MR. KRESS: Probably not.

11 MR. BUDNITZ: You might.

12 MR. KRESS: Probably not.

13 MR. BUDNITZ: In principle, you could achieve the
14 same protection with different mixes of your allocation, but
15 you don't even know about that unless you put that
16 allocation criterion on your slide, which it wasn't.

17 So, I'm calling people's attention to the notion
18 that you have to consider that, I think, as a piece of this
19 overall allocation mix.

20 MR. KRESS: Yes. I don't know what all the
21 criteria are for allocation, I just know that we needed
22 some, and those are good comments.

23 John, you're up.

24 MR. GARRICK: I'm a little sorry I prepared
25 anything, because I would probably be more constructive if I

1 took what Tom said point by point and commented on it, but
2 what I would like to do is come before you not as a
3 co-chairman of this meeting but as a plain vanilla risk
4 person and approach the problem from the point of view that,
5 if I had a license to do so, how would I address this
6 question of defense-in-depth, and again, as Tom said, I'm
7 not speaking for ACNW or ACRS, but I am trying to look at
8 this as a issue that it's time that the fuzziness of the
9 issue was removed somewhat and that, in keeping with the
10 transition to a risk-informed way of thinking, it's time to
11 think about quantification of defense-in-depth as a way of
12 taking the mystery out.

13 So, I looked at this from the standpoint of what
14 might be a conceptual framework for quantifying
15 defense-in-depth, and I recognize the various
16 interpretations of what constitutes defense-in-depth from
17 the three fundamental lines of defense that have been
18 articulated in the material that we have received -- the
19 plant, the safety systems, and the consequence-limited
20 systems -- as being somewhat of a classical display of the
21 three most talked about lines of defense, but even that can
22 be challenged, because there's the whole soft infrastructure
23 of quality control, of review, of assessment, of audit that
24 people would argue very strongly are and should be a part of
25 defense-in-depth.

1 But the position I'm going to take is what we need
2 to do is pick a piece of it and start looking at it in terms
3 of how we might quantify it.

4 So, the piece that I have picked is to look at a
5 reactor example, have a license to do that as a risk
6 assessor, and a waste example, and one of the things, I
7 think, that would help this process a lot would just be to
8 organize the way in which we talk about it and the way in
9 which we present it, and one of my favorite presentation
10 formats is a matrix format, a two-dimensional array, and if
11 we have more than two variables, I have a tendency to fix
12 those variables in some fashion and reduce it to a
13 manageable presentation.

14 So, what I have chosen to do, to illustrate, at
15 least conceptually, what I'm talking about, is to look at
16 protective systems, protection systems, again admitting that
17 defense-in-depth is more than protection systems, but to
18 take a very top-down perspective of it, and having just
19 spent three days on a safety committee at a boiling water
20 reactor in a very upbeat situation where it's a plant that
21 had its best all-time performance year, broke all kinds of
22 records in terms of capacity factors and availability, had
23 the longest run of any plant, any boiler in history between
24 outages, received an INPO-1 certification, and it's kind of
25 exciting, and when I'm at the PWR, maybe I'll do the PWR

ANN RILEY & ASSOCIATES, LTD.
Court Reporters
1025 Connecticut Avenue, NW, Suite 1014
Washington, D.C. 20036
(202) 842-0034

1 example.

2 But what I'd like to do is to suggest that, if we
3 laid out the information about a reactor in some fashion
4 similar to this, in a top-down fashion, this is at the very
5 functional level, and say that the safety functions are
6 basically those -- reactivity control, inventory control, by
7 which we mean coolant inventory control, heat removal -- as
8 we all know, the panic in Three Mile Island in the first two
9 or three days after the accident was a search for heat
10 sinks, and radio-nuclide containment, and then, in the
11 vertical direction, we talk about classes of initiating
12 events, and I won't even claim that this is complete, but
13 the idea is to make it as complete as possible, and
14 generally, we can divide that into these three classes --
15 loss of coolant, transients, and external events, and
16 generally, we can create information that would allow us to
17 construct probability curves associated with those kinds of
18 events, and I think we could also argue that, in most
19 large-scope PRAs, we could aggregate the information in this
20 form.

21 So, each of these kind of represent a group of
22 scenarios, and this is the end state core damage frequency
23 for the group of scenarios that are initiated by
24 loss-of-coolant events, and then the question -- and then,
25 of course, if we do this carefully and we probabilistically

1 sum these end states, that constitutes our core damage
2 frequency, our total core damage frequency.

3 Now, the question is what do we put into these
4 grid boxes, and that's what I'd like to talk about a little
5 bit, and I also would like to reduce this from the very
6 functional level down to a more hardware level to give it
7 more physical meaning.

8 Well, there's any one of a number of things and
9 combinations of things we could put in those grid boxes, but
10 here's some suggestions.

11 Certainly, in each function, we could put the
12 function unavailability in terms of the frequency per demand
13 for that class of initiating events, and also, we could put
14 something like this.

15 We could put what the core damage frequency would
16 be at the end state of that particular class of initiating
17 events, given that that function or system was unavailable.
18 That's material that we can all extract from a full-scope
19 risk assessment, with some debate, of course, but the most
20 important entry might be this one. It's the total core
21 damage frequency with and without the safety function.

22 This particular core damage frequency is a result
23 of the convolution of all of the scenarios, and this is the
24 same thing but without the safety function, and at least if
25 we did that for each of these grid boxes, we would begin to

1 see what the perspective was of the contribution of the
2 various safety functions.

3 Now, if we look at that at a slightly more
4 detailed level for something like a BWR -- and every time I
5 look at this, I want to re-tune the labels, and I'm not
6 going to apologize for the small of the print, you've got
7 copies, but the safety functions can be reduced basically
8 into vessel-level make-ups systems and a reactor coolant
9 system, and the one thing you have to remember, that to a
10 risk analyst, we don't think in terms of safety-related and
11 non-safety-related systems.

12 Every system has to prove that it's
13 non-safety-related.

14 So, I'm not adopting the classical NRC language
15 here, but I am adopting the classical risk language as to
16 what these systems are labeled and look like.

17 So, we have turned up the microscope on one grid
18 box of that functional diagram, and that's the grid box
19 "inventory control," this one.

20 So, the figure I just showed you is just a blow-up
21 of this one versus this class of initiating event, and we've
22 decomposed that into eight safety systems and six categories
23 of initiating events.

24 These are still categories of initiating events,
25 and so, when we talk about these entries, we're talking

1 again about the total core damage frequency being the
2 probabilistic sum of the end states of all these different
3 categories, and then the curve that we want to compare that
4 with -- this should be a double curve -- is the curve that
5 results -- that comes about as a result of making the system
6 of interest unavailable, recalculating this end state, and
7 adding that recalculated end state to the rest of these and
8 comparing that with this, gives us an in-context perspective
9 of what that system is providing us with respect to the
10 bottom line, and that seems to me one of the things we want
11 to do.

12 Now, how do we do this with respect to nuclear
13 waste?

14 Quite a different problem, because here passive
15 systems dominate the analysis, not only passive systems but
16 geologic natural setting are a major part of the analysis,
17 and again, you can think of it functionally, and I apologize
18 to the performance assessment people for choosing my own
19 labels here, but I see the performance assessment problem at
20 the protective barrier functional level as basically these
21 three things -- water location and flow control, waste
22 package containment, and source term creation, mobilization,
23 and transport -- and in a sense, you might look at this as
24 the base case, and I have also put down here geo-technical
25 events to account for earthquakes, igneous activity, and

1 anything else of that type that you'd care to include, and
2 in principle, given the way we've set this up, the
3 performance parameter, in principle you could add these
4 probabilistically.

5 Now, the way I've eliminated the time dependence
6 of the dose is to choose the time at which the annual
7 release is the maximum into the biosphere, and that allows
8 me to keep it in a two-dimensional space, and so, what this
9 is is the peak annual release to the biosphere in curies,
10 and of course, this is just an expression of the uncertainty
11 about that, hopefully reflecting both information
12 uncertainty and modeling uncertainty.

13 Now, this time, however, what we want to do is, if
14 we remove this function, what does this curve become, and
15 compare that risk curve, which would be the one on the
16 right, with what it is if you had the function. In other
17 words, this curve, the one on the left there, and this one
18 is the same, with all systems performing their intended
19 function. So, what that is is here.

20 This would be the measure of the performance with
21 and without the function or the system.

22 Now, how would we decompose that one, just to,
23 again, reduce it into more physical descriptive terms? This
24 is how it might be decomposed.

25 As far as water flow and spatial control systems,

1 you could imagine these kinds of systems, systems that would
2 somehow impact the way in which the water from the rainfall
3 is drained from the site, and I've distinguished between
4 water diversion systems that are brought about by doing some
5 engineering of the geology versus bringing engineering
6 systems into the near field, and as far as waste packaging
7 -- and I'll let you argue as to whether things like drip
8 shields would be here or here. I would put them here.

9 Waste package containment -- I'm talking primarily
10 about the performance of the waste package, and usually
11 there we think in terms of the waste package corrosion
12 resistance capability, fuel cladding, and what have you.

13 Now, as far as the creation of a source term is
14 concerned, some of the things that are involved here are
15 whether or not we have a back-fill for purposes of enhancing
16 geo-chemical conditions, also how much credit we give to
17 things like solubility, retardation, dilution, and so forth.

18 So, again, it's a retaining of this structure such
19 that you have components where you can get some visibility
20 into the contribution to the overall performance of the
21 taking away from, modifying, or changing or adding any
22 particular system/subsystem at any particular location.

23 So, I wanted to do this because I think that the
24 hope here is that we take advantage of what we've learned in
25 the risk field.

1 I think most of the kind of calculations that
2 we're talking about here have been done.

3 We can debate about the quality of them, we can
4 debate about whether they contain the right kind of
5 uncertainties, but that's okay.

6 Once we get it in this kind of form, and given
7 that those kind of issues apply to all the boxes, there is
8 great value in the comparisons, it seems to me.

9 So, I wanted to just throw this out as an opening
10 salvo, and as I say, we're in trouble on time, and the
11 chairman, and particularly me, have contributed to that, and
12 we'll take questions but probably later.

13 George?

14 MR. KRESS: The reason we're in trouble on time is
15 this is a particularly long-winded group.

16 MR. APOSTOLAKIS: I was asked to do two things:
17 one, to present some thoughts that Dana Powers had, the
18 chairman of the ACRS, and he couldn't be here to present
19 them, and since I happen to disagree with him on a lot of
20 things, the committee felt that I was the best guy to
21 present his ideas, and then, I will present some of my own
22 thoughts.

23 So, we start with Dana.

24 He gives us first -- and you have the write-up in
25 front of you, plus the view-graphs -- a sort of historical

1 background on defense-in-depth.

2 This is a concept that has evolved over the years,
3 from the early days when people realized that there were --
4 there was a possibility of catastrophic accidents from
5 reactors, the uncertainties were very large regarding the
6 likelihood of occurrence, so people devised this idea of
7 multiple defenses.

8 It turns out, though, that this safety strategy
9 that's called defense-in-depth may impose unnecessary burden
10 now on the licensees.

11 Everybody says that it has served the reactor
12 safety community well. I have some doubts about it, but I
13 will go along with it.

14 Oh, I'm sorry, I'm presenting Dana's.

15 Even within the reactor safety community, thoughts
16 have turned to limiting defense-in-depth.

17 Now, you probably have seen that paper that
18 several of us wrote and presented at the PSA conference last
19 August where we identified two schools of thought.

20 One is the structural school of thought,
21 defense-in-depth, and Dana is the primary advocate of that,
22 I believe, which says that, essentially, defense-in-depth is
23 an idea that is embedded in the regulations, this idea of
24 multiple defenses.

25 The rationalist school -- Tom and I happen to push

1 that a little bit -- advocates that defense-in-depth -- that
2 now that we can quantify uncertainties, we can use
3 defense-in-depth in a more limited way for those
4 uncertainties that have not been quantified.

5 Dana offers a couple of thoughts here, says that
6 the structuralist approach may be difficult to extend in
7 other areas -- he has in mind NMSS activities, other than
8 reactor, in other words -- whereas the rationalist approach
9 could be extended to other areas, but then, since you are
10 relying so much on what can be quantified and what cannot be
11 quantified, you really have to have the analytical
12 capability which perhaps does not exist in other areas.

13 Now, a favorite question that Dana raises is what
14 if you're wrong? That's why I use defense-in-depth. What
15 if my analysis is wrong? Okay?

16 So, he says that it may be a little paradoxical to
17 use analysis to specify where defense-in-depth is applied
18 when, in fact, defense-in-depth is used to protect you
19 against the possibility that your analysis wrong.

20 So, that's an interesting thought there.

21 So, again, some of the historical reasons for the
22 development of defense-in-depth here -- again, always
23 according to Dana -- at that time there was little
24 experience in the operation of nuclear power plants, there
25 were no industrial standards for the safe operation of

1 nuclear reactors, there was confidence that accidents were
2 unlikely but great uncertainties in the consequences given
3 that they would occur, that they occurred, potentially
4 consequential accidents would be difficult to interdict once
5 underway, and finally, if an accident happened at one
6 facility, it would affect the operation of other facilities,
7 as well.

8 So, Dana's conclusions are that, for the four
9 classes of NMSS activities, which are disposal of high-level
10 waste, engineered casks for transport of nuclear materials,
11 sealed and unsealed sources -- I don't remember the third
12 one, some sort of waste -- Dana believes that the
13 consequences for these classes of material licensees can be
14 easily bounded.

15 In many cases, there is a wealth of operational
16 experience.

17 I'm glad he said that, because I want to use it
18 later.

19 The timing is different. Severe accidents are
20 potentially -- have large consequences develop slowly, so
21 there is the possibility to interdict, unlike with reactors.
22 Phenomenological uncertainties are modest, and the technical
23 basis for rationally limiting defense-in-depth is not well
24 developed.

25 So, his main position is that he is against the

1 imposition of a defense-in-depth philosophy on material
2 licensees, which I guess includes high-level waste
3 repositories.

4 Now I will present you my thoughts.

5 The fundamental question is why do we bother? Why
6 are we having this meeting? What is it that has changed
7 over the years that has made us have meetings like this,
8 publish papers, and think about defense-in-depth and its
9 role in reactor regulation?

10 I believe most of us would agree that the thing
11 that has changed is that the uncertainties that forced the
12 pioneers to come up with defense-in-depth now -- a class of
13 those uncertainties can be quantified, whereas in those days
14 they could not quantify them.

15 They knew that the frequencies of these accidents
16 were very uncertain, the consequences could be very high,
17 but the uncertainty was not quantifiable at the time.

18 In the last 25 years, starting with the pioneer in
19 reactor safety study, of course, we started quantifying a
20 good part of these uncertainties, and again, people with
21 some experience in the field know that there is also a class
22 of uncertainties that perhaps we cannot quantify at this
23 time, un-quantified uncertainties.

24 The potential conflict, then, is between someone
25 who takes defense-in-depth as a principle and someone who

1 tries to use the rationalist approach and use
2 defense-in-depth or its tools as standard engineering tools
3 used within engineering calculations that include risk
4 assessments and quantification of uncertainty.

5 So, what I propose is that we avoid the word
6 "principle" and simply say limit defense-in-depth and say
7 defense-in-depth is a safety philosophy that requires that a
8 set of provisions be taken to manage un-quantified -- not
9 un-quantifiable -- un-quantified uncertainty associated with
10 the performance of engineered systems.

11 I believe this is consistent with Tom's
12 presentation.

13 So, I'm carefully avoiding the word "principle."
14 I'm using the word "safety philosophy." In this, of course,
15 "un-quantified uncertainty" are the key words here.

16 Now, some observations.

17 Many times, people use the words
18 "defense-in-depth" to mean multiple barriers.

19 Now, by "barriers," by the way -- the word
20 "barrier" is very general here. It includes siting, it
21 includes everything, not just physical barriers like the
22 primary system coolant boundary, and I want to make that
23 distinction. They are not identical concepts.

24 Even within the quantified uncertainties, where
25 I'm going to be using, you know, risk to decide how much I

1 need, I will use multiple barriers, otherwise I will never
2 be able to go down to 10 to the minus 4 and 5 per year, but
3 this is not using defense-in-depth; this is using standard
4 engineering tools.

5 So, let's start by saying that these two things
6 are not the same concepts.

7 Now, where does this un-quantified uncertainty
8 come from? It's primarily from models. We know that our
9 models are inadequate in many instances, or we know that
10 some of the things that may be important we cannot even
11 quantify, we haven't tried. Okay?

12 So, experienced analysts and practitioners do have
13 an idea how good these analyses are.

14 Now, if we focus on these un-quantified
15 uncertainties, then we have to debate them, and then we will
16 all understand better why these uncertainties are not
17 quantified.

18 We may be able to define new activities, research
19 activities or other kinds of activities, experiments,
20 perhaps, to quantify part of these uncertainties. So, it's
21 not that I'm ignoring them. I think I'm placing extra
22 attention on these un-quantified uncertainties.

23 But the crucial question, as I said earlier, is
24 under what conditions, if any, is defense-in-depth in
25 principle? I don't think there are any conditions. It

1 should never be called a principle.

2 It's a safety philosophy, as I gave in the
3 definition, where the uncertainty is un-quantified, and the
4 words should not appear at all within a PRA.

5 When the uncertainties are quantified, drop
6 defense-in-depth. You just use the tools to manage your
7 risk and achieve the uncertainty levels that Dr. Kress
8 talked about.

9 Now, Dana read this and said, well, I am much more
10 comfortable with defense-in-depth as a means to address the
11 question of what if we are wrong in our analysis. This is
12 his favorite question: What if you're wrong?

13 You can argue that this is just a kind of
14 uncertainty, as, indeed, I am arguing, but I think that
15 argument trivializes the problem or implies that we know
16 more than we do.

17 Well, instead of defending my position, I will
18 attack his.

19 This is exactly what's wrong with calling it a
20 principle. You are telling me, no matter what you do, what
21 if you are wrong? So, I will impose on you
22 defense-in-depth.

23 Well, I might as well give up. Why did we even
24 try to develop PRAs? We spent all these resources the last
25 quarter-century. Why? What if I'm wrong?

1 I will have to live with defense-in-depth forever,
2 and that's exactly what the word "principle" does to you.
3 If you call it a principle, you can't get out of it. It's
4 impervious to analysis.

5 And in fact, I'm glad that he said, in his
6 presentation -- it's really kind of unfair that he's not
7 here, but on the other hand, there is a certain pleasure in
8 this.

9 Why is this a reason to argue against the
10 imposition of defense-in-depth on material licenses? Why?
11 Because there are no un-quantified uncertainties. That's
12 why.

13 Thank you very much.

14 MR. MURLEY: My name is Tom Murley.

15 George, I very much, I guess, like your analysis
16 her, but are you suggesting that one should not make it a
17 principle and, therefore, if you are confident enough, you
18 could use PRA to justify removing a barrier like
19 containment, let's say? Would you push it that far?

20 MR. APOSTOLAKIS: First of all, I would not use
21 just PRA; I would use my total knowledge. Yes, I would.
22 Yes. There is nothing sacred about the containment. But
23 you better come back with some real good physics to convince
24 me that the uncertainties are not large.

25 MR. KRESS: George, if you adopted my principle of

1 allocation, you might say that allocating risk reduction to
2 CDF and to containment is a matter of policy, and then you
3 would set values for that allocation, and you would have a
4 containment, even though you could throw it away and still
5 achieve your risk acceptance, you would still have
6 containment, because it's a policy in allocation.

7 MR. APOSTOLAKIS: On the other hand, you might say
8 that the policy applies to a certain type of reactors --
9 LWRs, for example.

10 If somebody comes up with a new design that is
11 fundamentally different and can make a convincing case that
12 I don't need the containment, I don't see why I should.

13 What's next?

14 MR. KRESS: I guess now we turn to the rest of the
15 agenda, if I can find it.

16 That covers the preliminary presentations by the
17 committee members, and the second part of the agenda -- and
18 we're only about 25 minutes behind, which is not too bad at
19 all -- is presentations from our invited experts, and we
20 have first on the agenda Dr. Budnitz.

21 MR. BUDNITZ: Twenty years ago this week, I
22 appeared before the ACRS downtown, and Bob Bernero reminded
23 me that I sat up on this side of the table, with my jacket
24 off, tie off, shoes off, and talked this way, but I won't do
25 that today, because Chet Siess isn't here. May he continue

1 to prosper. Those were the informal days.

2 I also want to point out that the reason I'm first
3 is I'm the youngest of the three, and another reason why I'm
4 first is because I was the Director of Research for a very
5 brief micro-second 20 years ago, and these two guys were two
6 of my division directors.

7 I'm going to confine my remarks to Yucca Mountain
8 and Part 63, but before I do that, I want to start with a
9 bit of philosophy, because I want to be sure you understand
10 that I think the argument about whether it's a principle or
11 a criterion is moot, because it depends on how it's used,
12 and it's only how it's used that matters.

13 Let me try to make the point directly.

14 In Exodus, there are 10 commandments, and the two
15 that, by the way, are observed almost universally in all
16 societies everywhere are don't steal and don't murder.
17 Don't steal and don't murder.

18 Are they requirements? Are they laws? Are they
19 what?

20 I can tell you that, in the United States, in the
21 year 2000, we are still arguing about the definitions which
22 goes to the implementation. What really matters is the
23 implementation of those things.

24 For example, we're still arguing today about
25 whether abortion is murder in this country. So, it's not

1 simple just to say don't murder.

2 Second, can I steal from my community property
3 from my wife in California? It turns out that's ambiguous.
4 There's no real answer to that in California law.

5 So, things as simple as don't steal and don't
6 murder, which are principles which all societies follow --
7 never minding they're in the Bible, all societies follow
8 them -- can't be implemented without implementing rules, and
9 it's the rules that govern our behavior, our enforcement,
10 our regulations, and not what you call it, whether it's a
11 principle or a biblical commandment or what.

12 Same thing is true here, and when you come to see
13 what I'm going to say about Yucca Mountain, you'll see it
14 directly.

15 George, I don't know what to call it, but one
16 thing for sure is that, whatever you call it, at Yucca
17 Mountain or for reactors or for material licensees, it's --
18 what matters is how the rules and regulations of Part 50 or
19 Part 60 or Part 63 or whatever, or any of the regulations,
20 and all the stuff that goes with them, how it's used in
21 practice, and that's the real point.

22 In a way, you can imagine that they're high-level
23 criteria or high-level requirements which, if you meet this
24 stuff, you meet it, but you can't meet it by itself. You
25 don't know how to meet it by itself. You've got to meet

1 this stuff that's down below, and then, by definition, you
2 meet it.

3 But using it as a principle, then, or a philosophy
4 or whatever, is because it provides a intellectual framework
5 or a way of thinking about how this stuff works or how you
6 got to it, and you can argue about it, you can argue about
7 the details in light of those principles which you think
8 about, but you have to keep that in mind.

9 You can't enforce defense-in-depth anymore than
10 you can enforce what the Atomic Energy Act in 1954 ordered
11 the AEC or NRC not to do, which is to ensure adequate
12 protection, but you can't go to any licensee anywhere and
13 say, sorry, you don't meet adequate protection. What you
14 say is you don't meet part something-something of Part 50.
15 That's what you don't meet.

16 By the way, that got translated later into no
17 undue risk, and it took the Commission 30 years to decide
18 what undue -- you know, as Hal Lewis on this committee used
19 to say, you really want them to tell us how much risk is
20 due. That's the safety goal.

21 The safety goal finally told us, for reactors,
22 what undue risk meant, even though undue risk had been used
23 for 30 years before the safety goal was adopted.

24 You couldn't regulate on undue risk. You can't
25 regulate on adequate protection. What you can regulate to

1 is some rule somewhere or what an inspector is told to look
2 for or what can be enforced, and that's what I'm going to
3 talk about for Yucca Mountain.

4 So, now I'm going to talk about the dilemma, and
5 this is quoting straight from the supplementary information
6 for Part 63 that came out within the last year, where it
7 says in plain English, or reading the plain English -- and
8 then we're going to come to, you know, where the rubber hits
9 the road -- the Commission does not intend to specify the
10 numerical goals for the performance of individual barriers.

11 By the way, this is a draft; it still hasn't been
12 finalized. But were this adopted, it tells us the
13 Commission does not intend to regulate specific numerical
14 goals for barriers.

15 But -- and here's the big "but" -- in implementing
16 this approach -- the defense-in-depth was in the previous
17 sentence, so that insert is, in fact, completely -- I'm not
18 fooling you -- the Commission proposing to incorporate
19 flexibility into its regulations by requiring DOE to
20 demonstrate the repository comprises multiple barriers but
21 does not prescribe which barriers are important or describe
22 their capability.

23 Don't steal -- but without telling you what
24 stealing means. I'm just reading the page. Okay? You
25 can't implement don't murder or don't steal without the

1 details. You can't, because there are ambiguities about
2 what it means.

3 MR. GARRICK: Disagree.

4 MR. BUDNITZ: Okay.

5 So, what it says here is kind of odd. Propose to
6 incorporate flexibility by requiring barriers, not going to
7 prescribe. Well, of course, they go further. So, it's not
8 quite that bad.

9 This is just the next, you know, eight lines down.

10 The proposed requirements will provide for a
11 system of multiple barriers to ensure defense-in-depth and
12 increase confidence.

13 Probably what you meant was so that you could
14 increase confidence, but I'm just reading it, what it says.
15 I mean I'll give you the benefit of the doubt on how you
16 read it. Increase confidence so that the objective will be
17 achieved. Okay?

18 I just have to read it that way.

19 Now, here's the dilemma.

20 NRC, NMSS, Part 63, Yucca Mountain -- be sure you
21 understand the context.

22 Will NRC use this as a decision criteria? Which
23 is really, more directly, can DOE's license application
24 flunk based on insufficient defense-in-depth even if it
25 would otherwise pass?

1 That's where the rubber hits the road, and then
2 you've got to get into some details about that, but that's
3 the question, and it's apparently yes. Of course, the rules
4 aren't finalized yet, Part 63 is still draft, and EPA has to
5 come in and it has to get changed, but apparently, yes.
6 I've been reading testimony and talks and various positions
7 of the staff, and apparently, yes.

8 Now, if so, how? How will the decision be framed
9 and made? That's where we need to talk.

10 Observation -- and this is a crucial observation
11 of mine: The decision criteria, whatever they will be, need
12 to be clear, they need to be fair, and they need to be
13 technically logical.

14 MR. KRESS: In other words, the Commission needs
15 to revisit this statement that they do not intend to specify
16 numerical goals for the performance of individual barriers.

17 MR. BUDNITZ: I'm going to argue that what's there
18 is ambiguous.

19 MR. KRESS: Yes.

20 MR. BUDNITZ: And what piece of it they revisit,
21 I'm not sure, but what's there is ambiguous, and I know that
22 the staff agrees, because I've heard the staff say this in
23 public, that more is needed, and there are even some
24 tentative positions, and I'm thrilled that that's true.

25 MR. KRESS: I think somebody needs to specify what

1 those goals for individual barriers are.

2 MR. BUDNITZ: Fair enough.

3 Now, I'm going to switch the order of my slides if
4 you've got them in front of you, because I'm going to make
5 an observation.

6 I sent a letter to the docket on June 25, and I
7 also sent a letter to John Garrick, chairman of the ACNW,
8 but this quote is from both of them. This is from a letter
9 that I wrote six months ago, seven months ago. I'll read it
10 to you, but you can read it, too.

11 When I apply these ideas to Yucca Mountain, I
12 stumble principally because the notion of so-called
13 independent barriers, one of which can fail without
14 compromising the overall system, which notion has been so
15 useful conceptually for achieving and demonstrating power
16 reactor safety seems not to apply to Yucca Mountain, and
17 everybody that deals with Yucca Mountain understands this.

18 As I understand the design concept, one cannot
19 assume total failure of any of the so-called barriers
20 without seriously compromising overall performance, and
21 that's not necessarily true, by the way, for a power
22 reactor.

23 I can show you power reactors operating in the
24 world for which, if you didn't have a containment, you could
25 meet all the goals, safety goals and everything.

1 MR. APOSTOLAKIS: I'm confused by that.

2 MR. GARRICK: Just one question. Where in a power
3 reactor does it say how much liquid control has to
4 contribute to the risk?

5 MR. BUDNITZ: I understand that. I exactly
6 understand, but the idea here is -- without arguing about
7 what works for reactors, the idea here is that, for sure,
8 you can't totally remove -- by the way, the staff agrees
9 with this -- you can't totally remove barrier number four or
10 barrier number one and still show it at Yucca Mountain,
11 because it doesn't work that way.

12 It's not the same as the fact that, at many power
13 reactors, you can totally remove the containment and you can
14 still meet all operating NRC goals, except the goal that
15 says you've got to have a containment, but you know, the
16 overall safety goals and all that stuff -- you can meet it.

17 MR. APOSTOLAKIS: I'm confused by that. This is a
18 question of clarification.

19 MR. BUDNITZ: Yes.

20 MR. APOSTOLAKIS: Are you talking about a
21 particular technology?

22 MR. BUDNITZ: I'm talking about a particular
23 design.

24 MR. APOSTOLAKIS: PWRs as we know them today.

25 MR. BUDNITZ: Yes.

1 MR. APOSTOLAKIS: You are saying that, if I remove
2 the containment, I am not compromising overall performance?

3 MR. BUDNITZ: I am saying to you I believe that
4 you can still meet the overall safety goals for some
5 designs.

6 Now, without arguing whether that's true or not --
7 I don't want to argue that. What I'm saying is it is surely
8 true at Yucca Mountain that you can't remove -- totally
9 remove -- and the staff is not talking about that. That's
10 what we're going to come to.

11 You certainly can't remove the canister. You
12 can't remove the ground. So, we have to talk about what I'm
13 going to come to in the next slide, under-performance,
14 rather than removal, and that's where the details come in.

15 Let's not argue about what I said here about
16 reactors. I'm talking about Yucca Mountain.

17 Now, I'm going to go back and say, in practice,
18 perhaps -- and I don't know, I'm guessing. Perhaps in
19 practice, despite NRC's words to the contrary, DOE will
20 never actually flunk at Yucca Mountain, but defense-in-depth
21 will be used, instead, like ALARA.

22 Do what you can beyond meeting the thing -- you
23 met the dose in Amargosa -- do what you can beyond meeting
24 the bare regulations whenever it's cost-effective or
25 whatever you mean by effective -- again, some other

1 parameter that you have to pay for.

2 I don't know that, but that's one possibility as
3 to how it will actually be used.

4 But if that's true, how does NRC conceive this
5 would work in practice?

6 I mean there's the classic. Might NRC ask for
7 protection from one or another barrier in the name of
8 defense in depth even if the overall performance is okay?
9 In other words, you met it, but you still got to have a
10 containment.

11 I'm not arguing this is bad. I just want clarity.
12 You need clarity, just as when you say don't murder, you
13 need clarity whether abortion is murder or not.

14 And then there's the classic: What if one barrier
15 provides 90 percent of the total protection? Maybe that's
16 not enough of a mix. Go read the Congressional legislation,
17 which says you've got to have multiple barriers. But what
18 if one of them produces 90 percent of the protection?

19 Maybe DOE can say, great, we can weaken that
20 barrier so it only produces 40 percent and we still meet the
21 rules. None of us want that. That's nuts.

22 MR. GARRICK: Bob, you're missing, I think, an
23 extremely fundamental point that the pioneers had the
24 foresight to put in the fundamental Atomic Energy Act, and
25 that is the word "reasonable."

1 MR. BUDNITZ: Oh, no, I understand, of course.

2 MR. GARRICK: And I just think this is nonsense,
3 these arguments, because they're not reasonable.

4 MR. BUDNITZ: Exactly. But that's why we need
5 specific criteria so that people won't use unreasonable
6 arguments one way or the other, without specific criteria.

7 MR. GARRICK: You don't have specific criteria in
8 an of the reactor -- Part 50 -- along the lines that you're
9 talking about.

10 MR. BUDNITZ: Yes, we do. We tell you what the
11 containment must do. We prescribe its performance.

12 MR. GARRICK: You don't prescribe the performance
13 of the safety injection systems.

14 MR. BUDNITZ: No. We prescribe the performance of
15 the containment.

16 MR. GARRICK: I think you're splitting hairs.

17 MR. BUDNITZ: Let me go on. The staff has gone
18 further than this, thank God, because if you didn't go
19 further than this, we really would be in the soup, and
20 that's what I'm trying to say.

21 You can't have don't steal up here. You've got to
22 have some detail that they have to meet or they don't meet
23 or they can analyze against, that you can regulate against,
24 that you can decide, and the designers can use, and so on.

25 If all you had was the dose in Amargosa Valley,

1 you know, dose rate per year in Amargosa Valley, and that
2 stuff, the designers know what to do. They know what to do.
3 But if they've got to do this, too, the NRC has the
4 obligation to tell them what to do, tell them what they're
5 going to test against, what the criteria will be. That's
6 what I'm arguing.

7 So, we're talking here about under-performance.
8 That's a phrase I've seen recently. So, perhaps the staff
9 isn't thinking about -- don't assume total failure.

10 We all know that's nonsense. I don't know what
11 total failure means. What do you mean, total failure?
12 We're not saying the can isn't there. The can might not
13 behave as well. We're not saying the earth isn't there.
14 We're saying maybe we didn't understand travel times or
15 maybe the chemistry is different than we thought. It's at
16 the extremes of some state of knowledge uncertainty
17 distribution unluckily, even though we think it's over here
18 but we think it's possibly over there, but maybe it really
19 is over there.

20 So, maybe we're talking about under-performance
21 rather than -- you know, to assume under-performance of
22 barrier number two or whatever and go analyze it again.
23 Fine.

24 What does this mean? And that's the point. What
25 does this mean? What analysis requirements leading to some

1 sort of decision criterion will satisfy my three figures of
2 merit? It has to be clear and it has to be fair and it has
3 to be logical, and I haven't seen that yet, and short of
4 seeing that, to be argued about amongst the technical
5 community and understood, short of seeing that, you still
6 haven't told the Yucca Mountain project what they should do
7 in their design and in their analysis so that they know
8 where they're going, short of that. You need that. You
9 need to have the details.

10 Now, finally -- this is really a place where I am
11 truly stuck -- if NRC lets DOE decide what under-performance
12 means -- and there has been talk about in some of what I've
13 seen -- if DOE decides that under-performance means this and
14 says bring me the rock, wrong rock, late in the game --
15 remember, they're designing it now, they're finalizing their
16 design now, and then they're going to analyze for a couple
17 of years, and that's a terrible dilemma. You just don't
18 want that.

19 DOE will not assume so much under-performance that
20 it will flunk if, of course, it passes under the base case,
21 you see, because anybody can dream up a set of
22 under-performances that will flunk.

23 I can do that, but in fact, isn't that just what
24 NRC's concern really is?

25 NRC ought to be concerned, as the regulator, in

1 its statutory role, to be sure -- they've got to look for
2 combinations of under-performance that might lead to serious
3 compromises, whatever that means, find out whether there --
4 what the probability is and the consequences of those or how
5 much we don't know or what the uncertainties are or where we
6 have to go get more knowledge and make sure that's straight.
7 That's NRC's regulatory job, as I see it, under the
8 philosophy of an independent regulator, right?

9 So, you just shouldn't ask DOE unless you ask them
10 to explore the whole face base, and then I don't quite know
11 what to do with that, because then it's the
12 bring-me-the-rock thing.

13 So, perhaps NRC has to tell them how much to
14 assume, and that leads to the other problem, which I know
15 the staff is wrestling with, because I've seen discussions
16 and so on, mainly NRC is trying not to be overly
17 prescriptive -- thank God, by the way -- in using the
18 philosophy of performance-based analysis and decision-making
19 and so on.

20 So, this is the dilemma for defense-in-depth. The
21 Yucca Mountain project and the Department of Energy deserve
22 specificity as they're finalizing the design and doing the
23 analysis.

24 MR. APOSTOLAKIS: What's under-performance again?
25 I missed that.

1 MR. BUDNITZ: Under-performance is the assumption
2 that barrier number two or whatever, instead of totally
3 fails, only fails in a certain way. Just as we say, in the
4 reactor game, analyze as if you had a loss of off-site
5 power, even if the probability is low.

6 MR. APOSTOLAKIS: But why do I have to tell DOE
7 how much under-performance to assume? Aren't they going to
8 do it as part of the PA?

9 MR. BUDNITZ: Well, the face base is so vast.

10 MR. APOSTOLAKIS: But they have to do this, assign
11 probabilities to these things.

12 MR. BUDNITZ: No.

13 As I understand it, they are supposed to produce a
14 base-case performance assessment, with its uncertainties
15 explored, but they don't necessarily have to show what the
16 dose in Amargosa Valley is if barrier number two
17 under-performs by X percent or fails at 1,000 years instead
18 of 10,000 or has more juvenile failures than they think is
19 right or whatever.

20 MR. APOSTOLAKIS: But if they assign probabilities
21 to these various scenarios, 1,000 years versus 5,000 years,
22 then the performance assessment will reflect all these.

23 MR. BUDNITZ: Only if they're asked to reveal it
24 and if they're told that that will be the thing against
25 which they'll regulate, George.

1 Let me just describe a possibility.

2 Suppose I said to you that the department believes
3 that juvenile failures of the canister will compromise X
4 percent -- it might be X-tenths of a percent -- of all the
5 cans. That's their best estimate, and they have a
6 uncertainty distribution about that state of knowledge.

7 NRC might say I don't care what you do with that.
8 Put that in the performance assessment, but I want to see an
9 analysis that's 100-X percent.

10 In other words, instead of .02 percent, maybe 2
11 percent, as a means of assuring that, gee, you know, I
12 really don't know whether I trust -- that's Dana Powers'
13 argument.

14 That's a valid way to regulate, is to tell the
15 licensee to assume something that is unrealistically
16 conservative and still show you're okay, and that's not in
17 the performance assessment.

18 MR. APOSTOLAKIS: Let me take an example of a PRA.
19 Maybe I misunderstand what you are saying.

20 Somebody brings me a PRA and I review it. That
21 licensee wants to use it in their process.

22 MR. BUDNITZ: Right.

23 MR. APOSTOLAKIS: The licensee cannot come to me
24 and say I'm not going to worry about common-cause failures,
25 because you didn't --

1 MR. BUDNITZ: No. Let me make a postulate here
2 that the licensee, the applicant says we think that there
3 are going to be five juvenile failures of our canister in
4 the first 5,000 years, and our state of knowledge is such
5 that we're very confident it's no more than 20.

6 It's not inappropriate for the regulator to say
7 analyze for 400 and show me what that does, and if you still
8 perform -- that's not inappropriate. If you still perform,
9 great. On that aspect, we're going to give you your
10 license.

11 MR. APOSTOLAKIS: This is not a performance
12 assessment anymore.

13 MR. BUDNITZ: We're regulating, George. That's
14 just the point. We're regulating. We're trying to
15 regulate.

16 MR. APOSTOLAKIS: I'm playing devil's advocate.

17 MR. BUDNITZ: Of course. I understand.

18 MR. APOSTOLAKIS: So, DOE, the applicant, would
19 like the benefits of both performance-based regulation and
20 the --

21 MR. BUDNITZ: No, no, no. Quite the opposite.

22 I can't speak for them, but they're probably
23 thrilled with just the single figure of the dose in Amargosa
24 Valley, but if NRC is going to say we're going to impose
25 defense-in-depth by telling us that we have to under-perform

1 barrier number two as a means of exploring how
2 defense-in-depth actually works, somebody needs to write
3 down what under-performance means in detail so we'll know
4 what to analyze, and the under-performance is presumably
5 outside of the realm --

6 MR. APOSTOLAKIS: You're really coming back to Tom
7 Kress' point that you have to have some sort of allocation.

8 MR. BUDNITZ: I'm not arguing that
9 under-performance is the way to go, but if they're going to
10 do it that way, they need to prescribe it, and it may be
11 outside of the realm that DOE believes is the real world,
12 just as we said 2,300 degrees for the peak clad temperature
13 -- nobody thinks that's the right number, but if you meet
14 it, you get your license, and I'm worried that, absent --
15 and this is early, soon, not five or 10 years from now --
16 I'm worried that, absent specific criteria against which the
17 department, Yucca Mountain, the applicant can analyze and
18 know that he passed or he didn't pass and can change the
19 design now, before it's too late, in order to, you know,
20 improve and meet, that it's an open-ended, unsatisfactory
21 regulatory arena.

22 MR. GARRICK: Bob, you seem to be strongly
23 advocating an allocation process.

24 MR. BUDNITZ: No.

25 MR. GARRICK: Well, you seem to be.

1 MR. BUDNITZ: No, no, no. I don't think
2 defense-in-depth is necessarily the principle that others
3 do, but if they want to use it, they've got to tell them
4 how.

5 MR. GARRICK: The NRC has been very clear in
6 telling them that they want to know the role of the specific
7 protection barriers, and my whole point was that the only
8 place that makes any sense is in relationship to the bottom
9 line.

10 MR. BUDNITZ: I quite agree.

11 MR. GARRICK: I think one of the things that's a
12 problem here is that -- the great thing about the PRA
13 business is that we established a measuring process through
14 the PRA, and we got some experience on it before we started
15 fussing around too much and trying to calibrate that
16 measure, and I kind of see that here.

17 There are some fundamental principles that have
18 been laid down, and one of those principles is that all of
19 the protection should not come from just the engineered
20 systems or just the natural setting.

21 MR. BUDNITZ: Sure.

22 MR. GARRICK: Now, it sounds like what you're
23 saying is that, if they say that, they need to say more
24 about how much of it should come from where.

25 MR. BUDNITZ: No, not necessarily how much of it

1 should come from where. I don't like that either.

2 They need to establish specific performance
3 criteria or analyses or outcomes or something like that that
4 the department can analyze to now, while they're still
5 changing the design. Otherwise they get the
6 bring-me-the-rock problem.

7 They need to say under-performance of the canister
8 means X for juvenile failures, means Y for corrosion, means
9 Z for when it will happen, 1,000 years or 6,000 years. They
10 need to tell them what under-performance specifically means
11 for those things, assuming, I assume, that the
12 under-performance they're going to tell them about is
13 outside of where the department believes is the true
14 knowledge of the performance.

15 Now, you know, I don't care whether you say it's
16 this. Analyze that anyway. That's not an illegitimate
17 thing for regulators to do, and they do that all the time.

18 MR. APOSTOLAKIS: Why would the NRC ask them to do
19 that?

20 MR. BUDNITZ: Why don't you ask the NRC? But
21 they're talking about asking them to analyze
22 under-performance of various of the barriers, either one at
23 a time or maybe in combinations, but absent specific things,
24 the applicant doesn't know what to do.

25 MR. APOSTOLAKIS: Are they doing sensitivity

1 studies, then?

2 MR. BUDNITZ: Why don't you ask them?

3 MR. APOSTOLAKIS: It looks like you're saying the
4 department will come in here with a base case and what they
5 think is likely and this and that.

6 MR. BUDNITZ: Yes, sir, of course.

7 MR. APOSTOLAKIS: And then the NRC staff comes
8 back and says now do this, I would like you to do this,
9 which is a sensitivity study.

10 MR. BUDNITZ: That's what I said. These are
11 sensitivity studies. They're always a good idea.

12 MR. APOSTOLAKIS: And is it because we feel that
13 the uncertainties -- that right now we cannot quantify them?

14 MR. BUDNITZ: Well, why don't you ask them? But
15 here's what I think, and I'm reading minds.

16 Apparently, somebody somewhere in this Commission
17 and its staff thinks that defense-in-depth needs to be
18 invoked separate from the TSPA, the performance assessment
19 as a whole, taken with its state of knowledge, and I'm not
20 going to argue whether that's a good or a bad philosophy,
21 but if they want to do that, they need to tell the
22 department specifically, with specificity, what the things
23 are to which they're going to regulate, so they can change
24 the design and show it's okay now.

25 MR. APOSTOLAKIS: I'm not familiar with that

1 particular staff position, but if, indeed, they want to
2 apply defense-in-depth independently of the PA, then that's
3 exactly what I'm against, and I hope I learn more about it.

4 MR. KRESS: In fact, it sounds like a de facto way
5 of allocating, actually.

6 Bob, did you have a question?

7 MR. BERNERO: Bob Bernero.

8 I'd just like to add -- I was going to address it
9 in my talk -- there is a statutory difference here.

10 MR. BUDNITZ: Yes, there is.

11 MR. BERNERO: The 11th commandment, not out of the
12 Book of Exodus but out of the Nuclear Waste Policy Act,
13 simply says the repository must have multiple barriers. So,
14 there is a regulatory need to address how does one implement
15 that commandment, and that's part of this.

16 MR. BUDNITZ: Absolutely, but of course there's an
17 easy way to meet that.

18 The fact that there is engineered barrier design
19 and the earth is, by definition, a multiple barrier. If you
20 really wanted to be sloppy, you could say of course we've
21 got that.

22 But if you want to go further -- and I agree with
23 you, Bob -- if the Congress wants to go further, got to go
24 further, they've got to go further specifically. They just
25 can't let the applicant figure it out.

1 MR. APOSTOLAKIS: The words "multiple barrier" are
2 so fuzzy. Anything is a multiple barrier.

3 MR. BUDNITZ: George, the statute has that
4 language, though.

5 MR. APOSTOLAKIS: Well, then it must be right.

6 MR. KRESS: I think we have time for more
7 discussion later.

8 MR. BUDNITZ: Without specificity, it's like don't
9 murder. Without specificity, you don't know how to
10 regulate.

11 MR. APOSTOLAKIS: I find that very interesting,
12 Bob, because in reactors we see the same thing. People want
13 the performance-based regulation, and you give it to them,
14 they come back and say, what, you didn't tell me what you
15 want me to do.

16 MR. KRESS: Okay.

17 [Recess.]

18 MR. KRESS: Will the meeting please come to order?
19 Thank you.

20 Now we're at the point on the agenda where we're
21 going to hear from Tom Murley.

22 You're up, Tom.

23 MR. MURLEY: Thank you, Tom and John. Thank you
24 for the invitation, also. I don't have view-graphs or
25 slides, so I'll just sit here and say my piece.

1 I should say at the outset that I am not sure just
2 how much I can help on your discussion on Yucca Mountain.

3 I've not kept current with all the latest policy
4 statements and SECY papers and ACRS letters and things,
5 although I should say Jack Sorenson did an excellent job, I
6 think, in research this topic and sending the material out,
7 but I have given a good deal of thought over the years to
8 nuclear safety and defense-in-depth, and so, perhaps I can
9 discuss some philosophical issues, and if it helps you,
10 fine.

11 The first point I guess I would like to make is
12 that, in my experience, defense-in-depth is not a regulatory
13 requirement. It's not a principle. It never was.

14 I would characterize defense-in-depth as an
15 after-the-fact explanation to Congress and to the public of
16 how NRC achieves safety for reactors.

17 That is, after regulations were developed and
18 after the staff implemented them through branch technical
19 positions and reg guides and things, there was an
20 explanation of what it all meant, and one way to do that --
21 and I think a very useful concept -- was the
22 defense-in-depth concept, and as I read Cliff Beck's 1967
23 explanation to Congress, that's probably one of the early
24 things I read when I joined the AEC in 1968, but it was
25 never used as something that the staff used as a

1 requirement, a hard-and-fast requirement, and I think --
2 I'll give an example.

3 This was illustrated by the Three Mile Island 2
4 accident.

5 I recall a meeting some months after the accident
6 where an aerospace safety expert was giving his views of the
7 accident.

8 He may have been from NASA, and I think he might
9 have even have been assisting the Kemeny Commission, and he
10 observed that NRC talks about defense-in-depth but they
11 don't really enforce it, and he said, for example, the plant
12 was designed -- this particular plant, Three Mile Island,
13 was designed for the pressurizer relief valve to open during
14 a feedwater transient so that the high-quality primary
15 system was deliberately breached during a design basis
16 transient, and of course, we know that the relief valve
17 stuck open in that case.

18 He continued by noting that the operators defeated
19 the safety systems by shutting off the ECCS, the
20 high-pressure injection, and his point was that one of the
21 major fundamental barriers of defense-in-depth was
22 deliberately defeated by the operator action.

23 We now know, of course, that there were confusing
24 indicators and circumstances that led the operators to take
25 those actions, and finally, this observer noted that the

1 containment was open during the early part of the accident
2 and that that fact permitted radioactivity to be released
3 directly to the auxiliary building and to the atmosphere.

4 Eventually, of course, the sump pumps were secured
5 and the containment was isolated in that accident, but his
6 point was this philosophy of defense-in-depth was something
7 that the agency, back then, at least, talked about but
8 didn't really enforce, and it was not -- his point was, of
9 course, a negative point with regard to the NRC and the
10 staff, and this analysis -- I'm sitting there listening to
11 it, and I became very embarrassed as a NRC staff member,
12 because he was right, and it had a profound impact on my
13 thinking about safety at the time, and that was, if NRC has
14 a regulatory requirement and one relies on that requirement
15 in this defense-in-depth argument, then you really have to
16 enforce it.

17 So, you've got to make sure that the containment
18 is reliable and so forth.

19 In other words, the barriers of each level of
20 defense-in-depth should be highly reliable. That's the
21 message I took from that discussion, and it did follow me,
22 and I did use it and think about it during my career, at
23 least, in that term.

24 I sent the committees -- actually, to John Larkins
25 -- an old document dated April of 1989 on Shoreham emergency

1 preparedness that I had in my files, and insofar as that was
2 what we relied on -- that's what I relied on when I licensed
3 Shoreham in 1989, and it is, thus, official Commission
4 policy as of 1989.

5 So, it is a discussion of how emergency
6 preparedness fits into the defense-in-depth safety
7 philosophy, and so, there's an introduction in the first
8 page of where emergency preparedness fits in, and we termed
9 it, then, as effectively a fourth level of safety. I think
10 that's the phrase we used.

11 Now, the significance of that paper for this
12 discussion, I think, is that the topic of defense-in-depth
13 was used only as a philosophical introduction. It doesn't
14 say that it's a requirement.

15 I then stopped the discussion of where it fits in
16 and went through a point-by-point discussion of how Shoreham
17 met the actual regulations, and so, there was never a use of
18 defense-in-depth as a requirement per se.

19 As I said, it's kind of an after-the-fact
20 explanation of how NRC achieves safety, and my explanation
21 -- I should say the agency's explanation then, at that time,
22 was that emergency preparedness was, in effect, a fourth
23 level of safety, but it was not meant to be that it was an
24 absolute barrier, or there were no numerical guidelines or
25 requirements for each of those levels.

1 There were other instances where I recall falling
2 back on the defense-in-depth philosophy in my own thinking
3 about specific safety issues, and I'll give a couple of
4 examples.

5 The staff -- and I'll speak for myself, because I
6 can't speak for the staff today, but I was always sensitive
7 to conditions or accident sequences that could breach
8 multiple levels of defense-in-depth through a common cause,
9 and we always paid a lot of attention to those.

10 That's why steam generator tube integrity was
11 always such an important issue for the staff. We gave it
12 high attention, because multiple steam generator tube
13 ruptures could lead to bypassing containment either before
14 or after core damage, and that -- one may wonder why, I
15 guess, steam generator tube -- maybe it's obvious, but it
16 was for that reason, at least in my own thinking, that this
17 was a path that could breach multiple barriers of
18 defense-in-depth.

19 And then in the late 1980s, I recall thinking
20 about safety culture and what does it mean, where does it
21 fit into the overall picture of safety, and it slowly became
22 clear that and I concluded that it was extremely important,
23 safety culture was extremely important, because -- it was
24 Chernobyl, actually, that showed that a poor safety culture
25 at a plant could lead to actions that could cut through all

1 levels of defense-in-depth.

2 In other words, it could be a common cause for
3 breaching multiple safety barriers. If you've got a poor
4 culture, you can do stupid things that initiate the
5 accident. You can do a test that's not properly planned.
6 You can put the reactor in conditions it was never designed
7 for. You can shut off safety systems.

8 In other words, it is a means for slicing through
9 the defense-in-depth barriers, and it was that thinking that
10 personally I went through that caused me to conclude that
11 safety culture was an extremely important safety concept.
12 To me, it's not an abstract concept or idea, but it's an
13 essential aspect of nuclear safety.

14 So, I hope I'm giving some examples of how one
15 regulator, at least, on the staff used and thought about
16 defense-in-depth.

17 There are some questions that were posed in the
18 material that was handed out to us, and I know Bob Budnitz
19 and Bob Bernero have talked about some of them, and I'll aim
20 at a couple that I think I can contribute to.

21 One is, is there an over-arching philosophy of
22 defense-in-depth, or a discussion of it, and I have not
23 spent a lot of time on the definitions.

24 I know there are lots of them, but the philosophy,
25 to my mind, is fairly simple, and that is, there should be

1 multiple barriers for protecting public from radiation, such
2 that single mistakes and single failures, even of programs
3 -- like emergency preparedness is really a program, you can
4 think of it, but in that sense, as George said, it's a
5 barrier.

6 It doesn't have to be a physical barrier, and
7 insofar as possible, these barriers should be independent,
8 and I don't think that should be an absolute requirement,
9 but one should try to make them as independent as possible.
10 So, multiple independent barriers for protecting the public
11 from radiation.

12 It should be made a regulatory requirement, in my
13 judgement, but it should remain a guiding principle, because
14 it is a good way to think about safety, as I think I've
15 tried to illustrate.

16 A second question, how is it used in materials --
17 and I'll let Bob Bernero, who's thought about this a lot
18 more than I have and also speaks about it better -- give
19 some examples, but there's one that I've come across
20 recently that seems to me a perfect example of how
21 defense-in-depth thinking is used, and that is in
22 criticality safety.

23 There is this concept of single contingencies,
24 multiple -- double contingencies, triple contingencies as
25 protection against criticality, and that, to my mind, is a

1 perfect illustration of how one thinks about multiple
2 barriers of defense-in-depth.

3 Apparently there is -- well, I know there is a lot
4 of discussion of how should PRA be used in risk-informed
5 regulation consistent with defense-in-depth, what does that
6 mean, and I guess I don't have the answer to that, but I can
7 tell you how I interpret it, and that is it means don't use
8 risk arguments solely to weaken or remove levels of
9 defense-in-depth.

10 I think that's how I would use it if I had to use
11 that language, and even though one has to, I guess, hold
12 open the theoretical possibility, George, that you could use
13 risk arguments or numerical arguments to remove containment,
14 that comes very close -- well, it's a regulatory
15 requirement, so you probably can't do it, but it comes very
16 close, I think, to using defense-in-depth as close to a
17 requirement.

18 MR. APOSTOLAKIS: I'm coming back to Bob's
19 question of what is murder? What is a risk argument? A
20 risk argument, in my view, includes all the engineering
21 analysis and physics that is appropriate to do.

22 So, in my mind, one could use risk arguments to
23 reduce defense-in-depth, as long as the uncertainties are
24 handled properly and convincingly.

25 So, a risk argument -- I mean PRA, in my mind,

1 includes the underlying physics, chemistry, and engineering
2 that sometimes we call traditional analysis.

3 So, I assume that's what you mean by risk
4 argument?

5 MR. MURLEY: Yes. And I did not say and I
6 certainly didn't mean to imply that you cannot use risk
7 arguments or engineering analysis, the whole panoply of
8 arguments, to reduce margins where they're excessive and
9 that sort of thing, but I think you would run across some
10 severe resistance if you pushed the argument to remove an
11 entire barrier of what people view as defense-in-depth.

12 For example, people have used the argument, risk
13 arguments -- and I've heard them -- to remove emergency
14 planning, period, for advanced reactors. I think that's
15 going to run into some serious programmatic, you know,
16 policy problems.

17 I think it can be used to quantify the protection
18 offered by these levels, and I think John Garrick's paper --
19 I did skim it, and I did listen to him carefully. I think
20 it's a very good analysis, an appropriate use of how to
21 analyze and understand barriers.

22 If it's pushed to the level of using numerical
23 goals for those barriers, then I think that's maybe pushing
24 things a little further than people are ready for today,
25 although in principle, one has to hold open the possibility

1 that it can be done.

2 There is the notion of safety goals. Are they
3 clear for regulatory use in the materials area or even the
4 reactor area, for that matter, and I must say the safety
5 goals -- I found them to be not much use at all.

6 The public health goals -- I'm sure you realize,
7 of course, there's a big gap -- there's an order of -- two
8 orders of magnitude difference between the public health
9 goals and the plant performance goals in terms of the
10 protection that they offer to the public, and this has
11 always been a stumbling block for use by the staff.

12 The staff was told by the Commission -- they
13 worked with the ACRS for years to try to rationalize a large
14 early release goal with the public health goals, and it
15 couldn't be done, because there's this
16 two-order-of-magnitude difference.

17 One can have a TMI-2 meltdown accident every year
18 and still meet the public health goals. You can work it
19 out.

20 So, they were not very useful at all, and
21 certainly, when I was with the staff, we didn't use them in
22 our day-to-day activities, with one exception.

23 We found them -- we did -- in reviewing and
24 certifying the evolutionary advanced reactors, we used a
25 conditional containment failure probability of .1 as a

1 guideline, and we found that very useful as a guideline, but
2 even there, we had to back off using a numerical goal,
3 because -- in this case, it was General Electric complained
4 -- and I think they were right.

5 They complained that, in some cases, by forcing
6 that goal, you're actually increasing the core damage
7 frequency.

8 So, we did is tried to formulate an equivalent
9 deterministic requirement that we felt was equivalent to the
10 10-percent conditional containment failure probability, but
11 overall, I have to say I don't think that we found the
12 safety goals very useful.

13 Finally, there is a nexus in all this discussion
14 of defense-in-depth to risk-informed regulation, and I'm a
15 big fan of risk-informed regulation.

16 I wrote a paper about it five years ago or so
17 supporting it, and I think I am very pleased with the way
18 the agency is moving in this direction, but there is a
19 troubling aspect, and maybe I don't see it correctly, but I
20 would like to at least tell the committees what's troubling
21 me, and that is that there is a whiff in all of this
22 discussion, more than whiff, an aroma of relaxing
23 regulations and reducing burdens, almost as if this is a
24 deregulation exercise, and you know, there is room for that,
25 I agree with that, but people forget the other side of the

1 coin, and that is there is this role of risk-informed
2 operation, too, where the operators of reactors, in
3 particular, can use risk to improve safety, and you can do
4 them at the same time.

5 You can have reduced burden and improved safety at
6 the same time if it's done wisely, but I don't hear any
7 discussion of that coming out of this committee or coming
8 out of the staff these days, or the Commission, and I think
9 somebody needs to pay attention to this, because if
10 risk-informed regulation comes to be seen as just a code
11 word for deregulation, I think the whole thing is doomed,
12 because I don't think you will have public support in the
13 long run for that.

14 Some conclusions, then.

15 I agree with, I guess, John Garrick's
16 characterization that there is fuzziness in this
17 defense-in-depth concept and that it can stand some
18 clarification and even some numerical clarification, and I
19 commend the committees for shining some light on this
20 subject.

21 I am very uneasy with any notion of pushing
22 defense-in-depth to the level of a principle or a
23 requirement, and I am also uneasy if there is a trend to
24 allocate numerical goals to the levels of defense-in-depth.

25 I think you'll run into trouble just like the

1 safety goals kind of ran into trouble, and ultimately, it
2 would not be much use.

3 That concludes my remarks.

4 Tom?

5 MR. KRESS: Thank you.

6 That brings us to Bob Bernero.

7 MR. BERNERO: I, too, would like to thank you for
8 the opportunity to speak to the joint subcommittee, and as I
9 will explain in my remarks, I'm going to try to focus more
10 on the material licensing and the high-level waste arena, or
11 waste management arena, than on the reactor arena.

12 I would, however, like to start out with just an
13 exposition -- I used to tell people when I was here that the
14 greatest conflict of interest you'll face in your life is
15 defending what you said yesterday, and I feel a little bit
16 of that now, because I'm going to go back to statements I
17 made in the past decades, when I was working in the NRC and
18 had the good fortune to be involved in safety goals and
19 things like that, regulatory philosophy.

20 A safety goal has practical use as a description
21 of the levels of safety or reliability that is sought by a
22 regulatory system, and similarly, a probabilistic risk
23 assessment or any kind of risk assessment has value as a
24 description a display of your best knowledge about the level
25 of safety or reliability you are achieving but to regulate

1 to a safety goal, to define quantitative standards in a
2 safety goal as the formula for a safety decision on the
3 acceptability of a reactor or its features is not a wise
4 move, and for years and years, as safety goals were
5 developed, there was a very strong philosophy that, beware,
6 don't regulate to safety goals, use safety goals in
7 formulating regulatory systems or approaches but don't
8 regulate to the safety goal, and of course, I will
9 acknowledge that the high-level waste program, from the very
10 beginning, has as one, not the entire, but one basis of
11 acceptable judgement a safety goal.

12 That's what the performance assessment is
13 calculating.

14 So, a word of caution on that, but talking here
15 today about defense-in-depth, as I will say shortly,
16 defense-in-depth as an approach, as a strategy for safety
17 analysis, a strategy for design and safety analysis, is a
18 very good description of your caution in avoiding undue
19 reliance on any single feature, barrier, or thing or aspect,
20 and when you do that, your safety analysis should beware of
21 a prescriptive approach and the safety evaluation, with
22 quantification where you can do it, without quantification
23 when necessary, or with very, very vague or poor
24 quantification, it still has to rely on reasoned judgement
25 with the best display of information before you and then

1 make a decision.

2 Jack Sorenson gave us some questions. In the
3 slides you have, I slightly changed the questions, and I
4 geared them so that I could go through responses to the
5 general questions and the specific questions in the three
6 specific areas of regulation, and that, of course, would let
7 me emphasize the ones I'm more familiar with.

8 I, too, would like to endorse the book -- I have
9 it over there -- that Jack compiled, the research on
10 defense-in-depth. It's an excellent compilation.

11 When I made the view-graphs, I consciously
12 selected one of the papers to quote from, and now I have
13 forgotten which one, and I don't think it's worth the
14 research to go back, but the point is it's a good
15 description.

16 It's a good exposition not of a formula for
17 adequate protection but as a safety philosophy, and many of
18 those definitions fit this.

19 Cliff Beck's 1967 one -- I was very familiar with
20 that, because I came to the NRC in reactor licensing, and
21 that was treated sort of like a gospel, but I think it was
22 Tom or somebody said it was more a public exposition of what
23 we're about rather than a formula for a licensee to build a
24 reactor to.

25 Now, if I go to the very first question, is there

1 an over-arching philosophy, my answer is yes, there is an
2 over-arching philosophy as a strategy of safety analysis but
3 not as a formula, and the key thing here is the undue
4 reliance on any single factor, a rarity of occurrence, a
5 design feature, a barrier, a performance model.

6 An example comes to mind.

7 Many years ago -- in fact, right now, it's more
8 than 25 years -- I had the fortunate experience to be the
9 licensing project manager for TMI-1, and a principle safety
10 issue and contention in the hearing was adequate protection
11 against the crash of a large aircraft, because that plant
12 sits not far from the end of the runway of the Harrisburg
13 International Airport.

14 There was a great deal of analysis to make sure
15 that the standard review plan, which was just developing at
16 that time and used a screening probability for screening out
17 aircraft, that there was not undue reliance on low
18 probability of crash, and it ended up with a very detailed
19 analysis that included what would happen if an aircraft less
20 than 200,000 pounds hit, what would happen if the aircraft
21 greater than 200,000 pounds hit, and one of the good aspects
22 of it all was the licensee, or applicant in this case,
23 recognized all along that the responsibility for developing
24 a persuasive case to show no undue reliance on that factor
25 -- that licensee had that responsibility and fulfilled it,

1 and the staff didn't prescribe what was the due reliance.

2 The applicant demonstrated that there was not
3 undue reliance.

4 Barriers are an issue peculiar to material
5 licensing in many ways.

6 Basically, as I've said, it's not a formula for
7 defining acceptability, and I would caution that simply
8 because one has defense-in-depth, that doesn't mean that
9 there is acceptable safety.

10 You can have very frail defenses, and on those
11 grounds, I would suggest, when you move to the additional
12 thought of risk-informed regulation, that's going beyond
13 defense-in-depth.

14 It is looking at barriers or dependencies or
15 uncertainties and seeking to achieve a sufficient margin of
16 safety, not too much and not too little, and it goes to the
17 degree of knowledge that you can have, or the degree of
18 experience, in many cases, with material regulation

19 MR. APOSTOLAKIS: Before you go on, Bob, I think
20 one of the issues before this subcommittee, I think, or
21 maybe this meeting, is to try to understand words like
22 "undue reliance."

23 I'm trying to put it in the context of
24 uncertainties. Perhaps it would mean the same thing. When
25 you say "undue reliance," I would say I'm too uncertain

1 about the effectiveness of these barriers for some reason.
2 Maybe I don't understand all the conditions under which the
3 barrier is supposed to function. I don't trust, perhaps,
4 the calculations that the event is really very rare and so
5 on.

6 Would that be consistent with your thinking? Why
7 is there undue reliance?

8 MR. BERNERO: Undue reliance -- as an example, in
9 the TMI-2 case -- or TMI-1, actually. TMI-2 adopted the
10 analysis verbatim.

11 In the TMI-1 licensing case, based on the traffic
12 that the Harrisburg International Airport supported and was
13 reasonably expected to support, a screening criterion like
14 10 to the minus 6, 10 to the minus 7 per year likelihood of
15 impact, using a conservative footprint for the reactor plant
16 -- that screening criterion was relied upon only with
17 respect to jumbo jets.

18 Basically, it was concluded that it is a relative
19 rarity for a jumbo jet, something substantially in excess of
20 200,000 pounds loaded weight, to be in this airport or to be
21 using this airport.

22 That left the screening criterion having (a) some
23 good traffic analysis as a basis and (b) the margin of
24 safety implicit in the robustness of the plant given that it
25 was designed for aircraft up to 200,000 pounds, and it had

1 things like a condensate storage tank on each side of the
2 reactor, so that your decay heat removal wasn't compromised
3 by the aircraft crash immediately.

4 You know, condensate storage tanks are out in the
5 open. You know, they're unshielded.

6 So, you had two things. You had an extraordinary
7 robustness, and frankly, the applicant said I'll change
8 sites if I have to get a degree of crash resistance beyond
9 the inherent robustness of a dry containment.

10 You know, a large dry containment is a very robust
11 structure, and they said that's what we'll do. We're
12 willing to expand this facility to that degree of
13 robustness.

14 So the uncertainty of a screening criterion of
15 probability had two factors to make an evaluation: Is this
16 undue reliance or not? But there's no formula for that
17 evaluation.

18 Now, our current safety goals and objectives -- I
19 said a few words about safety goals to begin with, but of
20 course, it goes without saying -- you're all aware that the
21 current safety goals and objectives are very explicitly
22 reactor-oriented, and there's years and years of that
23 dialogue, and if you go into the material regulation or
24 especially into waste regulation, the only thing you find is
25 in high-level waste disposal the criteria that originally

1 derived from the EPA standard, 40 CFR 191, which is a
2 performance assessment with a quantitative release limit
3 probabilistically set.

4 So, I say they're not clear, because first of all,
5 the scope is not clear.

6 There's a span of protection or a scope of
7 protection implicit in NRC regulation that includes public
8 safety.

9 In reactor regulation, you're almost always
10 talking about off-site public safety and not talking much
11 about the worker safety.

12 That's within the NRC jurisdiction but not quite
13 so robustly.

14 You know, look at the steam-line
15 erosion/corrosion, that old Surry incident, 1970-something,
16 where a relief valve -- tail pipe came out of the hole in
17 the deck and scalded two workers to death.

18 Things like that -- NRC's jurisdiction for
19 industrial safety is not clear, and when you go into
20 material regulation, you'll find that ALARA for chronic
21 exposure is an important aspect, but accidental safety is
22 dominated by chemical safety.

23 So, you have -- issues that are far more complex
24 don't lend themselves to formulation.

25 Go into medicine and there is serious challenge or

1 question about NRC's jurisdiction for patient safety -- you
2 know, that is, the person receiving nuclear medicine
3 treatment, and of course, environmental protection -- we
4 have a congruence of NRC's responsibilities and authority
5 with EPA.

6 The practices at NRC, you're quite aware, has a
7 very large range, and I would just single out
8 transportation, which I listed at the bottom, as a very
9 interesting example of lack of defense-in-depth.

10 Transportation relies on one barrier, a great big
11 heavy, bullet-proof, super-strong cask to hold spent fuel,
12 and especially in transport, you have one barrier, and the
13 real question is not do I have multiple barriers, but the
14 real question is am I placing undue reliance on that one
15 barrier, and of course, here, you have a wealth of
16 experience, engineering, metallurgy, testing capability,
17 quality assurance. You have a variety of tools. But the
18 test is, is there undue reliance on a single factor or a
19 single barrier?

20 Reactors -- I would just point out that, in
21 reactor technology, defense-in-depth discussions are, in my
22 experience, invariably associated with accidental releases,
23 not chronic releases, and that comes to be an important
24 consideration in material regulation and waste management,
25 and of course, waste management is a chronic release.

1 The very nature of it is you take the waste and
2 you put it somewhere and say it will stay there until it's
3 gone or forever.

4 In the reactor regulation area, seismic safety,
5 here again you have a probabilistic screen, and you have
6 behind it -- some of you certainly had an experience in the
7 seismic margin analyses that were popular a long time ago,
8 and my favorite term, "HCLPF," the high-confidence of the
9 low probability of failure, which is a very good concept,
10 but it's interesting, if you ever go through the DOE
11 regulations and safety analyses for seismic safety, they
12 actually try to quantify, specific a specific requirement
13 for seismic safety that you go up to your design basis,
14 probabilistically set, and then you go beyond it by some
15 formula and show that this level of acceleration exceeded
16 doesn't do some quantitative damage, rather interesting
17 experiment.

18 But these are all, in my view, things where you're
19 looking at do I have undue reliance on a single thing,
20 whether that single thing is reactor vessel rupture or, as
21 happened in TMI-2, a cognitive error by the operators that
22 bypassed the whole event tree.

23 MR. GARRICK: One of the things that is kind of
24 important in that point about having undue reliance on a
25 single thing is that there's never a single thing even when

1 it appears to be single.

2 By that, I mean, if you're talking about a reactor
3 vessel, for example, you have lots of things that give you
4 indications of the condition of that reactor vessel in terms
5 of monitoring, etcetera.

6 So, it seems that, in those cases -- and the fuel
7 cask transportation is another example -- you may not have
8 multiple barriers in the classical sense, but in most of
9 those cases, you have a great deal more information about
10 the -- its behavior.

11 If a cask -- we have seen it in tests at Sandia
12 under the most severe circumstances you can possibly
13 imagine, and absolutely everything was destroyed but the
14 cask.

15 So, I think that, sometimes, that may be an
16 oversimplification, just because from a phenomena standpoint
17 or from a process standpoint, it may have that pinch point,
18 and we have to offset the vulnerability of that pinch point
19 by additional levels of protection that come in the form of
20 information-gathering, diagnosis, monitors, transducers,
21 etcetera.

22 MR. APOSTOLAKIS: And all that means less
23 uncertainty, right?

24 MR. GARRICK: Yes.

25 MR. BERNERO: Yes.

1 One could reformulate the whole system to say,
2 rather than undue reliance on a single barrier, you could
3 have inadequate response to a single challenge.

4 You know, you could restructure the whole thing
5 logically to do that.

6 MR. APOSTOLAKIS: We're interrupting you too much,
7 Bob, but counting the number of barriers has the same
8 problem that in some earlier times people were ranking
9 minimal cut-sets according to the number of events.

10 Ultimately, it has to come to the probabilities.

11 MR. BERNERO: Yes. And in reactor safety, I don't
12 believe you get there -- you have a regulatory system that
13 gives you multiple barriers rather prescriptively -- that
14 is, reactor coolant pressure boundary requirements,
15 containment requirements.

16 It just doesn't give you the performance, and to
17 resurrect an old argument, you know, the regulations
18 prescribe containment performance predominantly as
19 condensers for LOCAs rather than respondents to
20 loss-of-coolant accidents and core melts.

21 But anyway, one point I'd like to make on reactors
22 is, when you have a defense against some challenge, you need
23 to have graded goals.

24 You know, everything doesn't come out to the old
25 PWR-1 release off-site, and I remember, years ago, in

1 reactor licensing, we used to have spent fuel handling
2 accidents analyzed, and we consciously used one-tenth of the
3 Part 100 release guideline for analyzing a spent fuel
4 handling accident in the pool, which is almost a trivial
5 analysis, because you're under 20 feet of water and
6 virtually nothing happens off-site, and you have to look at
7 that.

8 What are the consequences of the event?

9 When you get into material and waste, that becomes
10 extremely important.

11 In material regulation, the concept of accidental
12 release is certainly with you, but chronic release and even
13 deliberate release has to be considered.

14 Exempt products -- I list there -- if you're not
15 familiar with the terminology in material licensing, when
16 you go home and look in the ceiling of quite a few rooms in
17 your house, you'll see a smoke detector, and the agency had
18 a major deliberating problem in regulation, because a
19 typical battery-powered smoke detector has one-half of a
20 micro-curie of a 500-year half-life alpha emitter,
21 americium-241, stuck in there to ionize the air so that the
22 smoke can cause an electrical phenomenon that will make the
23 little buzzer go off or siren or whatever, the horn, and in
24 regulating such a thing, you have to recognize, you're never
25 going to get them back.

1 They're not going to end up in a low-level waste
2 or high-level waste repository.

3 They're going to be thrown in the garbage.
4 They're going to be picked open by people. And so, you have
5 to look at what I would call chronic release and
6 uncontrolled, routine release for things like that.

7 In order to have graded goals, you have to think
8 through what are the potential consequences of the act which
9 you would authorize, or the procedure, the barriers,
10 protective actions, if they are possible, and evaluate, a
11 balanced choice of defense.

12 You can't prescribe it. It's far too complex.
13 But as you know, a lot of experience -- and you can bound
14 consequences practically.

15 There are knotty problems. That's really a
16 jurisdictional problem.

17 In 1975, when the agency became NRC, there was the
18 Food and Drug Act that transferred patient safety for
19 nuclear medicine to the Food and Drug Administration, and
20 ever since then, the states have authority over patient
21 safety, which is clear, but the NRC does not, and it's
22 argumentative.

23 It's really aside from here, although we had a
24 lethal accident about 1991. In Indiana, Pennsylvania, a
25 brachytherapy patient was killed by radiation, and the NRC

1 requirements which were imposed on that brachytherapy
2 treatment had a device which reeled out wire with, at that
3 time, a four-curie source on the end of it into the
4 patient's body, and that device said I am now safe because I
5 reeled the wire up.

6 The NRC required on the wall an alarming radiation
7 dosimeter and a personnel requirement that you would use a
8 hand-held radiation dosimeter in supplement. That was the
9 defense-in-depth.

10 The source broke off. The machine said I got the
11 source back in its shield.

12 The alarming dosimeter went off, or it had gone
13 off, and stayed on. It was judged to be a false alarm, and
14 they didn't use the hand-held, and the lady died a very
15 horrible death.

16 In that practice, there is a serious question,
17 what is due reliance or undue reliance on any barrier? What
18 is the defense-in-depth appropriate to that?

19 MR. BERNERO: Now, in waste, it definitely applies
20 to release barriers. As I said earlier, interjecting, the
21 Nuclear Waste Policy Act requires multiple barriers. So
22 somewhere in a licensing finding, somewhere in the licensing
23 exposition by DOE, they have to show the statutory
24 requirement is satisfied because we have multiple barriers
25 and this is our demonstration of the adequacy of those

1 multiple barriers, as well as our performance assessment.

2 I underline the word "one" because the fundamental
3 basis of acceptability is not simply the total system
4 performance assessment. That's only one basis. You don't
5 license to the safety goal.

6 There are other considerations that must be taken
7 into account. Some of these uncertainties are readily
8 quantified, many are not readily quantified. So you have to
9 look at the whole body of information in order to do it.

10 There is often confusion because defense-in-depth
11 or multiple barrier analysis is just another form of
12 uncertainty analysis and in this particular case, the staff,
13 in Part 63 and in their intentions for their review plan,
14 have talked about guidance on how one might do -- what's a
15 sensitivity analysis, really, in supplement to the
16 appropriate uncertainty analysis in the total system
17 performance assessment, and I think that's good.

18 The one thing, and I talked to the ACNW in
19 November, the one thing that I think still needs attention
20 is graded goals for graded uncertainties. See, in high
21 level waste, you deliberately put it out. It's out there
22 and now you're talking about what uncertainties do I have
23 about the barriers that inhibit the release and exposure of
24 the public.

25 And one of the difficulties that exists is

1 everyone that talks about it seems to say the performance
2 standard for exposure of someone so far in the future,
3 10,000 years, 30,000 years in the future, is such that it
4 would not be greater than we would accept today, and they
5 come out and they use licensing acceptance criteria, which
6 are clearly acceptable. They're very low, they're very
7 conservative.

8 There is no gradation of objectives to say, okay,
9 well, how far from the edge of the cliff am I, and I suggest
10 that one can put grades on radiation exposures from waste
11 releases; that you can have the clearly acceptable level of
12 exposure, an acceptable level of exposure, clearly tolerable
13 levels of exposure, tolerable level on counting orders of
14 magnitude, life- threatening, and then clearly unacceptable.

15
16 And I have included a chart that I used before in
17 November and I just penned in. This is counting -- this is
18 chronic doses and then when you get to the top of the scale,
19 you're really talking about accident doses. For instance,
20 when you get up to 10 rem, the accident dose that's
21 acceptable and has been for years, in things like reactor
22 accidents, 25 rem whole body exposure, is really a
23 clinically detectable threshold.

24 What you're really saying is if you limit the
25 accident dose to 25 rem, that is a sufficiently harmless

1 level because there are no clinically detectable effects in
2 the human body from that kind of an exposure. You have to
3 go up a factor of three or something like that. I usually
4 use 10 rem as that.

5 But when you get up in this high level we were
6 discussing earlier, you get up in cancer therapy, and you
7 get doses like that. My wife has just had very substantial
8 doses.

9 So the whole point I'm trying to make, the focus
10 is down here. When you do the uncertainty analysis, it is
11 nice if you meet your clearly acceptable goal with your base
12 case, but if you are depending on some shaky uncertainty
13 analyses, you should be looking for the edge of the cliff;
14 not only in uncertainty variation, but in objective or goal
15 variation, because you've got these orders of magnitude of
16 tolerance behind it.

17 So that completes what I would like to say.

18 MR. KRESS: Thank you very much. Any questions,
19 before we move on the agenda? Very good. We are now at a
20 point in the agenda that calls for a general discussion of
21 the people at the table and anyone in the audience who wants
22 to join in, and we need to define the issues for further
23 consideration.

24 I don't know exactly how to approach this, except
25 ask for any volunteers that want to make additional points

1 or question the speakers.

2 MR. APOSTOLAKIS: If I could make a suggestion.
3 Why don't we start out by defining perhaps three or four or
4 five points that need some discussion, because otherwise we
5 will be going in ten different directions.

6 MR. KRESS: That's a good suggestion, George. Do
7 you want to make a stab and give us a couple of points?

8 MR. APOSTOLAKIS: Well, this issue of uncertainty
9 that I raised, I think, deserves some discussion and whether
10 we want to place defense-in-depth in that context. That's
11 certainly something that I'm interested in.

12 MR. KRESS: That's a good one. What I'm
13 interested in, of course, is the issue of should there be a
14 specified allocation.

15 MR. APOSTOLAKIS: That's a good point.

16 MR. KRESS: That would be one.

17 MR. APOSTOLAKIS: And I must say I am still not
18 comfortable with my understanding of the issue of how to use
19 defense-in-depth in the high level waste repository. So
20 maybe a summary of the issue and then a discussion, a
21 summary perhaps by John, would help me understand.

22 MR. GARRICK: One of the points I'd like to see on
23 here, too, we keep hearing this observation that licensing
24 decisions should not be based on PRA/TSPAs alone. I'd like
25 to see us discuss that more.

1 MR. APOSTOLAKIS: Okay. That's a good point.

2 MR. KRESS: Yes, that is, particularly when we're
3 talking about entering into a mis-conformed regulatory
4 system. That's four pretty good items. Are there others
5 people would like to add to the list? I think those are a
6 pretty good set of things.

7 I would like to add one more, and that is we have
8 heard some contrary and different opinions on this. Should
9 we have -- well, we've been calling them safety goals, but
10 I've been calling them risk acceptance criteria that we
11 regulate to.

12 Should we have risk acceptance criteria that we
13 regulate to?

14 MR. GARRICK: And I don't think, by the list here,
15 that we would want to bound up anybody from jumping the
16 fence here.

17 MR. KRESS: Absolutely.

18 MR. GARRICK: If they have a burning issue that
19 they think is critical to the subject.

20 MR. KRESS: Okay. That's, I think, five pretty
21 good issues. How should we approach the discussion of
22 these? George, do you have an idea on that? Would you like
23 to, say, take one and I take another one and John take
24 another one and --

25 MR. APOSTOLAKIS: Sure.

1 MR. KRESS: -- just throw out some thoughts and
2 see what kind of response we get?

3 MR. APOSTOLAKIS: We could do that, yes.

4 MR. KRESS: Why don't you start with the issue of
5 uncertainty?

6 MR. APOSTOLAKIS: Okay. Well, I tried to make a
7 case earlier today that the reason why we are revisiting the
8 issue of defense-in-depth is that we can now quantify a good
9 part of the uncertainties associated with the performance of
10 the systems that we're talking about that we could not
11 quantify 15, 20, 30 years ago.

12 That includes identification, quantification,
13 characterization, all the words.

14 I also made the point that the language is
15 extremely important here. I was glad to hear Tom Murley say
16 that, in his mind, defense-in-depth has always been a
17 philosophy and not a principle, although the word principle
18 is being kicked around. But I think Bob Budnitz's point is
19 well taken, that it ultimately comes down to what you do.

20 I mean, what you call it is nice to have good
21 terminology, but what you actually do at the lower level, at
22 the working level, is what counts, and that's what I want to
23 address.

24 I really think that for the uncertainties we have
25 quantified, defense-in-depth, the words don't belong there.

1 You're going to use the tools of defense-in-depth, barriers,
2 diversity and so on to manage your uncertainty and you have
3 an excellent means, a numerical standard against which you
4 can decide how much is enough, which is really a fundamental
5 question today, how much defense-in-depth is enough.

6 MR. KRESS: But, George, we don't have numerical
7 standards on how much is enough, unless you allocate --

8 MR. APOSTOLAKIS: Yes.

9 MR. KRESS: Now, if you would throw in this word
10 allocate, I would agree with you. But then, by my
11 definition, that becomes defense-in-depth in a regulatory
12 sense, if you allocate.

13 MR. APOSTOLAKIS: But I would avoid the words
14 defense-in- depth, because they carry a certain baggage.
15 Now, I understand where you're coming from and in an ideal
16 world, but I want to reserve the words defense-in-depth to
17 mean what they have meant all along; handling unquantified
18 uncertainty by using barriers, emergency plans.

19 MR. KRESS: Let me give you my problem with that.
20 I mentioned I my talk that I don't think we can live with
21 unquantified uncertainties in a defense-in-depth regulatory
22 system. The reason I said that is I don't know what to do,
23 I don't know how to put limits on defense-in-depth, I don't
24 know how many barriers I need, I don't know how good they
25 have to be, I don't know where to put them.

1 And then when I do this, I don't know how well I
2 have compensated for the unknown uncertainties, and I'm
3 saying you really do have to have some knowledge of what
4 that level of uncertainty is and how putting barriers in
5 different positions will compensate for it; how much of that
6 uncertainty will you get rid of or will you lower your
7 achieved risk to a level that that uncertainty is
8 acceptable.

9 So I'm saying you really do need a quantification
10 metric in this, even for what we're calling unquantified
11 uncertainty.

12 MR. APOSTOLAKIS: Okay. My response to that is,
13 first of all, the problems that you delete and the problems
14 that you just gave us, I would say that's the price you pay
15 for not quantifying uncertainties.

16 The second is, again, one of my bullets said that
17 if we do that, we will focus attention on unquantified
18 uncertainty, and then my hope is that by doing that, we will
19 eventually do what you're saying, because somebody might
20 say, well, gee, is it really unquantified. Maybe we can
21 have an estimate of the probability that all this is wrong,
22 but right now we don't do that.

23 Therefore, right now, you pay the price. You put
24 the barriers and you pay the price. I'm sorry, what?

25 MR. BERNERO: I'd like to interject on this. In

1 the earlier discussion, we talked about if you quantify the
2 uncertainties, you could make a case to eliminate the
3 containment, say, on a class of reactor.

4 MR. APOSTOLAKIS: Right.

5 MR. BERNERO: Setting that aside, if, on the other
6 hand, and to Tom's point that I've got to know what to
7 require, like some prescription, consider, for the moment,
8 if one would resurrect the question of urban siting of
9 reactors, because of the growth in the United States and the
10 availability of industrial property, getting close to load
11 centers, now, that is almost impossible to quantify the
12 uncertainty associated with that siting ramp.

13 And it's an interesting thought experiment to say
14 what quantification of uncertainties or what formulation
15 would be appropriate to reconsider that. I don't think you
16 can do it by having a regulatory agency invent a new siting
17 policy, saying here exactly are the population distribution
18 criteria and everything that we would have to set rational
19 bounds on it.

20 If you go back to the 1980s, the late '70s and
21 early '80s, the agency was very heavily involved in a siting
22 study or a series of siting studies to attempt that.

23 MR. KRESS: I'm going to make a provocative,
24 radical statement, so everybody knows that that's what this
25 is when I say it.

1 I basically think the Europeans have the right
2 idea that it's irrational to rely any at all on emergency
3 response to meet risk acceptance criteria. Now, that's a
4 radical, provocative statement, but I think it is
5 irrational. I think it's part of the whole problem of why
6 there is lack of public acceptance in nuclear power.

7 And if you could design into the system to meet
8 risk acceptance criteria at an acceptable uncertainty level,
9 without requiring emergency response, then I think then
10 emergency response becomes a true defense-in-depth, because
11 you're not relying on it to meet your risk acceptance
12 criteria. You're just saying suppose we're wrong, let's
13 have it anyway.

14 MR. BERNERO: But you aren't now.

15 MR. KRESS: I know. You don't meet risk
16 acceptance criteria without emergency response in this
17 country.

18 MR. BERNERO: I don't agree with you. Reactor
19 siting studies that were done in the late '70s and early
20 '80s, it is there as defense-in-depth, but you didn't have
21 to meet it on emergency response.

22 MR. KRESS: I do not think you will meet the
23 safety goals without effective emergency response. This is
24 a point we'll agree to disagree on.

25 MR. BUDNITZ: I have a puzzle for you, staff and

1 ACRS, that I can put in a pretty stark context. I want you
2 to imagine you're running a reactor in one of the former
3 Soviet countries. Soviet's gone, but there were, of course,
4 several countries, Lithuania, Armenia, Russia, Ukraine, that
5 are running reactors, and a lot of those don't have a
6 containment at all. The old 442- 30s certainly are BMKs.

7 The United States Government, as a matter of
8 policy, implemented through the Department of Energy and the
9 State Department, has, as a policy, that we are trying to
10 get those governments to shut down all of those reactors as
11 a matter of our policy. We have stated that to them at the
12 highest levels and it's part of our detailed policy, too, I
13 know, because I work in this arena a lot.

14 So that, for example, Richardson is going to go to
15 Lithuania in February. He is likely to tell them that we
16 continue to oppose running Ignolena and RBMK because it's
17 not safe enough.

18 Now, suppose a government there says we've done a
19 PRA. Suppose a water reactor, not an RBMK, where the PRAs
20 are more reliable, and the core damage frequency is several
21 times ten-to- the-minus-four, but considering our desperate
22 economic situation, we need that reactor and that's safe
23 enough for us.

24 The U.S. Government policy position today is no
25 containment, shut them down. By the way, it's not the only

1 reason, but no matter what else you do, no containment,
2 let's say for the 442- 30s, whatever, now.

3 What do you think of that? Knowing as much as we,
4 everybody around this table that knows reactors knows about
5 them, about what those probabilities mean, knows what -- and
6 you understand the government says we're going to take a
7 bigger risk than you would be willing to take in the United
8 States because we need the power, that's their prerogative,
9 as a matter of sovereignty, and they say we know it's not
10 contained, we know that the consequences were we to have one
11 of these would be greater than they would be in the United
12 States for a water reactor of the same size.

13 They have said that one crucial element that we
14 invoke of our defense-in-depth philosophy, as implemented
15 through the containment, is absent and is still acceptable.

16
17 Now, I'm not arguing about their right to make
18 that, that they're sovereign, but what about that here, what
19 would you say?

20 MR. APOSTOLAKIS: It's a different objective.

21 MR. BUDNITZ: I understand that, but what do you
22 think --

23 MR. APOSTOLAKIS: So it's not an issue of
24 defense-in-depth.

25 MR. BUDNITZ: But what do you think about whether

1 -- suppose they were three-times-ten-to-the-minus-seven and
2 440 megawatts, would that be acceptable in the United States
3 without a containment? No, not today in the regulations.
4 But what do you think about that as a matter of whether it
5 should be?

6 MR. APOSTOLAKIS: There's nothing we can do about
7 it.

8 MR. BUDNITZ: No, no. But in other words, we're
9 at three- times-ten-to-the-minus-seven core damage frequency
10 in the United States, 440 megawatts, would that be
11 acceptable here to you?

12 MR. KRESS: The question would it be acceptable or
13 not is a tough question to ask, because it's a judgment to
14 be made on --

15 MR. APOSTOLAKIS: It's a policy issue.

16 MR. KRESS: The question is whether it's a
17 rational position to take, a different question, and I think
18 it's entirely rational to say that that's a reasonable
19 position to take. As long as you state your goals on what
20 risk acceptance criteria you're willing to live with in
21 terms of the uncertainty and its determination.

22 If you meet that ten-to-the-minus-whatever at a
23 level of uncertainty that's acceptable, then it's a
24 perfectly rational position, and that would be the
25 rationalist view of defense-in- depth.

1 MR. BUDNITZ: I heard you expound that, and George
2 saying. On the other hand, I heard my close friend Tom
3 Murley say, and I think I'm with you here --

4 MR. APOSTOLAKIS: Unlike me, you mean?

5 MR. BUDNITZ: No, no. You're another close
6 friend. But Tom said, and he's sitting here, so maybe he --
7 he's two meters to my left, so he'll say what it he wants
8 for himself; that no, no, in the United States, we wouldn't
9 like a reactor without a containment, just totally
10 uncontained.

11 MR. KRESS: That's another question. I think it's
12 probably true, we wouldn't like it.

13 MR. BUDNITZ: I'm not saying whether we wouldn't,
14 not whether we wouldn't, but whether we should.

15 MR. GARRICK: I think it's a bit irrelevant. I
16 think it is a policy question. First off, at these reactors
17 you're talking about, if I had to make that judgment, I
18 would -- getting back to George's topic -- I would really
19 want to turn up the microscope on the uncertainty of the
20 core damage frequency.

21 MR. BUDNITZ: Of course. I wasn't arguing that
22 case.

23 MR. GARRICK: And I think I would find the kind of
24 information that would suggest to me that the U.S. policy is
25 sound.

1 MR. BUDNITZ: I'm not arguing that for a minute.
2 I subscribe to that policy.

3 MR. MURLEY: John, could I make a point, too?

4 MR. BUDNITZ: Of course.

5 MR. MURLEY: Coming from the outside now, there's
6 almost an air of unreality to this discussion, because
7 you've got to take into account the human safety culture
8 issues, which do cut across a lot of these sequences and
9 stuff.

10 MR. BUDNITZ: Of course.

11 MR. MURLEY: So Bob's premise, I think, is
12 unrealistic. I agree if you could absolutely prove that you
13 had five times or four-times-ten-to-the-minus-seventh or
14 something, but I don't think anybody believes you can ever
15 do that with humans.

16 So you just have to keep that in your discussion
17 somehow. I think I understand what you're saying and the
18 premises and so forth, but the public, listening to this,
19 think that what were these guys -- what do they own, what do
20 they have.

21 MR. GARRICK: I would like to comment to the
22 allocation issue, because I think it's --

23 MR. APOSTOLAKIS: That's another issue.

24 MR. GARRICK: Well, we've drifted into it from
25 talking about uncertainty. I've got plenty to say about

1 that, too.

2 I need to understand a lot better, Tom, what your
3 bounds and references are with respect to the issue of
4 allocation. But on the surface, it bothers me a great deal.

5
6 The reason it bothers me is that the risk
7 assessment is, in my view of a risk assessment, a set of
8 scenarios and the performance of a particular system that
9 you may want to allocate some risk criteria to is strongly
10 dependent upon where that piece of equipment sets in what
11 scenario.

12 I'm sort of reminded about the situation following
13 the Three Mile Island accident, when there was all this fuss
14 about maybe we should add a third auxiliary feed water pump
15 to all of the reactors.

16 So there was an analysis that was performed as to
17 what benefits you would get from adding that third auxiliary
18 feed water pump. The answer to the analysis was that, well,
19 if you added, in the context of what the NRC views as a
20 safety grade auxiliary feed water, the benefit is very
21 marginal. But if you remove the NRC criteria and are
22 allowed to not have that auxiliary feed water system have to
23 depend on a coolant system, a chilled water system, get it
24 out of a hard room, so to speak, and put it in something
25 like the turbine building, where you don't have to rely on

1 certain support systems, you get a heck of a lot of benefit.

2
3 And I can point to hundreds of those kinds of
4 examples in a nuclear plant, and so I have a great deal of
5 difficulty knowing how you could possibly allocate risk
6 criteria in a situation where you have reactors and plants
7 as different as they are, where you have accidents extremely
8 dependent upon -- or the performance of systems extremely
9 dependent upon where they fit in the accident sequence.

10 And that may not be what you're talking about, but
11 it's something that bothers me. And I think that one of the
12 things that's fundamental and crosses a lot of these issues
13 is that we're still learning and the safety goal issue only
14 began to formulate some meaning after we started to get some
15 results of risk assessments.

16 I remember the Commissioners arguing about -- and
17 it was a ridiculous argument -- about whether it should be
18 one-times-ten- to-the-minus-four or
19 five-times-ten-to-the-minus-four, on a parameter where the
20 uncertainty is a factor of ten.

21 That's why the uncertainty is so absolutely
22 critically important here. As one of my colleagues would
23 say, the uncertainty is the risk. That's where the ballgame
24 should be played.

25

1 I've never been one to think in terms of
2 uncertainty being complimentary to risk, but rather
3 uncertainty being an inherent element of risk assessment,
4 just as I would argue, and that brings me down to the
5 TSPA/PRA issue and how much we should depend on it, that if
6 we can think of something in addition to the TSPA or the PRA
7 that's a basis for decision-making on the safety of the
8 plant, we damn well ought to be bringing that into our risk
9 assessment and our TSPA.

10 Expert opinion, for example, is not something that
11 should be outside the scope of a risk assessment. So we
12 should be striving in that regard to make the TSPA and the
13 PRAs as encompassing as possible.

14 Now, when the NRC got into the PRA act and was
15 trying to respond to the criticisms of the industry that
16 they were too expensive and went to a highly simplified and
17 limited scope, and as the image started to develop, in
18 people's minds, that a PRA was something much less than what
19 it might be, then I can understand why you would have to
20 conclude that you've got to consider things beyond what's in
21 a PRA, if by what's in a PRA is what the NRC meant by the
22 old IPE, where there was essentially no uncertainty, no
23 external events, and not much scope.

24 So I think these are things that really make it
25 very difficult for me to imagine how we can get unduly

1 specific with respect to something like allocation.

2 MR. KRESS: Let me respond a little bit to that.
3 You can envision all sorts of levels of allocation. You
4 could allocate system reliability or even component
5 reliability. That's not what I had in mind. I think
6 basically with defense-in-depth, we're dealing with
7 prevention versus mitigation. That's basically what we're
8 doing.

9 The four elements of that I talked about. What I
10 had in mind here was let's take the case of nuclear
11 reactors, power reactors. We're talking about core damage
12 frequency versus conditional containment failure
13 probability.

14 How are we going to allocate between those two to
15 meet, say, LERF, which is our overall thing. What I'm
16 saying is that in decision theory, you ask the question if a
17 core damage manifests itself, what are the consequences of
18 that in terms of my loss function; how valuable is it to me
19 to prevent that from happening, as a regulatory agency.

20 You've got to make a decision theory process and
21 you arrive at a loss function that says that's so valuable
22 to me that I want to place goals on core damage frequency or
23 risk acceptance criteria, and there are probably going to be
24 a lot more going into the prevention than there is to the
25 mitigation.

1 Then you also ask yourself, well, suppose you do
2 the same thing with the conditional core damage frequency.
3 You take another loss function. What is -- and it basically
4 becomes what's remaining of LERF, because you've already
5 established the loss function with your CDF.

6 That's a level at which I would advocate the
7 allocation.

8 MR. GARRICK: Well, that's what I said, I
9 qualified my comments with not knowing what you really meant
10 by criteria.

11 MR. APOSTOLAKIS: But in this context, then, when
12 you talk about, first of all, prevention and mitigation, in
13 this case, are terms with respect to core damage.

14 MR. KRESS: Yes, absolutely.

15 MR. APOSTOLAKIS: Because you are preventing the
16 release of radioactivity to the environment. In this sense,
17 then, there is no prevention in performance assessments.
18 It's all mitigation, isn't it? It would be released from --
19 no? What are you preventing?

20 MR. BUDNITZ: If you can keep it inside the
21 canisters, long as it's inside the canisters --

22 MR. APOSTOLAKIS: For 10,000 years?

23 MR. BUDNITZ: If you can keep it inside the
24 canister for 10,000 years, that's prevention. I would -- in
25 other words, it hasn't gone anywhere. That is, in fact, the

1 case for canisters that we talked about.

2 MR. GARRICK: If you can keep the water away, you
3 can show that.

4 MR. BUDNITZ: So, George, I see that break between
5 prevention and mitigation as very hazy for Yucca Mountain,
6 but I certainly know what prevention means. Prevention is
7 keeping it from going anywhere. It's just in the can.

8 MR. BERNERO: I beg to differ on prevention. The
9 inherent act of waste disposal is to place the material in
10 the biosphere or geosphere and from then on, the performance
11 assessment is modeling what happens.

12 MR. BUDNITZ: Right.

13 MR. BERNERO: Does it stay in place or does it
14 ever so slowly corrode, decay or whatever, and there are
15 features in waste disposal systems that can enhance, say,
16 containment performance.

17 If Yucca Mountain adopted, as I wish they would,
18 the addition of depleted uranium filler in the container, I
19 think that would greatly enhance --

20 MR. KRESS: That would be a wonderful addition, I
21 agree with you.

22 MR. BERNERO: Yes. But, see, this is the thing.
23 You're not preventing something, you're inhibiting it.

24 MR. BUDNITZ: That's fair.

25 MR. BERNERO: And I think there's a danger -- it's

1 really a barrier, an inhibition to the movement of the
2 waste, because that is the measure of performance.

3 MR. BUDNITZ: Yes, but when we talk about
4 prevention in a reactor, we mean keeping it inside where it
5 started. In that sense, it's not a perfect analogy, but
6 it's not such a bad one to say that prevention is -- the
7 earliest state -- keep it inside the can.

8 MR. KRESS: I also added -- in my definition of
9 prevention, I added the word intervention and you have lots
10 of time and lots of intervention strategies one could
11 choose. So I would say there is --

12 MR. BUDNITZ: Except as a matter of public policy,
13 the NRC has said that they're not going to count on any
14 human intervention 6,000 years hence.

15 MR. KRESS: I know, but that's a policy statement.

16
17 MR. BUDNITZ: I understand that.

18 MR. GARRICK: I think I can make one observation
19 that covers a lot of my concern here about issues of
20 allocation and definitions and what have you, and it has to
21 do with I don't think we should do anything that bounds our
22 thinking about the safety of what we're dealing with, be it
23 a repository or a reactor plant.

24 We all know that we've had experience with this.
25 When we adopted the design basis philosophy of safety of

1 nuclear power plants, we, in a sense, bounded our thinking.
2 The game became if you come forward with a design basis
3 accident and you convince everybody that it's acceptable,
4 then you're okay. It's the same thing. The other language
5 we've heard about is beyond Class 9 accidents.

6 There shouldn't be those kind of artificial
7 thresholds and boundaries, even though it made it more
8 convenient, from a regulatory standpoint. And allocations
9 have a tendency to do that and subsystem requirements have a
10 tendency to do that. They have a tendency to narrow the
11 view of what we should be analyzing, what we should be
12 designing against, and what we should be analyzing, what we
13 should be designing against, and what we should be
14 controlling.

15 Even core damage frequency is a limitation,
16 because I can think of scenarios in lots of plants that
17 would decrease the core damage frequency and increase the
18 public risk, and I think we have to be very open and clear
19 about that, and I think that's the virtue of PRA.

20 MR. APOSTOLAKIS: I disagree, though. I think
21 there is an element that's missing here.

22 MR. GARRICK: You disagree?

23 MR. APOSTOLAKIS: No. It's not -- when we say
24 allocation, we should not take it only in the mathematical
25 sense that you want to have a certain -- meet certain goals

1 and that you allocate the performance of various systems.
2 There is a more fundamental reason why the staff wants to do
3 some of that.

4 Even though there may be situations where you are
5 -- you know, a certain measure, as you just said, may
6 decrease or increase the core damage frequency, but the role
7 is beneficial, the staff wouldn't go for it, because core
8 damage by itself is an undesirable event.

9 See, the assumption in what you said was that all
10 I care about is the QHO and the staff will tell you no,
11 that's not all I care about. In fact, the new oversight
12 process makes it very clear in black and white. The staff
13 says we care about initiating events, we don't want to see
14 any of those. Why? Well, they aren't going to put it on
15 paper. They will tell you, though, that they don't want to
16 be on the front page of the newspapers. We don't want to
17 see the primary system being breached?

18 Why? It creates public outcry. We don't want
19 that. So there are more objectives that perhaps have not
20 been spelled out in the books until recently for which --
21 which you are trying to meet, and if you look at it that
22 way, then you are saying, well, maybe core damage frequency
23 is something I worry about, because it's not just a QHO.

24 The fundamental question is, though, whether you
25 have similar situations in the performance assessments and I

1 think one of the reasons why you don't is time.

2 In reactors, we can have a problem tomorrow with
3 an initiating event. In your case, you're talking about
4 thousands of years.

5 MR. GARRICK: Yes, the conditions are entirely
6 different. The real issue of risk probably in the waste
7 field is the operational risk and the handling and the way
8 in which you do things.

9 MR. APOSTOLAKIS: But my point, John, is that
10 maybe the word allocation for reactors is not the right
11 word, because they are not allocating anything. They are
12 saying I don't want this to happen, I don't want the core
13 damage event, I don't want an initiating event.

14 MR. KRESS: When I say allocation, I mean I don't
15 want that to happen at this frequency, with this
16 uncertainty, with this confidence level.

17 MR. APOSTOLAKIS: I understand that.

18 MR. KRESS: That's what I mean by allocation.

19 MR. APOSTOLAKIS: But there is a reason why they
20 don't want it to happen, because that by itself is bad; not
21 only as a contributor to core damage, but if I have a LOCA
22 tomorrow, the agency doesn't look good.

23 MR. GARRICK: But, George, you're not saying that
24 the NRC disallows the core damage. They can't do that.
25 They can't do that. Are you saying that -- what you seem to

1 be suggesting is that the NRC really doesn't think in terms
2 of a ten-to-the-minus- four core damage frequency, but a
3 ten-to-the-minus-infinity.

4 MR. APOSTOLAKIS: When did I say that?

5 MR. GARRICK: Well, you made the point that they
6 wouldn't accept it. Well, what are they not accepting?
7 They can't stop it. They can't stop the fact that the core
8 damage frequency has a likelihood of occurrence.

9 MR. APOSTOLAKIS: What I'm saying is when we say
10 allocation, we have to be very clear what we mean. That
11 comes back to what my objectives are when I regulate. I got
12 the sense from your earlier comments that what you thought
13 was the objective of the regulation for Yucca Mountain or
14 for reactors was the ultimate quantitative health objectives
15 or, in Yucca Mountain, the dose. The ultimate criteria, in
16 other words.

17 And then allocation, in that sense, means that
18 some engineer says, well, gee, you know, this is really my
19 objective, but I would like to see this performance here,
20 that performance there, in the system. What I'm saying is,
21 no, there is a fundamentally different view of regulation
22 for reactors. It's not only the public health and safety.

23 That's how we start, but that's not our only
24 objective. We don't want to see core damage events by
25 themselves, even though they don't affect public health and

1 safety, because they're contained.

2 But even more than that, in fact, the staff said
3 it very clearly, the initiating events, we don't want to see
4 too many of those. They create those sorts of headaches,
5 other things. We don't want to see -- whatever -- the four
6 cornerstones they have. So what I'm saying is that the
7 decision problem is different in this case in the sense that
8 I have different objectives and I'm not allocating anything
9 anymore.

10 All I'm telling you is I really don't want to see
11 this.

12 MR. LEVINSON: But, George, I think historically
13 we have confirmation. The importance of TMI was not
14 exposure of the public. The importance of TMI was that it
15 was core melt.

16 MR. APOSTOLAKIS: Yes. Yes. And we saw the
17 reaction and so on. So that supports, in fact, the staff's
18 position. You may have -- I mean, as Tom said earlier, you
19 can have a TMI every year and you still meet the goals. You
20 tell me who at the NRC would accept that.

21 MR. GARRICK: And my only point is be careful
22 about the blinders you put on to support the staff's
23 position, because we put blinders on us to support the
24 staff's position in the past and we probably should have
25 not. Be careful about that.

1 MR. APOSTOLAKIS: I'm not sure they're blinders.

2 MR. GARRICK: Well, you're the one that's
3 suggesting that. I think that all I'm suggesting, all I'm
4 suggesting is that the real virtue of the risk thought
5 process, and by which I mean all these things we've been
6 talking about, quantification of uncertainty, complete set
7 of scenarios, doing the best possible job we can, is that we
8 have not built ourselves artificial thresholds, like
9 safety-related systems.

10 I think that that's the thing that is an important
11 virtue of it that we should not lose by adding some
12 constraints.

13 MR. APOSTOLAKIS: And I agree that they should not
14 be artificial. But look what happened at Northeast
15 Utilities. Was that artificial, was that a real reaction?
16 Was public health and safety threatened at any time?

17 So it's clear to me that for reactors, it's not
18 just public health and safety.

19 MR. GARRICK: Well, I agree with you and I want to
20 stop because I want to hear from a lot of people. I would
21 say one of the greatest advances we've made in the improved
22 performance of the nuclear plants in this country is not the
23 business of the traditional safety analysis and what have
24 you, but it is the emphasis that the utilities have been
25 giving to human performance.

1 I am really impressed with what you will find at
2 most utilities today on evaluating human performance and how
3 to motivate them and how to challenge them and how to make
4 them accountable for what they're doing. And it's true, in
5 the sense that it's outside our database, which it isn't
6 totally, we don't consider a lot of those kind of things.

7 MR. LEVINSON: If I can make just one more
8 comment, John. I think these are not at all inconsistent.
9 The value of good analysis to reduce uncertainty, PRAs, et
10 cetera, certainly is something we should all strive for, but
11 I think the point is what we get from it is not just a
12 single number, like dose to some person in the population.

13 It can also be used to achieve other objectives,
14 like reduced core melt. So the fact that you might have
15 multiple objectives for the PRA is not inconsistent with
16 depending on PRAs and proving them.

17 MR. BUDNITZ: Let's go to Yucca Mountain for a
18 minute. When Part 60 was under development, I was on the
19 staff 20 years ago when we were thinking hard about it, and
20 at that time, nobody had confidence that what we now call
21 performance assessment could be good enough to be relied on
22 as a principal means for understanding. And because of
23 that, the staff, at the time, wrote the subsystem
24 performance requirements, the canister lifetime and some
25 canister leakage rate per year and the thousand year travel

1 time and so on into the regulation.

2 Notwithstanding everything else you did, you had
3 to show this thousand year travel time, for example. The
4 staff explicitly, in the statement of considerations of Part
5 63, just this year, said 15-18 years have passed; we now,
6 says the staff, and I agree with this entirely fully, we now
7 have the confidence in the analysis methods and the data
8 that we didn't have them, we the same staff or the different
9 folks of the same staff, and, therefore, we feel that those
10 things have been superseded by this new technology and its
11 use and our confidence in it.

12 So they have come to the stage where they used to
13 have what you'd call barrier -- the concept of these
14 multiple, whatever else you do, you've got to do barriers or
15 something, performance, they've abandoned it for the moment.

16
17 I mean, there's still this other thing, and I
18 think that's completely correct. When evolution of
19 knowledge enables you to say I now don't have uncertain
20 values to have, I now can do certain analyses and I can have
21 confidence in them at a certain level, I no longer need what
22 I used to need 18 years ago. That is completely rational.

23 MR. APOSTOLAKIS: But your objective is still to
24 meet the dose criteria. I fully agree with that approach.
25 You don't have any intermediate objectives. So what I'm

1 saying is that in reactors, it's --

2 MR. BUDNITZ: No, no. I'm not -- of course, I'm
3 not arguing with you for a minute, but then all of a sudden,
4 in the same statement of consideration, Part 63, they say
5 but besides the dose objective in Amergosa, we have this
6 defense-in-depth. My slide showed, I asked the question,
7 well, if we're going to invoke it, can they flunk on
8 defense-in-depth, even if they meet that other thing with
9 lots of margin, and apparently the answer is yes.

10 The staff has said yes, they could flunk on
11 defense-in-depth and then you have to ask, well, what does
12 that mean. I was trying to probe in my slides what that
13 might mean in terms of some sort of allocation or in some
14 sort of a figure or in some sort of a do it analysis of a
15 degraded or under-performing barrier and tell us what it
16 means and whatever it means, are we going to flunk you on
17 that one.

18 If Yucca Mountain can flunk on one of these, even
19 though they meet the overall thing with lots of margin, then
20 you have to figure out what does it mean, what sort of
21 allocation have you come up with, you see.

22 MR. APOSTOLAKIS: You just said that now we have
23 confidence that we can calculate these.

24 MR. BUDNITZ: It's not a perfect tool.

25 MR. APOSTOLAKIS: But let me ask you this. What

1 are the major unquantified uncertainties in performance
2 assessment?

3 MR. BUDNITZ: Unquantified uncertainties.

4 MR. APOSTOLAKIS: Yes.

5 MR. BUDNITZ: I suppose they'd be some of the
6 models that we still haven't tested well enough.

7 MR. APOSTOLAKIS: This is not something people
8 talk about?

9 MR. BUDNITZ: Of course, we talk about it every
10 day.

11 MR. APOSTOLAKIS: So models --

12 MR. BUDNITZ: It's at the center of what we talk
13 about.

14 MR. APOSTOLAKIS: Are these uncertainties large
15 enough to invalidate the performance assessment itself?

16 MR. BUDNITZ: Well, my personal view is that Yucca
17 Mountain is very likely to meet that dose criterion out
18 there in Amergosa with lots of margin, including these.

19 MR. APOSTOLAKIS: Including the unquantified.

20 MR. BUDNITZ: Including -- I mean, there is some
21 judgment about the models. You always have to bring some
22 judgment in the end, because not everything has been tested,
23 especially with those long timeframes and that's certainly
24 true of the metallurgy of the can.

25 But it is my view that in the end, that will be

1 the case. I'm still holding open judgment because the final
2 design isn't here and certainly analyses haven't been done
3 on that. But if that's true, if it turns out that there's
4 lots of margin against the dose, the staff says but you can
5 still flunk because you flunk something about
6 defense-in-depth, what is that?

7 I'm struggling with it, because it isn't the same
8 as what you're saying, well, a core melt is bad. You know,
9 Millstone was bad. It's not the same sort of thing.

10 MR. APOSTOLAKIS: I understand that. That's what
11 I keep saying for the last ten minutes. They are two
12 different things. If you guys knew, if the Commission
13 believed that by building Yucca Mountain, you will have a
14 major incident five years later, I'd bet you there is going
15 to be an objective there in order to have it.

16 MR. BUDNITZ: Yes, of course, or --

17 MR. APOSTOLAKIS: If it's a thousand years --

18 MR. BUDNITZ: Or even if it's a thousand years,
19 because they have a 10,000 year criteria. So I think it's a
20 challenge. I'm looking at Ray and John from the ACNW and
21 all of us that have thought about this hard. It's a big
22 challenge to figure out what you mean and what you do.

23 MR. APOSTOLAKIS: I see there are two different
24 variables.

25 MR. BERNERO: Tom, I'd like to interject here.

1 The discussion of an incident in the near term against a
2 waste disposal and also a remark that John made earlier
3 about if you've got some significant uncertainties, get them
4 into the performance assessment, which is an admirable
5 objective.

6 First of all, there has to be not an allocation,
7 in my mind, but a recognition that in waste management, and
8 I will use low level, near surface waste disposal, as an
9 example, there is a sequence of allocated allowances or
10 decisions; is this site acceptable, is this emplacement
11 design going to be an acceptable compliment with the site,
12 and, of course, taking the whole system into account, is it
13 going to satisfy the performance assessment requirements,
14 the dose limits off-site and so forth, taking account of the
15 uncertainties and climate and flow and intrusion and so
16 forth.

17 Now, if you go, as a practical matter, in Part 61,
18 there are explicit site criteria and there is an extensive
19 body of guidance on performance assessment, but there is not
20 a good way to analyze, to do the uncertainty analysis of
21 emplacement techniques.

22 Basically, what any new site that was going to be
23 built east of the Rocky Mountains, what they did is just
24 adopt the French approach, and the French approach is select
25 the site that's proper, build it with dual liner leachate

1 collection system caps and all the bells and whistles, and
2 do your level best to make sure it never leaks.

3 And you don't quantify that in the performance
4 assessment. You have uncertainties and you live with those
5 uncertainties. Take the item 129, if you go to a low level
6 waste disposal site, all these shipments that come in, and
7 you're talking 100,000 shipments, big numbers, they all have
8 item 129 is less than or equal to X.

9 It's detectability limit and if you take 100,000
10 times less than or equal to X, it's five orders of magnitude
11 higher than that. I've had the authority for the French low
12 level waste site at Loeb tell me that halfway through, we're
13 going to hit the limit on item 129, and he doesn't have a
14 performance assessment technique to get out of that. He
15 doesn't have an analytical detection technique. He's got to
16 use some judgment.

17 And ultimately I think they will get out of it.
18 They're not going to stop and say this is the limit for this
19 site, because it's not real and it's also not a real threat,
20 item 129.

21 So there are many things in waste disposal that
22 you cannot firmly quantify. You've got to evaluate and make
23 a judgment. It's very difficult. And the decisions, right
24 now the staff is heavily involved, and the Commission, too,
25 in advising or concurring in what DOE is doing to clean up

1 its waste tanks and a high level waste tank, when you
2 extract that waste, the Commission promulgated criteria on
3 how can you stand up and say the high level waste is out,
4 when you know there is residue there.

5 The residue isn't well quantified, it isn't well
6 located, and it's the difference between two very large
7 numbers and it's very difficult to do uncertainty analysis
8 on it.

9 You can't characterize it, you can't sample it.
10 And so your performance assessment for that site is going to
11 say I'm satisfied that you've extracted enough, DOE, and
12 that you have made a persuasive case about how you grouted
13 it, how much grout there was, how much residue you estimated
14 it to be, and so forth, and then you're going to do a very
15 elementary or simple performance assessment that doesn't
16 take any real credit for the grout and the can and many of
17 the barriers.

18 MR. KRESS: This is an interesting discussion,
19 Bob, because I think what you're saying is here is a
20 circumstance where we just have uncertainties that we can't
21 quantify, so what we do we do in that case, in a
22 risk-informed regulatory world.

23 MR. BUDNITZ: That will be true at Yucca Mountain.
24 There will be some uncertainties we can't quantify.

25 MR. KRESS: So it's an interesting question, what

1 do you do when you can't quantify the uncertainties. I
2 think you fall back on arbitrary defense-in-depth.
3 Arbitrary in the sense that you put the best you can here
4 and there.

5 MR. GARRICK: You fall back on a combination of
6 some sort of judgment, too.

7 MR. KRESS: I want to just introduce a conceptual
8 note here, because what you're really saying, Tom, is that
9 it's not so much you can't quantify it, but you just don't
10 like the result, because the principals ought to be there,
11 that you can always quantify it. It just may be that you
12 have ten orders of magnitude of uncertainty when you would
13 like to have two.

14 And in the presence of that level of uncertainty,
15 then you have to do something. But I think that the whole
16 discipline that we're talking about here is to be able to
17 assign values to parameters based on the evidence that you
18 have, and you always have some, but in the problems we're
19 dealing with, there are too many areas where we have much
20 less than we'd like.

21 One of the things I would like to do here before
22 the break is look to my colleague, Ray Wymer, on the
23 performance assessment angle, who has been doing a lot of
24 thinking lately about some of the key uncertainties
25 associated with one aspect of performance assessment that's

1 critical to improving the models, and I suspect, Ray, you
2 could identify some examples of areas of uncertainty on the
3 chemical side and offer opinion about the likelihood and
4 what needs to be done to resolve those.

5 Would you comment on those and kind of against the
6 background?

7 MR. WYMER: I suspect you think I've been too
8 quiet for too long.

9 MR. KRESS: Yes. I know you have a lot to say and
10 I hope that there is an opportunity for you to do so.

11 MR. WYMER: I'll say a little bit about chemical
12 uncertainties, which is fairly specific, and then I think
13 tomorrow, when we adjourn discussion, I want to make some
14 general comments that I've noted down here that are not
15 necessarily appropriate to this specific discussion we're
16 having right now.

17 But there are a lot of chemical uncertainties with
18 respect to Yucca Mountain and the repository. For example,
19 there still is uncertainty about the corrosion behavior of
20 alloy C-22 and while there is a lot being done, it still
21 remains that you can't take a couple of years worth of
22 studies and extrapolate them for 10,000 years very well,
23 although the more basic understanding you have, the better
24 off you are in your extrapolations.

25 So the primary line of defense, which somebody

1 mentioned, maybe Bob Budnitz, that the waste package, the
2 waste container is really the principal reliance, which is
3 true, for containing the waste and preventing exposure,
4 there is uncertainty remaining there, which people are
5 working trying to narrow, both in the NRC and in the
6 Department of Energy.

7 In addition, there's a good deal of uncertainty
8 about the -- once you breach containment and you get into
9 the fuel material itself, there is a lot of uncertainty with
10 respect to the formation of secondary precipitates,
11 materials that would tend to provide another line of defense
12 against release of radioactivity.

13 People don't really know what these second phases
14 are. They are extraordinarily complex because of the
15 complexity of the nature of the fuel and the nature of the
16 corrosion products that meet that fuel and the complexity of
17 the water that's coming in.

18 So there may be additional barriers to release.
19 There's a lot of uncertainty there, though, and there's been
20 no real attempt, no real concerted attempt to quantify those
21 processes that may limit release of radioactivity in a
22 significant way.

23 It's been mentioned briefly here that you can put
24 in backfill materials, like UO₂, into drift, or you can
25 actually put those inside the waste package, which, by a

1 saturation effect, can reduce the rate and extent of
2 dissolution of the fuel, and also lead to additional
3 secondary phase formation.

4 These are all uncertainties. Most of what I
5 mentioned, with the exception of corrosion, is an
6 uncertainty at the direction of greater containment of the
7 radioactivity to make the waste environment more retentive
8 than the analyses are currently showing.

9 But without belaboring the point too much, there
10 are chemical uncertainties which are, in my view, large.
11 There are a number of mitigating things that could be
12 explored, like backfill materials, that could enhance the
13 safety of the repository and could decrease somewhat the
14 uncertainty in the analysis, and all of these things, in the
15 best of all possible words, would be examined.

16 The time constraints that we have with respect to
17 the license application would seem to pretty severely limit
18 the amount of investigation you could make of some of these
19 potentially very important chemical thought processes.
20 However, if, for some reason, we get into the
21 bring-me-another-rock mode, there may be more time available
22 to solve some of these problems.

23 MR. APOSTOLAKIS: Are these uncertainties in the
24 PA's now?

25 MR. WYMER: Only in a very general way, George.

1 There is practically nothing that I could think of or that
2 anybody could think of that hasn't been mentioned in the
3 performance assessment, but mentioning them is one thing and
4 dealing with them competently and comprehensively is quite
5 another thing, and I think it's that latter that's weak.

6 MR. GARRICK: One of the things that's very
7 interesting about these problems, I'm always looking for
8 comparisons. The key to the reactor safety problem is
9 water. The key to the safety problem is the absence of
10 water. Also, it turns out that one of the attractions of
11 using core damage frequency as a measure of performance in
12 the reactor is because of the step change in uncertainties
13 that occur once the melt occurs, and you try to quantify the
14 accident progression.

15 But we're kind of in that position in the waste
16 field. We have a problem that's not too dissimilar in terms
17 of the bounding of the problem and what have you.

18 Fortunately, the time constants are much longer and that's
19 to our advantage, but the problem in the waste field is once
20 you get the material mobilized, coming up with models that
21 do a rational, reasonable job of defining the mobilization,
22 the retardation, the dilution and the transport of the
23 radioactive material.

24 It's a problem not too unlike the accident
25 progression following core melt, although the thermodynamic

1 conditions are clearly very, very different and the
2 concentrations of materials are clearly very different. But
3 there are some interesting analogies.

4 MR. LEVINSON: I'd like to make a couple of
5 comments. One, I want to emphasize something that Ray said
6 that slid by very quickly, because it was one of the points
7 I had before, and that is everybody is talking as though
8 uncertainties were all negative.

9 In fact, that's not true at all. There is a
10 substantial number of uncertainties which are positive, that
11 reduce dispersion of materials, et cetera, and we just have
12 to remember that not all uncertainties are negative in any
13 sense of the word.

14 MR. GARRICK: What you're saying is that an
15 uncertainty distribution has a negative side and a positive
16 side.

17 MR. LEVINSON: Absolutely, absolutely. But we
18 talk about it as though all uncertainties were bad. As I
19 sit here and listen, I hear more and more reasons for why
20 the waste issue and the reactor issue really are very, very
21 different sorts of things. For instance, in the waste
22 thing, after you start out, the potential risk steadily
23 deteriorates as stuff decays away.

24 At a reactor site, the potential risk increases,
25 as over the life of the reactor, you continually increase

1 the inventory of fission products on the site. Thing after
2 thing.

3 Bob showed his dose curves out at one MR or ten
4 MR, it doesn't make any difference. When you get to the top
5 of the chart, rate is probably at least as important as
6 dose. Bob has, on his chart, a thousand rad is certain
7 death, but both his wife and mine, in the last couple of
8 years, have received significantly more than that in
9 treatment of cancer.

10 The dose effect -- now, in a reactor accident, the
11 dose rate basically, from a prompt criticality, it's an
12 instantaneous thing. There is no way, in a waste disposal,
13 that anybody is going to get a high rate of dose. So I just
14 think these things are completely different.

15 On history, I want to throw in one comment, since
16 I'm probably the oldest person here. The NRC may have
17 invented the words defense-in-depth, but they didn't invent
18 the philosophy. When I joined the project in 1944, DuPont
19 -- and it wasn't the chemical part of the company, it was
20 the explosives division of DuPont that was in the Manhattan
21 Project, and they brought that concept.

22 It was the first lesson I got when I went to work
23 there. It's been around a long, long time and I don't know
24 that we're going to define it or cage it in. It's been a
25 very useful device for designers and builders, and it's been

1 there a long, long time.

2 Just one other comment. There was a comment by
3 Bob Budnitz about U.S. policy for shutting down reactors
4 without containment. Clearly, that's not a technical based
5 issue at all. But the Soviets have very, very limited --
6 now, they have more because we've given it to them, but they
7 had very, very limited ability to do analysis. I probably
8 know about as much about it as anybody in this room, since I
9 spent eight years on the board of directors of the Soviet
10 Nuclear Society.

11 They did do an analysis in regard to shutting down
12 the RBMKs at Chernobyl and in a very basic way, in one of
13 the discussions I had with them, they said maybe our risk of
14 duplication of the Chernobyl accident is
15 ten-to-the-minus-third, and I said is that acceptable to
16 you, and they said, wait, we haven't finished telling you
17 the analysis.

18 If we duplicate the Chernobyl accident, we'll kill
19 30-some people. If we shut it down tomorrow, probably ten
20 times that many will die this first winter. And in this
21 country, we have the luxury of being able to say you can
22 shut down a reactor without major consequences. In other
23 parts of the world, that's not the case at all.

24 Their analysis -- it isn't that they have
25 different values for what's an acceptable number; they have

1 other considerations.

2 MR. MURLEY: Tom, could I ask a question that
3 occurred to me about your concept of allocation? I guess I
4 have different reaction, if you want to impose it as a
5 requirement or if it's a target.

6 If it's a kind of aiming goal or target, I think
7 that's a very good concept. But if you're suggesting that
8 it become embedded in regulations or something, I have a
9 different reaction about it.

10 MR. KRESS: And I'm sorry to tell you I had the
11 second, the latter. The reason I have that is I think in a
12 risk-based regulatory -- risk-informed regulatory system,
13 you can no longer have targets for individual plants. You
14 have to have risk acceptance criteria for individual plants.

15
16 If you have to have those, then they have to be
17 part of the regulation. So I really did mean the latter,
18 which I know gives you heartburn.

19 With that, I think this is a good time for us to
20 break for lunch until 1:00, at which time we will hear some
21 interesting comments from the staff. We're recessed until
22 1:00.

23 [Whereupon, at 12:05 p.m., the meeting was
24 recessed, to reconvene at 1:00 p.m., this same day.]
25

A F T E R N O O N S E S S I O N [1:00 p.m.]

1
2
3 MR. KRESS: The meeting will come back to order,
4 please.

5 Before we get started, there's just a very minor
6 change in the agenda I'd like to point out to people. We
7 were up to item five on the agenda, which was NRC staff
8 presentations by Gary Holahan and Tom King.

9 Instead, we're going to interchange that with item
10 six, because of some problems, and we're going to have the
11 NRC staff presentations on the defense-in-depth in high
12 level waste first, and then move to the defense-in-depth in
13 reactor regulation.

14 So with that, I will turn the floor over to John
15 Greeves.

16 MR. GREEVES: My name is John Greeves. I'm
17 Director of the Division of Waste Management in the Office
18 of Nuclear Materials Safety and Safeguards. Mr. Chairman,
19 let me thank you for making a schedule change. Norm
20 Eisenberg, the principal brief, is coming down with
21 something. He's been coming down with it for days and I
22 think he's sort of running out of energy. So we thank you
23 for your discretion in leaving the schedule a little bit.

24 We also apologize to the audience for moving the
25 time around a little bit, but for the sake of Norm being

1 able to deliver his presentation, I think it was the best
2 thing to do.

3 Again, I am the Director of the Division of Waste
4 Management. I have spent a fair amount of time interacting
5 with the Advisory Committee on Nuclear Waste. So obviously
6 this is a time for us to comment and bring some of our ideas
7 to the process.

8 I appreciate the difficulty which people were
9 addressing this issue this morning. Defense-in-depth for
10 materials and waste licensing actions presents a number of
11 challenges, and you bumped into a number of those this
12 morning.

13 Unlike reactors, we have the full spectrum of
14 activities within NMSS, from exempt sources, which you
15 discussed this morning, medical activities, sealed sources,
16 fuel fabrication facilities, transportation, low level
17 waste, high level waste.

18 It's really a family of different types of
19 licensing activities. So I think a lot of that was brought
20 out this morning. I was pleased to see that. I was also
21 heartened by some of the views expressed. I can tell you
22 there's a number of views within the staff on these issues,
23 also.

24 The topics, depending on what type of a licensing
25 activity you're talking about, have different time spans,

1 have different radio activity, have different human action,
2 have different criteria, and have different rates. You
3 touched on all that this morning.

4 I would like to just punctuate that the staff
5 certainly looks at the Commission policy statement on
6 risk-informed performance-based regulation, and I think it's
7 probably in your package and it has a definition on
8 defense-in-depth, and the staff, in its efforts, is looking
9 to make sure we stay consistent with that particular policy
10 statement. It's on the web and is available to people.

11 As I said, Norm Eisenberg, Dr. Eisenberg is
12 walking this way. I'll try and not get too close to him.
13 Norm is going to do the principal presentation. He's going
14 to try and set the context for all the materials types of
15 activities and a couple of things about Norm.

16 One, this may be your last chance. He's retiring
17 this month. He's moving on. The second thing is I think
18 he's a defense-in-depth expert. This is a gentleman that
19 lives defense- in-depth. When he gets up, you will notice
20 that he has belts and suspenders. I've heard statements
21 that people thought they were the best at certain things.
22 Norm lives this issue.

23 The second presentation will be by Christiana Lui,
24 to my left, and that's more focused on Yucca Mountain
25 specifically. I will have some wrap-up statements regarding

1 that.

2 As I said, we keep in mind the Commission policy
3 statement and what we are expressing are our preliminary
4 considerations on a number of these issues.

5 With that, I'm going to stop and ask Norm to go
6 through what I think is a thoughtful presentation. I think
7 it's a bit thought-provoking, as some of you put forth
8 earlier.

9 MR. BERNERO: Do you have slides handed out?

10 MR. GREEVES: There are slides, should be. Norm,
11 you concentrate on the presentation. We'll get the slides
12 to Bob.

13 With that, Norm, take over.

14 MR. EISENBERG: Thank you. I appreciate the
15 subcommittee letting me go ahead and do this. I am feeling
16 under the weather and I feel confident that if I start to
17 become incoherent, nobody will notice. They'll just figure
18 it's me acting normally.

19 I should say that I'm going to talk about a
20 provisional NMSS perspective on defense-in-depth for
21 risk-informed performance-based regulation. These are some
22 staff ideas that have been circulating around and a lot of
23 them were sharpened by considering the case for high level
24 waste regulation.

25 So you have to understand that these are

1 provisional ideas and they are subject to change.

2 So what I intend to talk about are what are some
3 of the motivations for defense-in-depth in NMSS; what are
4 some of the current things that are causing us to focus on
5 it; what is it, which, of course, we've heard a lot of
6 discussion about that this morning; how does
7 defense-in-depth differ from margin and other safety
8 concepts, which I think is a very important issue; what are
9 some provisional conclusions; what are some things that we
10 have to determine if we're going to follow this path; and
11 then I'd like to make a summary.

12 So NMSS has been engaged in a number of activities
13 that prompt a focus on defense-in-depth and a risk-informed
14 performance-based regulatory environment.

15 One of the first things is SECY 99-100, which was
16 approved by the Commission, which is an activity to develop
17 a framework for materials regulation similar to the
18 framework for reactor regulation that was developed by the
19 Offices of Research and Nuclear Reactor Regulation for
20 risk-informing selected NMSS activities.

21 So this certainly has brought the subject up,
22 certainly the consideration of refining the approach on high
23 level waste regulation, as indicated in the proposed Part
24 63, is another area where defense-in-depth needed to be
25 considered, and we got a fair number of public comments on

1 that aspect of the proposed rule.

2 There are other activities in specific areas,
3 interim spent fuel storage facilities are being
4 risk-informed. We have ISAs, which is a type of risk
5 assessment for fuel cycle facilities, and we are
6 risk-informing the transportation regulation. So there is a
7 lot of current interest in this.

8 Let me just say that the performance-based aspect
9 of risk- informed performance-based regulation places an
10 emphasis on the overall system performance and the
11 risk-informed aspect considers the uncertainties and the
12 sources of those uncertainties.

13 All right. So what's the regulatory environment
14 in NMSS that we have to deal with? First of all, we have a
15 lot of diversity. We have a wide range of licensees and
16 systems regulated. They have varying degrees of complexity,
17 everything from gaseous diffusion plants, which are complex,
18 to smoke detectors, which are not.

19 Different systems have different degrees of human
20 interaction or are dominated by human interaction. We have
21 certainly different levels of hazard. Some things are not
22 very hazardous at all. This gives rise to general licenses.
23 Other things are, frankly, hazardous.

24 There's diverse capabilities among our licensees
25 for being able to do analyses of any kind and especially

1 risk analyses, and there's many different tradeoffs in the
2 need for risk-informed regulation, the benefits and the
3 costs in different areas that we regulate.

4 We also need to consider, if you will, the
5 taxonomy of the risks, and Bob Bernero alluded to this
6 earlier, that we have individual risk to workers and we have
7 the individual risk to members of the public. We have
8 normal risks and accident risks. We have perceived risks
9 and actual risks and we have a variety of initiators,
10 mechanical failures, external events and human error are
11 some of the things.

12 MR. APOSTOLAKIS: Why do you have perceived risk?
13

14 MR. EISENBERG: Because we have to consider the
15 communication with the public and even though the actual
16 risk in quantitative terms may be small, the public reaction
17 may be great. So there will be a response. So we have to
18 consider not just the actual risks, but, to some degree, the
19 perception of risk by the public, by policy-makers, and
20 others.

21 MR. APOSTOLAKIS: But I realize that communication
22 is important and so on, but surely you're not implying that
23 you will take actions based on perceived risk rather than
24 actual, as actual meaning technical. We are not regulating
25 based on perceived risk, are we?

1 MR. EISENBERG: The agency may have to respond to
2 some things with an effort which is not in proportion to the
3 actual risk involved.

4 MR. APOSTOLAKIS: That I agree with and I think,
5 in fact, the cornerstones that we have on the reactor side
6 are the result of perceived perceptions.

7 MR. EISENBERG: I'm just trying to lay this out as
8 the environment in which we work. Now, how we actually
9 treat it is another issue, but it is a factor and it does
10 influence what goes on.

11 MR. APOSTOLAKIS: I agree that it is a factor.

12 MR. EISENBERG: Well, I'm glad you agree with me.
13 So kind of moving to the next step, what are the factors for
14 defense-in- depth in NMSS, what's the current status?

15 Well, it's the nature of the licensees and the
16 activities regulated. We have to recognize that NMSS, by
17 and large, regulates systems with less hazard than nuclear
18 power reactors. NMSS regulations are a mix of
19 performance-based and risk-informed regulations versus
20 prescriptive and deterministic regulations.

21 This is a little bit different, from my
22 understanding of the reactor side, where things have been
23 dominantly a deterministic approach. And for some NMSS
24 licensed activities, the hazard does not warrant a very
25 strong preventative measure of any type, whatever they are,

1 performance-based or prescriptive or anything. The risks
2 are too low. Once again, general licenses are not worth
3 very much concern.

4 Okay. So what's the NMSS safety philosophy?
5 Well, our strategic plan says that we want reasonable
6 assurance of protecting public health and safety, common
7 defense and security, and the environment. Some concepts
8 that assist in achieving defense-in-depth in this context
9 are safety margin, diversity, redundancy, no single point of
10 failure, and quality assurance. There is a whole spectrum
11 of things we do to try to achieve reasonable assurance.

12 And in this context, defense-in-depth is a
13 component of a risk management strategy. This does not
14 imply that we do risk management, all the risk management
15 that a licensee might want to do. They have other reason to
16 do risk management, but we are obligated to do risk
17 management in the public health and safety context.

18 MR. KRESS: When you say risk management, what
19 exactly do you mean there, Norm?

20 MR. EISENBERG: In other words, putting forward a
21 structure of regulations makes certain things less likely
22 and other things more likely and it is a way of determining
23 what the risks are and how large they might be allowed to
24 become.

25 If you take the Kaplan-Garrick definition of risk

1 as the risk tripled, then regulations provide one constraint
2 on the risk, meaning that whole aggregate of points.

3 MR. KRESS: I think I know what you mean now.

4 MR. EISENBERG: Okay. All right. So if we're
5 going to use defense-in-depth to help achieve our top level
6 goals of public health and safety, what is it? Well, this
7 is what was taken, and I forget who threw it up this
8 morning, but this is from the Commission white paper on
9 risk-informed performance-based regulation, and this is a
10 paraphrase of the two key features for defense-in-depth,
11 which are, one, safety is not wholly dependent on any single
12 element of the system and, two, incorporation of
13 defense-in-depth into a system produces a facility that has
14 greater tolerance of failures and external challenges.

15 MR. KRESS: That's a pretty loose definition.

16 MR. APOSTOLAKIS: It's, in fact, not a definition.

17
18 MR. GREEVES: This is right out of the Commission
19 paper.

20 MR. APOSTOLAKIS: We realize that.

21 MR. KRESS: We realize that. Thank you.

22 MR. APOSTOLAKIS: I thought our comment at the
23 time was that this is still evolving.

24 MR. GREEVES: This is what the staff is looking at
25 in terms of guiding its efforts and being consistent with

1 the Commission paper.

2 MR. EISENBERG: We took this as one of our
3 starting points.

4 MR. BERNERO: This is the same thing I put up.
5 This is just a paraphrase of it.

6 MR. APOSTOLAKIS: It's what? I'm sorry.

7 MR. BERNERO: It's the paragraph I put up. The
8 paragraph that I put up on the screen, this is a paraphrase
9 of it. It's one of the attempts at defining
10 defense-in-depth. You've got a whole book full of them.

11 MR. EISENBERG: And here is the whole statement,
12 which I think -- okay. Well --

13 MR. GARRICK: I think if you put it in the context
14 we were discussing this morning as a way of doing business,
15 as a way of how we provide protection, it fits in that
16 scheme.

17 MR. EISENBERG: So then the question is how do you
18 do defense-in-depth in a risk-informed performance-based
19 context. Things change when you get into a risk-informed
20 performance-based context, rather than a prescriptive
21 deterministic context. This, I thought, was stated very
22 nicely in this paper by Sorenson, et al, in which there was
23 the structuralist and rationalist approach.

24 So this is, once again, a paraphrase and may not
25 be complete enough to satisfy everybody in the audience, but

1 basically the structuralist approach maintains that the need
2 for and extent of defense-in-depth is related to the system,
3 structure. Many manifestations are based on the novitant
4 perspectives that were current at the time that the systems
5 were developed or they were first licensed and some
6 manifestations have an ad hoc basis.

7 The rationalist approach articulates a philosophy
8 that says defense-in-depth should be related to the residual
9 uncertainties in the system and the rationalist approach is
10 just beginning to be adopted in this risk-informed,
11 performance-based environment.

12 And we have taken the structuralist -- I'm sorry
13 -- the rationalist approach as appropriate for risk-informed
14 performance-based regulation. But the question is how do
15 you implement it and what are those uncertainties that you
16 need to address.

17 MR. APOSTOLAKIS: What do you mean by residual
18 uncertainties? Unquantified?

19 MR. EISENBERG: Yes.

20 MR. APOSTOLAKIS: Okay. There is something that

21 --

22 MR. GREEVES: I'm going to talk more about this.

23 MR. APOSTOLAKIS: Is there something wrong with
24 the word unquantified or why are you avoiding it?

25 MR. GARRICK: Don't be so sensitive, George.

1 MR. APOSTOLAKIS: Residual is different, because
2 some of the residual uncertainties have been quantified.

3 MR. EISENBERG: Remember, what we're assuming here
4 is that you have a risk-informed performance-based approach.
5 So you've already folded into your compliance demonstration
6 -- this is very much the case with Part 63. You've already
7 folded into your compliance demonstration --

8 MR. APOSTOLAKIS: I understand.

9 MR. EISENBERG: -- consideration of the
10 uncertainties that you have quantified. They are in there.

11
12 MR. APOSTOLAKIS: Right.

13 MR. EISENBERG: And whatever the criterion is, and
14 for Part 63, it's that the peak of the mean dose be less
15 than 25 millirem, as long as you meet that, you're okay.

16 MR. APOSTOLAKIS: But what I'm saying is that
17 after I have implemented the risk-informed system, yes, I
18 will tolerate certain -- some uncertainty that things will
19 go the wrong way. But that doesn't mean I'm going to invoke
20 defense-in-depth to handle those, because those I have
21 quantified.

22 It's the things that I have not included in my
23 analysis. So the word residual perhaps is not so fortunate.

24
25 MR. GREEVES: He's got some slides that are going

1 to touch on your issue.

2 MR. APOSTOLAKIS: I think conceptually we agree.

3 MR. GREEVES: I think he's going to hit another
4 button here shortly.

5 MR. EISENBERG: Just briefly. So what are the
6 uncertainties that we consider in these safety assessments,
7 and there's

8 MR. BUDNITZ: Regulatory.

9 MR. EISENBERG: Well, there is that
10 differentiation, but there is also, for those of us that are
11 doing the pragmatic, there's parameter of data uncertainty,
12 there's model uncertainty, there's scenario uncertainties,
13 which, for a lot of waste work, involves the exposure
14 scenario as opposed to some physical scenario, and, also,
15 programmatic factors; the safety culture, for example.

16 So this is one cut at uncertainty.

17 MR. GARRICK: And on way you could look at that,
18 Norm, is I might even view scenario uncertainty as an
19 integral part of the modeling uncertainty, given that the
20 scenarios are usually a fundamental part of the modeling
21 process.

22 MR. EISENBERG: It's the model of the world or the
23 model of the system.

24 MR. GARRICK: And the programmatic factors, like
25 QA, those are there primarily because we don't normally

1 address them explicitly. In other words, it's not that they
2 couldn't be, it's just that we don't.

3 MR. APOSTOLAKIS: In fact, the last three, I call
4 them modeling uncertainty, but if it makes you happy, that's
5 fine.

6 MR. GARRICK: Well, we agree.

7 MR. APOSTOLAKIS: We don't want to make Norm
8 unhappy. Not yet.

9 MR. EISENBERG: Okay. So now, if we get back to
10 the residual uncertainties or the unquantified
11 uncertainties, I would suggest that there may be two types.
12 The first type is if you have the best available risk
13 assessment, if you do the best possible job you could do,
14 there are still unquantified uncertainties and it's because
15 human knowledge is finite and you just can't put everything
16 in there. You don't know everything.

17 So that's one type of uncertainty. But there's
18 another type of uncertainty and that's got to do with
19 there's practical realities and we can't always get the best
20 available risk assessment. Very often, in the real world,
21 we have to deal with a risk assessment that was done. It
22 may not be the best available one. There may be significant
23 flaws.

24 And we also have to consider, in those cases, that
25 there are unquantified or residual uncertainties.

1 MR. BUDNITZ: Norm, as a distinction here, in the
2 first one, you characterize that you did the best you could.
3 You said the reason why it's not better still is because the
4 state of knowledge is incomplete. Now, that's epistemic.

5 I want to argue to you that there are also
6 aliatory uncertainties that you can't know well.

7 MR. APOSTOLAKIS: Like what?

8 MR. BUDNITZ: Like, for example, suppose you would
9 really like to characterize the environment below the
10 repository horizon, but above the saturated zone at Yucca
11 Mountain down to the one meter scale, but, frankly, we
12 can't. So there is a variability naturally in the system
13 which is going to cause uncertainty in your performance
14 assessment, and that is certainly aliatory and not
15 epistemic.

16 So I think that that's incomplete, as written,
17 unless you acknowledge that this isn't only the state of
18 knowledge. Some of it has to do with variability in the
19 natural world, which we can't characterize always.

20 MR. EISENBERG: I don't want to get into a
21 semantic argument.

22 MR. APOSTOLAKIS: We understand what you're
23 saying, though.

24 MR. EISENBERG: And you can --

25 MR. BUDNITZ: But it's a crucial conceptual point.

1
2 MR. EISENBERG: But some people would argue that
3 all uncertainty is --

4 MR. BUDNITZ: We've been there.

5 MR. EISENBERG: -- epistemic. It's not worth
6 talking about. I mean, some people would argue what you're
7 talking about is the inability to characterize an aliatory
8 uncertainty.

9 MR. APOSTOLAKIS: But it's not worth talking about
10 it today.

11 MR. EISENBERG: Some other time.

12 MR. BUDNITZ: Except that when you define
13 defense-in-depth, you need to understand that distinction, I
14 insist.

15 MR. APOSTOLAKIS: So the second one then would be
16 something like the IPEs.

17 MR. EISENBERG: Then I thought I would go into a
18 little further detail on what these things are, what are the
19 limitations on knowledge. Well, you may not have included
20 all the failure modes because you may not know them all and
21 you haven't had enough experience to learn them all.

22 You may not have included all the phenomena for
23 the same reason. The range of variability in the system
24 parameters may be under-estimated or biased, and this
25 happens not infrequently that people make an estimate, take

1 data, and their uncertainty increases.

2 Well, it doesn't mean that the uncertainty
3 increases. It means that their original estimate of
4 uncertainty was an under- estimate. Probabilities and
5 consequences for rare events are based on sparse or
6 non-existent data. Models can't be validated. For the
7 waste business, we cannot wait 10,000 years to see if our
8 predictions are correct.

9 Although the systematic analyses methods can give
10 great insights on how a new system might perform, some
11 problems only come to light with experience. In other
12 words, the state of knowledge is evolving. I think that is
13 the bottom line, for one type of uncertainty.

14 And there is a similar litany for the other kind.
15 Why are these risk analyses as -- and this includes
16 performance analysis -- why aren't they as good as they
17 could be. Well, not all failure modes are included because
18 of limitations on time and resources, because the people
19 that try to enumerate everything didn't do it right, because
20 not all the phenomena were included because it would cost
21 too much to model everything in that detail, because in some
22 cases, only certain kinds of uncertainty are explicitly
23 represented in the risk assessment.

24 Parameter uncertainty may or may not be propagated
25 in the consequence models. Some people would use point

1 estimates. Model uncertainty may or may not be represented.
2 Probabilities of varies scenarios and the uncertainty in
3 those probabilities may or may not be included, and not all
4 the uncertainties that could be quantified have been
5 quantified.

6 MR. APOSTOLAKIS: Where are you going with this?

7 MR. EISENBERG: I'm trying to lay a groundwork
8 that if you just look at the results of risk assessment and
9 compare it to a safety goal, that there are uncertainties
10 that you haven't considered.

11 MR. APOSTOLAKIS: But there is a difference
12 between somebody saying I will not propagate the parameter
13 uncertainty and somebody saying I will not do model
14 uncertainty calculations. I will be extremely hostile to
15 the first guy and very sympathetic to the second, because
16 it's inexcusable not to propagate parameter uncertainty in
17 reactors, at least. In your case, it's expensive, but you
18 have other means to do it.

19 MR. EISENBERG: But suppose the model
20 uncertainties are the thing that dominates the result.

21 MR. APOSTOLAKIS: I understand that, but -- of
22 course. Of course, model -- but, I mean, just to say real
23 life tells us that some people don't do parameter
24 uncertainty propagation, I don't know where that leads us,
25 because that is not something that you can tolerate these

1 days.

2 MR. GARRICK: I think the other issue here that is
3 a little bit troublesome in this regard is this implies that
4 there is an alternative and if there is an alternative, why
5 doesn't it become a part of the risk assessment. That's
6 something I'm always wrestling with.

7 MR. GREEVES: Let me ask you to keep in mind that
8 as Norm goes through this, this represents our whole
9 program. It's not in Yucca Mountain and it's not reactors.
10 I think that some people can't afford to carry these things
11 so far and appropriately so.

12 So Norm's presentation was trying to give you a
13 spectrum across the problem that NMSS has.

14 MR. GARRICK: We'll let him continue.

15 MR. GREEVES: Okay.

16 MR. EISENBERG: I was trying to make the point
17 that there appears to be a case for doing something beyond
18 merely demonstrating that you meet the risk goal. So before
19 I talk some more about defense-in-depth, I'd like to try to
20 differentiate between defense-in-depth and margin, which I
21 think is an important concept, and I will see how much
22 controversy this raises.

23 If you will, margin is the cushion between the
24 required performance of a system and the anticipated or
25 predicted performance. Defense-in-depth, if you take the

1 quasi definition from the Commission white paper, is the
2 characteristic of the system not to rely on any single
3 element of the system and to be more robust to challenges.

4 Margin describes the expected performance of a
5 system versus the safety limit. Defense-in-depth describes
6 the ability of the system to compensate for unanticipated
7 performance results from limitations on knowledge.

8 For example, increasing the margin in a system
9 that relies on a single component doesn't necessarily
10 increase defense-in- depth. You're still relying on a
11 single component. Defense-in- depth provides that if any
12 component under-performs, the rest of the system has enough
13 good qualities in it that it can compensate and provide that
14 the consequences are not unacceptable.

15 In going through this briefing for different
16 audiences, some of the other things that have been suggested
17 is that defense-in- depth is like a safety net. If you're
18 walking on a high wire and you fall, the safety net does not
19 assure that you get to the other side. But it means that
20 you may not get killed. So this can be a good quality of
21 the system.

22 The same with seat belts and air bags. Neither
23 one of them keep you from getting into an automobile
24 accident, but they both may prevent -- they put a lid on the
25 consequences.

1 So if I can follow this -- you're shaking your
2 head, George.

3 MR. APOSTOLAKIS: Finish, and I will tell you why.

4
5 MR. BUDNITZ: He wants you to quantify those
6 differences.

7 MR. EISENBERG: This is an example where there's
8 two systems and we're assuming that components A, B and C,
9 on the left-hand one, are diverse and they don't have common
10 cause failures, and they both meet the same risk goal, but
11 the one on the left has the quality that if any one
12 component fails to perform as expected, you could still meet
13 the ten-to-the-minus-four risk goal.

14 On the system on the right, if that one component
15 is off, you may have had it.

16 MR. APOSTOLAKIS: But this is a very misleading
17 example, Norm. Where are the uncertainties in these
18 numbers? You can't present an example like this on the
19 basis of point estimates. I would say that the system on
20 the left, if it's an engineered system, will have smaller
21 uncertainty about the ten-to-the-minus- six.

22 So it may be preferable that way.

23 MR. KRESS: Or it may not.

24 MR. APOSTOLAKIS: Or it may not. It could be. If
25 we take the vessel --

1 MR. KRESS: And you might want to elect it because
2 it --

3 MR. APOSTOLAKIS: So giving examples like this on
4 the basis of point estimates doesn't really help.

5 MR. EISENBERG: Well, what is it that you're
6 shooting for, and when you say that the uncertainties on the
7 left may be smaller, you're talking about the quantified
8 uncertainties.

9 MR. APOSTOLAKIS: Yes.

10 MR. EISENBERG: And I thought I had made it clear
11 that I was talking about the unquantified or the residual
12 uncertainties.

13 MR. APOSTOLAKIS: But even for the original
14 uncertainties, I would expect them to be smaller on the
15 left.

16 MR. EISENBERG: Why?

17 MR. APOSTOLAKIS: Because for systems, components
18 that are at the ten-to-the-minus-two, in the
19 ten-to-the-minus-two range, I wouldn't expect the residual
20 uncertainties of the unquantified to be significant.

21 Now, you might say but if you put them together,
22 there might be something. Still, I wouldn't expect the
23 probability of a dependency that would defeat three
24 components to be so significant as to overwhelm the
25 probability that one component that I wanted to be so

1 reliable at the ten-to-the-minus-six level, you know, the
2 uncertainties are different.

3 The whole issue of defense-in-depth is an issue of
4 uncertainty in the frequencies, not to the point values. If
5 we don't accept that, then defense-in-depth doesn't make any
6 sense or it will be a principal forever.

7 MR. EISENBERG: I guess I don't understand how you
8 would fold in to this consideration the unquantified
9 uncertainties.

10 MR. APOSTOLAKIS: Because if I had to have the
11 discussion I mentioned this morning, focusing on the
12 unquantified uncertainties, I would have a bunch of experts
13 arguing why, how can a system with three components, a
14 particular way it's configured, first of all, that must be
15 an "and" gate, not an "or" gate.

16 MR. EISENBERG: Yes.

17 MR. APOSTOLAKIS: And/or, what does it matter,
18 right? It's an "and" gate. They would have to focus on
19 these -- on the failure modes of a three-component system
20 that would defeat all three of them at the same time and
21 express whatever uncertainty they have about those, and it
22 seems to me that is something that -- that's the value of
23 defense-in-depth.

24 By spreading it over three components, this
25 residual risk is smaller than on the right, where you have

1 one. Think about all - - if you read the documents from the
2 agency over the last 40 years, I think that's the running
3 philosophy and I had about ten quotations from SECY 98-225,
4 where the issue of confidence, uncertainty comes up every
5 other paragraph.

6 Anyway, that's my view and we can continue.

7 MR. EISENBERG: I think you're agreeing with me.

8 MR. APOSTOLAKIS: I won't do it on the basis of
9 point values, because my basic thesis is that
10 defense-in-depth deals with the uncertainties in these
11 probabilities, frequencies.

12 MR. EISENBERG: One way of thinking about
13 defense-in-depth in the NMSS context is there appear to be
14 two things that you want to be concerned about. One is the
15 hazard level and the other is the uncertainty in the
16 performance of the safety system. Here, again, I'm talking
17 about the residual uncertainty or the unquantified
18 uncertainty.

19 This is not necessarily related to the behavior of
20 the system as modeled. It's related to the experience with
21 the system, whether, in fact, it ever has been built and
22 operated or tested. So there's a qualitative scale. This
23 is not intended to be quantitative. There is a qualitative
24 scale in the Y axis that relates to the degree of
25 uncertainty.

1 There is a qualitative scale on the horizontal
2 axis that relates to the hazard. Small hazard, you don't
3 need much defense-in-depth because the consequences are not
4 great. High hazard, you need more defense-in-depth. So
5 this kind of outlines three bands of degrees of
6 defense-in-depth and depending upon where you fall on a
7 chart like this or, in practice, the way we have decided to
8 regulate these determines how much defense-in- depth you
9 have in each area.

10 But this might be a semi-quantitative, but
11 rational approach to deciding how much defense-in-depth is
12 needed based on these two qualities.

13 Now, there may be other qualities that are
14 important in making those decisions, also. This is a
15 suggestion of how we might approach it on, let's say, an
16 NMSS-wide basis.

17 MR. APOSTOLAKIS: I like it. I like it a lot as a
18 first step and I think pictorially it shows -- I mean, I
19 would translate that, again, to uncertainty language. What
20 you're saying is that if the hazard is high, I really have
21 an interest in the consequences. If it's small, I probably
22 don't care. If it's high, I have an interest.

23 And then on the vertical scale, you have put it
24 very well. If I have data and experience, in my language,
25 there is no residual uncertainty, there is no need for

1 defense-in-depth.

2 So this is great. And as you move up, you hit a
3 brick wall.

4 MR. KRESS: I'm wondering why you chose to
5 stair-step this particular thing instead of straight lines.

6
7 MR. EISENBERG: I think it's easier with the
8 graphics program.

9 MR. KRESS: Okay.

10 MR. APOSTOLAKIS: I must say, though, that your
11 presentation up to now probably has nothing to do with this.

12
13 MR. EISENBERG: We thought it did.

14 MR. APOSTOLAKIS: I think you could have started
15 with this. That's not a criticism.

16 MR. GREEVES: I think this kind of conveys the
17 spectrum of issues that challenge NMSS. It's multiple
18 licenses and we've got we've got to think in this context.

19 MR. APOSTOLAKIS: But, see, the problem I had with
20 your earlier viewgraphs is -- and I don't -- I suspect you
21 didn't mean that, but I don't think we should regulate
22 taking into account the fact that people don't like to do a
23 few things, like propagating parameter uncertainties.

24 On the other hand, you may have a problem on your
25 hands with the medical uses, all this, and where do you draw

1 the line? I don't know myself. When do you say, no, you
2 have to do this? Otherwise, we will do such and such a
3 thing to you.

4 And I have seen nothing in this diagram that is
5 based on that. That's what I meant, that it's independent
6 of what you presented before.

7 I take the vertical axis as meaning it's an
8 objective axis. It says it has never been analyzed. That's
9 a statement of fact. Analysis are confirmed by data.
10 That's a statement of fact. It has nothing to do with the
11 choices that the licensee makes.

12 MR. EISENBERG: This is choices for us. This is
13 choices for us and the preceding material, I think, made two
14 points. One is that it's the unquantified or the residual
15 uncertainty that should have an effect on how much
16 defense-in-depth you need and, also, that what you're really
17 concerned with is not what the risk is. It's with the
18 hazard level, because the potential there is that if you're
19 relying heavily on a single element of your system, if you
20 didn't do something right and something goes wrong, you can
21 be in trouble.

22 So it's the hazard and the residual uncertainty
23 that you really want to think about, not necessarily risk.
24 Risk we covered because we already said we were operating in
25 a risk- informed performance-based context.

1 MR. GARRICK: You want to be a little careful with
2 pushing this too far, because if you're concerned about
3 dose, let us say, and you have ten-to-the-ninth curies of
4 fission products in one mode versus another mode, the
5 problems are grossly different.

6 In the case of a reactor, where you have lots of
7 stored energy and you have lots of mechanisms to enhance the
8 distribution of this material, that's very much different
9 than having ten-to-the-ninth curies in an unstored energy
10 environment.

11 So you really have to be careful about drawing too
12 many conclusions about risk from these kind of diagrams.

13 MR. EISENBERG: I agree with you, and you also do
14 not want to use this as an open-ended invitation to require
15 more and more things. You don't want to imagine totally
16 impossible or extremely unrealistic eventualities.

17 MR. APOSTOLAKIS: I think this is a good
18 communication tool, that's all it is. It really conveys the
19 idea. I don't see how you can make this practical. You're
20 going to tell us later, right?

21 MR. EISENBERG: Yucca Mountain is somewhere on the
22 graph. I don't think it's got as much hazard as a power
23 reactor, but I don't think we have as much experience with
24 it as we do for the power reactors. We don't have it built
25 and tested yet.

1 Christiana is going to answer your question,
2 because she is going to tell you how --

3 MR. APOSTOLAKIS: You're doing a pretty good job
4 yourself of that. Don't be so defensive.

5 MR. EISENBERG: But in terms of how it's being
6 implemented, we're still working on it and maybe the first
7 thing out of the box is Yucca Mountain and we haven't gotten
8 all the way there on that yet either.

9 Remember, the comment period is closed. We're
10 working on developing the position. We haven't gotten it up
11 to the Commission yet.

12 So what are the conclusions about
13 defense-in-depth, some provisional conclusions? Well, it's
14 related to, but different from other safety concepts like
15 margin. It's not equivalent to meeting a safety goal or the
16 margin to be associated with meeting the goal. It can be
17 implemented in a risk-informed performance-based context as
18 a system requirement rather than as a set of subsystem
19 requirements.

20 So that what we would suggest is that you can look
21 at the uncertainty, the residual uncertainty related to any
22 particular barrier in your system or any particular feature
23 of your system and demand a degree of defense-in-depth that
24 is proportional to the uncertainty. More uncertainty, you
25 want more defense-in- depth. And all this is leavened by

1 the amount of hazard.

2 MR. APOSTOLAKIS: Now, that's an interesting
3 thought. You say you would look at each element and the
4 residual uncertainty and do this. How about if I take
5 another approach? I look at each element, I look at the
6 residual uncertainty in each one. But then I use a
7 convolution there to find the residual uncertainty regarding
8 the performance of the whole system and then I impose
9 defense-in-depth.

10 What's wrong with that? Instead of doing it at
11 each element.

12 MR. EISENBERG: Let me be clear. If you do it on
13 an element-by-element basis, it's all pointing at the
14 ultimate risk goal. It's all pointing to the performance
15 objective.

16 MR. GARRICK: So your answer is you agree with it.

17
18 MR. APOSTOLAKIS: You agree with me.

19 MR. EISENBERG: I think we agree again.

20 MR. APOSTOLAKIS: Or it could be a combination of
21 the two.

22 MR. KRESS: Let me sort of rephrase what I heard.
23 I've heard that more the residual uncertainty, and George
24 has qualified residual to mean unquantified, the more the
25 defense-in- depth you need and then George says you use

1 defense-in-depth where you have unquantified uncertainties,
2 so you don't know what the meaning of the word more is, and
3 I keep saying you do have to quantify it.

4 I'm a little confused. What are we talking about
5 here?

6 MR. APOSTOLAKIS: Unquantified in the sense that I
7 hadn't put down a probability distribution. But there is
8 something, in my mind, I mean --

9 MR. KRESS: You mean, it's big or medium or small?

10
11 MR. APOSTOLAKIS: Yes. I could say --

12 MR. KRESS: Isn't that quantified? See, I'm
13 saying you can quantify it to some extent.

14 MR. APOSTOLAKIS: To some extent, I agree. Yes.
15 You're right.

16 MR. GARRICK: And I agree with you, Tom. It's a
17 very abstract concept. In fact, I still struggle with what
18 we mean by unquantified or residual uncertainty and if we
19 can handle it by some other means, why can't we fold it into
20 the basic parameters.

21 MR. APOSTOLAKIS: We could. We could. We could.

22
23 MR. BUDNITZ: I don't understand why, George, it's
24 the unquantified uncertainty and only that that you're
25 emphasizing. I can conjure up a system where it's a

1 quantified, but large aliatory uncertainty and you invoke
2 defense-in-depth to find a way to do it anyway that's safe
3 enough.

4 MR. APOSTOLAKIS: I would say, in that case, I
5 would use the uncertainty diversity and so on to manage that
6 uncertainty.

7 MR. BUDNITZ: In other words, aliatory is
8 something that's random in nature.

9 MR. APOSTOLAKIS: That's fine.

10 MR. BUDNITZ: But large, but we don't know how to
11 control it. So we find another way using defense-in-depth.
12 But in that sense --

13 MR. APOSTOLAKIS: But it's not defense-in-depth
14 anymore in the sense that it's not arbitrary. If I
15 postulate a barrier, I can calculate it.

16 MR. BUDNITZ: Defense-in-depth isn't arbitrary
17 here. He said defense-in-depth involves -- we're now going
18 back to the white paper -- it involves assuring that there's
19 -- you're not relying only on one barrier.

20 MR. APOSTOLAKIS: But that's arbitrary.

21 MR. BUDNITZ: Well, wait. Whatever you say,
22 however they defined it, I insist that I think it is not
23 only the unquantified uncertainty, by any means, especially
24 in some of their systems, where they may have a very large
25 -- by the way, aliatory, maybe they have 800 licensees and

1 they're all different in the arena of some little thing and
2 in order to have one rule for them, they may have to do it
3 another way, with the defense-in-depth idea, but maybe two
4 barriers or something, rather than -- so that might be a
5 variability in nature, because all the hospitals are
6 different or something.

7 MR. APOSTOLAKIS: Let me tell you --

8 MR. BUDNITZ: It's more than unquantified
9 uncertainty, is my point.

10 MR. EISENBERG: But remember, this is predicated
11 on meeting already the risk-informed performance-based
12 goals.

13 MR. BUDNITZ: I understand that.

14 MR. EISENBERG: Your aliatory uncertainties, if
15 you have included them, have already been taken care of.
16 You've already arrived at a satisfactory performance of the
17 system.

18 MR. BUDNITZ: I understand.

19 MR. APOSTOLAKIS: I want to give an example, John
20 Garrick, what is an unquantified uncertainty. If there is a
21 fire in a nuclear plant, we have now a methodology that
22 calculates, to some extent anyway, but it calculates the
23 probabilities of failure of cables and so on due to
24 overheating.

25 We know that the fire creates smoke and we know

1 smoke is hazardous. Yet, right now, we are not quantifying
2 -- this is not part of my risk assessment. So I can say
3 now, okay, that's not part of your risk assessment,
4 defense-in-depth, help. So I want you to have barriers
5 between compartments so that smoke doesn't propagate, I want
6 you to have smoke detectors, I want the people to have masks
7 and oxygen and this and that.

8 So I'm giving you a set of measures and you say,
9 fine, I'll implement them. This is a traditional way of
10 regulating defense- in-depth. Then tomorrow somebody does a
11 calculation and he includes smoke into this, into the fire
12 risk assessment. Now I can see what the impact on the
13 frequencies of failure, for example, of core damage or
14 whatever is of having those barriers or having the oxygen
15 masks and so on, and I may very well decide that some of
16 them are not needed.

17 So that's what I mean by unquantified, that you
18 invoke then the principle of traditional engineering and you
19 say then put a few barriers there that make sense.

20 In this particular case, I happen to believe that
21 given sufficient time and will, we can include it in the
22 fire risk assessment. It's not something -- it's not like
23 safety culture, which is much more difficult.

24 So that's what I mean by -- and then we will just
25 have to do -- and from the engineering perspective, does

1 this make sense? Yes. To contain the smoke and make sure
2 that people are not hurt and so on, the firefighters and so
3 on. So you are invoking a series of measures to manage this
4 risk, which you have not quantified at this time, and it may
5 very well turn out in the future that some of these measures
6 were not the best or were not necessary, they contributed
7 very little, after you quantified it. It's very good.

8 MR. EISENBERG: I think we have two problems in
9 our arena. We have a diverse set of things we regulate. So
10 for each arena, we have to decide how much defense-in-depth
11 should we have for this particular set of licensees, how
12 much should we have for the radiographers, how much should
13 we have for medical licensees.

14 Then once we decide that, within each system, we
15 have to decide how do we put in defense-in-depth
16 appropriately to counter the residual uncertainty. So it's
17 a two-step question.

18 MR. APOSTOLAKIS: I agree.

19 MR. EISENBERG: So we think that defense-in-depth
20 can be used to address these residual uncertainties and we
21 also think that it should depend on the degree of residual
22 uncertainty and the degree of hazard.

23 But it's not easy. Regulatory life is not easy.
24 So given this, we still have to decide how to measure the
25 degree of defense-in-depth, how to measure the degree of

1 uncertainty in the performance of the safety system,
2 encompassing both quantified and unquantified uncertainty;
3 how do we measure the potential hazard posed by a system.

4 Some of these we've already discussed. How to
5 implement defense-in-depth when there is different
6 uncertainties in different parts of the system; how do you
7 use the current state of knowledge to make reasonable tests
8 for the system to have an appropriate degree of
9 defense-in-depth when what you're trying to accommodate is
10 imperfect knowledge.

11 And then the real killer, how do you explain this
12 to stakeholders so that we can preserve the flexibility
13 that's inherent in a risk-informed performance-based
14 approach to defense-in-depth, but also provide for
15 reasonable assurance of safety. This is not easy.

16 MR. KRESS: I think this is a good list of issues.

17
18 MR. EISENBERG: So in summary, we intend to
19 consider defense-in-depth in the context of risk-informed
20 performance-based regulation and a lot of ongoing
21 activities and as part of the continuing evolution of the
22 risk-informed framework in NMSS.

23 As a general safety principle, the degree of
24 defense-in-depth needed to assure safety depends on several
25 factors, including the degree of residual uncertainty and

1 the degree of hazard. We would like to implement
2 defense-in-depth as a system requirement, where feasible,
3 rather than by prescriptive subsystem requirements, and
4 please remember, NMSS needs flexibility in any overall
5 approach to implementing defense-in- depth to permit us to
6 appropriately regulate the wide range of systems and
7 licensees that we have.

8 MR. APOSTOLAKIS: I think this is very good, Norm.
9 You did a good job.

10 MR. EISENBERG: Thank you.

11 MR. APOSTOLAKIS: Even if I sounded critical. The
12 only thing that bothers me a little bit is this degree of
13 hazard. I'm sure there is another way of putting it, but
14 for this stage of development, I guess it's okay.

15 I think it has probably to do with the goals, the
16 risk goals, that the degree of hazards affects the goals,
17 the acceptance criteria, and then that affects the residual
18 uncertainty. So it's really only one of the hollow bullets
19 there that come at us.

20 MR. EISENBERG: I'm not sure I agree.

21 MR. APOSTOLAKIS: The degree of hazard, how you
22 manage it is a policy issue and the Commission says I have
23 the quantitative health objectives. Then trying to quantify
24 now your actual system to compare with your objectives, you
25 end up with a residual uncertainty which is driven by the

1 Commission's health objectives.

2 If the Commission had told me that
3 ten-to-the-minus-two is the individual risk I will tolerate
4 from nuclear reactors, I will need to worry about residual
5 uncertainty in nuclear power plants. Right? The goal is so
6 high that it's irrelevant.

7 So I think the goal itself is really the driver
8 that determines the residual uncertainty. But that's a
9 technicality.

10 MR. EISENBERG: You're tending to look at
11 uncertainties strictly in terms of uncertainty in
12 frequencies of events of failures.

13 MR. APOSTOLAKIS: Uncertainty about the occurrence
14 of something.

15 MR. EISENBERG: I think that's what I said. But
16 there are a lot of other ways that the uncertainty can come
17 in.

18 MR. GARRICK: My concern with the statement, the
19 bullet on degree of hazard, is a little different. I think
20 that I worry about the non-linearity between hazard and
21 risk. I wouldn't bank too much on the degree of hazard
22 being a particularly important factor on this.

23 MR. APOSTOLAKIS: I think there will be other
24 things driven by the degree of hazard that will have more
25 direct impact.

1 MR. KRESS: I would like to see a statement of
2 what is meant by degree of hazard. I would have interpreted
3 it to mean that if I didn't have any of the protective
4 systems around this piece of scrap, whatever it is, the
5 reactor or what, then what is the probability of producing
6 certain consequences.

7 If we just laid the fission products in the hole
8 up there, why, you can come up with it, or if you didn't
9 have any protective systems around a reactor, you would
10 conclude that the degree of hazard of the reactor is much,
11 much greater than one of a repository.

12 I think you can quantify the degree of hazard, if
13 you just ask yourself what it means. And it would
14 incorporate your comment about driving forces and mobility
15 and where it can go and that sort of thing.

16 MR. EISENBERG: One of the problems of just
17 considering the risk is that the risk is predicated upon
18 things behaving as they have been modeled, and one of the
19 things you want to get to with defense-in-depth is what if,
20 what if they do not behave that way.

21 MR. GARRICK: Of course, you can even take into
22 account that by the way in which you assign uncertainty to
23 your model parameters. There is nothing that prevents you
24 from even accounting for residual risk at the parameter
25 level or at the barrier level by how you assign your

1 uncertainty, as long as you've got a case for it, as long as
2 you've got a story behind it. And I would agree with
3 George. That was a good presentation.

4 MR. GREEVES: And I think we'll keep Norm up here.
5 Christiana, at this point, as I introduced, the challenge
6 that we have is thinking across all of the NMSS activities
7 and Christiana Lui will give you some insight of our current
8 thinking in the Yucca Mountain context.

9 So Norm will stick around, because I'm sure it's
10 going to cause some additional discussion. Christiana?

11 MS. LUI: As Norm is getting his act together.
12 Thank you. Good afternoon. My name is Christiana Lui and I
13 work in the Division of Waste Management in the High Level
14 Waste Branch, and we heard a lot -- we heard a lot of
15 interesting discussion this morning and hopefully in my
16 presentation I will be able to help answer some of the
17 questions and make some clarifications to some of the issues
18 that have been raised regarding the high level waste program
19 this morning.

20 I just want to provide the context of where we
21 are. The extended public comment period on the proposed
22 Part 63 ended on June 30, 1999. Staff is in the process of
23 analyzing the public comments and preparing responses to
24 those public comments.

25 The current schedule is to have the final Part 63

1 go to Commission by the end of March this year.

2 Again, to emphasize that this is still work in
3 progress. So the objective today is to share our best
4 current thinking with the committee, and the focus is going
5 to be on the post-closure safety evaluation, how the
6 multiple barriers requirement is being addressed in the
7 post-closure safety evaluation.

8 For pre-closure, the defense-in-depth follows the
9 approach of prevention, mitigation, and if you want to put
10 emergency planning, a separate category, but basically it's
11 the same concept as the operating facilities that you are
12 most -- you are definitely will hear from our colleagues
13 from NRR and Research in the next two presentations.

14 I'm going to go from pretty much the very top
15 level and provide more detail as the progression of the
16 presentation. So we want to clarify what is the intent of
17 multiple barriers first.

18 Just a side note that we received approximately 20
19 sets of public comments on the issue of multiple barriers
20 during the public comment period, including Dr. Budnitz's
21 comment asking us to clarify what we mean by the multiple
22 barrier requirement in Part 63, and we appreciate your
23 comment.

24 As both John and Norm have mentioned, the intent
25 of the multiple barriers is we are going to -- we are using

1 the Commission's white paper on the risk-informed and
2 performance- based regulation as the guidance for our
3 approach to clarify multiple barriers requirement.

4 We also are going to measure at this point. We
5 are targeting the multiple barrier requirement as an
6 assurance requirement, and I will say about -- I will
7 provide you more detail on this a little bit later.

8 The known certainties are all captured,
9 appropriately captured in the performance assessment to
10 demonstrate compliance to an individual protection standard.

11
12 MR. APOSTOLAKIS: Are the model uncertainties also
13 appropriately captured?

14 MS. LUI: Yes. I'm going to talk about that. I'm
15 going to give you a little bit more detail on that. So just
16 be patient, bear with me. Thank you.

17 MR. APOSTOLAKIS: You're asking for the
18 impossible, be patient.

19 MR. GARRICK: I'll help you, Christiana.

20 MS. LUI: Okay. And --

21 MR. APOSTOLAKIS: But wait a minute.

22 MS. LUI: And the repository system is
23 sufficiently robust to account for -- maybe imperfect is not
24 the best word here. Maybe incomplete is a more appropriate
25 word here, the incomplete knowledge.

1 MR. APOSTOLAKIS: This is the second time that we
2 hear this today. The first one was from Dr. Budnitz. So it
3 is the community's view that even without imperfect
4 knowledge and the uncertainties and so on, we are meeting
5 the goals of the Commission, that Yucca Mountain meets the
6 goals?

7 MR. BUDNITZ: We don't know.

8 MR. APOSTOLAKIS: So what does it mean then, that
9 it's sufficiently robust or accounts for imperfect
10 knowledge? To do what? This morning you were more
11 explicit. You said, Bob, that even if I include those
12 uncertainties, I know that this thing is --

13 MR. BUDNITZ: I expressed an opinion, but of
14 course, we don't know, because we don't have a final design
15 or analysis of it. I was of the opinion that I think it's
16 likely that when the final decision is put in place and it's
17 analyzed, I think and hope that it will meet the dose limits
18 in Amergosa with a lot of margin.

19 MR. GREEVES: In spite of imperfect knowledge.

20 MR. BUDNITZ: No, not in spite of, taking into
21 account. Not just in spite of. Taking into account. So
22 that's a prediction, because I don't know, the final design
23 may have some more difficult analysis problems than the
24 things I've seen.

25 So this is still an evolving sort of judgment and

1 I don't want to preempt even my own final judgment there,
2 but I was just sort of expressing and I was stipulating that
3 if that's true, then what.

4 MR. LEVINSON: Well, the slide identifies this as
5 the intent. It doesn't say they have achieved it.

6 MR. BUDNITZ: Yes, of course. That's there, yes.

7
8 MS. LUI: There will be a lot of discussion. Next
9 slide. Now I'm going to be a little bit more specific on
10 what are the considerations of the multiple barriers
11 requirement in Part 63.

12 I'm going to take you step-by-step here. The
13 reason why the fourth bullet is in yellow is because that's
14 one particular item not included in the proposed Part 63,
15 but is being -- but is under consideration. That as part of
16 the clarifying language for Part 63, we are intending to add
17 that part to the regulation.

18 The first thing is to assess all significant and
19 negative impacts on safety in a compliance demonstration
20 calculation. This morning -- or what I really mean by that,
21 this morning we have heard quite a bit about TSPA or that
22 particular terminology being used.

23 Basically, what we asked DOE to do is in the total
24 system performance calculation, that they carefully consider
25 all the data obtained from site characterization program,

1 consider all the applicable natural analog experimental and
2 field testing information and justify the models for the
3 total system performance assessment.

4 In that, they also have to quantify and
5 incorporate the uncertainty for all the input parameters
6 that go into a calculation. DOE also needs to take into
7 consideration the alternative conceptual models that are --
8 that basically fits all the information that we have
9 up-to-date, provide that particular description, and provide
10 a description of what conceptual models they have considered
11 and what they have chosen to include in the total system
12 performance assessment.

13 They also have to provide support that a model
14 output is trustworthy.

15 MR. APOSTOLAKIS: Again, let me play devil's
16 advocate here. Suppose you hadn't told them that. Don't
17 you think they would have done all this? This is nothing
18 special about what you are doing. I think they would have
19 identified the barriers, they would have described and
20 quantified the capabilities, they would have provided a
21 technical basis. There is nothing new here.

22 MS. LUI: But these are the requirements that are
23 under consideration in Part 63.

24 MR. APOSTOLAKIS: You mean under consideration
25 that you may decide not to demand some of this?

1 MS. LUI: No, because as what John has stated up
2 front, that we are still in the stage of preparing the final
3 rule package to the Commission.

4 MR. GREEVES: The staff is being a little careful
5 here. Recognize, we've got a proposed rule on the street.
6 The period of comment is closed. We're going through a
7 deliberative process, which is what is in the regulation. I
8 wouldn't make any more than that of it.

9 MR. APOSTOLAKIS: But there is nothing special to
10 Yucca Mountain here. I mean, you would do that for any
11 system.

12 MR. GREEVES: I don't think there is a trick
13 question.

14 MR. APOSTOLAKIS: Now, this business of wholly
15 dependent. What does that mean? I can build a --

16 MR. GARRICK: I hope it doesn't mean that you
17 would discourage them from providing you a design where a
18 single barrier could do the job.

19 MR. APOSTOLAKIS: I think that's what it means.

20 MR. GREEVES: No, it doesn't mean that.

21 MS. LUI: No, it's not that.

22 MR. APOSTOLAKIS: What does it mean?

23 MR. GARRICK: That would be terrible.

24 MR. BERNERO: John, there is a statute that says
25 you have to have multiple barriers. That colored, the

1 fourth bullet could be interpreted as a way to verify that,
2 but I would think it would be worded something like unduly
3 dependent, rather than wholly dependent.

4 MS. LUI: The reason these words are here, they
5 are taken directly out from the Commission's white paper.
6 We may -- in terms of the exact language in the rule, that's
7 still being crafted.

8 MR. BERNERO: But, Christiana, there has to be a
9 finding somewhere down the road that the statute is
10 satisfied. DOE has to make that finding in their submittal,
11 and I agree with George, all of these things are appropriate
12 to a reasonable total system performance assessment, except
13 that fourth one. That's a ringer in it, because that's the
14 implementation of multiple barriers, and, by inference, the
15 implication of defense-in-depth.

16 MS. LUI: Right.

17 MR. BERNERO: The statute requires multiple
18 barriers.

19 MS. LUI: Right.

20 MR. BERNERO: I would argue that defense-in-depth
21 is a strategy, not a statutory requirement, and it says
22 don't unduly depend on one barrier.

23 But if you could have a state of knowledge and a
24 state of certainty that could support one barrier doing the
25 job, then you would have a statutory conflict but not a

1 logical conflict.

2 MR. BUDNITZ: In fact, let me postulate something
3 that isn't true. Suppose --

4 MR. BERNERO: Are you going to tell us a lie?

5 MR. BUDNITZ: No, no.

6 [Laughter.]

7 MR. BUDNITZ: It is a "suppose" -- suppose DOE
8 came with a canister design that they had extremely high
9 confidence in they could back up and everybody agreed the
10 last 20,000 years, all of them, for the first cracks, just
11 as, by the way, if they asserted that for one year we would
12 agree, so then I am just supposing.

13 Now let's suppose they also had a site in which
14 anything that leaked the travel time was 50,000 years and
15 they had a 10,000 year requirement. You're home free --
16 either is wholly dependent, but it's not because either one
17 can actually be -- you could have them use a paper bag and
18 still be there and you didn't have to have the earth, you'd
19 still be there -- and we want to encourage that. Nobody
20 wants to discourage them from doing as best they can.

21 MS. LUI: Right.

22 MR. BUDNITZ: But --

23 MR. APOSTOLAKIS: So it is a model of language.

24 MR. BUDNITZ: No, no, but then if that is the
25 case, let me stick to it -- just pretend -- suppose that was

1 the case. Would the NRC ask them to do more? I my prepared
2 remarks this morning I asked that question.

3 In other words, if you are there --

4 MR. APOSTOLAKIS: I think the question would be,
5 Bob, whether you are there. The NRC will ask them -- I mean
6 if you demonstrate you are there, I don't think the NRC
7 would ask them to do any more.

8 MR. BUDNITZ: No, no, no, no, no. Wait -- no, no,
9 no. I want to insist. I ask another question. Let's
10 suppose that the total system performance assessment they do
11 next year, two years from now, for the design they are
12 putting together now shows the doses are met by three orders
13 of magnitude. I insist that as best I can tell the
14 Department could still flunk on defense-in-depth. It was
15 all one item.

16 MR. APOSTOLAKIS: I don't know what all one means.

17 MR. BUDNITZ: Let me describe.

18 MR. APOSTOLAKIS: I think the paper background, a
19 second one?

20 MR. BERNERO: Now let me give you an example. If
21 the repository was chosen to be in a site that's subject to
22 significantly -- subject to erosion such that the deposited
23 waste could be exposed in the long range and you did have a
24 gorgeous package, you know, boy, this package is marvelous,
25 best can in the world, but it could flunk the test because

1 the erosion would shift you to be wholly dependent on the
2 one as against unduly dependent on it.

3 You know, the erosion might be very far-fetched.

4 MR. APOSTOLAKIS: I understand that.

5 MR. BERNERO: But your dependence is upon the
6 package.

7 MR. GARRICK: Well, you have cited a weakness in
8 the defense-in-depth concept.

9 MR. BERNERO: I still argue there is a difference
10 between defense-in-depth as a strategy or safety philosophy
11 and what the statute requires the high level waste
12 repository to have, multiple barriers.

13 MR. APOSTOLAKIS: No, but the point, I agree with
14 John again that you can't do these things by counting
15 barriers.

16 MR. BERNERO: Of course.

17 MR. APOSTOLAKIS: You can't for the same reason
18 that you can't rank minimal cut sets in a fault tree by
19 counting the number of events. The probability of failure
20 must play a role. We are not going to go back 20 years now
21 and I think, you know, I can restate what you just said,
22 Bob, in terms of uncertainty and probability and then I will
23 conclude that it relies unduly on one barrier. I can do
24 that.

25 MR. BUDNITZ: I agree.

1 MR. APOSTOLAKIS: It all comes down to the
2 probabilities of failure of pathways and so on, so by
3 saying, you know, multiple barriers and count them and so
4 on, this is a first step.

5 MS. LUI: I don't think we are suggesting counting
6 the barriers.

7 MR. APOSTOLAKIS: We were not criticizing you. We
8 are talking to each other. When we talk to each other --

9 MS. LUI: Okay.

10 MR. APOSTOLAKIS: It's best to change viewgraphs.

11 MS. LUI: Should we go on to the next slide?

12 MR. APOSTOLAKIS: Yes.

13 MS. LUI: Okay. On multiple barriers, some of the
14 concepts we tried to express on these particular slides has
15 actually come out during the discussion you just had. What
16 I want to make sure is that because of the uncertainty in
17 the barriers' capabilities based on current state of
18 knowledge, there are uncertainties in the barriers'
19 capabilities over 10,000 years and as the regulator why we
20 want to know is what if all of these barriers do not perform
21 as well as what we currently know.

22 We want to make sure if that kind of situation
23 happens the public health and safety is still protected, so
24 what we are going to be aiming at is that the demonstration
25 of multiple barriers is going to show that the balance of

1 the system has the ability to compensate for that kind of
2 "what if" situation.

3 MR. APOSTOLAKIS: Now the "what if" -- are you
4 going to put any probabilities on the "what if"?

5 MS. LUI: We do not plan to do that at this point
6 because, remember, the TSPA is as good knowledge as possible
7 based on the current state of knowledge. What we are doing
8 here --

9 MR. APOSTOLAKIS: Sensitivity studies.

10 MS. LUI: Yes.

11 MR. APOSTOLAKIS: That is really what you are
12 doing.

13 MS. LUI: Or it is similar to a stylized
14 calculation like human intrusion. You really cannot
15 quantify the probability. If you can, then it should be
16 really part of your TSPA.

17 MR. APOSTOLAKIS: I would do it in a different
18 way. I would start with "what if" and let's say that in
19 "what if" Number 5 I do not protect public health and safety
20 to my satisfaction. Before I do anything else, I would ask
21 myself whether "what if" Number 5 has a probability that
22 would really upset all the calculations and the confidence
23 that I have.

24 In other words, I would not rely on a "what if"
25 analysis without addressing the issue of how likely that is.

1 MR. EISENBERG: But if you are trying to look at
2 your imperfect state of knowledge, you are speculating about
3 what you don't know.

4 MR. APOSTOLAKIS: I am not speculating because --

5 MR. EISENBERG: Then how do you know --

6 MR. APOSTOLAKIS: Wait a minute, wait a minute.
7 At some point you draw the line. I mean there must be some
8 sort of an upper bound that you can put. I mean it comes
9 down to Tom's point and John's that you can always give a
10 number or do something, you know? The problem with "what
11 if" calculations is the same one as defense-in-depth. There
12 is no control over it.

13 This committee 20 years ago, 25 years ago, the
14 moment the Reactor Safety Study hit the streets several
15 members for years took extra pleasure by taking a few
16 parameters, multiplying by 10 and saying my god, look what
17 happens to the result, and everybody said yeah, look at what
18 happens to the result.

19 The question is can you multiply it by 10? Is
20 that real? And I think you are going that way. You can
21 start playing games here that have no bound.

22 MR. EISENBERG: The key thing here is that the
23 underperformance would be related to the degree of
24 uncertainty in that particular barrier, so if you have a
25 very good case, if you have lots of evidence, then you would

1 underperform it very little. If you don't have a whole lot
2 of data, if you have a 20,000 year waste package and you
3 have two months of data, well, maybe we would want to see it
4 underperformed more, but it is not unbounded speculation and
5 it is not intended to be unbounded speculation.

6 MR. BUDNITZ: I have peeked ahead but --

7 [Laughter.]

8 MR. BUDNITZ: -- but it is a fair comment to say
9 that although I wasn't in Las Vegas in November I read the
10 transcript and your thinking here is the same as there and
11 that's great because, you know, it's only been a couple
12 months and I understand what you are doing.

13 I am still troubled by two things. Unless I
14 peeked ahead and didn't get it right, you are still asking
15 the Department, the Applicant, to select the amount of
16 underperformance that they will analyze, and I think that is
17 not necessarily right.

18 MR. GREEVES: Well, why don't we move to the next
19 one.

20 MR. BUDNITZ: Maybe we can go to that.

21 MR. GREEVES: I am not sure you read that slide
22 right.

23 MR. BUDNITZ: Maybe I didn't get that one right,
24 but the second point is on this slide. Go back to this
25 slide. It has to do with the word "compensate."

1 The word "compensate," my plain English reading of
2 that convinces me it is the wrong word. You can't expect
3 that if you underperform a certain barrier that you would
4 necessarily still meet the dose limit at Amargosa Valley or
5 maybe you do mean that. It's very important to understand
6 that.

7 MS. LUI: Right.

8 MR. APOSTOLAKIS: What did you say?

9 MS. LUI: If you look at it carefully, it's not
10 fully compensated. We are talking about compensate.

11 MR. BUDNITZ: So let me try to say this. Suppose
12 the dose limit at Yucca Mountain is "x" millirem per year
13 and the base case calculation shows one-hundredth of "x" and
14 then they undercompensate Barrier Number 2, underperform,
15 excuse me, underperform Barrier Number 2, and instead of
16 being .01 of "x," whatever the limit is, it's now 5x. Do
17 they get a license or don't they?

18 Now that depends on something that they haven't
19 told us yet. It's really a crucial point.

20 MR. APOSTOLAKIS: What is it that you haven't been
21 told?

22 MR. BUDNITZ: They haven't told us whether or not
23 they are going to get a license or not.

24 DR. KRESS: And is that acceptable. You haven't
25 defined an acceptable performance --

1 MR. APOSTOLAKIS: Isn't the obvious thing to do to
2 ask yourself how likely this postulate we made was?

3 MR. BUDNITZ: That is a piece of it, of course.

4 MR. APOSTOLAKIS: That is the most important
5 piece.

6 MR. BUDNITZ: I am not arguing the case, but you
7 see, if in fact something becomes 5x instead of .01x but "x"
8 is the limit, right? -- we may all judge that that is
9 sufficiently unlikely that we will give them the license,
10 right? But they haven't told us, the public, and here I am
11 a member of the public because I am not under contract to
12 anybody right now, or certainly they haven't told the
13 Applicant yet, unless I've peeked ahead and haven't seen it,
14 whether -- what the decision criterion is and in my remarks
15 I said it has to be fair and it has to be technically sound
16 and it's very, very important that that be clarified.

17 MR. APOSTOLAKIS: The weak calculations set a bad
18 precedent there. Look at the spaghetti curves.

19 MR. BUDNITZ: Well, we are not arguing the case.

20 MR. APOSTOLAKIS: All of them are below.

21 MR. BUDNITZ: You see what I'm saying? So keep
22 going.

23 MR. GREEVES: I understand what you are saying and
24 you are not going to be satisfied.

25 MR. BUDNITZ: I know I am not going to be

1 satisfied and I want to say that if I was designing the
2 repository and some of the guys behind me are, and if I was
3 trying to put it together now so that I could analyze it
4 next year, so I could bring you the thing in the year after
5 next and I didn't even know whether the design I am
6 contemplating freezing for this will do this, that is a real
7 problem, that's a real problem.

8 MR. GARRICK: I think that the more realistic
9 issue here, it seems to me, and I am reminded of an earlier
10 working group where one of our consultants said it's the
11 water, stupid, the more realistic thing that is likely to
12 happen here is that the initial conditions that are the
13 basis for the TSPA may not be appropriately represented.

14 MR. BUDNITZ: That's a fair comment.

15 MR. GARRICK: Because the thing that really
16 distinguishes this from the reactor case is the fact that
17 the peak dose may not occur for 300,000 - 400,000 years.

18 MR. BUDNITZ: Well, they have a 10,000 year
19 requirement.

20 MR. GARRICK: I don't care. I don't care. I'm a
21 risk analyst. I am not a regulator, and so the thing that
22 drives that -- there is almost as much of a singularity in
23 the waste disposal problem as core damage is in the reactor
24 problem in terms of the release, and so I think that what is
25 really where we are going to find the most opportunity for

1 having miscalled this thing is not so much with the design
2 of the barrier but with the initial conditions that are the
3 basis for the performance assessment in the first place.

4 MR. BUDNITZ: You could be right.

5 MS. LUI: Okay. Next slide. There are two
6 technical issues that we are wrestling with in terms of the
7 multiple barriers analysis. Basically we mentioned about
8 underperformance of a barrier. What we can do is we can
9 prescribe what should be the degree of underperformance or
10 we can take a more performance-based approach. Let DOE look
11 at the amount of evidence that they have in terms of
12 supporting the barriers' capability they claim in the TSPA
13 analysis and then they can make a judgment of what should be
14 the appropriate degree of underperformance for that
15 particular barrier in the barrier underperformance analysis.

16 Another issue we are looking at is how should NRC
17 evaluate the outcome of the underperformance analysis?

18 MR. APOSTOLAKIS: Which is what I have been
19 saying. You haven't said anything about the assumptions
20 that the analysis makes. Is that buried somewhere here?
21 I don't understand.

22 MS. LUI: The assumptions for the barriers
23 underperformance analysis?

24 MR. APOSTOLAKIS: Yes, for transport of
25 radionuclides.

1 MS. LUI: It is all part of the total system
2 performance assessment.

3 MR. APOSTOLAKIS: I understand that.

4 MS. LUI: Right.

5 MR. APOSTOLAKIS: But where in this scheme of
6 things do you worry about the assumptions being wrong?

7 MR. GARRICK: That's what I mean by the initial
8 conditions.

9 MR. APOSTOLAKIS: I know, but I don't see where it
10 is.

11 MR. GREEVES: I think Dr. Garrick would say that
12 that is included in the original performance assessment.
13 When you step off and start doing these under performance
14 evaluations, I think you would have to talk about
15 understanding what those assumptions were and try to justify
16 why you made those.

17 MR. APOSTOLAKIS: Right.

18 MR. GREEVES: The DOE could make a statement this
19 is my assumption, we think it's reasonable. The Staff could
20 look at it and say looks good but we have a little wider
21 band. I think that is part of what we are about.

22 MR. APOSTOLAKIS: But that brings me back to my
23 earlier question where I was told that I was impatient. How
24 do you handle model uncertainty then in the base case? You
25 say known uncertainties are appropriately captured. What

1 does that mean?

2 MS. LUI: If part of the consideration of the
3 alternative conceptual models --

4 MR. APOSTOLAKIS: But do we know how to do that?
5 Do we understand the conceptual framework? Do we know how
6 to do that?

7 MS. LUI: Okay. There are a couple -- there is a
8 stepwise process. Basically DOE will have to identify what
9 are the alternative, what are the conceptual models, what
10 are the different conceptual models that are consistent with
11 all the information that we have up to date and that they
12 have to make a justification why they have included certain
13 ones and they have excluded certain ones from their
14 consideration in the total system performance assessment.

15 MR. APOSTOLAKIS: What if they take all 11 of them
16 and give them different weights?

17 MR. EISENBERG: They can do that, but we would
18 also want to see that information disaggregated and we would
19 look to see to some degree what the bounding one would be
20 and we would probably want them to show compliance with that
21 one.

22 MR. APOSTOLAKIS: Which each one?

23 MR. EISENBERG: Yes.

24 MR. APOSTOLAKIS: With each of the 11?

25 MR. EISENBERG: No, with whatever the bounding one

1 was.

2 DR. KRESS: That is each of them.

3 MR. APOSTOLAKIS: That is each of them, yes, if
4 the bounding one does it -- it's each of them.

5 Is that something that people have really thought
6 about?

7 DR. KRESS: It is not clear to me where you are
8 using probabilities in this process at all.

9 MR. APOSTOLAKIS: They are not.

10 DR. KRESS: That seems to be the shortcoming in
11 this whole thing.

12 MR. APOSTOLAKIS: That's right.

13 MS. LUI: Probabilities fall into a total system
14 performance assessment.

15 DR. KRESS: It is part of the performance
16 assessment, I understand.

17 MS. LUI: Right.

18 MR. APOSTOLAKIS: Yes, but --

19 MS. LUI: There are disruptive scenarios that have
20 the equivalent of initiating events probability and then you
21 have expected evolution of the repository behavior.

22 MR. APOSTOLAKIS: We just agreed that maybe in one
23 piece of this evolution there are questions about the
24 medium, for example, okay, and we have transport through
25 fissures, fissures or something else, and I think I heard

1 Dr. Eisenberg say that if there are questions like that and
2 you have 11 different ways you can go, you better meet the
3 regulations with each one of them.

4 I am asking whether this committee has discussed
5 this issue, because that sounds to me like a license to
6 kill.

7 MR. GREEVES: I think that there has to be a
8 qualification on 11. It has to be something that is
9 reasonable. You can come up with something that is
10 non-physical and that one should be discarded.

11 MR. APOSTOLAKIS: Well, physical I understand, but
12 how about likely?

13 MR. BERNERO: You know, I am sorry to hear Norm
14 use the word "compliance." The total system performance
15 assessment which is supposed to take due account of
16 uncertainties is being used as a compliance tool, is the
17 result of it consistent with the objective, the safety
18 isolation objective as stated?

19 . These are sensitivity analyses and these
20 sensitivity analyses, somewhat arbitrarily chosen, somewhat
21 arbitrarily applied, should explore how close to the edge of
22 the cliff of unacceptability they are or their results would
23 be, and it is not compliance --

24 MR. EISENBERG: For a particular barrier --

25 MR. BERNERO: I mean it is license to kill if you

1 say now change that assumption to the worst case and show me
2 you still comply. You just made that your compliance case.

3 MR. EISENBERG: No, I think we are talking about
4 two different things. I think what George was talking about
5 was how do we consider conceptual model uncertainty in the
6 performance assessment as a whole, not how do we do these
7 defense-in-depth calculations.

8 MR. APOSTOLAKIS: They are related though, Norman.
9 They are related, very much related.

10 MR. EISENBERG: I thought how the question was
11 phrased I thought the predicate for it was that you had 11
12 different conceptual models and you had no information to be
13 able to distinguish --

14 MR. APOSTOLAKIS: Yes.

15 MR. EISENBERG: -- between one and the other.

16 MR. APOSTOLAKIS: Well, I didn't say, the second
17 part I didn't say.

18 MR. EISENBERG: Well, then do you have a preferred
19 model and do you have evidence to support the preferred
20 model?

21 MR. APOSTOLAKIS: I don't know. Maybe there are
22 two or three possibilities. I don't know. We may do what
23 NUREG 1150 did, collect a bunch of experts and try to assign
24 weights. I don't know but I would really question the
25 wisdom of saying that I will do it for each model and see

1 what --

2 MR. EISENBERG: But that -- my answer was
3 predicated on the basis that there was nothing to
4 distinguish between --

5 MR. APOSTOLAKIS: Okay.

6 MR. EISENBERG: -- between the different
7 conceptual models. Now you are telling me you have more
8 information. Well, if you have more information, you should
9 use it.

10 MR. APOSTOLAKIS: But is it being used now?

11 MR. EISENBERG: Yes.

12 MR. APOSTOLAKIS: Yes?

13 MR. GREEVES: Both the Staff and DOE have done
14 these calculations and we have briefed the committee on
15 them.

16 MR. BUDNITZ: But I am still stuck with, sorry,
17 with my question.

18 Let's suppose that we have a barrier and we have
19 enough of a quantification of our state of knowledge of its
20 performance so that we can say its performance is in a
21 certain range -- just to be numerical about it, without
22 knowing quite what it means, it is between 4 and 400, this
23 is a completely arbitrary discussion, and 400 is worse than
24 4, right, and let's suppose we knew nothing more than that.
25 It was a complete maximum entropy. We said we knew damn

1 well it couldn't be lower than 4 or greater than 400.

2 You would be saying, gee, you better assume 400
3 and show us it works. I am not disagreeing with that, but
4 if you have a state of knowledge that says, well, I am sure
5 that it is between 4 and 400, but I actually have knowledge
6 that tells me that there is a curve and distribution and the
7 probability it's at either end is really quite small
8 although it is possible, and we know it is bounded. It
9 can't be more than 400. Then it is not right -- by the way,
10 if you use 400 and you still pass, great. You do that every
11 day of the week in every analysis we know. That is the best
12 way to show it, but it is not right to insist that when, and
13 I know you understand this, but now we come to this question
14 about underperformance and compensation.

15 Are you going to ask for that barrier -- now this
16 is just very conceptual -- that DOE decide which
17 underperformance number to pick and then they are going to
18 come and bring you the rock, and the thing I said, "Wrong
19 rock" or are you going to tell them in advance what your
20 decision criterion can be so that they can spend more money
21 on a better design or spend more money on more analysis or
22 something so that they know going in what they can expect
23 from you, because I think unless they know that, this
24 process is unsatisfactory for me as a citizen, and I hope it
25 ought to be unsatisfactory for the Commissioners as the

ANN RILEY & ASSOCIATES, LTD.
Court Reporters
1025 Connecticut Avenue, NW, Suite 1014
Washington, D.C. 20036
(202) 842-0034

1 statutory authority because the Department needs to know the
2 rules and the speed limit before they submit the
3 application.

4 MR. EISENBERG: The Department doesn't have its
5 design finalized yet and it doesn't have its safety strategy
6 finalized yet, so it can't tell us how much reliance it is
7 placing on different components of the system.

8 MR. BUDNITZ: I understand what you are saying.

9 MR. EISENBERG: I am too. We are understanding
10 each other.

11 MR. BUDNITZ: It's iterative but those guys have
12 to do -- they are the Applicant.

13 MR. GREEVES: And those guys did a viability
14 assessment.

15 MR. BUDNITZ: Yes, I know it.

16 MR. GREEVES: So they are not without ability.

17 MR. BUDNITZ: We all know that. We all know that.

18 MR. BERNERO: But I have got to quarrel with you,
19 Bob, on the regulator can't take the burden of sharp
20 prescription of what does it take to prove safety. You
21 can't do that. It is, like it or not, it is a show me the
22 rock. DOE has the primary responsibility and there has to
23 be some kind of guidance on what size rocks and what
24 texture.

25 MR. BUDNITZ: The boundaries.

1 MR. BERNERO: But at the same time you can't get
2 away from the fact that DOE has far more capability and far
3 more responsibility to develop these arguments to show that
4 there is not undue reliance --

5 MR. BUDNITZ: Bob, I agree with you absolutely,
6 completely about whose responsibility is where. What I was
7 worried about was that the amount of underperformance the
8 Department will assume may be way short of what you would
9 have done and then they have got their design they have
10 frozen. They are in the licensing process and they could
11 have fixed it earlier.

12 MR. GARRICK: Bob, I suspect that if you
13 calculated the matrix I showed you this morning, the more
14 detailed one, the answer would be obvious.

15 MR. BUDNITZ: You may be right.

16 MR. GARRICK: Yes. If you have the performance of
17 the individual barriers with and without in context, that to
18 me would be the strongest piece of evidence you could
19 possibly have for me to make a judgment about the
20 performance and I know you said in your talk that you can't
21 remove the barrier --

22 MR. BUDNITZ: Completely, of course.

23 MR. GARRICK: -- completely, but you can do
24 variations on it and, as a matter of fact, as you decompose
25 it into more and more detailed barriers you can increasingly

1 remove it more easily.

2 MR. BUDNITZ: That's fair.

3 MR. GARRICK: And with increasing accuracy.

4 MR. BUDNITZ: Just as your microscope goes --

5 MR. LEVENSON: John, as I have been listening to
6 this, I'm thinking what would bother me about it if I were
7 trying to conform and this word "compensate" is a very loose
8 end, that it would change completely what needed to be done
9 if you said adequately compensate as opposed to totally
10 compensate, and without a modifier there is an implication
11 of total.

12 I would give an example. In your base case maybe
13 the dose to the public is -- I will use Bob's one
14 one-hundredth of what is allowable, but you fail one barrier
15 and now you are only one-tenth of what is allowable.
16 Clearly you are way under what is allowable but you haven't
17 fully compensated and so I think the choice of the word
18 "compensate" without a modifier is likely to cause all kinds
19 of problems.

20 MS. LUI: Yes, we agree with you basically. That
21 is why these are two key technical issues that the Staff is
22 struggling with, to make sure that the rule and the guidance
23 is going to follow and be consistent with the Commission's
24 mandate on a risk-informed, performance based regulatory
25 approach and at the same time provide sufficient model to

1 the Department so that they will be able to submit a quality
2 license application.

3 I think we have kind of skipped over some of the
4 points that are discussed on the next slide, so proceed to
5 Summary.

6 MR. GARRICK: Which number are you on, just for
7 clarity's sake?

8 MS. LUI: Slide Number 8. The multiple barrier
9 requirements go to be a system requirement.

10 We shied away from the subsystem -- qualitative
11 subsystem performance objective in Part 63, in the proposed
12 Part 63 and we will continue the track that we will keep the
13 multiple barrier requirement as a system requirement.

14 In other words, we will not set performance goals
15 for barriers such as waste package and natural settings.

16 In our evaluation of DOE's license application,
17 the goal is to look for that Both the engineered and
18 geologic systems contribute to safety. That goes back to
19 safety that is not wholly dependent on a single barrier
20 concept.

21 I think we have pretty much beaten the second
22 check-mark here to death --

23 [Laughter.]

24 MS. LUI: -- and the last one is we not seeking
25 complete redundancy for the barriers.

1 The last remark is just to reiterate that the
2 public comment period is over and we are well underway in
3 terms of analyzing the public comments and providing and
4 preparing the response, and whatever information that we
5 hear during these particular meetings that will be available
6 to us in terms of finishing up the final rule and drafting
7 the Yucca Mountain Review Plan. We intend to put the
8 transcript of this meeting on the website so that it will be
9 available to the general public.

10 MR. GARRICK: Let me postulate a situation. We
11 have learned a lot from the TSPA work. We have learned so
12 much that where we used to use the word frequently
13 "geological isolation" we are using it less and less,
14 because we have pretty much learned that if we have a source
15 term and it is mobilized, it just delays the transport of
16 that material into the biosphere. It doesn't isolate it
17 from the biosphere.

18 At least we haven't been able to characterize, we
19 don't think we are able to characterize any site where we
20 could achieve complete isolation in the absence of
21 assistance from engineered systems.

22 Now supposing somebody came along and suppose they
23 convinced you that I have designed the one million year
24 waste package and my confidence in that containment
25 capability is far greater than my confidence in the

1 containment and transport capability of the natural setting.
2 Obviously if you have a defense-in-depth philosophy like you
3 are stating here and that we are seeking balance, which I in
4 principle kind of agree to, you'd deny them the license.

5 MR. GREEVES: Why would you deny them the license?
6 You lost me.

7 MR. GARRICK: Well, what I am saying, if somebody
8 comes along with the perfect, with a million year waste
9 package, and there's engineers that believe they can do
10 that, and yet the geologic setting they couldn't convince
11 you that if there was a source term that there would be
12 adequate containment, but with the waste package of course
13 there is adequate containment, so you don't have the
14 defense-in-depth but you have a waste package that
15 convincingly will last a million years.

16 With Part 6 could you license that?

17 MR. GREEVES: I think you have carried us too far
18 of a stretch.

19 MR. GARRICK: Well, I don't think it is so far a
20 stretch. Frankly, I think it is probably much easier to
21 design a million year waste package than it would be to
22 characterize Yucca Mountain down to the few meters.

23 MR. GREEVES: Your dialogue was saying that the
24 site gives you nothing is the way you --

25 MR. GARRICK: Eventually it doesn't give you

1 anything. It gives you dilution. It gives you something.

2 MR. GREEVES: I don't agree with that statement.

3 MR. GARRICK: But the one thing that the Nevadans
4 are coming to us very strong on is, and the NRC is agreeing
5 with them, at least in the public media, that we are now
6 talking about delay, not isolation.

7 MR. GREEVES: Anybody that's been in this
8 business, Bob Bernero said it earlier, it's just a question
9 of time whether it is high level waste, low level waste.
10 You cannot guarantee containment. There will be some time
11 when you have to --

12 MR. GARRICK: The argument being, John, that
13 there's a lot of people that believe I can do a much better
14 job at building something to a specification than I can at
15 characterizing a mountain into a level of detail necessary
16 to give me the same output.

17 MR. GREEVES: I am aware there are people out
18 there like that. We are also aware that there is a piece of
19 legislation that calls for multiple barriers.

20 MR. GARRICK: That's all I am getting at. That's
21 back to my question --

22 MR. GREEVES: The simplest -- an engineered
23 barrier and the site --

24 MR. GARRICK: Are we ending up with a law, with a
25 regulation here where we couldn't license a repository that

1 has overwhelming evidence that it will retain its integrity
2 for a million years?

3 MR. EISENBERG: Dr. Garrick, there is no intent to
4 put a roof on the quality of any barrier. DOE should make
5 each barrier as good as they can.

6 MR. GARRICK: That isn't my point. My point is

7 -- MR. EISENBERG: Well, it sounds like it is your
8 point.

9 MR. BERNERO: I would like to interject on behalf
10 of the Staff, as if I was still there.

11 What you describe is a very good description of
12 the Swedish strategy.

13 MR. GARRICK: Yes.

14 MR. BERNERO: Which is the sole purpose of the
15 repository isolation is to maintain reducing chemical
16 conditions so that this very nicely designed million year
17 package will live for a million years.

18 MR. GARRICK: Right.

19 MR. BERNERO: And besides that, that water down
20 there is fossil water It isn't going to move for a long,
21 long time, and it is a marvelous system.

22 They of course are a piece of granite that is
23 rising up out of the sea and you have a choice of granite,
24 granite and granite for a Swedish repository

25 [Laughter.]

1 MR. BERNERO: The United States has a system of
2 laws which gives us a statutory requirement that says you
3 must have multiple barriers. It also has a statutory
4 requirement that DOE cannot look at crystalline rock.

5 Now that is not a technically based requirement.
6 It's an entirely politically based requirement.

7 There is a system of laws and there is a
8 distinction that one has to make in what would constitute an
9 acceptable repository as against what would constitute a
10 preferable or ideal repository. At one time we had three
11 sites to be simultaneously characterized, and we used to
12 call it "The Beauty Contest." Insanely expensive. Just
13 imagine doing Yucca Mountain in triplicate and trying to
14 keep them on the same schedule.

15 What we have to have in the United States is what
16 is an acceptable repository. It's been accomplished in the
17 WIPP case, warts and all, you know, and certainly we can
18 talk for hours and hours on what should have been done
19 there, but it's been done and I am convinced it is an
20 acceptable repository and warts and all this Yucca Mountain
21 thing --

22 MR. APOSTOLAKIS: I think it also comes back to
23 the issue of prevention versus mitigation. Maybe -- I
24 really don't like, to generalize a little bit, regulatory
25 documents that talk in terms of number of barriers. In

1 fact, if this subcommittee writes a letter, that would be a
2 good thing to attack, because it is such a fuzzy concept
3 that can be misused and so on. I don't know what it means,
4 multiple barriers, to begin with, and I think a lot of the
5 debates we are having here come from the fact that the Staff
6 naturally feels that they have to comply with what the
7 Commission says and the Commission says multiple barriers,
8 the legislation, I'm sorry. But this is an independent
9 advisory committee so we can write --

10 DR. KRESS: Did the Senate say how many barriers
11 was multiple?

12 MR. BERNERO: No.

13 MR. APOSTOLAKIS: Well, the more I think about it,
14 it's really the root cause of a lot of emotional debates,
15 because I am not even sure -- you gave us a good example
16 with the reactor vessel.

17 Up until this morning I would call it one barrier.
18 Now you tell it is not one barrier. Now I have no basis of
19 saying it's not or it is or it is not. I think it's wrong
20 to count barriers, to count something you have not defined.

21 MR. LEVENSON: But John, in response to your
22 question, I think the answer is it could be licensed because
23 the legislation, as I understand it, does not say that each
24 barrier has to be 100 percent effective.

25 The legislation just says there must be more than

1 one barrier.

2 MR. APOSTOLAKIS: Which defeats the whole idea, of
3 course.

4 DR. KRESS: I think at this point -- are you
5 finished?

6 MR. GREEVES: Let me just summarize. We are
7 finished.

8 [Laughter.]

9 MR. APOSTOLAKIS: Good.

10 MR. GREEVES: You think I should stop there? He
11 said we were finished. He didn't say we've had it. I think
12 we have worn it out, right?

13 Just to summarize, I think Norm did a good job of
14 showing you the spectrum of issues that face us across the
15 licensees that NMSS has. It is a difficult issue and I
16 think we have learned something from watching the process
17 here, and I think some things are going to come out in the
18 future that will help us, and each one of those -- it is
19 almost like the chart that Norm showed. For each one of
20 those arenas, we have got to start making some decisions.

21 You spoke at length about the DOE issue, but each
22 of those we have got to sort of make some decisions. I know
23 you all appreciate that the Staff needs to be consistent
24 with the Commission policy and the legislation, so that is
25 something that we will be holding in our minds as we draft

1 the regulations.

2 Something that has come out to me is listening to
3 us all talk around the room is transparency. I think we
4 have got to find a way to explain these things that is a bit
5 more clear. I think we talked past each other on occasion,
6 so I challenge us to -- over time we are going to have to
7 make this more transparent to other stakeholders.

8 I do ask you to keep in mind what the Staff
9 presented are preliminary considerations. We are working
10 under the requirements for developing the rule process, and
11 I know Bob is disappointed he didn't see the number he was
12 looking for, but that is something we are about.

13 MR. BUDNITZ: Doesn't have to be a number.

14 MR. GREEVES: Well, I think you raised some good
15 points and I agree with the need to do it one way or the
16 other, and we didn't tell you today.

17 MR. BUDNITZ: That's fine.

18 MR. GREEVES: And so those will be my closing
19 remarks and I assure you we are still considering these
20 issues and we are going to look at this transcript and I
21 think it will be helpful. Thank you.

22 DR. KRESS: Thank you very much. At this point
23 I'll take another break for about fifteen minutes, and that
24 would be be back at ten minutes, by this clock, after 3:00.

25 [Recess.]

1 DR. KRESS: We are at the point on the agenda
2 where we are going to hear from Gary Holahan and Tom King.
3 Our pleasure, gentlemen.

4 MR. HOLAHAN: Good afternoon. This is Gary
5 Holahan. I am the Director of the Division of Systems
6 Safety and Analysis in the Office of Nuclear Reactor
7 Regulation, and Tom King and I are going to discuss what
8 defense-in-depth means to the reactor program. I think you
9 will hear a lot of things that you heard this morning,
10 because I think we are all playing from the same historical
11 book, so some of what we discuss will be historical, some of
12 it is recent and ongoing activities, and some of it is
13 looking to the future, so I will start out with a bit of the
14 historical perspective and Tom is going to cover the future.

15 I think it is interesting the first point we are
16 making is that in fact there is no formal regulation or
17 agency policy statement on defense-in-depth and I think this
18 goes back and is consistent with Tom Murley's comments this
19 morning about defense-in-depth isn't a rule or a specific
20 requirement, which I think leaves a little bit to a number
21 of comments this morning about are we talking about a
22 philosophy or a policy or a guidance or a rule or a
23 requirement or a commandment?

24 I guess at that point I would have to agree with
25 Dr. Budnitz that what really matters is how you implement

1 it, so in fact we have called defense-in-depth a philosophy,
2 not a specific regulatory requirement, and in our recent
3 guidance documents we have said that it is one of our
4 principles that we preserve that philosophy, so George might
5 be offended. We used the word principle and philosophy in
6 the same sentence, but luckily George and his subcommittee
7 concurred in that document, so we'll feel comfortable about
8 it.

9 [Laughter.]

10 MR. HOLAHAN: But it was two or more years ago.

11 MR. APOSTOLAKIS: Nothing less is expected of
12 Gary.

13 MR. HOLAHAN: The second point in fact is that as
14 with the materials program, the reactor program is really
15 working with the same philosophical concept of
16 defense-in-depth. In fact, we are quoting the same version
17 that Bob Bernero mentioned this morning where
18 defense-in-depth, as was said earlier, has successive
19 compensatory measures and it has this element of not being
20 wholly dependent upon any single element of the design.

21 There have been previous definitions of
22 defense-in-depth and they have all been more or less
23 consistent. I am going to show you a couple of historical
24 examples in just a minute.

25 The third point I would like to make on this

1 introductory slide is that what really counts is that this
2 philosophy, the same philosophy can be implemented in a
3 number of different ways and what you see in the reactor
4 program is not necessarily the same thing as you see in the
5 materials program and I think the agency feels reasonably
6 comfortable calling both of those defense-in-depth
7 philosophy.

8 In the reactor program I am going to discuss the
9 regulations themselves where defense-in-depth is included in
10 the regulations even though it isn't a specific regulation
11 itself, also how the licensing process and the license
12 amendment process have dealt with the subject and the new
13 reactor oversight process, where oversight includes
14 inspection, enforcement, monitoring of licensee performance,
15 where the elements of defense-in-depth are embedded in that
16 process as well. Next viewgraph.

17 Well, you can see on this viewgraph Part 50
18 includes defense-in-depth in a number of ways. The concepts
19 of prevention, mitigation, single failure, redundancy,
20 diversity -- these are all elements of defense-in-depth.
21 When we talk about it, you can talk about defense-in-depth
22 in a number of ways. You can talk about physical barriers.
23 You can talk about functional barriers. You can talk about
24 I think Tom Kress has suggested a number of times risk
25 allocation in fact is a defense-in-depth concept. You can

1 put numerical goals on things like core damage frequency and
2 large early release, and that in effect is a way of
3 providing defense-in-depth. Next viewgraph.

4 There are two viewgraphs that are used as part of
5 a training program that NRC has. It's called "Perspectives
6 on Reactor Safety" and it is sort of, in part it is a
7 history book that Denny Ross and a number of people worked
8 on with Sandia to put together so that NRC's new Staff
9 members have an appreciation of not only what the
10 requirements are but how they got that way, and it covers
11 sort of the history of the '60s and '70s as the requirements
12 were built.

13 As part of that, in fact there is a section on the
14 concept of defense-in-depth, what it means and how it was
15 developed and I am going to show you two viewgraphs from
16 that material.

17 What you see here is one concept of
18 defense-in-depth, which I think I would call the functional
19 definition. That is, you look at prevention, mitigation in
20 terms of having safety systems and containment, and siting
21 and emergency planning. In this particular example you will
22 see that accident management is also identified as a level
23 of defense-in-depth. Some people would push it a little bit
24 into a containment performance issue. Some people would
25 talk about it as an emergency response issue, but you see

1 how the measures of defense-in-depth basically show that
2 public safety is protected by a series of functional type
3 barriers. Tom, can I see the other one?

4 I think especially years ago people generally
5 talked about defense-in-depth in terms of physical barriers,
6 and in fact in the training book these are two pages right
7 together, and so these concepts sort of grew up together
8 over the years and the concepts of physical barriers
9 including the fuel pellet and the cladding, reactor coolant
10 system, containment, and then things like exclusion areas
11 --these are the physical barriers.

12 Now what we know is this is a defense-in-depth
13 concept. Each of these defense-in-depth concepts really has
14 its own sort of strengths and weaknesses. If physical
15 barriers were the only defense-in-depth concept, I think we
16 would have come quickly to the realization that common cause
17 failures and interdependencies make this an incomplete
18 concept for defense-in-depth. In fact, the functional
19 concept in my mind is more complete and in a number of ways,
20 using PRA and whether you call it allocation or other ways
21 of looking at core damage frequency, even the concept of
22 Level 1, 2 and 3 in PRA in my mind are a form of
23 defense-in-depth and probably a more complete form.

24 One of the ways in which the regulations call for
25 defense-in-depth, and this is just one example that I have

1 picked out, you could probably find dozens, if not hundreds,
2 of places where a concept is embedded in the regulations,
3 right in the general design criteria.

4 In fact, it is broken up into six sections. One
5 of the sections itself is called "Protection by Multiple
6 Barriers" but in addition to that, the other sections of the
7 general design criteria, which really play a strong role in
8 determining what an acceptable reactor design looks like, in
9 fact call for a reactor core that behaves well, a primary
10 coolant system with low failure probability, and then fluid
11 systems, either normal ones or emergency ones, to handle
12 failures and the reactor containment and fuel and
13 radioactivity control really talks about fuel in the sense
14 of fuel handling, and that doesn't mean that when it is in
15 the core, it means when it is a potential source, so the
16 very structure of the regulations down to the general design
17 criteria have embedded in them a defense-in-depth concept.

18 I think I said I would talk about licensing but I
19 think I skipped -- let me do the oversight program and then
20 I'll talk about the license amendment process because that
21 is one that we have been changing lately and it has a good
22 kick-off point for Tom to get into our more future
23 activities.

24 The reactor oversight process was really given
25 almost a 100 percent overhaul in the last year, where the

1 inspection program, the enforcement program have basically
2 been totally rewritten, and they have been rewritten with
3 two concepts in mind. One is to be more performance-based,
4 to look at licensee performance and react to it, and the
5 other is to use more risk insights in the process, but in
6 doing so the defense-in-depth concept is being preserved by
7 the use of what are called cornerstones, and I am going to
8 show you how the cornerstones fit into the process.

9 Basically the message is that the cornerstones in
10 the oversight process are the ways of embedding
11 defense-in-depth. Cornerstones are defense-in-depth
12 features and in fact if you read the papers on the subject,
13 the concept of defense-in-depth comes up in a number of
14 points.

15 This is a viewgraph that many of you may have seen
16 before. It is used in a lot of the presentations on the
17 oversight process and if I can lead you from the top down,
18 public health and safety really means that we worry about
19 how the reactors behave and radiation safety, both in terms
20 of the public and workers. That's the Part 20, Part 100
21 type issue, and safeguards, so the issues to the right are
22 really in addition to what we have talked about most of the
23 day in terms of public health and safety from unusual type
24 of severe accidents.

25 If you will look at the way the program is

1 structured, reactor safety has four basic elements to it.
2 They are called cornerstones but you could have called them
3 defense-in-depth elements if you wanted to.

4 We look at initiating events, mitigating system
5 performance, barrier integrity, and emergency preparedness,
6 and those are basically I think a combination of functional
7 and physical barriers.

8 The way the oversight process works, the licensee
9 performance, both in terms of performance indicators and
10 inspection results from our inspections staff are put into
11 these categories, and then we make judgments about the
12 licensee performance in those areas. If you go to the next
13 slide, I can continue.

14 I am going through this kind of quickly, just not
15 to explain the whole process to you but just to show how the
16 concepts, defense-in-depth concepts, are built in here.

17 The performance indicators as used in the reactor
18 oversight process are in fact groups together depending on
19 which of the cornerstones they relate to, so things like
20 reactor scrams or significant initiating events and
21 transients, they go into the initiating event cornerstone,
22 and things like the safety system performance and
23 unavailability, those go into the mitigation system, and so
24 the licensee performance in terms of performance indicators
25 and inspection findings are measured with respect to

1 thresholds to identify their significance and they are
2 folded into these cornerstones. We can go to the next one.

3 In fact, I am not going to discuss this viewgraph.
4 Just for completeness it shows how each of the cornerstones
5 has indicator input to it.

6 The next viewgraph is a little hard to follow, but
7 the basic concept is across the top you will see a spectrum
8 of results in which various levels of performance of
9 increasing safety significance are monitored, and so on the
10 extreme left what you will see is everything is pretty
11 normal, and that is the inputs to the cornerstones, each of
12 the cornerstones, not just public health and safety sort of
13 dose limit, but each of the cornerstones is performing well.

14 If you will look down that column it says we have
15 a routine inspection program and licensee fixes issues on
16 their own, and sort of everything runs sort of normally and
17 this is, you know, we use the terminology of "green" -- this
18 is normal green performance in terms of for a licensee. As
19 you move to the right, across the top columns, you will see
20 increasing level of concern, and that is indicated by
21 degraded performance in one or more cornerstones.

22 As you can see, as it sort of escalates, it
23 is not only that the total licensee performance seems to be
24 unacceptable in some way, but the NRC response will escalate
25 when the performance in one cornerstone area becomes of

1 increasing concern to the level of being warranting
2 interactions at Regional Branch Chief level, Regional
3 Division Director, Regional Administrator, EDO and even
4 getting to the point of the Commission.

5 So what it says, and there's lot of detail on here
6 that I am not going to cover today, the basic message is we
7 are looking at licensee performance at the cornerstone, but
8 that's basically at the defense-in-depth functional levels
9 and making judgments about how well the licensees are doing,
10 what level of interaction we ought to take with them,
11 whether their performance looks normal and we ought to sort
12 of be restrained and allow them to deal with their own
13 issues, take corrective action when problems occur, or
14 whether a higher level of management involvement and more
15 extreme expectations are appropriate

16 Now the system is set up basically as an early
17 warning system. It is not so easy to go from green to red.
18 Part of the workings of the systems is you expect the
19 licensees to know very well what the rules of the game are.
20 If their performance begins to degrade, they know it
21 early-on. We expect them to be dealing with it early. We
22 don't expect licensees to be in the yellow and red area
23 because there's plenty of warning for them to turn things
24 around, but the scheme shows how the Staff will be
25 responsive to cornerstones or defense-in-depth weakenings,

ANN RILEY & ASSOCIATES, LTD.
Court Reporters
1025 Connecticut Avenue, NW, Suite 1014
Washington, D.C. 20036
(202) 842-0034

1 and in fact potential failures. Tom?

2 I know that is kind of a lot to digest. The only
3 point I wanted to get across is that even though
4 defense-in-depth is not written as a regulatory requirement
5 it has a value as a guiding philosophy and it can be built
6 into various programs in a practical and usable manner.

7 Now in the license amendment process we have
8 developed Regulatory Guide 1.174. Even though 1.174 has a
9 lot of general safety philosophy in it, it was really meant
10 as a licensing amendment guidance document and there are
11 five safety principles associated with deciding whether a
12 license amendment change is acceptable or not.

13 I know the ACRS members are very familiar with
14 that. We spent a lot of time with the committee on these
15 issues and if my memory is accurate, and I think it is, even
16 the concept of having five relatively high level safety
17 principles was a concept that came up at this table in the
18 interactions between the Staff and George, your ACRS PRA
19 Subcommittee.

20 One of those five principles is that there ought
21 to be a defense-in-depth philosophy and my recollection is
22 we talked a long time about this issue of should there be
23 defense-in-depth, should there be defense-in-depth
24 philosophy where we are talking about never giving up any
25 measure of defense-in-depth, and I think it was an important

1 issue. I think in a number of ways it still is an important
2 issue and I think next month we will talk about ACRS has a
3 session on impediments to risk-informed regulation, and I
4 know a lot of people are concerned that this is a potential
5 impediment, and I think we have certainly got it on our list
6 of one of the things we want to talk about.

7 Reg Guide 1.174, its corresponding Standard Review
8 Plan, and the related documents on how to do risk-informed
9 regulation not only mention that there should be a
10 defense-in-depth philosophy but give you some insights as to
11 what that means and it identifies issues like balance
12 between prevention and mitigation, avoidance of
13 over-reliance. Now these are general concepts. They are
14 not numerical values. I think George has expressed the idea
15 that you should be very careful about not counting the
16 numbers of defense-in-depth or try to quantify it too much,
17 and I think we recognize the danger in doing these things.

18 Those concepts are discussed in the guidance
19 documents. I think it clearly says we are not trying to
20 assure that there is no change in the level of
21 defense-in-depth. What we are saying is there should be no
22 change in the philosophy. So if a licensee wants a license
23 amendment to remove the containment, they ought not to
24 bother because we are not going to pursue that.

25 MR. APOSTOLAKIS: One important point here, which

1 I believe is an assumption on your part and most people when
2 they talk about these things is you are talking about these
3 issues for the current generation of nuclear power plants.

4 There is a certain assumption here that -- in
5 other words, would you be as absolute in rejecting a request
6 for no containment for any future reactor? I doubt that,
7 because you don't know what physical pieces of those --

8 MR. HOLAHAN: I wouldn't reject it categorically.

9 MR. APOSTOLAKIS: So this is really for the
10 current generation, which is I think a reasonable thing to
11 do.

12 MR. HOLAHAN: Well, for the current generation and
13 I think for the evolutionary and advanced reactors that we
14 have seen.

15 MR. APOSTOLAKIS: Yes. I agree.

16 MR. HOLAHAN: But I think this ought to be left as
17 a relatively high hurdle.

18 MR. APOSTOLAKIS: I agree.

19 MR. HOLAHAN: Okay. By its nature, what we are
20 trying to do in the reactor area, and I recognize that in
21 the materials area there are some other considerations, we
22 are providing a very high level of protection, that is very
23 low probabilities for high consequence events. Almost by
24 definition, if that is the arena that you are in, you are
25 not going to have a lot of experience to deal with and you

1 are going to be extrapolating from pieces of what you know,
2 and issues like completeness and modelling are going to be
3 difficult ones.

4 One of the things that I sort of keep an eye on is
5 the accident sequence precursor program, previously in AEOD,
6 now in the Office of Research, and my recollection of if not
7 the last but one of the recent Commission papers on that
8 program, maybe a year ago or so, I think it said something
9 like half of the accident sequence precursors, the ones of
10 some significance, were things that were not previously
11 modelled, and so the signal is we are still at a time in
12 which there are surprises to be had, and by its very nature,
13 you know, you are going to have to develop an awful lot of
14 operating experience before you get to the point in which
15 you say my modelling and my completeness are minor issues.

16 MR. APOSTOLAKIS: Well, again, I would put some
17 qualifiers to what you just said. What does it mean it's
18 not modelled? I mean maybe the exact sequence of events was
19 not modelled but maybe it is a subset of something bigger
20 that was modelled.

21 MR. HOLAHAN: Well, I think --

22 MR. APOSTOLAKIS: I agree with that.

23 MR. HOLAHAN: I think it is worse than that.

24 MR. APOSTOLAKIS: I think in some instances it
25 might be, but the other, I mean in all fairness you should

1 also mention then the very important findings of the former
2 AEOD people that the system unavailabilities they find are
3 either -- are within the range of values of PRAs found --

4 MR. HOLAHAN: Yes.

5 MR. APOSTOLAKIS: -- which is really a very good
6 confirmatory piece of evidence that what we are doing is not
7 off the mark.

8 MR. HOLAHAN: And in general initiating event
9 frequencies are somewhat better and in fact in my mind, more
10 important than either of those is that common cause failures
11 are lower than is generally assumed.

12 MR. APOSTOLAKIS: Right. They are going down and
13 they are going down.

14 MR. BUDNITZ: You are looking under the lamppost
15 some of the time because half of the risk overall of the
16 fleet comes from fires and earthquakes and configuration
17 compromises that would make you more vulnerable to fires and
18 earthquakes are not modelled in ASP today, as George and I
19 know, since we wrote a NUREG about it which hasn't been
20 implemented yet.

21 MR. KING: But there haven't been that many fires
22 and we are looking --

23 MR. BUDNITZ: Well, there haven't been fires or
24 earthquakes, but we are talking about configuration
25 compromises that will make you more vulnerable if you had

1 one.

2 MR. KING: Yes.

3 MR. BUDNITZ: Those happen all the time.

4 MR. KING: There haven't been any earthquakes.

5 MR. HOLAHAN: And my recollection is isn't that
6 issue number one of twelve that we are dealing with in the
7 risk-informed fire protection?

8 MR. BUDNITZ: I hope so.

9 MR. HOLAHAN: I think it is on top of the list.

10 MR. BUDNITZ: I hope so.

11 MR. HOLAHAN: So the message I want to leave you
12 with is in the reactor area for the plants we are currently
13 dealing with, which basically are operating plants -- not so
14 long ago we dealt with advanced reactor designs -- but in
15 this context I don't think they were all that different.

16 Defense-in-depth has been an integral part of our
17 decision process, what we envision for risk-informing Part
18 50, and Tom is going talk to Option 3, but certainly if I
19 remember the ways the options are set up for risk-informing
20 Part 50.

21 Option 1 is just to continue with some of the
22 rulemakings that we have ongoing, 50.59 and maintenance rule
23 and things like that.

24 Option 2 is to take those issues related to day to
25 day operational performance and parts of the plant that get

1 special treatment in operations, things like quality
2 assurance and technical specifications, and maintenance type
3 activities, and to risk inform those sort of operational
4 type activities.

5 In doing so, we intend to preserve the current
6 design basis and that means that the level of
7 defense-in-depth in the plant probably is not going to be
8 changed very much, and also the other important
9 characteristic is in deciding what is of safety
10 significance, because in effect what Option 2 is going to
11 do, it's going to take the old model of safety-related and
12 not safety-related, something that John Garrick mentioned
13 this morning, that the PRA world, the risk analysts don't
14 care much about, and it's going to look at what is
15 risk-significant and what is not risk-significant.

16 It's going to overlay those two concepts but in
17 deciding what is risk-significant or not, we are going to
18 use a concept somewhat akin to the maintenance rule expert
19 panels where not only are we going to use the risk analysis
20 numbers, whether it's bottom line numbers or importance
21 measures, we will use the insights from experienced plant
22 people who can bring some defense-in-depth and safety margin
23 thoughts into that process, and we are developing some
24 guidance as to what sort of things they ought to be thinking
25 about in doing that.

1 So my message is we currently have
2 defense-in-depth in the reactor designs, it is in our
3 programs, it is even in our, what I would say is our most
4 modern risk-informing programs have the concept of
5 defense-in-depth.

6 Tom is going to talk about Option 3.

7 If I look about where we are going with
8 risk-informed license amendments and those sort of changes,
9 there is a challenge on the table for us.

10 I don't think we are going to quantify how much
11 defense-in-depth you need but we may put some more guidance
12 in place as to how to deal with issues where maybe it looks
13 like we are either doing -- I mean I must say I haven't
14 heard any "too littles" but maybe we are doing too much to
15 preserve more defense-in-depth than a more risk-informed
16 insight would tell us is necessary.

17 So the program is ongoing. Defense-in-depth is a
18 -- call it a philosophy or a guidance concept, and it's
19 basically built into where we are.

20 MR. APOSTOLAKIS: But the point though, Gary, is
21 that it is not whether one should have that philosophy and
22 whether one should ignore, for example, the items you have
23 under Regulatory Guide 1.174.

24 The question is not what role the risk -- the PRA
25 methods we have should play here, and I would say, for

1 example, if I took -- given the evidence that I have
2 including the AEOD evidence, that PRAs have done a pretty
3 good job modelling system unavailability for individual
4 safety systems, there is strong evidence that we have done a
5 hell of a job, then again from my point of view that means
6 that maybe the issue of unquantified uncertainty is not that
7 important there, although you might make the point that
8 under severe accident conditions we haven't seen those and
9 so on but let's take that -- so I would say that now I have
10 a good tool in my hands to take the seven or eight items you
11 have there and optimize my operations, optimize my design,
12 and I don't really have to have a diverse train for example
13 because I manage to achieve the required levels or the
14 inspected levels simply with redundant trains.

15 I can make a good case that I have handled common
16 cause failures and so on, so I suppose the heart of the
17 matter here is is there anything that will stop me from
18 doing that, another input, another principle, a philosophy
19 that will say, yeah, you can do all these things but boy, I
20 really want all seven, and what I am saying is I am not
21 willing to drop all seven, but first of all if you try to
22 drop them you will never achieve the numbers you want.

23 MR. HOLAHAN: Yes, that's right.

24 MR. APOSTOLAKIS: And second, all I am saying is
25 these are guidelines. It is a philosophy that you would

1 like to have at your disposal and use it, but now you have
2 this tool which is reliable in this particular context, so,
3 you know, I can afford maybe to drop one or I can afford to
4 minimize the role in one place versus another and so on and
5 I think that is really what we are doing with the case
6 specific risk-informed guides.

7 MR. HOLAHAN: Yes.

8 MR. APOSTOLAKIS: So this is a good example in
9 fact of a case where the PRA, it's almost risk-based here,
10 where risk is the unavailability.

11 MR. HOLAHAN: Well, I think what I would say is if
12 you go back and read the section on defense-in-depth in
13 1.174, I think it's okay, but that does not mean that in
14 implementing it we won't run into some tough cases, okay?

15 MR. APOSTOLAKIS: Sure.

16 MR. HOLAHAN: And we may be better off just
17 fighting over those cases than trying to write a guidance
18 document that avoids any fights in the future.

19 It may not be possible to write the definitive set
20 of guidelines on defense-in-depth that never has a problem.

21 MR. APOSTOLAKIS: And I realize that but I think
22 some sort of a high level discussion of these issues
23 probably would be beneficial because I agree that we can't
24 really be too specific at this point.

25 MR. KING: Reg Guide 1.174, if you recall, in the

1 defense-in-depth discussion does talk about using PRA, not
2 to do away with defense-in-depth but to optimize how you
3 achieve it and in effect in Option 2 and Option 3 risk
4 informing Part 50 it is the same philosophy, the same
5 approach we are taking.

6 What I was going to talk about is Option 3 and
7 what are we doing in our technical study or study of the
8 technical requirements, how are we folding in
9 defense-in-depth considerations and melding them with PRA
10 considerations, because for all the risk-informed activities
11 what we are talking about is not a risk-based approach but
12 using PRA to complement our traditional way of doing
13 business, which includes deterministic analysis and
14 defense-in-depth considerations, so we are trying to keep
15 that approach in both Option 2 and 3, and I will talk to you
16 about what our thinking is today for doing that under Option
17 3.

18 The last piece of this viewgraph I am not going to
19 talk about. You are going to get a separate presentation on
20 that at some point in the next month or two from Joe Murphy,
21 but again the reactor safety goal policy discusses
22 defense-in-depth and we had identified that as an item for
23 consideration for modifying the safety goal policy. Perhaps
24 it needs to be updated, expanded, and so forth, consistent
25 with the risk-informed regulation thought process that we

1 have gone through in discussion there.

2 Maybe I'll just take one more minute for
3 background, particularly for the folks from ACNW on what is
4 Option 3, what are we trying to do. As Gary mentioned, NRR
5 is working on a rulemaking now that's called Option 2 that
6 is basically looking at the scope of what ought to be
7 regulated based upon risk insights and that is in the sense
8 of special treatment rules -- by special treatment, what
9 should get QA, what should get equipment qualification and
10 so forth.

11 The functions would have to remain the same but
12 maybe depending upon the risk associated with -- the risk
13 significance of the various systems, structures and
14 components, maybe they don't need the pedigree that they are
15 receiving today, but again the functions would all have to
16 be accomplished.

17 What we are doing under Option 3 is going in and
18 looking at the functions, the design requirements, what
19 changes should be made there based upon risk insights.

20 Maybe to put in context what you are going to
21 hear, the Option 3 study is going to take place during this
22 calendar year, calendar year 2000. We are in the initial
23 stages of getting started. What you are going to hear about
24 is work in progress today. Some of the details have to be
25 worked out.

1 What you are going to hear about today we are also
2 going to put out for public comment fairly soon and we have
3 a workshop, public workshop, scheduled the end of February
4 to talk about this as well as the other things we have been
5 working on in the Option 3 study, so this is subject to a
6 lot of comment and a lot of further discussion. This is not
7 cast in concrete at this point.

8 In trying to do the Option 3 study we did realize
9 we had to come up with what we call a working definition of
10 defense-in-depth, something that the folks looking at the
11 regulations and the Reg Guides and the SRPs can take and
12 take the risk insights and sit down and make some decisions
13 on does what is in there look okay or are some changes
14 warranted?

15 So what we wanted to do was basically develop an
16 approach under this working definition that would consider
17 defense-in-depth that traditionally provides some multiple
18 lines of defense -- are not calling them barriers, we are
19 not counting barriers -- provides some balance between
20 prevention and mitigation and provides a framework by which
21 we can address uncertainties in the various accident
22 scenarios, so that is sort of the scope of what we thought
23 this working definition ought to contain.

24 There are two elements to the working definition.
25 One, which is probably the structuralist element, that in

1 our view there ought to be some floor on defense-in-depth
2 regardless of what your PRA says, there are probably some
3 things you want to retain, just call it deterministic or
4 engineering judgment, and then beyond that, there would be
5 the rationalist piece or implementation elements that can
6 vary depending on the uncertainty and the risk goals and so
7 forth.

8 MR. APOSTOLAKIS: This is the pragmatic
9 preliminary proposal we have?

10 MR. KING: Yes.

11 MR. APOSTOLAKIS: Structuralist at the high level
12 and rationalist at lower levels?

13 MR. HOLAHAN: The rationalist-informed
14 structuralist approach.

15 [Laughter.]

16 MR. KING: It doesn't have to be one way or the
17 other. They each have some advantages.

18 MR. APOSTOLAKIS: No, but this is the compromise
19 we came up with, otherwise the paper would never have been
20 published.

21 [Laughter.]

22 MR. APOSTOLAKIS: Isn't that right, Tom?

23 MR. KING: Yes.

24 MR. APOSTOLAKIS: This is the pragmatic.

25 DR. KRESS: That's pretty much we covered.

1 MR. APOSTOLAKIS: High level structuralist and
2 --good.

3 MR. KING: On Slide 15, it talks about the
4 fundamental pieces or the structuralist pieces. We want to
5 build upon the cornerstone concept that Gary showed,
6 particularly building upon the first four cornerstones that
7 are affected by reactor design, initiating events,
8 prevention and core melt, containment of fission products,
9 and emergency planning and response.

10 We feel that this working definition ought to
11 address those things. We feel that there ought to be some,
12 in the prevention side there ought to be some again I will
13 call it a floor on design features that prevent core melt
14 and whether we call those -- we put back in the single
15 failure criteria or somehow specify some redundancy or
16 diversity, we haven't worked out exactly the wording of
17 that, but we would not rely strictly on a risk number to say
18 I have got a highly reliable system, therefore I don't need
19 any redundancy, diversity, single failure protection and so
20 forth.

21 Again, other things you have to consider are how
22 do you factor the human in and the active versus passive
23 failure, particularly if we are into the single failure
24 question which in the past has always been limited to an
25 active component.

1 We feel that we should retain the ability to
2 contain fission products given a core melt, that that ought
3 to be a fundamental concept of part of this working
4 definition and emergency planning and response ought to be
5 retained. Clearly emergency planning and response is also
6 affected by siting criteria if you are talking about new
7 plants, but for existing plants it is pretty well fixed.

8 Now in addition to assuring the prevention and
9 mitigation we wanted to assure a balance between the
10 prevention and mitigation and we felt that we needed to be
11 consistent with the subsidiary risk guidelines that were
12 developed and used in Reg Guide 1.174.

13 Those actually came from Commission guidance that
14 we received over the past years where they gave us a 10 to
15 the minus fourth core damage frequency damage goal to use
16 and then we developed, as part of developing Reg Guide 1.174
17 worked backwards from the safety goal quantitative health
18 objectives and came back and developed a 10 to the minus
19 fifth large early release frequency goal that we felt was a
20 good design objective that if it was met would ensure you
21 would meet the quantitative health objectives.

22 MR. GARRICK: In your use of a mitigation here,
23 does it reach to consequence limiting? In other words, if
24 you are having a goal with respect to a large early release,
25 now you have material. What do you mean by mitigation

1 beyond the usual engineered safety features or do you mean
2 anything beyond that?

3 Do you include consequence limiting?

4 MR. KING: The large early release, the word
5 "large" has no limit on it. It can be a large release --

6 MR. GARRICK: You are not including --

7 MR. KING: No. It can lead to early fatalities
8 offsite.

9 DR. KRESS: Yeah, but it does include emergency
10 response measures for --

11 MR. KING: Sure.

12 DR. KRESS: -- for this LERF to be equivalent to
13 the early fatalities so that is in there.

14 MR. KING: Credit is given -- yes -- credit is
15 given for emergency response.

16 DR. KRESS: Credit is given for emergency
17 response.

18 MR. KING: But there is no limit on what large
19 should be.

20 MR. GARRICK: Well, I am also thinking of fission
21 product cleanup, retention --

22 MR. KING: Well, maybe I ought to say a little bit
23 about large early release. It is not large if it is cleaned
24 up.

25 DR. KRESS: Yes.

1 MR. KING: In other words, if it goes through the
2 suppression pool and scrubbed, it is not considered a large
3 release because not much gets out of --

4 DR. KRESS: Those things are inherent in the
5 definition.

6 MR. GARRICK: Yes, but I am getting at the 10 to
7 the minus five number.

8 MR. KING: Yes. That is for unscrubbed stuff.

9 MR. GARRICK: Unscrubbed, yes.

10 MR. KING: And it can lead to early fatalities.

11 MR. APOSTOLAKIS: It is directly related to early
12 fatalities.

13 MR. HOLAHAN: In effect what happens is if you
14 have a scrubbed release or a late release or a minor release
15 in fact core damage frequency 10 to the minus four by
16 default becomes its limit.

17 DR. KRESS: Yes.

18 MR. GARRICK: Yes.

19 MR. KING: Okay. The next thing we have done was
20 say okay, for this bottom piece what does that mean in terms
21 of looking at the cornerstones and some practical guidance
22 when you want to go in and look at the regulations?

23 We developed sort of a chart that works its way
24 down from the cornerstone concept and in fact I guess it is
25 a high level allocation.

1 It is not intended to get down to the individual
2 component or system level. This is to be looked at as
3 fairly high level guidance but the idea is the following,
4 that you have got various initiating events and they have
5 various frequencies associated with them.

6 Some of them are things that you know are going to
7 happen -- loss of offsite power, turbine trips and so forth.
8 They are fairly frequent and then there is the more
9 infrequent initiators, the large LOCAs, the large reactivity
10 insertion accidents and so forth, and then there's the rare
11 events that today aren't included in the design -- the
12 vessel rupture, the steam generator rupture and so forth.

13 You can have a list of those, and you can have an
14 estimate of their frequency and their uncertainty
15 distribution that goes with that frequency.

16 And then you want to look at, for each of those,
17 how does the plant ensure that the core damage frequency and
18 the large early release frequency is met?

19 And the idea is that for the more frequent
20 initiators, you want to be able to have systems in the plant
21 that respond with a high degree of reliability; so that when
22 those things happen, you're assured you still meet your 10-4
23 core damage frequency, and you still have a robust
24 containment that will meet your LERF goals.

25 For the things that occur less frequently, maybe

1 you don't need as much in terms of highly-reliable systems,
2 but the combination of the two still ought to ensure that
3 you meet your core damage frequency goal, and you still want
4 to be sure to have containment with the same degree of
5 protection.

6 And you still have emergency planning out here,
7 for which you get some credit.

8 MR. KRESS: That second line there, does that
9 imply you have different responses to those initiators, for
10 example, shutting down the power or the emergency cooling to
11 prevent core damage? You'd have those same initiators.

12 If you had to have them for the infrequent
13 initiators, you'd have to have them for the more frequent
14 ones also. I don't understand this allocation.

15 MR. HOLAHAN: It may turn out that way, but, in
16 fact, for example, you might find that for large loca you
17 need, you know, low pressure injection, and ECCS
18 accumulators, but for small locas, you only need the high
19 pressure injection system.

20 MR. KRESS: I see what you mean.

21 MR. HOLAHAN: So that says redundancy in high
22 pressure injection is very important, valuable, but
23 redundancy in those other systems may not be so important.

24 MR. APOSTOLAKIS: One comment on this: This would
25 work well for the so-called internal events.

1 Now, if you have an earthquake, and possibly a
2 fire, or any external event that could affect elements of
3 prevention and mitigation, somehow we need to have maybe a
4 different approach and rethink the concept of mitigation
5 versus prevention of those big, common-cause failures.

6 MR. KING: Common-cause failures, yes, how you
7 apply these to common-cause failures, and how to you apply
8 these to something like steam generator tube rupture.

9 MR. APOSTOLAKIS: Although one could apply the
10 same approach to the sequences that are initiated, perhaps,
11 by the fire, for example, and have certain requirements in
12 the initiator frequency, the systems that will mitigate it.

13 But somehow these two dashed-line boxes come
14 together when you have those big --

15 MR. HOLAHAN: I think I agree with you for
16 seismic, but for fire and flood, I think you can deal with
17 these. In fact, more modern plants, and certainly
18 evolutionary and advanced plants have dealt with fire and
19 flood in terms of separation, which allows this to work out
20 very nicely.

21 What we see is that fire protection for older
22 plants, barriers, fire barriers and things like that, are
23 ways of getting isolation, even though it's not as complete
24 as you see in the modern plants.

25 With seismic, everything shakes at the same time,

1 and so you have to deal with that maybe a little
2 differently.

3 MR. GARRICK: An important part of the large scope
4 PRAs were the recovery models that were employed. Does the
5 respond include that?

6 MR. APOSTOLAKIS: Yes. Human recovery actions --

7 MR. GARRICK: Are over on the right.

8 MR. APOSTOLAKIS: -- respond to prevent core
9 damage.

10 MR. GARRICK: Well, also things like recovery of
11 offsite power, recovery of --

12 MR. KING: They're in both of these boxes here.
13 And that's when you go in and look at the --

14 MR. APOSTOLAKIS: Even prevent initiators. An
15 initiator is a complete blackout, and human actions to
16 recover diesels and so on is part of it.

17 MR. HOLAHAN: I think Dr. Kress made a good point
18 this morning. Some of these differentiations are a little
19 bit arbitrary. And whether you say mitigation is mitigation
20 of an initiator, or whether it is mitigation of core damage,
21 you can break this into finer pieces if you like, and so a
22 little bit of it is terminology.

23 MR. KING: The other thing this will help you do
24 is, when you have something like a steam generator tube
25 rupture where you now have lost the containment barrier,

1 you've got some frequency associated with it, and this now
2 becomes one.

3 That tells you I better have some fairly highly
4 reliable systems to be able to deal with that.

5 MR. APOSTOLAKIS: So the message you are sending
6 here, Tom, is that one cannot really have goals
7 independently of the accident sequence.

8 And what really matters here is really what you
9 have there, the basis.

10 MR. HOLAHAN: And defense-in-depth --

11 MR. APOSTOLAKIS: And the allocation issue,
12 depending on reality, on preferences --

13 MR. HOLAHAN: And defense-in-depth doesn't mean
14 equal allocation among cornerstones or defense levels. But
15 it means you don't skip them.

16 MR. APOSTOLAKIS: And even there is a seismic
17 issue that maybe doesn't even allow you to do this, right?
18 So depending on the sequences --

19 Now, why on the performance indicators that the
20 oversight process uses, sequence or site-specific?

21 MR. HOLAHAN: Are they are aren't they?

22 MR. APOSTOLAKIS: Why aren't they?

23 MR. HOLAHAN: Oh, they are.

24 MR. APOSTOLAKIS: They are not.

25 MR. KING: The data is site-specific. The

1 indicators and the thresholds are generic right now.

2 MR. APOSTOLAKIS: Yes. The thresholds are
3 generic.

4 MR. HOLAHAN: The thresholds are generic.

5 MR. APOSTOLAKIS: Would it be consistent with this
6 approach to have site-specific thresholds?

7 MR. HOLAHAN: Well, I think that just -- that
8 would be nice, but it's complicated. What we've committed
9 to is, in the process where there are inspection findings or
10 events, we will use as part of this process, what's called
11 the significance determination process.

12 MR. APOSTOLAKIS: Yes.

13 MR. HOLAHAN: And we've committed to that process
14 basically being site-specific.

15 MR. APOSTOLAKIS: But isn't it true that in the
16 maintenance rule, the licensees themselves set the goals?

17 MR. HOLAHAN: Yes.

18 MR. APOSTOLAKIS: Why can't we ask the licensees
19 to set goals for their plants for each of the performance
20 indicators? What's different? Why can't we do it? Somehow
21 we are scared of it.

22 And then we review it and say fine, or we say
23 change this and that, and let them do the work. You don't
24 want to do that for 140 units.

25 MR. HOLAHAN: Well, we did it once.

1 MR. APOSTOLAKIS: Well, in fact, why don't you
2 build on the maintenance rule, and say, you know, for a San
3 Onofre, this is what they're using now for the trains, and
4 San Onofre can --

5 MR. HOLAHAN: I'm not sure that that level of
6 refinement is really --

7 MR. KRESS: I don't think you can justify that
8 level of refinement.

9 MR. APOSTOLAKIS: I think you can.

10 MR. HOLAHAN: If you think of the scarcity of
11 data, if a reactor has, you know, four reactor scrams in the
12 same year, whether it's this type of reactor or that type of
13 reactor, or something, you know, something funny is going
14 on.

15 MR. APOSTOLAKIS: I'm willing to grant you that,
16 yes, for several indicators, probably a generic number would
17 be good enough.

18 But what I'm questioning is the philosophical
19 approach. I mean, this is really great.

20 But when it comes down to actually regulating and
21 interacting with the licensees, we are switching and going
22 to generic numbers as a starting point.

23 MR. KRESS: This thing comes very, very close to
24 what I had in mind by the allocation process as meaning the
25 defense-in-depth.

1 Let me ask you a strange questions, Gary: That
2 fourth box up there, emergency planning and response, with
3 the .1, if that box wasn't there, and you still had to meet
4 a safety goal that was early fatalities, your LERF would
5 simply be 10-6 instead of 10-5, I think , because that .1 is
6 about the mitigation you get.

7 MR. HOLAHAN: Yes.

8 MR. KRESS: Do you think all of the plants out
9 there could, at their present time, meet a LERF of that
10 value?

11 MR. HOLAHAN: This is a side discussion that Tom
12 and I had this morning while the discussion was going on. I
13 think it came during Bob Bernero's presentation.

14 MR. KRESS: Yes.

15 MR. HOLAHAN: In general, most of the studies
16 we've seen -- and you've got to recognize that there is
17 completeness and uncertainties and all those sorts of
18 issues.

19 Most studies show that current generations of
20 plants meet the safety goal. That's a little bit of a funny
21 thing to say since we don't have a safety goal for each
22 plant, but if you extend the concept, they meet it. And
23 they usually meet it by a factor of more than 10.

24 So I would think that if you took out a factor of
25 10 or 20, which is not unusual, right, for a credit in

1 evacuation, you would be close. Whether it would exceed the
2 safety goal, maybe not on paper, but in reality, it would be
3 close enough so that maybe you would say you couldn't -- you
4 don't really know, right? That's about as close as I could
5 get.

6 MR. KING: The assumptions that went into NUREG
7 1150 where they actually modeled emergency planning, they
8 were based upon looking at some historical information,
9 chemical spills and so forth, how long did it take to move
10 people.

11 And they assumed some lag time from the time the
12 accident started and you notified people, till they actually
13 moved. And people moved at a pretty slow rate, and they
14 assumed 95 percent effectiveness of the evacuation. They
15 didn't assume everybody got out.

16 And then you see the resulting QHO numbers that
17 came out of that.

18 MR. HOLAHAN: And basically, if I remember them
19 correctly, Tom, and you would know better than I do, my
20 recollection is that if you moved, you didn't get a lethal
21 dose, right?

22 I mean, if there were any fatalities, it came from
23 those left behind, not from some fraction of the people that
24 moved.

25 MR. BERNERO: I'd like to go back. This is long

1 ago, and the Sandia siting study in the early 80s had the
2 large early release PWR-1 or BWR-1 release postulated, and
3 then looked at all the sites that were proposed or actually
4 selected.

5 And my recollection is that the site remoteness
6 and meteorology alone gave you, without -- and I don't
7 remember what the modeling of emergency response was, if any
8 -- but it gave you .1 for all sites but Limerick, Indian
9 Point I, and Zion.

10 MR. APOSTOLAKIS: But wait. I thought the safety
11 goal said that you postulate the individual is just outside
12 the boundary.

13 MR. HOLAHAN: No, it's the average.

14 MR. APOSTOLAKIS: So it doesn't matter how far you
15 are.

16 MR. BERNERO: What I'm saying is, is there
17 defense-in-depth that comes from site remoteness?

18 MR. APOSTOLAKIS: No. The way we're calculating
19 the risk now, no.

20 MR. KRESS: If you had a societal goal.

21 MR. APOSTOLAKIS: If you had a societal goal --

22 MR. BERNERO: I'm not talking about goals; I'm
23 talking about actuality. Right there, there is a box,
24 Emergency Planning and Response, and it says .1, .1, and
25 that is the defense-in-depth factor or share that is

1 provided by emergency planning and response.

2 And what I vaguely recollect is that there was a
3 calculation that said the site, the remoteness and the
4 meteorology are such that the typical reactor site provides
5 you .05 or something like that, and only Limerick was .25 or
6 something.

7 MR. GARRICK: Well, another study that I recall
8 indicates something when there was all this debate about the
9 exclusion zone and what it should be and what was the
10 technical basis for the 10-mile, of which there wasn't one,
11 some analyses were done, and it turned out that on a couple
12 of plant-specific cases that some 95 percent of the acute
13 fatalities occurred within a mile and a half of the site.

14 MR. HOLAHAN: There is also a quirk in the way
15 that these are calculated, and I think Dr. Kress, you had an
16 ACRS staff member do some calculations not so long ago.

17 And every one of these calculations basically
18 shows that the value is .06, which means a 1/16th sector
19 around the plant, and it's driven by a modeling of where
20 does the plume go and who gets affected and who doesn't.

21 MR. KRESS: Right.

22 MR. HOLAHAN: So, it's a little bit of an odd
23 issue.

24 MR. APOSTOLAKIS: Go ahead. You've given me an
25 idea for now. I think you should make the last column 1.

1 MR. KRESS: That was the suggestion that I made
2 this morning.

3 MR. APOSTOLAKIS: Because you're supposed to
4 postulate that that individual is at the perimeter of the
5 site. So emergency planning should have nothing to do with
6 risk calculations.

7 MR. KRESS: That was the suggestion I made this
8 morning.

9 MR. HOLAHAN: That's not a PRA.

10 MR. KRESS: That's a --

11 MR. APOSTOLAKIS: You're saying, I don't care
12 whether you evacuate.

13 MR. HOLAHAN: That's not a PRA.

14 MR. APOSTOLAKIS: The Commission says, put this
15 guy there, and tell me what is the probability of death.

16 So we want it both ways. We don't want to have a
17 societal health objective, but we want to take advantage of
18 it.

19 MR. KING: The meteorology still affects that.

20 MR. HOLAHAN: Those are PRA numbers.

21 MR. APOSTOLAKIS: But it's the way PRA calculates.
22 PRA takes the actual population, divides by the number.

23 MR. KRESS: George is saying we need other risk
24 acceptance criteria besides the --

25 MR. APOSTOLAKIS: How can evacuation affect

1 individual risk?

2 MR. HOLAHAN: It' can't.

3 MR. APOSTOLAKIS: It can't.

4 MR. HOLAHAN: You can't evacuate 95 percent.

5 MR. KRESS: In reality, we do have implied other
6 risk acceptance criteria, and one of them is involved in
7 that.

8 MR. APOSTOLAKIS: I think we should rethink this
9 .1, without individual risk.

10 MR. HOLAHAN: The problem is that you can't
11 evacuate 95 percent of a person.

12 MR. APOSTOLAKIS: That's correct.

13 MR. HOLAHAN: They're either there or they're not.

14 MR. APOSTOLAKIS: If you read the statement from
15 the Commission, it very clearly says person within one mile.
16 You can't say I have an average in one mile.

17 MR. HOLAHAN: Well, average.

18 MR. APOSTOLAKIS: The definition of the individual
19 risk is the probability of death of a postulated individual
20 someplace. But somehow it has been modified over the years.

21 MR. BERNERO: It's a one-mile annulus.

22 MR. HOLAHAN: Yes.

23 MR. BERNERO: The point I'm concerned about is, if
24 what is looking for a balance between prevention and
25 mitigation, considering the cornerstones; that there is a

1 part of the emergency planning and response cornerstone that
2 comes from just being there in Lower Alloways Township, New
3 Jersey or wherever the plant is, that even if you said you
4 don't have to have emergency planning anymore, or we'll just
5 give you a telephone call and do the best you can, that
6 there is a level of mitigation that comes from siting
7 remoteness and low population.

8 MR. HOLAHAN: Yes, I mean, that's true.

9 MR. BERNERO: And in the future, that could
10 change.

11 MR. HOLAHAN: Yes. As a matter of fact, my
12 recollection is the study done by Rick Sherry showed that
13 the safest site in the country was St. Lucy, and it had
14 nothing to do with the population; it had to do with it
15 being on the ocean and which way the wind blew.

16 MR. BUDNITZ: I have two comments about
17 earthquakes, and they're really very different, and you have
18 to listen to them both.

19 The first is that, for sure, the very large
20 earthquake -- we're talking about the earthquakes that cause
21 trouble for plants, which are much bigger than any
22 earthquakes we've even had in California. They're very
23 large earthquakes, and I hope everybody understands that.

24 The earthquakes at any site, not just California
25 sites, that are bigger than the 1906 San Francisco

1 earthquake, that magnitude, they're very large earthquakes.

2 And for sure, that last column has got to be one
3 for those earthquakes. You can't count on evacuation for
4 them, so you have to be very careful for earthquakes, what
5 you do there, and be sure not to be optimistic.

6 The second point, and this is from the PRAs:

7 If you look at the LERFs from the seismic PRAs --
8 and I have probably studied that more than most of the
9 people in this room, and I plead guilty to that -- they come
10 from two kinds of things:

11 Part of it comes from very large earthquakes, you
12 know, really, real large earthquakes where it basically
13 knocks almost everything out, you know, all -- enough is
14 knocked out so that -- and, by the way, some are
15 recoverable, but it's just that things break.

16 And those are, you know, these real rare events.
17 But there's another piece; there is a piece where I will
18 call -- they're not 10-6 earthquakes, they're 10-3 or 10-4
19 earthquakes. They're still infrequent, but they're not 10-6
20 earthquakes, in which you get a 10-3 or 10-4 earthquake, and
21 what causes it is the failure of something else.

22 If there are two failures of something else, some
23 of them are non-seismic failures. For example, and a
24 crucial one, is non-seismic failures of containment
25 isolation, and the second is, seismic containment isolation,

1 all right?

2 That seismic loss of containment isolation leads
3 to the LERF, because you're open, and you know you have your
4 core melt, but you're -- so in order to make sure that that
5 was not a big, big concern, in the IPEEE -- I'm proud of
6 having been part of making sure that got done -- we -- and I
7 was here helping the staff at the time --

8 We wrote guidance to make sure that every plant
9 did a specific evaluation of the seismic capacity of
10 containment isolation. Does everybody remember?

11 That was the one thing we asked them to do in
12 containment, separate from the rest. And to our delight,
13 actually, the seismic capacity experts who were telling us
14 this, told us that, but, you know, it was very strong.

15 What we found wasn't a single plant in which that
16 was a problem. That is containment isolation, the valves,
17 you know, they turned out to be extremely robust.

18 People were telling us that, but we found it.
19 Nobody -- no plant that I can remember found a seismic leak
20 of containment isolation capacity.

21 And that then provides you with the additional
22 confidence that for those infrequent initiators, the
23 contained fission product, you know, isn't really what I
24 will call the common cause part.

25 There is still the other part, you know, which is

1 that earthquake you've got going by the earthquake, but then
2 the rest of it is an accident, you know, just the usual
3 stuff that happens in an accident -- the fact that the
4 earthquake occurred 12 hours ago isn't really what's driving
5 the rest of that.

6 So that .1, you know, for the contained, is
7 because of the rest of it, not because of the earthquake,
8 and that's a very important thing that we've learned from
9 these analyses.

10 MR. HOLAHAN: There is an analogous thing in fires
11 that we've found; that the risks are either driven by the
12 very big fire, or a smaller fire when other things are out
13 of service for other reasons.

14 MR. BUDNITZ: You mean, a non-fire failure?

15 MR. HOLAHAN: Yes, right. Now, for CDF, as
16 opposed to LERF, about half of the seismic CDFs are seismic
17 and non-seismic combinations, and the other half are all
18 seismic.

19 But for LERF, they're dominated by something else;
20 for LERF, they're dominated by these large, all-seismic
21 failures, and some of it is seismic -- is random failures of
22 containment isolation.

23 MR. APOSTOLAKIS: Just to move on, how can we
24 convey the thought that when we say .1, we really don't mean
25 .1? It's not a speed limit.

1 MR. KING: These are guidelines. I mean, this is
2 not intended to be a risk-based application.

3 MR. APOSTOLAKIS: I understand that. But if it
4 really has an excellent containment, modern and so on, and
5 they say, look, mine is really .4, would you let them raise
6 the 10-4 to 10-3 in response to core damage?

7 Is an order of magnitude too much, in other words?

8 MR. HOLAHAN: The answer is no. Give me a harder
9 question.

10 [Laughter.]

11 MR. APOSTOLAKIS: I don't know why you would say
12 no. I mean, one in a thousand is not --

13 MR. HOLAHAN: For core melt?

14 MR. APOSTOLAKIS: I think that comes back to the
15 discussion this morning that it's not just that you're
16 trying to optimize, you really don't want to see core
17 damage.

18 MR. HOLAHAN: Right, exactly. Yes.

19 MR. KRESS: There is some floor on core damage.

20 MR. APOSTOLAKIS: How do we send that message that
21 maybe a factor?

22 MR. HOLAHAN: We have a subsidiary numerical
23 objective of --

24 MR. APOSTOLAKIS: These are supposed to be a
25 means, mean values, right?

1 MR. HOLAHAN: Yes, of 10-4 for core damage
2 frequency, and we have a safety goal that says prevention of
3 core damage is one of our objectives.

4 MR. APOSTOLAKIS: If we put this in a diagram form
5 and put shades of gray --

6 [Laughter.]

7 MR. APOSTOLAKIS: This is really misleading, .1.
8 Actually, we're going to the three-region regulatory scheme
9 where there is an unacceptable region, we talk about between
10 that and the goal, and then it's fine.

11 MR. HOLAHAN: That sounds like a speed limit.

12 MR. APOSTOLAKIS: Variability -- no, for the
13 unacceptability, yes. Oh, I bet they're going to give you a
14 speed limit.

15 Anybody who comes in here with a core damage
16 frequency of 5-10-3, will be arrested. There is a speed
17 limit.

18 MR. GARRICK: Is there a limitation on --

19 MR. HOLAHAN: If the term, arrested, means stop
20 their actions, that's probably correct, yes.

21 Is there a limitation on the distribution, as well
22 as on the mean value?

23 MR. APOSTOLAKIS: Not yet, not yet. They only
24 have the mean value. I know you guys have thought about -

25 MR. HOLAHAN: I think if you let Tom finish the

1 discussion, you'll find out that you're most likely not
2 going to find these numbers in the regulation.

3 MR. APOSTOLAKIS: No, no.

4 MR. KING: These will result in some deterministic
5 requirement.

6 MR. HOLAHAN: Right.

7 MR. KING: The way I envision this will be applied
8 is that you will take each initiator and you go through and
9 you look at, you know, given the system that's there are
10 systems that are there, giving the initiating event,
11 concurrently -- these are sort of aggregate numbers.

12 When you add them all up, you want to make sure
13 you've got the 10-4 CDF -- minus fifth -- LERF, and I
14 wouldn't propose we require each one to meet a tenth of
15 that, so there could be some flexibility.

16 Maybe some would meet it very well, and some would
17 be a little higher. But when you add them all up, you want
18 to have the aggregate come out to the 10-4, 10-5.

19 If you go through and you find out the regulations
20 today don't assure that you can meet these kinds of numbers,
21 that's when I think you come in and start looking at, do I
22 need additional redundancy, diversity, you know, additional
23 QA, additional inservice inspections, inservice testing, EQ,
24 whatever it is to increase the reliability.

25 And that sort of gets to the --

1 MR. HOLAHAN: Before you leave this, I think this
2 is a good exercise. Conceptually, I've gone into this with
3 the expectation that if you look at the way the requirements
4 were written in the first place, if there were credible
5 events, whether it was one a year or one in a million years,
6 we required multiple gold-plated systems to deal with it.

7 The natural consequence of that is, we provided
8 too much protection for the relatively rare events, and not
9 enough protection for the frequent events, okay?

10 And so, you know, my expectation is that when it
11 comes to large loca plus loss of offsite power, and these
12 relatively rare things, you know, we have too many
13 requirements.

14 When you look at things like reactor scram and aux
15 feedwater, you have to make sure that you have enough, okay?

16 And that's generally what I think this is going to
17 -- this sort of analysis is going to lead to.

18 MR. APOSTOLAKIS: I would suggest, Tom, that given
19 the discussion of a few minutes ago, in addition to a goal,
20 given upper limits, I think it's important information.

21 And, again, the upper limit can be interpreted the
22 same way the goal is interpreted, not as a crisp line, but

23 --

24 MR. KING: You mean an upper limit like this?

25 MR. APOSTOLAKIS: No, no, that's on a different

1 quantity. Let's go back to the previous one.

2 MR. KING: That's on the total.

3 MR. APOSTOLAKIS: Like let's you talk about
4 anticipated initiators. My goal is for the event response
5 to prevent core damage of a 10-4 number.

6 But anything above 10-3 is unacceptable, too. Two
7 numbers instead of one, in other words. Because that's the
8 reality today, and I don't see why we can't reflect reality
9 there.

10 And if you have a problem with interpretation of
11 10-3, I suggest you have the same problem with the 10-4. So
12 these numbers should not be interpreted as being absolute
13 speed limits.

14 But at least you send the message, and I think
15 this idea of an acceptable, tolerable, and don't care
16 regions, is a good one.

17 MR. KING: I understand what you're saying. I'm
18 not sure --

19 MR. APOSTOLAKIS: Whether it's 10-3 or something
20 else, I don't know. That's what we just threw out.

21 MR. KING: Clearly, if we were going to apply this
22 in a mandatory fashion to existing plants, what you said
23 would probably have to be done. But remember, this is a
24 voluntary program.

25 MR. APOSTOLAKIS: Sure, but even in a voluntary

1 situation, or even guidelines, it helps to give to
2 guidelines as much as you can, so people know where they
3 stand.

4 I mean, the truth of the matter is that the core
5 damage frequency right now, greater than 10-3 starts also
6 some valid -- management of the attention and so on. And
7 yet we don't say that anywhere, we just act that way.

8 What I'm saying is, why don't we say it someplace?
9 If you have a goal of 10-4 for core damage frequency, but we
10 don't say anywhere, what we really do.

11 What we really do is we allow 19 units to be above
12 the goal and we do nothing, but if anyone comes in here with
13 a calculation that the core damage frequency is greater than
14 10-3, things do happen.

15 MR. KING: Remember what we're trying to do in
16 Option 3; we're trying to come up with some revised
17 regulations and if the plant volunteers to meet those, they
18 will now have to have system structures and components and
19 an operation that does bring them in at 10-4, not 10-3.

20 MR. APOSTOLAKIS: I understand that, but what I'm
21 saying is, you will be giving them a more concrete guidance
22 if you follow that approach, because you're telling them,
23 really what you expect them to do.

24 And that's something to think about, or maybe Joe
25 Murphy can think about it.

1 MR. KRESS: Let me ask one more question about
2 this table. If you look at the conditional containment
3 failure probability line, I contend the lower that number
4 gets, smaller the uncertainty is in the LERF.

5 Do you reach a limit of the uncertainty in the
6 bypass, but you get rid of all the other uncertainties to
7 the failure, early failure in the mode and the location.

8 And if then they got down to a level of .01
9 instead of .1, I think you're near that minimum in
10 uncertainty in the LERF.

11 It seems to me like that's a desirable -- since
12 the defense-in-depth is to deal with uncertainties, unknown
13 and known, it seems to me like having that uncertainty at a
14 minimum level would be a desirable thing to shoot for.

15 MR. KING: I'm not sure why you say the
16 uncertainty would go down. I mean, you still may have a
17 wide band of uncertainty about it, even though it's small.

18 MR. KRESS: It would be minimum. I don't know how
19 big it would be, because you get rid of the uncertainties
20 due to the failure -- design versus failure location, the
21 location of the containment.

22 As that conditional containment failure goes down,
23 it means you've got a bigger, stronger containment with more
24 reliable systems.

25 MR. KING: You get rid of scenarios that lead to

1 failure.

2 MR. KRESS: Get rid of all the scenarios that lead
3 to failure, except the bypass.

4 MR. KING: But the ones that are left, well, if
5 it's just bypass, yes, that --

6 MR. KRESS: Yes, so I'm saying there is some
7 reason to make that number smaller, and that is because it
8 minimizes the uncertainty in LERF.

9 And I don't know if that's -- I just thought I'd
10 throw that out as a concept.

11 MR. KING: I hadn't thought about it.

12 MR. APOSTOLAKIS: Did you say you will think about
13 it?

14 MR. KING: I said I had not thought about that
15 aspect of it.

16 MR. KRESS: That was in my talk this morning.
17 That was the red herring.

18 MR. APOSTOLAKIS: Did you reject my suggestion, or
19 you will think about it?

20 MR. KING: I'll think about it.

21 MR. APOSTOLAKIS: Good.

22 MR. HOLAHAN: I believe he's thinking about it
23 right now.

24 [Laughter.]

25 MR. KING: All right, I think we talked about most

1 of this. We would use mean values.

2 In the table we show that numbers is associated
3 with full power, but we'd also apply this similar concept to
4 the shutdown condition as well.

5 And then my last slide, okay, what do we do with
6 this working definition? As I said, the idea was to take
7 each initiating event and follow it through to see if you
8 can meet those risk goals or what you need to do to meet the
9 risk goals.

10 We're also going to take a top-down look where you
11 take these four cornerstones and line up today, what's in
12 the regulations, Reg Guides, SRPs, under each of those and
13 take a look at the balance in terms of there are probably a
14 lot of things that affect reliability and availability and
15 redundancy and diversity of systems to respond to initiating
16 events.

17 Do we need similar types of requirements when you
18 talk about containment? Is there more we should do under
19 prevention? What's the balance when you come down
20 vertically at each of the cornerstones?

21 So, that's sort of the concept that we're going to
22 apply in the application of that table.

23 Again, I just want to say that in terms of wrapup,
24 what we're talking about this is the basis for looking at
25 the regulations. We're not talking about putting these

1 numbers into regulations; we're talking about using these to
2 come up with some change in the deterministic requirements.

3 And we're not talking about putting in the
4 regulations, a rule or a definition of defense-in-depth. I
5 think it's a philosophy behind everything that's going to
6 end up going into the rules.

7 MR. KRESS: I think the table itself is almost a
8 definition.

9 MR. APOSTOLAKIS: Yes. Okay.

10 MR. KRESS: I like the approach myself. It's
11 pretty much what I was advocating this morning, I think.

12 MR. APOSTOLAKIS: This is the pragmatic approach.
13 Very good.

14 MR. KRESS: Very good. We appreciate that very
15 much.

16 MR. APOSTOLAKIS: Based on what we saw today, it's
17 very good.

18 MR. KRESS: I don't know how we'll apply that to
19 Yucca Mountain, but --

20 MR. APOSTOLAKIS: The staff refuses to take it
21 seriously, but maybe one of these years.

22 MR. KRESS: Well, it's a way to handle
23 uncertainty. I'm not sure how we apply this to Yucca
24 Mountain, but --

25 MR. APOSTOLAKIS: I think it's a different beast.

1 MR. KRESS: I think it is, too.

2 MR. APOSTOLAKIS: I think the fundamental
3 difference is time, the time scale.

4 MR. KRESS: We're due for another break. Does
5 anybody need one?

6 MR. APOSTOLAKIS: Yes, we do.

7 MR. KRESS: Another 15-minute break.

8 [Recess.]

9 MR. KRESS: The next item on the agenda is to hear
10 some words from the NEI and the industry, and from
11 Westinghouse, so I'll turn the floor over to you, Alex, and
12 let you introduce the subject and introduce the people.

13 MR. MARION: Good afternoon. My name is Alex
14 Marion, and I'm the Director of Programs at the Nuclear
15 Energy Institute. I recognize the time is late, but I do
16 have a few brief comments to talk about some of the things I
17 heard today relative to the application of defense-in-depth
18 philosophy to operating plants.

19 But I would like to introduce Rodney McCollum, who
20 is the Project Manager at NEI involved with high level waste
21 management, and he has a few comments he would like to make
22 on the application of that philosophy to the Yucca Mountain
23 Project.

24 Rodney?

25 MR. MCCOLLUM: Do you want me to go ahead and do

1 that first?

2 MR. MARION: Yes, please.

3 MR. McCOLLUM: I've been working for NEI now for a
4 little more than a year, specifically to follow Yucca
5 Mountain and related issues, so I have been attending
6 meetings such as this one, and hearing discussions such as I
7 heard today for most of that time.

8 I always find these discussions very interesting
9 and very intellectually challenging. I think this one was
10 definitely no exception and perhaps even a little bit too
11 much so on the intellectually challenging part, but that's
12 how I learn things.

13 I also feel it's a very important discussion, and
14 it's certainly a very timely discussion because the nation
15 is entering into a critical window of decisionmaking
16 opportunity here where over the next 18 months, our leaders
17 are going to be called upon to make a decision about the
18 future of Yucca Mountain.

19 And one of the things that will weigh most heavily
20 in that decisionmaking process is the topic of uncertainty
21 that's been discussed a lot today.

22 How will the decisionmakers, relying on the
23 Nuclear Regulatory Commission, the ACNW, the TRB, and all of
24 the political forces that come to bear, how will they view
25 uncertainty?

1 And uncertainties will exist; that's really the
2 only thing that is certain. In fact, if it's good enough
3 science, every answer will simply generate more questions,
4 it will bring up more uncertainties.

5 And, therefore, because these uncertainties will
6 inevitably exist, the decisionmakers need to have some tools
7 in place that will allow them to address this.

8 And we firmly believe that the DOE, in the
9 viability assessment, and the NRC in the draft Part 63, is
10 giving them these tools. We feel that in referring to what
11 Christiana was talking about earlier, the way multiple
12 barriers are being interpreted, that it is a qualitative and
13 not a quantitative argument, and that it should be up to DOE
14 to make the safety case. We feel that's appropriate.

15 We are concerned to the extent to which at this
16 point, having seen what's been done by both the DOE and the
17 NRC staff to develop those tools, what could be gained by
18 inserting knowledge on the reactor side from the reactor
19 notion of defense-in-depth into the repository process?

20 We've had a lot of discussions along this line
21 with our friends in EPRI included, and perhaps the best way
22 for me to relate what might happen if we were to bring these
23 things in is:

24 I, once a upon a time, was a Branch Chief of
25 Nuclear Safety for a DOE operations office that had

1 responsibility for a lot of very unique, one-of-a-kind,
2 non-reactor nuclear facilities. We had a couple small
3 reactors. This was the Chicago operations office so we're
4 talking about the Brookhaven's, the Argon's , the
5 Princeton's, et cetera.

6 And I was in that position at a time when DOE was
7 coming out of its post-Cold War cocoon of beginning to
8 realize that it needed to have some credible nuclear safety
9 requirements, a regulatory structure in place that it didn't
10 have before when it simply did what it knew was right or
11 thought was right.

12 And doing so, they naturally looked to the best
13 source of expertise for that kind of a regulatory structure,
14 and that was the NRC. So the DOE made a lot of requirements
15 that were first under the guise of DOE orders, and later
16 became -- a couple of them became rules, DOE rules, that
17 basically took NRC regs that were intended for the reactor
18 world, and put DOE order numbers on them and they were to be
19 applied to these non-reactor nuclear facilities.

20 Once that happened, I found myself spending a lot
21 of time trying to fit square pegs into round holes, and
22 trying to explain why the square pegs wouldn't go in the
23 round holes. That they just don't fit, never quite seem to
24 be enough of an answer.

25 I saw a lot of effort being made at the five

1 National Laboratories to address all those misfitting pegs
2 that didn't contribute to their safety cases, and, in fact,
3 just detracted from it.

4 I was very appreciative to hear what Dr. Garrick
5 said earlier about arbitrary thresholds and subsystem
6 requirements that detract focus from risk. I know from
7 experience that that that does, indeed, happen.

8 And I think we have a pretty similar situation
9 here with Yucca Mountain, because Yucca Mountain would be a
10 very unique, one-of-a-kind, non-reactor nuclear facility.

11 I think that the differences between Yucca
12 Mountain and reactors are so fundamental, it really becomes
13 almost impossible to try and draw from reactor
14 defense-in-depth to multiple barriers in the repository
15 site.

16 A couple of those things have been mentioned, a
17 couple of others, I would mention: Of course, obviously you
18 have more active and passive barriers at Yucca Mountain,
19 whereas you have more active, engineered and more engineered
20 features at a reactor.

21 Yucca Mountain has one common failure mode,
22 really, a two-part failure mode. It's water and time. And
23 it's really a question of where you are on the radioactive
24 decay curve when those things attack each of your barriers.

25 There are different timeframes to be considered.

1 In reactors, fractions of a second can be important; in
2 repositories, millennia are what's important.

3 You have a safety case in reactors where you're
4 trying to figure out where to best apply PRA; in a
5 repository, your safety case is a PRA.

6 You rely on humans to operate reactors; your
7 expectation for the repository is that once you seal it up,
8 except for potential human intrusion, humans won't be
9 involved at all.

10 And probably the most important distinction that
11 allows you to treat uncertainty in a fundamentally different
12 way at a repository would be that you have this performance
13 confirmation period. You have not a two, but a three-stage
14 licensing process.

15 And this is a 50-year period where you have a
16 chance to constructively address those what-if-we-were-wrong
17 questions.

18 You don't have that at a reactor, and I don't
19 think any utility would want that, although some time felt
20 they were approaching that.

21 But it does give you an opportunity, and it does
22 give the decisionmakers to say, when they are faced with
23 uncertainties, that here's what we know, and here's what
24 what we know tells us, and then here's what we need to know
25 before we close the thing, and put in place the right

1 research program that can answer those questions.

2 But you can't do that in the reactor world. So,
3 given that, and having heard the discussions -- and this is
4 another one of the things we appreciate where the staff is
5 going with multiple barriers. I was very thankful to see
6 Christiana's presentation entitled Multiple Barriers and not
7 defense-in-depth.

8 We wonder -- and this is kind of the conclusion of
9 the discussions we had internally -- whether
10 defense-in-depth is even an appropriate term; whether it
11 would be more appropriate to call what you're doing at Yucca
12 Mountain multiple barriers and call what you're doing in the
13 reactor world, defense-in-depth, and not even try to mix the
14 terminology.

15 It could only lead to a confusion in expectations,
16 and as I mentioned before, you know, we think the
17 expectations are evolving well for Yucca Mountain. We think
18 that Part 63 will answer that.

19 We think that from what we've seen at EA, and from
20 DOE's draft Environmental Impact Statement, they'll be able
21 to say that when, you know, the final dose, if it's 1.3
22 millirems, 10,000 years from now or whatever it is, that
23 that dose is a function of a performance assessment that
24 includes a dry climate and includes a thousand feet of rock
25 to keep the water out of the repository.

1 It includes a lot of things in the repository,
2 some of which are engineered, and includes another thousand
3 feet between the repository and the water, and it includes
4 things in the water that retard the movement of
5 radionuclides.

6 And it includes a sparsely populated area that
7 keeps people away from even those moving radionuclides.
8 And, of course, the D0e will have looked at a certain amount
9 of variations and been cautious and reasonable in looking at
10 each one of those barriers. It will assume a somewhat
11 wetter climate. It won't take credit for the features of
12 the rocks that it doesn't understand as well as it
13 understands some others.

14 When I visit the folks -- and in the year, I've
15 had three tours of Yucca Mountain now, and I talked to the
16 scientists in the tunnels and hear them talk. I appreciate
17 what Dr. Levinson mentioned about some uncertainties are not
18 bad.

19 They are tending to find out things about the
20 rocks that are good news. And they will do that during the
21 performance confirmation period.

22 But based on what they know, they can make a case
23 that that 1.3 millirems or 13.2 millirems, or whatever
24 number it is less than 15 or 25, is a function of a number
25 of things. And those things all contribute to it.

1 And in that respect, it need not be much more
2 complicated than that. They will have then answered what
3 Congress has asked for in terms of multiple barriers, and
4 the NRC can and should, in accordance with its regulations,
5 look very hard at that and make sure it's credible, that
6 it's believable before the Commission says to the
7 decisionmakers, we think this is sufficient, which is the
8 sufficiency comment component of the site recommendation.

9 Then we go on to the next stages in the process,
10 and we continue to look at it, realizing that the scientists
11 will never stop asking questions, and that every one of
12 those questions will bring into the proces, more
13 uncertainties, and that's not a bad thing.

14 So, you know, I'm very encouraged that these
15 discussions are occurring, and I learned a lot from them,
16 and look forward to this going forward.

17 MR. MARION: Are there any questions of Rodney
18 before I make a couple of comments?

19 MR. APOSTOLAKIS: I don't so much have a problem
20 with the regulations, the way Christiana presented them.
21 It's really the quality of the performance assessment that
22 would be of concern to me, given the time scales we're
23 talking about and the uncertainties that are involved.

24 And I still don't believe that the model
25 uncertainties are completely addressed. Even in WHIP, you

1 know, there was primarily parameter uncertainties. At one
2 point they had two different models for something relatively
3 minor. I don't remember what it was.

4 They said, okay, we'll put a weighting factor of
5 1/3 to this, and 2/3 to the other, and just add them up.
6 But I think the uncertainty is a key issue here.

7 MR. MCCOLLUM: Oh, they clearly are. As I
8 mentioned, they'll be the major thing weighing on the
9 decisionmakers.

10 And that is why, in demonstrating multiple
11 barriers, DOE needs to talk about what each of those
12 barriers mean to the safety case, and what is the meaning of
13 those uncertainties?

14 And they're starting. And every time I have heard
15 DOE present on this subject now, dozens of time, and the
16 story gets better every time, that the science was always
17 there, I believe. It's been there since the VA.

18 But it's being able to talk, and it can't be
19 completely quantified. It shouldn't be. But to be able to
20 talk about the relative importance, what does that
21 uncertainty mean, what if the climate does get wetter? Have
22 we looked at that?

23 Have we been appropriately cautious in what we've
24 assumed the rocks do for us, and what we've assumed the
25 rocks don't do for us?

1 And so that if some of those uncertainties turn
2 out to be bad, are there offsetting things? And it's really
3 going to be a challenge in the next 18 months when we have
4 this decision before us, for that to be discussed.

5 And I have also heard Dr. Garrick talk a lot about
6 plain english, and that's why that's so important. Because
7 those things may be buried in the performance assessment in
8 any number of ways, but if we can't bring them out and
9 discuss them in plain english so people understand that
10 that's what this means, that's what that means.

11 And because we know what all these things mean to
12 the safety case, we can say this is a good place for a
13 repository or not. And we can make a decision.

14 MR. GARRICK: George, I think that the Committee
15 kind of shares the concern for the TSPA. We know that in
16 the early days of the PA for WHIP, there were many, many
17 problems, and through another Committee, I was directly
18 involved in that.

19 And I saw a major change. The big difference
20 there over Yucca Mountain is that except for human
21 intrusion, there was geologic containment at WHIP.

22 And the only way WHIP could get in trouble was
23 through some rather arbitrary human intrusion scenarios. Of
24 course, we don't have that luxury on Yucca Mountain.

25 MR. APOSTOLAKIS: Right. The other thing that we

1 did that you guys may find disturbing is that later on, I
2 believe, 60 hypercube simulations. All 60 of them were
3 below the goal, which brings us back to your comment, what
4 if it is 5X?

5 What if Yucca Mountain, 58 of them are below and
6 two are above? That will create an interesting
7 interpretation of the regulations.

8 And why should all 60 be below? Just because it
9 happened there?

10 Now if you think of the state of knowledge on
11 uncertainty, the whole distribution is below -- I mean, the
12 two high percentile, so that -- anyway, these are not
13 directly related to the subject matter.

14 MR. GARRICK: It's a good comment.

15 MR. MARION: Thank you. I'd like to make a couple
16 of comments about the operating reactor side.

17 I found Dr. Murley's comments this morning kind of
18 interesting. Having worked at a nuclear utility for 15
19 years, it sure felt like defense-in-depth was a regulatory
20 requirement at times.

21 [Laughter.]

22 MR. MARION: But I decided not to challenge it.

23 MR. APOSTOLAKIS: It was a voluntary requirement.
24 We have a lot of those.

25 MR. MARION: But I thought he made an interesting

1 comment about -- or a caution, I should say, as I
2 interpreted it, about applying risk insights to remove or
3 otherwise eliminate barriers.

4 I think we need to be very careful, and I think
5 that's an appropriate cautionary statement. However, I
6 think with risk insights and operating experience, we can
7 better define what's important in the implementation of the
8 very elements, specific elements of those various barriers
9 of protection, specifically in the area of emergency
10 planning.

11 I believe we're very close to the point of
12 providing a case to reduce the exclusion zone, based upon
13 the robustness of the designs, as well as the analysis
14 supporting the advanced reactors.

15 And there are opportunities. We're not offering
16 to get rid of emergency planning as a concept, but better
17 define it with the latest intelligence and knowledge base we
18 have.

19 And I think that's consistent with the comment
20 that Dr. Budnitz made about the evolution of knowledge to
21 better focus on barriers of protection, integrating
22 operating experience and new analytical techniques.

23 And I think we need to keep that in mind and take
24 advantage of those kinds of opportunities when they present
25 themselves.

1 I think the example that Dr. Apostolakis used on
2 the fire analysis and the element of smoke and uncertainty
3 associated with it is an excellent one in terms of applying
4 an engineered approach to address uncertainties.

5 And then when knowledge comes to bear and the
6 analytical techniques improve to better reduce the
7 uncertainty in the area of smoke propagation, et cetera,
8 then you can make adjustments along the way.

9 And I think those were excellent examples, and
10 we're in full agreement with those concepts and processes.
11 And in NRC staff's presentation this afternoon, I was
12 sitting back there with Biff Bradley's, the project manager
13 at NEI directly involved in risk-informing Part 50 and these
14 PRA risk insights, applications, et cetera.

15 And he indicated to me that we're in full
16 agreement with the approaches. And I think, between the
17 industry and the NRC, we're in a good position where we
18 understand the importance of striking a balance between the
19 deterministic thinking that's made this industry very
20 successful within the defense-in-depth philosophy, and
21 applying that in some balanced way with probabilistic
22 techniques and approaches that we have today.

23 And from what everybody tells me, things are going
24 well in terms of the applications of risk-informed
25 regulations, but we do have a lot of work ahead of us.

1 And I just want to caution everybody that we want
2 to be careful not to limit our thinking or limit our
3 approaches such that when new knowledge or when new
4 analytical techniques come to bear at some time in the
5 future, we can still take advantage of those and improve our
6 knowledge and understanding.

7 This is the defense-in-depth philosophy balanced
8 with risk-informed approaches, and is very fundamental to
9 our thinking for regulatory reform, more specifically in the
10 area of risk-informing the Part 50 regulations.

11 So we think it's very important to work
12 hand-in-hand, shoulder-to-shoulder, so to speak, in a
13 complementary way with the NRC staff, and to strike this
14 balance and determine what we need to do with future
15 applications of the current state of knowledge.

16 And that completes the comments that I have. Are
17 there any questions about anything I said about operating
18 plants, or that Rodney said?

19 [No response.]

20 MR. MARION: Okay, with that, I'd like to
21 introduce Gary Vine from EPRI, who is going to take a few
22 minutes and provide you with a general overview of the
23 defense-in-depth philosophy as it was applied in the design
24 requirements for advanced reactors.

25 I think you will find that informative and

1 beneficial. And he will be followed by Brian McIntyre from
2 Westinghouse, who is going to specifically discuss the
3 application of that philosophy in the AP-600 designs.

4 MR. APOSTOLAKIS: One of the victims of
5 defense-in-depth.

6 MR. MARION: We were going to bring that up a
7 little later, Dr. Apostolakis.

8 MR. APOSTOLAKIS: Perhaps the only one still
9 alive.

10 [Laughter.]

11 MR. APOSTOLAKIS: While these are getting settled,
12 somebody said this morning that there may be a perception
13 out there that we're using risk-informed regulatory
14 approaches to remove barriers, to remove regulations and
15 requirements.

16 I think it's important to say that where PRA
17 indicated that additional requirements were needed, the
18 Agency acted immediately. And in the last 20 years, in
19 fact, the eagerness of the Agency to add requirements based
20 on PRA insights created a somewhat hostile view within the
21 industry towards PRA, because PRA was used only to add
22 requirements.

23 So the fact that now we are finally looking at
24 removing some, should not be misconstrued as the Agency
25 using PRA to remove requirements. We have already added a

1 lot, okay. That's in case anybody reads the transcript.

2 MR. KRESS: Thank you, George, I think that was
3 well said.

4 MR. VINE: Good afternoon. I'm going to start
5 off. My name is Gary Vine. I'm from EPRI. Unfortunately,
6 I didn't have the benefit that Alex and Rodney and Brian did
7 of all the prior discussions. I got here about 4:00 from
8 another meeting in Tower I.

9 But Alex does tell me that a number of the points
10 that I intended to cover have been covered in some way, and
11 so I'm going to try to focus only on either new material or
12 kind of an industry perspective on some of the things you
13 have heard from the NRC side.

14 I'm going to probably skip over the first slide or
15 two. The only key point on the first slide is simply that
16 we did in the ALWR program, which goes back 10-15 years now,
17 fully embrace the concept of defense-in-depth.

18 And we did that in a traditional way. I think we
19 didn't use the terms that you've been discussing today,
20 structuralist and rationalist models, but we pretty much
21 followed the traditional structuralist approach.

22 I also have a slide on ALWR policy statements, and
23 I intended to go through two or three of them in some
24 detail, and I'm going to skip that as well.

25 I have a high-level brochure document that

1 provides a two- or three-sentence description of each of
2 these policies, some of which have a bearing on
3 defense-in-depth, and I'll just leave that for you to look
4 at.

5 Moving on to Slide 4, just a couple of key points:
6 It's very important to recognize that public health and
7 safety is important to both the NRC and to the
8 owner/operator of a plant. In fact, the owner/operator has
9 the primary responsibility of protecting public health and
10 safety.

11 So his interest in safety is just as high as that
12 of the regulatory. Where the difference lies in the way we
13 fundamentally approached establishing design requirements
14 for advanced reactors is in the investment protection side.

15 That is where the industry has an equally high
16 interest in preserving their investment. But the NRC
17 doesn't have a comparable interest.

18 And so what that forced us to do was to make a lot
19 of tradeoffs as we were trying to optimize prevention
20 mitigation decisionmaking where the industry's interest was
21 naturally always to achieve safety as early in a sequence as
22 possible.

23 We always wanted to prevent an accident or
24 actually have a robust enough design so that we wouldn't
25 even get into an accident sequence before we had to get into

1 questions of mitigation.

2 We also found when we had a fresh sheet of paper
3 and we could look at these decisions, that almost always --
4 not always, but almost always, when you had a particular
5 sequence you were trying to drive down or improve the safety
6 for and you had a mitigation option and a prevention option
7 to do that with, the prevention option was usually less
8 expensive.

9 So there were a lot of incentives on the industry
10 side to truly tackle areas where we wanted to achieve
11 improved safety by doing it on the prevention side. Of
12 course, this, as you can tell, created some friction between
13 the industry and the NRC, on occasion on certain issues
14 where the thought was that we were maybe not maintaining the
15 proper balance in defense-in-depth.

16 We maintained a strong commitment to mitigation as
17 well. Requirements for containment, for example, are just
18 as strong or stronger for advanced reactors than they are
19 for current plants.

20 But as we pressed to achieve improvements on the
21 prevention side, there came some questions about balance.

22 Explicit consideration of severe accidents via a
23 safety margin basis, that's a very important concept which I
24 think is probably worth some discussion. I think there were
25 some understandings in kind of a process way in the program

1 with the NRC that have stood the test of time.

2 We fundamentally committed to the licensing design
3 basis as it was captured in Part 50. And we did not, with
4 just a very few exceptions, try to make any changes to the
5 regulations.

6 The only example on this schematic where we tried
7 to make some improvements in the regulatory basis in the
8 licensing design basis side was in improving the source term
9 that was analyzed in the licensing case.

10 But we pretty much bought into the entire
11 licensing design basis approach as, quote, the "formal speed
12 limit" for design.

13 But we were very careful in defining very separate
14 and distinct from that licensing design basis, the way we
15 would approach all other safety questions and primarily all
16 questions associated with severe accidents.

17 In this area, there were differences in almost
18 every aspect. We approached it, first of all, from a
19 standpoint of a much more risk-informed evaluation of the
20 plant's overall performance.

21 Second, we insisted that we use best estimate
22 analysis methods, models, and so forth in addressing those
23 issues.

24 Third, we proposed and the NRC accepted, the
25 concept of the industry pretty much driving the specific

1 design approaches to address severe accidents, and get the
2 NRC to provide an overall approval to the approach that we
3 took, as opposed to agreeing on detailed prescriptive
4 requirements that would then become part of the licensing
5 design basis or some formal regulatory requirement for this
6 right side of the equation.

7 So the industry really drove this. We decided how
8 we wanted to satisfy the Commission's concerns about severe
9 accidents, all the research findings, the Commission policy
10 statements and everything else.

11 The NRC then provided an SER on these utility
12 requirements, and then the vendors had a clear picture of
13 how they had to achieve basically what they had to do to
14 know that they would have regulatory approval in this area.

15 There were a number of areas, even though we
16 pretty much approached things in a conventional way with
17 regard to defense-in-depth, where we kind of pushed the
18 envelope, and what I'm going to cover now are some areas
19 where I suppose if you get to the definitions you're using
20 now, where we used a more rationalist model approach or a
21 more risk-informed approach to the way we did business.

22 First of all, let me jump back to Slide -- yes,
23 this is the right slide. I'm sorry.

24 Major alliance on PRA and the process: It drove
25 our side, the industry side, very significantly. We made

1 major plant policy decisions and major plant design
2 decisions based on findings of the PRA.

3 The regulatory side used PRA much more just as a
4 confirmatory tool, as opposed to a decisionmaking tool. One
5 exception which Brian will get into is the way we dealt with
6 the regulatory treatment of non-safety systems for the
7 passive plants.

8 But beyond that, the regulatory side was pretty
9 much a confirmatory process. We established quantitative
10 safety requirements on the industry side that well exceeded
11 the regulatory requirements.

12 And the idea here was that we wanted assured
13 license ability by knowing we had significantly exceeded
14 what the regulatory requirements were going to be in the
15 area of safety.

16 I list our two quantitative safety requirements,
17 and these were requirements; they weren't just targets: The
18 designers had to have a CDF much less than 10^{-5} , and they
19 had to address mitigation by meeting a goal of ensuring that
20 whole-body dose would be less than 25 rem at the site
21 boundary which is about at a half mile as we defined it for
22 all sequences with a cumulative frequency of greater than
23 10^{-6} .

24 You will notice that these two prevention and
25 mitigation goals are not coupled; they are decoupled, which

1 gets to my final point on that slide:

2 We did oppose the concept of coupling these
3 independent layers of defense-in-depth. We opposed the
4 concept of a CCFP. We didn't win that argument, but we do
5 believe that CCFP is not an appropriate means of enforcing a
6 defense-in-depth approach because it couples things that
7 should remain independent.

8 Because one is set by design, you end up forcing
9 the operator or the designer to make less than optimum,
10 sometimes dumb decisions in having to reduce the safety of
11 the plant in order to maintain this spread of a factor of
12 ten between prevention and containment performance.

13 And there are -- you can go through some scenarios
14 down on the low probability events where the imposition of a
15 CCFP becomes even more ridiculous.

16 So we felt that that was an inappropriate approach
17 and still do.

18 Regulatory stabilization: I already mentioned
19 assured licensability by exceeding the regulations wherever
20 feasible. This was an important concept to us, and we've
21 faced some problems in dealing with the NRC on this because
22 we wanted to assure significant and visible and demonstrable
23 margin between the regulatory requirements and actual design
24 performance and operational performance.

25 And there is just a natural tendency on the part

1 of the regulator to say, well, gee, since you're that much
2 better, let's just change the speed limit so we're a lot
3 closer to where you are.

4 Well, that creates huge problems for us, because
5 it eliminates that assured licensability. And so we think
6 that the regulatory requirements ought to be based on the
7 first principle and the bases upon which NRC makes its
8 regulations on adequate protection and so forth, and allow
9 the user of those regulations to exceed them and not have
10 that difference gobbled up into regulation.

11 There were a few case where we attempted to change
12 the regulations. We would propose in some areas -- these
13 are usually some modest areas -- we didn't go after things
14 like large break loca and so forth.

15 We did propose some changes to the regulations,
16 and some of them were accepted and some of them were not.
17 Some examples that were talked about were: More realistic
18 source term; elimination of the operating basis earthquake
19 and going only with the safe shutdown earthquake; changes to
20 hydrogen regulatory requirements.

21 This optimized or simplified emergency planning
22 that Alex mentioned earlier, and so forth.

23 And the last slide I think is more just personal
24 views as we look back over the ALWR program and how we
25 approached defense-in-depth. We think that looking forward,

1 that risk-informed regulation and specifically a more -- an
2 approach to defense-in-depth that is closer to the
3 rationalist model is really important to the future.

4 We are going to have to find ways to reduce the
5 capital costs of ALWRs, and we believe that can be done
6 easily and safely, and, in fact, probably in many ways
7 improve safety.

8 But it does require more flexibility on the
9 regulatory side, and a rationalist approach would allow for
10 that.

11 Further, I don't see how the NRC will ever be able
12 to license a reactor design such as a high-temperature gas
13 reactor, unless there is a more flexible approach to
14 defense-in-depth, including something similar to the way
15 you've characterized this rationalist model.

16 I think the die is cast; the rationalist model is
17 ultimately going to become the future approach for
18 regulation, and I don't think we need to be afraid of that.
19 I think there are really no downsides to that model, if, in
20 fact, it's done prudently and carefully and safely, and done
21 with the things that are already pretty much established in
22 regulatory policy, namely, that it's not going to be a
23 risk-based approach; it's going to be a risk-informed
24 approach.

25 There will be a balance, there will be still

1 consideration of defense-in-depth, there will be clear use
2 of engineering judgment and care and so forth in how you
3 approach risk insights.

4 And just finally one comment on U.S. leadership:
5 The ACRS paper on defense-in-depth mentions a couple of
6 INSAG reports, and it's true that in the international
7 arena, there is a much more rigorous definition, a much more
8 traditional and formal approach to defense-in-depth.

9 And I think there probably will be some resistance
10 on moving quickly toward, say, a rationalist model,
11 internationally, and the reason is that I think there is a
12 concern by IAEA and probably some of the industrialized
13 world regulators that if you move too quickly, you're going
14 to find some countries, third-world countries, people who
15 don't have the maturity and infrastructure, safety culture,
16 and so forth, that if you move to quickly in optimizing
17 defense-in-depth philosophies, that you're going to remove
18 some significant safety protection.

19 And so there will be some desire, I think, in the
20 international community to move slowly and to make sure
21 that, especially for those who define defense-in-depth very
22 broadly -- and I've seen it defined this way to include
23 things like safety culture and your infrastructure and your
24 regulatory infrastructure and so forth -- that those things
25 still are not subsumed under a risk approach, and you don't

1 make them subservient, but you still keep them at a high
2 level.

3 MR. APOSTOLAKIS: It's important, of course, to
4 note that terms like quickly and slowly are relative.

5 MR. VINE: Yes.

6 MR. APOSTOLAKIS: And that the first major risk
7 assessment in the United States was published a quarter of a
8 century ago. So for us, it's not too quickly.

9 MR. McINTYRE: My name is Brian McIntyre, and I'm
10 the AP-600 License Manager. I'm two things: I'm the
11 practical application of what Gary just talked about; and
12 I'm also, I think, the most recent example of where the
13 rubber has met the road with the staff on defense-in-depth.

14 And this is -- we have really talked at lot about
15 this, I think, earlier, that it's more than the three
16 barriers that was originally put in to deal with
17 uncertainties.

18 What I had written down is that we are never sure
19 exactly what it was. And after sitting through this
20 morning, I think it's that everybody was more or less sure
21 what it was, and it was whatever it needed to be, and it was
22 sort of a flag that we all wrapped ourselves in, both sides,
23 I mean, the industry and the regulators.

24 But we never quite knew when enough was enough,
25 and I'll talk about that at the very end of this. And now

1 it's clear that we are moving towards some sort of a balance
2 between the things that are on the top there and the
3 risk-informed information.

4 In the AP-600 case, for us, I broke this down into
5 two things, something that I called the unquantifiable
6 aspects -- and this goes beyond just power reactors. For
7 us, it was a design philosophy. Now, at the bottom I have
8 some things that are quantifiable.

9 We actually, since we were starting from scratch,
10 weren't trying to figure out how good the plant was; we were
11 more interested in how good we could make the plant. And
12 you really take a different approach if that's what you're
13 doing.

14 And our design philosophy looked at -- people have
15 kind of wondered about passive plants -- that we have
16 multiple levels of defense.

17 And the first thing that you see there is that it
18 was usually a non-safety, active feature. We have a passive
19 plant, and that made the staff -- these are my words -- made
20 them a little bit crazy.

21 Because, as you're going to try to address your
22 transients by using non-safety systems, this is as a first
23 shot, yes. And then almost the backups would be the passive
24 systems which were the safety systems.

25 And if you want to look at what this looks like,

1 the next figure or the thing that actually is the figure,
2 this is -- and we did this for a number of transients where
3 we went through and we looked.

4 On the left side is a current plant -- and I need
5 to put my glasses on to see this -- that what they would do,
6 their SSAR safety case is that they would automatically
7 actuate their high-end safety injection, their aux feed;
8 they'd isolate the steam generator, and they'd start to cool
9 down and depressurize, and that was their safety case.

10 And if that isolated the leak, that was great, and
11 if not, then they had a non-safety case which would be in
12 their emergency operating procedures someplace, and they had
13 a couple of things that they could do. If not, then they
14 were at a core damage situation.

15 For the AP-600, if you take a look at our top
16 block, which is the non-safety case, really, it's the same
17 things that in a traditional plant would be their SSAR
18 safety case, except we had now made these systems
19 non-safety-related, which was really a change.

20 And there were some long discussions we had with
21 the staff. Gary talked about regulatory treatment of
22 non-safety systems, and I'll talk a little bit at the end
23 about how we did approach that.

24 And then we got to our safety case, all these
25 passive features of automatically actuating the core makeup

1 tank; the PR/HR heat exchanger, which was basically
2 replacing the axillary feed or startup feed system in the
3 safety case; the CVCS.

4 We'd isolate the steam generator and start the
5 passive containment cooling system, and if that isolated the
6 leak, then that was our safety case. And that's what we
7 basically met the safety requirements with.

8 The important thing to look at in the AP-600 is
9 that down below it there were then two or three other
10 options that the guy could go through. And this was
11 important because, you know, we could have just really
12 stopped at the top, at the safety case, and with the top
13 two.

14 For various reasons, because these features were
15 in the plant, that they all managed to work together, and as
16 a result, we got really some good PRA results. But this, to
17 us, was what we considered to be the defense-in-depth.

18 We also used the PRA as the design tool. And
19 that's like a lot different if you're trying to figure out
20 how good you can make the plant, as opposed to how good the
21 plant is.

22 We did a total of seven PRAs on the AP-600. And
23 we weren't doing them just to make the PRA different; we were
24 doing them because we'd made the plant different.

25 We'd run the PRA, we'd find out where the weak

1 spots were. This is where you're looking for the unduly --
2 not unduly dependent on one system, so we were looking if
3 something really stuck out, and we'd go back and we would
4 make the system better.

5 There was a lot of design with arguments even
6 between the risk analysis people and the designers. We
7 actually got better PRAs as a result of that, because
8 sometimes the PRA people didn't understand exactly how the
9 system should have worked.

10 In a lot of cases, the designer said, you mean
11 that if this fails, then that's the result you're going to
12 get in the PRA space. And we made some significant changes
13 to the plant as a result of the PRA.

14 We went through a lot of just discussions, review,
15 understanding the results. We looked at some of the backup
16 slides.

17 When we got to reviewing things to see how we
18 would expect the systems to work, this is just one example.
19 This is the PR/HR heat exchanger. How would it fail? We
20 would then walk through the various things and decide what
21 we needed to either to try to fix or to model or not model
22 in the PRA.

23 We went through each one of the various items, for
24 example, for the inadequate IRWST water level, and then that
25 was broken down to look. Are there things that we could

1 fix, are there things that we needed to do better?

2 I mean, we really did chase this design down to
3 look for ways that you could improve the plant.

4 And this is a philosophy, so it's not just
5 applicable to an AP-600 or a BWR or something like that.
6 But if you think like this and you bring this approach to
7 the design and bring whatever it is from a design to
8 actually a facility, this works.

9 This is another way to look at defense-in-depth,
10 but there is no way that we could put a specific number on
11 what we got out of this.

12 We also looked at shutdown operations. We looked
13 at low power operations. We pretty much covered the
14 waterfront.

15 One of the bullets on the previous slide was that
16 for systems that were more -- or for events that were more
17 likely, initiating events, we had more backups.

18 For steam generator tube rupture, a reasonably
19 likely event, there are five or six different thing you can
20 do. When you get down to the more unlikely things like
21 large loca, you don't have quite as many options of things
22 that you can do, so we tried to focus our efforts on the
23 things that are more likely going to happen.

24 Also, one of the big reasons we were doing this is
25 the big push from the industry was this investment

1 protection concept. If something is more likely to happen,
2 then we don't want to lose the plant as a result.

3 We want to have things that the guy can do. He
4 might have to clean the plant up, but he won't lose the
5 plant as a result of it.

6 We looked at a much wider range. We didn't
7 restrict ourselves to the design basis transients. We
8 really looked at multiple steam generator tube rupture, not
9 willingly, but we looked at multiple tube rupture, because
10 this was a case of the staff's concern which was, okay, you
11 guys met the design requirements, but do you fall off the
12 table somewhere?

13 And the staff went to the extent of, after we had
14 completed our testing at the Oregon State facility, which
15 was a quarter scale model of an AP-600, it was a low
16 pressure facility, but they went out and ran beyond design
17 basis transients there to look to see if there was someplace
18 that we hadn't tested that they could look to see if we were
19 going to fall off the table.

20 And the conclusion was, no. It was a surprisingly
21 robust plant. I mean, we'd been telling them that for a
22 long time, but eventually, it became obvious.

23 We also looked at a broad range of initiating
24 events. And as I said, this was to look beyond where you
25 would normally go.

1 And, again, we're trying to figure out how to make
2 it better, not how good it is. And it's almost like IPEE
3 and IPEEE, except we could make the changes, because it's
4 quite easy really to make a change.

5 If you look at the quantifiable aspects, we ended
6 up with really a nice low core damage frequency. I'll talk
7 about the focused PRA in a second.

8 For large releases, what we were required to do by
9 NEPA was to look -- and SAMDA, if you're not familiar with
10 those, those are severe accident mitigation design
11 alternatives.

12 I look at it as we had to explain to the staff,
13 why we didn't do what we didn't do. It turns out we're not
14 really good at documenting that, so we went through and have
15 to figure out, why didn't you make these changes to the
16 plant, and you have to look at that on a cost basis, the
17 cost/benefit basis.

18 And it turns out there was nothing that we had to
19 add, nothing that could be cost effective when we finished
20 the design of the plant.

21 Our PRA results: This is looking at two things,
22 the core damage frequency and the large release frequency.
23 It's the at-power and the shutdown events.

24 The baseline PRA is pretty much a traditional PRA.
25 It has the safety systems and the non-safety systems in it.

1 As part of our ongoing discussions with the staff
2 and the regulatory treatment of non-safety systems, we had
3 an approach proposed by the industry, accepted by the staff,
4 that if this plant was so good that we could go out and meet
5 the safety goals to 10-4 and 10-6, with only the
6 safety-related systems, then these non-safety systems that
7 were in that top tier or the first thing that the operator
8 might actually do to the plant to mitigate an accident, then
9 they wouldn't require any additional treatment.

10 And it's a sensitivity study, but we went back and
11 looked at it, and we showed that without the safety systems,
12 we still, in the core damage frequency area, we quite
13 handily met the safety goal. In the large release, well, it
14 was close.

15 And the staff's concern was, well, uncertainties
16 in the PRA, we're not so sure about this, and we went back
17 and forth and back and forth and back and forth and back and
18 forth.

19 And finally, it just went forth, and we said,
20 okay, to move this forward, we would put some administrative
21 controls on certain systems. And so we actually have in the
22 AP-600, safety-related, non-safety-related, and then there
23 are these RT&SS important systems that we have availability
24 controls. So we're actually --

25 I would actually look at this as beyond

1 risk-informed. It's almost risk-based, this sort of an
2 approach that you have a milestone that you're trying to
3 meet, that if you do this then you will be okay, and if not,
4 then you'll have to do some things to make it so.

5 And at the time, this was quite novel. It was
6 much for discussion, but it certainly is, I think, a case of
7 how defense-in-depth can come and be played through and be
8 applied to a facility.

9 One of the reasons that you're here -- and this is
10 sort of -- if you look at Tab 1 in Jack's book of
11 defense-in-depth discussions, it was that we had a long
12 discussion with the staff on containment spray. The AP-600
13 does not have a containment spray.

14 Well, it does have a containment spray; it didn't
15 have a containment spray. Let's put this in perspective and
16 in the proper tense here.

17 And we didn't think that we need it, and it got
18 back into arguing about the uncertainties and the PRA and
19 the models. In the end, we ended up, as I said, with a
20 containment spray system.

21 If you look at it from a risk-informed
22 perspective, the -- and this is a slide that was put
23 together by an ACRS fellow at the time back in June of 1997
24 when this discussion was going on.

25 It gives you an idea of where our risk

1 contributors are. And for this plant, if you look at what a
2 containment spray would help you with, it's not going to
3 help you with the bypass events or with the early
4 containment failure. It might some -- it would help you
5 with the containment isolation failures.

6 A presentation that I made to the staff had -- and
7 you haven't seen this one, George, but it has the more
8 quantified basis of what we would expect to get out of the
9 spray.

10 And the spray here where it says low flow, it's
11 lower flow than the spray that we actually ended up putting
12 in the plant. This was a study that we were doing at the
13 time to figure out how much water we needed to make -- this
14 is like 400 gpm, and I think we have a thousand gpm actually
15 in the plant.

16 So the spray that we have in the plant would work
17 better than the spray that's on this. But it shows that for
18 earlier failure, it would reduce it by about a factor of
19 two, and it would help the intermediate failures, but those
20 are really pretty low-risk events. The isolation failure,
21 it would help that a fair bit.

22 It doesn't help the bypass, so by putting the
23 spray in, we ended up reducing a very small number by a
24 factor of two. And this is the reason that it didn't make
25 the cut, if you will, in putting it in the plant from the

1 SANDA category.

2 And we took this actually as far as the
3 Commission. There was a SECY paper, and I think it's really
4 one of the reasons that we're here, because defense-in-depth
5 really got down -- this was one of the harder arguments that
6 we have had about what is defense-in-depth?

7 And I'm going to read from one of the vote sheets
8 on this SECY, just one paragraph, because I think this
9 answers your question about if you pass all the
10 requirements, would they still make you put something in?
11 Yes.

12 And the argument was that in spite of the fact
13 that the proposed system cannot be justified under any of
14 the rational decisionmaking guidelines that we have
15 established for ourselves, the staff would require it
16 anyway.

17 The ultimate reason seems to be that it is
18 justified to compensate for uncertainties in how the design
19 will behave under severe accident conditions. Even this
20 reason is not well supported because we have not established
21 a relationship between the proposed spray and the particular
22 uncertainties it is supposed to address.

23 Defense-in-depth becomes the final justification.
24 And then it goes on to say that the Commission and the staff
25 should not continue ad hoc decisionmaking indefinitely, and

1 here we are. That's why we're here today.

2 But the answer to your question is, yes. And I
3 think that we've perhaps moved beyond this now, and I was
4 glad to see Gary's and Tom's presentations. I'm not too
5 sure, but I can probably use that to take the spray out.

6 [Laughter.]

7 MR. McINTYRE: Since it's not a Tier I
8 requirement.

9 MR. HOLAHAN: We'd have to talk about that.

10 MR. McINTYRE: So that's the way that
11 defense-in-depth actually gets applied. If you make it a
12 way of life, almost a mantra, you pray to it, you decide and
13 you think like that, and it can really result in a lot of, I
14 think, good things in the design. That should answer your
15 question that you asked about five times today.

16 MR. KRESS: Thank you very much. I'm not so sure
17 that if we had had Gary's risk-informed matrix table back
18 then, whether or not we would have come down on the side we
19 came down on.

20 MR. McINTYRE: I think what's important is that
21 they were looking at the balance between prevention and
22 mitigation, because my argument or complaint -- complaint,
23 that's fair -- at the time was, what are the units on this
24 balance?

25 And I think there's an attempt to do that, and I

1 certainly applaud that.

2 MR. KRESS: That is exactly right.

3 MR. GARRICK: What would be much more interesting
4 than these point estimates, which see -- would be the PDF
5 stacked on top of each other for these two cases.

6 MR. KRESS: Yes, that was one of our problems,
7 too. We didn't have any of the PDFs. And all we had were
8 point estimates, and that made the decision much more
9 difficult.

10 Had we had those, it might have been a different
11 story.

12 MR. HOLAHAN: My recollection is that you didn't
13 have them because they were never generated.

14 MR. KRESS: That's right. That's why we didn't
15 have them.

16 MR. APOSTOLAKIS: That's a good reason.

17 MR. BUDNITZ: But the difference at Yucca Mountain
18 is a qualitative difference about the staff behavior, I
19 believe. See, you were having this argument about a
20 theoretical plant that wasn't sited or being built anyplace
21 in particular, in a room in an office building like this.

22 But in Yucca Mountain, it's going to be in an
23 arena in which the Governor, the Senators and almost the
24 entire population of a real state are using every political
25 opportunity they can and every legal opportunity they can,

1 not only to get in the way, but to embarrass the staff.

2 And the staff is acutely aware that that
3 embarrassment has to be avoided, if they can, and that's why
4 they can't find themselves, if they can avoid it, in a
5 situation where they're backfitting a positive decision on
6 what would have been a negative decision by changing their
7 minds halfway through.

8 MR. KRESS: Yes.

9 MR. BUDNITZ: And so they really have a different
10 dilemma than you and the reactor staff and at that time.
11 It's much more difficult for them.

12 MR. APOSTOLAKIS: Good.

13 MR. KRESS: Very, very difficult. I'm going to
14 ask if anyone in the audience feels compelled to add
15 anything to what they've heard.

16 [No response.]

17 MR. KRESS: Seeing no rush to the front --

18 MR. APOSTOLAKIS: Are the experts going to be back
19 tomorrow?

20 MR. KRESS: That's a good question.

21 MR. APOSTOLAKIS: Are they coming tomorrow?

22 MR. KRESS: Tomorrow, we're going to try to wrap
23 some of this up and see if we can reach some conclusions,
24 and maybe spell out what the remaining issues are, and
25 things of that nature, and as many of the experts as we

1 could get would be nice.

2 MR. APOSTOLAKIS: So we lost Dr. Murley then?

3 MR. KRESS: Lost Dr. Murley.

4 MR. APOSTOLAKIS: Are you going to be here
5 tomorrow, Budnitz?

6 MR. BUDNITZ: Yes.

7 MR. KRESS: We'll quit at precisely noon or pretty
8 close, or maybe even before noon, but more around there.
9 Okay, great. The staff, will you be here?

10 MR. HOLAHAN: Yes.

11 MR. KRESS: So we'll try to wrap it up then
12 tomorrow, and it will be more of a roundtable discussion.

13 MR. APOSTOLAKIS: Is NEI going to be here
14 tomorrow?

15 MR. KRESS: You're welcome to be here. So if
16 there are no other comments from --

17 MR. GARRICK: Let me remind the ACNW and the ACNW
18 staff that our meeting will start in ten minutes.

19 MR. APOSTOLAKIS: And go on for eight hours.

20 [Laughter.]

21 MR. KRESS: With that, I'm going to recess until
22 tomorrow morning at 8:30.

23 [Whereupon, at 5:40 p.m., the meeting was
24 recessed, to be reconvened at 8:30 a.m., on Friday, January
25 14, 2000.]

REPORTER'S CERTIFICATE

This is to certify that the attached proceedings before the United States Nuclear Regulatory Commission in the matter of:

NAME OF PROCEEDING: MEETING: ACRS/ACNW JOINT
SUBCOMMITTEE

CASE NO:

PLACE OF PROCEEDING: Rockville, MD

were held as herein appears, and that this is the original transcript thereof for the file of the United States Nuclear Regulatory Commission taken by me and thereafter reduced to typewriting by me or under the direction of the court reporting company, and that the transcript is a true and accurate record of the foregoing proceedings.



Mike Paulus

Official Reporter

Ann Riley & Associates, Ltd.

71
(FIRST DAY)

**INTRODUCTORY STATEMENT BY THE CHAIRMAN OF THE
JOINT SUBCOMMITTEE OF THE ADVISORY COMMITTEE ON REACTOR
SAFEGUARDS AND THE ADVISORY COMMITTEE ON NUCLEAR WASTE
11545 ROCKVILLE PIKE, ROOM T-2B3
ROCKVILLE, MARYLAND
JANUARY 13-14, 2000**

The meeting will now come to order. This is a meeting of the Joint Subcommittee of the Advisory Committee on Reactor Safeguards and the Advisory Committee on Nuclear Waste.

I am Thomas Kress, Co-Chairman of the Joint Subcommittee. On my left (right?) is Dr. John Garrick, also Co-Chairman of the Joint Subcommittee.

Joint Subcommittee members in attendance are Dr. George Apostolakis of the Advisory Committee on Reactor Safeguards, and Dr. Raymond Wymer of the Advisory Committee on Nuclear Waste. Also present is Dr. Milton Levenson, a consultant to the Advisory Committee on Nuclear Waste.

The purpose of this meeting is for the Joint Subcommittee to discuss the defense-in-depth philosophy in the regulatory process, including its role in the licensing of a high-level waste repository, its role in revising the regulatory structure for nuclear reactors, and how the two applications should be related to each other. The discussion will also include the role of defense in depth in the regulation of nuclear materials applications, and other related matters.

The Subcommittee will gather information, analyze relevant issues and facts, and formulate proposed positions and actions as appropriate, for deliberation by the full Committees.

Michael Markley is the designated Federal Official for the initial portion of this 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 December 21, 1999.

A transcript of the meeting is being kept. It is requested that the speakers first identify themselves and speak with sufficient clarity and volume so that they can be readily heard.

We have received two requests, one from the Nuclear Energy Institute and one from Westinghouse, to make an oral statement later in the meeting. Otherwise, we have received no written comments or requests for time to make oral statements from members of the public.

We have three invited experts with us this morning, all of them former office directors in the Nuclear Regulatory Commission and now highly regarded consultants in the general field of nuclear safety. They are Bob Bernero, Bob Budnitz, and Tom Murley.

Mr. Bernero spent 13 years in naval and space nuclear work at GE, and then served for 23 years, from 1972 to 1995, with the AEC and NRC regulatory staff. After 5 years in reactor and fuel cycle licensing, Bob began work in regulatory development, including decommissioning standards and spent fuel licensing. After investigating the TMI accident, Bob formed the

Division of Risk Analysis in the Office of Research, served later in NRR licensing divisions, and then went back to NMSS until he retired as Director in 1995.

Dr. Budnitz worked at the University of California Lawrence Berkeley Laboratory, from 1967 to 1978, and held the position of Associate Director and Head of the Energy and Environmental Division. In 1978 he joined the Nuclear Regulatory Commission as Deputy Director of the Office of Research, and was appointed director of that office in 1979. In 1980, Bob left the NRC to found Future Resources Associates, a small consulting firm working mostly in risk analysis. His current consulting activities include PRA, emphasizing external hazards, upgrading the safety of older reactors, and using risk in safety regulation, including performance analysis of waste disposal systems.

Dr. Murley was the Director of NRC's Office of Nuclear Reactor Regulation from 1987 to 1994. Prior to that, he was Regional Administrator of NRC's Region 1 office, beginning in 1983. Dr. Murley retired from NRC in 1994 after 25 years of service. He is presently a consultant on nuclear management and safety matters in the U.S. and foreign countries.

(Chairman's Additional Comments - If any)

We will proceed with the meeting.

THOUGHTS ON DEFENSE IN DEPTH

D.A. Powers

January, 2000

DEFENSE IN DEPTH

- **a very expensive safety strategy**
- **has served the reactor safety community well**
- **even within the reactor safety community thoughts have turned to limiting defense in depth**
- **two schools of thought**

- Structuralist -

difficult to extend to other areas

- Rationalist -

can be extended to other areas if analysis capabilities are sufficiently developed

paradoxes may arise if analyses are used to specify where defense in depth is applied to protect against the possibility that analyses are wrong!

DEFENSE IN DEPTH

arose in the reactor safety community because:

- little experience in the operation of nuclear power plants at the time,**
- no industrial standards for the safe operation of nuclear power plants,**
- confidence that accidents were unlikely, but great uncertainties in the consequences of accidents should they occur,**
- potentially consequential accidents would be difficult to interdict once underway, and**
- an accident that affected the public at any facility would lead to shutdown of all nuclear facilities.**

CONDITIONS FOR DEFENSE IN DEPTH

- **do not appear to arise in the four classes of material licences:**
 - **in many cases, consequences are easily bounded,**
 - **in many cases, there is a wealth of operational experience,**
 - **severe accidents that potentially have large consequences develop slowly so there is the possibility to interdict,**
 - **phenomenological uncertainties are modest, and**
 - **technical basis for rationally limiting defense in depth is not well developed.**

- **I would argue against the imposition of a defense in depth philosophy on material licensees.**

**DESIGN DEFENSE-IN-DEPTH
in a
RISK-BASED REGULATORY SYSTEM
with
IMPERFECT PRA**

or

BEATING A DEAD HORSE WITH A RED HERRING

**T. S. Kress
ACRS**

**Presented at
ACRS/ACNW Joint Subcommittee Meeting
on
Defense-in-Depth
January 13-14, 2000
Washington DC**

CONCERNS

WE ALL CAN AGREE THAT DEFENSE-IN-DEPTH IS A DESIGN (AND OPERATIONAL) STRATEGY (PHILOSOPHY?) FOR DEALING WITH UNCERTAINTY IN RISK ASSESSMENT

BUT.....

1. THIS DOES NOT CONSTITUTE A PRECISE (DESIGN-TO) DEFINITION IN TERMS OF RISK ASSESSMENT

2. THERE DOESN'T CURRENTLY EXIST A DEFINITION OR CRITERIA THAT ALLOWS FOR PLACING LIMITS ON DID (how do we recognize it and how much is enough?).

I SEE A MAJOR OBJECTIVE OF THIS MEETING TO BE TO ADDRESS THESE TWO CONCERNS.

BASED ON THE FOUR PRINCIPLES, MY PREFERRED GENERALIZED AND RISK RELATED DEFINITION OF DEFENSE-IN-DEPTH IS:

DESIGN DEFENSE-IN-DEPTH IS A STRATEGY OF PROVIDING DESIGN FEATURES TO ACHIEVE ACCEPTABLE RISK (IN VIEW OF THE UNCERTAINTIES) BY THE APPROPRIATE ALLOCATION OF THE RISK REDUCTION TO BOTH PREVENTION AND MITIGATION.

HOW CAN THIS DEFINITION BE IMPLEMENTED TO PUT LIMITS ON DEFENSE-IN-DEPTH?

THE KEYWORDS ARE "APPROPRIATE ALLOCATION"

- **YOU MUST HAVE RISK ACCEPTANCE CRITERIA THAT YOU DESIRE TO ALLOCATE (PREFERABLE EXPRESSED IN TERMS OF CONFIDENCE LEVELS)**
 - Quantifiable uncertainty should come out of the PRA
 - "Unquantifiable" uncertainty should be estimated by expert opinion
 - The acceptance criteria should include both uncertainties

- **ALLOCATION IS A VALUE JUDGMENTWE NEED CRITERIA FOR HOW MUCH WE VALUE PREVENTION VERSUS MITIGATION**
 - Could depend on the level of inherent hazard (the more hazardous the activity the more we should value prevention)
 - Could depend on the extent of uncertainty in the risk assessment
 - Could depend on how much of the uncertainty is unquantifiable
 - May want to minimize uncertainty (after all this is a classic optimization problem)
 - May be based on the "loss function" of decision theory

THOUGHTS ON DEFENSE IN DEPTH

D.A. Powers

January, 2000

DEFENSE IN DEPTH

- **a very expensive safety strategy**
- **has served the reactor safety community well**
- **even within the reactor safety community thoughts have turned to limiting defense in depth**
- **two schools of thought**

- Structuralist -

difficult to extend to other areas

- Rationalist -

**can be extended to other areas if
analysis capabilities are sufficiently
developed**

**paradoxes may arise if analyses are
used to specify where defense in
depth is applied to protect against the
possibility that analyses are wrong!**

DEFENSE IN DEPTH

arose in the reactor safety community because:

- little experience in the operation of nuclear power plants at the time,**
- no industrial standards for the safe operation of nuclear power plants,**
- confidence that accidents were unlikely, but great uncertainties in the consequences of accidents should they occur,**
- potentially consequential accidents would be difficult to interdict once underway, and**
- an accident that affected the public at any facility would lead to shutdown of all nuclear facilities.**

CONDITIONS FOR DEFENSE IN DEPTH

- **do not appear to arise in the four classes of material licences:**
 - **in many cases, consequences are easily bounded,**
 - **in many cases, there is a wealth of operational experience,**
 - **severe accidents that potentially have large consequences develop slowly so there is the possibility to interdict,**
 - **phenomenological uncertainties are modest, and**
 - **technical basis for rationally limiting defense in depth is not well developed.**

- **I would argue against the imposition of a defense in depth philosophy on material licensees.**

SOME COMMENTS ON DEFENSE IN DEPTH AS A SAFETY STRATEGY

D.A. Powers

**Chairman
Advisory Committee on Reactor Safeguards**

I regret that I cannot be with you in the meeting of the Joint ACRS/ACNW Subcommittee. I do, however, want to share with you some of my thoughts on the subject of defense in depth as a safety strategy and, especially, as a safety strategy for materials licensees. Some of these thoughts are included in a paper coauthored with Jack Sorensen and other members of the ACRS.

Defense in depth is a safety strategy that has served the nuclear power industry well. Defense in depth is, however, a very expensive safety strategy. Because of the expense associated with defense in depth, even the nuclear reactor safety community that has been so well served by this strategy is wrestling with ways to limit the imposition of defense in depth. We ought, then, to think carefully before imposing such a safety strategy in other areas. At the very least, we need to think of how to limit the requirements for a defense-in-depth safety strategy. Two schools of thought have emerged within the nuclear reactor safety community on the limitation of defense in depth. One of these, the 'Structuralists' school of thought does not extrapolate to any other field of endeavor. The other school of thought, the 'Rationalist' school, can be extrapolated to other areas. The Rationalist school of thought would restrict application of the defense-in-depth safety philosophy to those areas where safety analysis capabilities (PRA in the reactor safety world) cannot be applied or areas where these safety analysis methods yield very uncertain results.

Though this Rationalist approach to the limitation of defense in depth has much merit within the reactor safety community where the PRA methods of safety analysis are being aggressively developed and applied, I question whether this approach "travels well" so it can be applied in areas that have different or less developed methods of safety analysis. But, mostly, I question the Rationalist's approach because I see defense in depth as a method for addressing the question of what happens if the analyses are wrong and potentially consequential accidents do occur. If this is, indeed, the purpose of defense in depth, then one ought not use the error-prone analysis methodologies to determine where defense in depth is needed. I am confident that paradoxes will arise if this method of self-identification is used.

I think one has to go back and understand why defense in depth was adopted as a safety strategy for nuclear power plants if one is to understand its applicability to other areas. Defense in depth sounds so good as a safety strategy. It just sounds strong and reassuring. I do not

discount, then, the importance of the good ring to the widespread acceptance of defense in depth as a strategy for nuclear power plants. One has still to ask why the reactor safety community felt that such a robust safety strategy was needed.

My reading of the history of the nation's nuclear power enterprise leads me to believe that defense in depth was created as a safety strategy because:

- there was limited experience dealing with large nuclear power reactors,
- there were no applicable industrial standards for the safe operation of nuclear power plants,
- there was a confidence that accidents at nuclear power plants were unlikely, but there were very serious uncertainties about the consequences of accidents should they occur,
- a severe accident at a nuclear power plant that could pose substantial consequences would be most difficult to interdict once it was underway, and
- there was a confidence that a nuclear accident that affected the public near any facility would lead to shutdown of all nuclear facilities.

Lack of experience was quite an important issue at the time. Even after years of operational experience with research reactors and nuclear materials production reactors, the technical community was still encountering new physical phenomena (Xenon instabilities were fresh in safety analysts' minds.). Uncertainties in the behavior of radionuclides under accident conditions are much mentioned in the literature of the time, and, indeed, even today we have only the most primitive of an understanding of how radionuclides will behave in reactor accidents. We have no codes, for instance, that will predict all of the behaviors of fission products observed during the Chernobyl accident. The Windscale accident certainly emphasized the difficulty of interdicting a severe accident once it was underway. The widespread belief in the inevitable progression of a severe accident in a nuclear power plant has not been completely overturned even by the experience of the Three Miles Island accident. But, I suspect that the most driving concern that led to development of the defense in depth was concern over the political fallout from an accident that affected the public.

Though one can debate which of the safety issues was most important for the development of defense in depth, I believe that the existence of all five of the conditions listed above was necessary to the widespread acceptance of defense in depth within the reactor safety community. It is apparent, however, that maintenance of this safety strategy does not require that all five conditions still exist. Still, as any one of the conditions is mitigated (for instance as one gains experience in the operation of nuclear power plants) one becomes more willing to chip away at the defense-in-depth structure.

I do not believe that the five conditions that led to the imposition of defense in depth on the nuclear power industry exist in any of the four categories of licensees regulated by NMSS. As has been noted in the discussions of the Joint Subcommittee, many of the licensees have a great deal of operational experience. Many of the applications have the potential to produce only modest consequences even if bounding accident events occur. Even in the case of nuclear waste repositories where very severe accidents can be envisaged, these accidents will develop quite slowly and there will be opportunities to interdict. In none of the licensee activities will an accident result in the general shutdown of an entire industry even if the accident affects the public.

Were I with you at the meeting, I would argue vigorously against the imposition of defense in depth concepts on the material licensees. I don't think such a costly safety strategy is at all needed to achieve very high levels of safety. For most material licensees a standards-based safety strategy akin to the ASME boiler and pressure vessel safety code, but based, perhaps, on results of risk analysis ought to be adequate. Even in the case of a large, geologic repository for spent fuel, a safety strategy based on conservative engineering analyses guided by risk analyses ought to be satisfactory. In this regard, I hasten to add that I am not a 'fan' of design basis accidents for safety analyses, but this is a subject for some future meeting.

If defense in depth is imposed on material licensees, one immediately encounters the problem of rationally limiting the defense in depth. That is, if defense in depth is a strategy to address the possibility that analyses are wrong, there is in principle no end to the number of independent layers of increasing conservatism that can be applied to an activity. A rational basis not based on an arbitrary judgement is difficult to define. Within the reactor safety community the limitations on defense in depth were done arbitrarily. Now there is an ongoing effort to further limit defense in depth. The analysis capability to follow the Rationalists' approach to the limitation of defense in depth does not exist for many of the licensees. I do not see within the affected safety community an enthusiasm to marshal the wherewithal that would be necessary to develop a suitable analysis capability.

Draft Technical Note

ON THE QUANTIFICATION OF DEFENSE IN DEPTH

B. John Garrick
January 13, 2000

PURPOSE

To propose a conceptual framework for quantifying the "defense-in-depth" aspects of the various levels of protection, provided in nuclear plants and nuclear waste repositories, against the release of radiation to the public and the environment.

GENERAL FEATURES OF THE APPROACH

The question is how can we best use probabilistic risk (performance) assessment (PRA and PPA) results to quantify and make visible the performance of the various "defense-in-depth" systems designed to provide multiple "levels of protection" against the release of radiation. Part of the answer lies in the way that the results are presented.

The key to the proposed approach, therefore, is a presentation format that clearly displays 1) the role that the individual safety systems play in providing protection against the release of radiation to the environment and 2) the effect of the individual systems acting in concert. This format allows for important risk and performance comparisons to be made at both the functional and system levels of a nuclear plant or a nuclear repository. It helps us make the important judgments of whether we are getting our money's worth from these multiple levels of defense, and whether we need more or less.

The approach utilizes the results of PRA and PPA. The scope of the PRAs and PPAs must include quantifications of information and modeling uncertainties, in the parameters used to measure risk or safety performance, and explicit identification of the supporting evidence on which these quantifications are based. The PRAs and PPAs must be structured in such a way as to reveal the process of assembling the results into the final measures of risk or performance, and to reveal the contributions, to these final measures, of the various levels of protection.

SPECIFIC FEATURES OF THE APPROACH

The answer to "how can we best use PRA and PPA results to quantify --- defense-in-depth ---" is believed effectively addressed using a two-dimensional structuring of risk and performance results. The structuring can be done in stages or phases in the spirit of a top-down approach. To illustrate the process at the functional level for reactors, consider Figure 1 with respect to the PRA of a boiling water reactor.

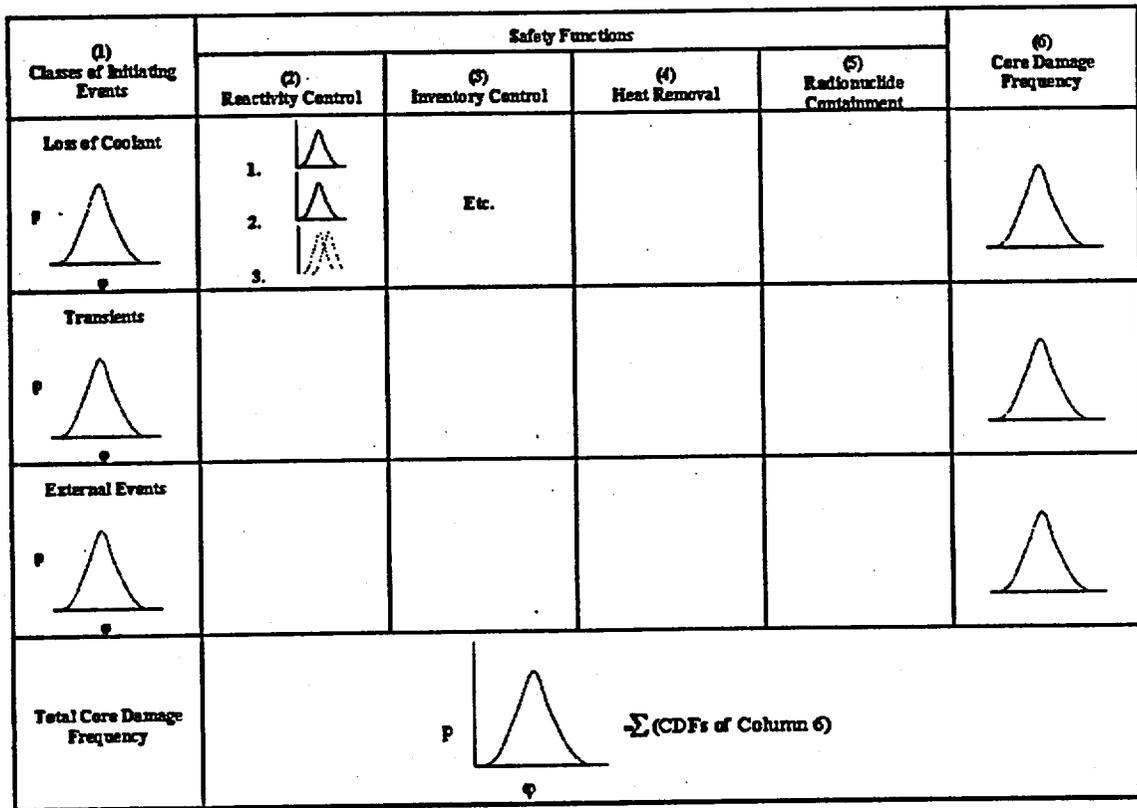


FIGURE 1. BWR SAFETY FUNCTIONS

The rows of Figure 1 represent classes of initiating events at the functional level that can lead to core damage. In the first column (column 1) we plot probability curves showing our state of knowledge about the frequencies of the initiating events in the "probability of frequency" format. Columns 2—5 now represent the various safety functions that may respond to a particular class of initiating events. Column 6 contains the core damage frequencies for each class of initiating events. The sum of the Column 6 results represents the total core damage frequency, as illustrated in the last row.

The question is what entries should go in the boxes under the safety functions? The answer is to show the entries that best expose the defense-in-depth contributions of the safety functions. There are many possibilities. One possibility is to include three entries in each grid box, as shown in Figure 2.

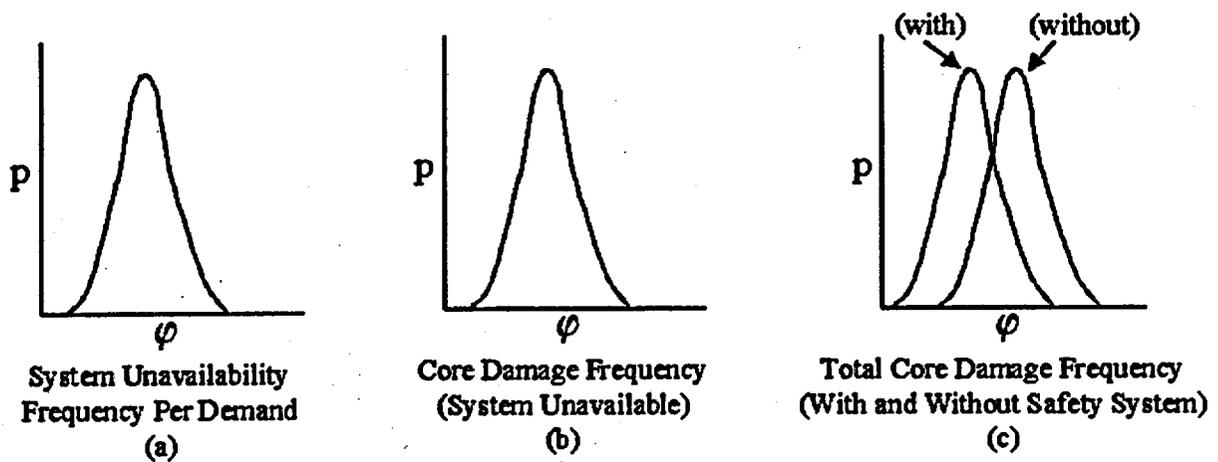


FIGURE 2. SYSTEM PERFORMANCE INDICATORS

As discussed further below, Entry 1 (Figure 2a) could be a probability curve indicating the unavailability frequency per demand of the safety function, given the particular class of initiating events. Entry 2 (Figure 2b) could be the core damage frequency, given the unavailability of the safety function, and Entry 3 (Figure 2c) could compare this result with the total core damage frequency of the last row. Doing this for each of the grid boxes would provide a clear perspective of the amount of protection provided by each of the functions. Different combinations of safety function availability and unavailability could be presented through the use of additional columns for making performance comparisons. Such analyses and comparisons provide a process for quantifying the role of various levels of protection, and hence, a quantification of contribution to defense-in-depth provided by different levels of protection.

TURNING UP THE MICROSCOPE

Now, the functional level shown in Figure 1 is too high a level to reveal performance characteristics of specific systems and barriers. To do that we need to turn up the microscope. Consider the grid box formed by the intersection of "Loss of Coolant" and "Inventory Control" of Figure 1. Suppose we detail that grid box into Figure 3.

Loss of Coolant Initiators	Safety Systems								Core Damage Frequencies
	Vessel Level Makeup								
	Feedwater and Condensate	High-Pressure Core Spray	Reactor Core Isolation Cooling	Automatic Depressurization	Residual Heat Removal (Low-Pressure Core Isolation)	Low-Pressure Core Spray	Fire Water	Reactor Coolant System	
Extreme LOCA	1. 2. 3.	Et.							
Large LOCA									
Small LOCA									
Breaks Outside Containment									
Interfacing System LOCA									
Other LOCAs									
Core Damage Frequency Due to Loss of Coolant IEs	$= \sum (\text{CDFs of IE Categories})$								

FIGURE 3. BWR SAFETY SYSTEMS

Figure 3 divides the "Loss of Coolant" class of initiating events into six initiating event categories. It divides the "Inventory Control Systems" into eight more clearly defined protection systems. This level of detail is usually sufficient to provide quantitative engineering information on the levels of protection against exposing the public and the environment to radiation. The entries in the grid boxes can be the same as Figure 1 or modified as appropriate. In particular, Figure 2a indicates the unavailability of the safety system on demand, given the applicable initiating event. It reveals the reliability of the system under the conditions that the system is called on to operate and is the input used in the calculation of the core damage frequency for each specific category of initiating events. Figure 2b is the core damage frequency as a result of a particular category of initiating events, given the unavailability of the safety system (e.g., if that safety system were not present).

Figure 2c is a key result in the quantification of the defense-in-depth of safety system protection. It is the total core damage frequency with and without the specific safety system being analyzed. It is important to note that Figure 2c is a different CDF than the one on which Figure 2b is based. The Figure 2b CDFs are those of Column 6. The Figure 2c CDF is the probabilistic sum of the Column 6 CDFs.

APPLICATION TO NUCLEAR WASTE REPOSITORIES

Defense-in-depth of a nuclear waste repository takes the form of passive barriers whose performance must be analyzed over tens and hundreds of thousands of years. A two-dimensional display similar to the above can be constructed to exhibit the contributions of the levels of defense associated with a repository design. The functional barriers protecting the biosphere from radioactive contamination are, as shown in Figure 4, the spatial and flow control of water, the waste package containment, and the control of the mobilization and transport of radionuclides. The effectiveness of these barriers must be analyzed under a set of "geological scenarios" representing the possible climatological and geological events that might occur over tens and hundreds of thousands of years of the repository history. In Figure 4 these scenarios are represented in rows 2, 3, and 4. Row 1 represents the "base case" or "expected" scenario.

The point of Figure 4 is to display the contribution of the individual functional barriers to preventing the release of radioactivity to the biosphere. For this purpose we take, as the repository performance measure, the peak annual release to the biosphere, measured in curies.

In Figure 4, the rightmost column shows our state of knowledge about the peak annual release to the biosphere under the four geological scenarios. In the individual boxes of Figure 4 we display a pair of curves of the type shown in Figure 5. The curves show the contributions of the individual protective barriers by showing how the peak annual release would increase if that barrier were not present.

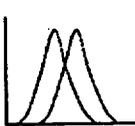
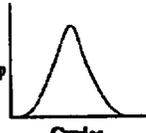
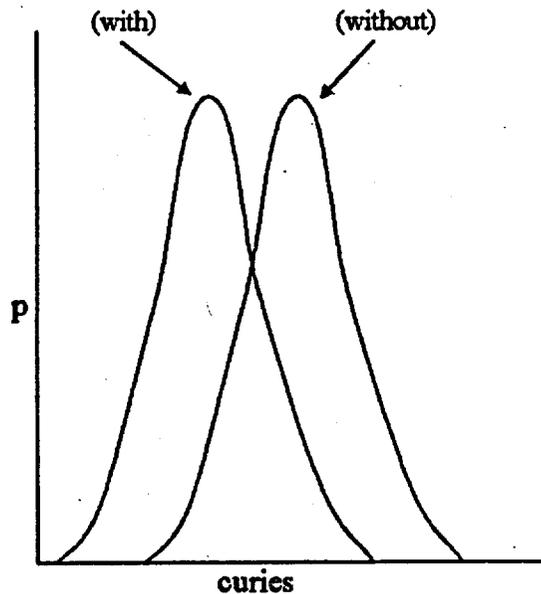
Initiating Conditions	Protective Barrier Functions			Peak Annual Release to the Biosphere (Curies)
	Water Flow and Spatial Control	Waste Package Containment	Radionuclide Mobility Control	
Current Climate		Etc.		
Geotechnical Events				
Wet Climate				
Increased Geotechnical Activity				

FIGURE 4. REPOSITORY PROTECTIVE BARRIER FUNCTIONS



Peak Annual Release
(With and Without Barrier)

FIGURE 5. PERFORMANCE COMPARISON

In Figure 6 we "turn up the microscope" on Figure 4 and recognize that the "barriers" shown in Figure 4 are actually composed of specific protective barriers. For example, the barrier "Water Flow and Spatial Control" of Figure 4 is now recognized as being composed of "Surface Runoff," which refers to a drainage system on the surface above the repository. Such a drainage system would divert the surface rainfall so as to prevent it from infiltrating into the ground above the repository. The column labeled "Water Diversion (Geotechnical)" refers to engineering the subsurface geology such as by the design of a Richards barrier. The column labeled "Water Diversion (Engineered Systems)" represents those engineered systems in the near field explicitly introduced to keep water from reaching the waste package. The rest of the columns are pretty much self-explanatory.

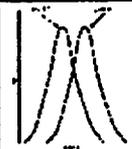
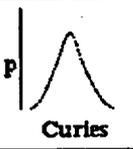
Initiating Conditions	Protective Barriers							Peak Annual Release to the Biosphere (Curies)
	Water Flow & Spatial Control Systems			Waste Package Containment		Radionuclide Mobility Control Systems		
	Surface Runoff	Water Diversion (Geotechnical)	Water Diversion (Engineered Systems)	Corrosion Resistance	Fuel Cladding	Chemical Additives	Solubility, Retardation, Dilution	
Current Climate		Etc.						
Geotechnical Events								
Wet Climate								
Increased Geotechnical Activity								

FIGURE 6. PROTECTIVE BARRIERS

The individual boxes of Figure 6 show the impact of the protective barriers on repository performance by displaying what the peak annual release would be if that protective barrier were not present.

A Definition of Defense in Depth

G. Apostolakis, January 13, 2000

Defense in depth is a safety philosophy that requires that a set of provisions be taken to manage unquantified uncertainty associated with the performance of engineered systems.

Observations:

- **"Defense in depth" and "multiple barriers" are not identical concepts. For quantified uncertainties, "multiple barriers" are standard engineering tools.**
- **"Multiple barriers" will always be used regardless of whether defense in depth is a principle or not.**
- **"Unquantified uncertainty" is primarily due to model inadequacy.**
- **The focus on unquantified uncertainty will force an examination of the quality of the analyses and will suggest improvements.**

- **Crucial question: Under what conditions, if any, is defense in depth a *principle*?**
- **Calling defense in depth a *principle* makes it impervious to analysis.**
- **"I am much more comfortable with defense in depth as a means to address the question of what if we are wrong in our analyses. You can argue that this is just a kind of uncertainty, but I think that argument trivializes the problem or implies that we know more than we do." (D. Powers)**
- **This is what is wrong with declaring defense in depth a *principle*. Regardless of the quality of the analysis, a Damoklean sword¹ will always hang over my head. Why should I even try to improve my analysis? (GA)**

¹Damokles: A courtier of ancient Syracuse held to have been seated at a banquet beneath a sword hung by a single hair.

DEFENSE-IN-DEPTH for YUCCA MOUNTAIN:

SOME COMMENTS

ROBERT J. BUDNITZ

Future Resources Associates, Inc.

2039 Shattuck Avenue, Suite 402

Berkeley, California 94704 USA

Tel: (510) 644-2700

e-mail: BUDNITZ @ PACBELL.NET

ACRS-ACNW JOINT SUBCOMMITTEE MEETING

ON DEFENSE-IN-DEPTH

JANUARY 13 - 14, 2000

A DILEMMA

"The Commission does not intend to specify numerical goals for the performance of individual barriers." [page 8649, third column]

"In implementing this [defense-in-depth] approach, the Commission proposes to incorporate flexibility into its regulations by requiring DOE to demonstrate that the geologic repository comprises multiple barriers, but"

BUT

"... but not prescribe which barriers are important to waste isolation or the methods to describe their capability to isolate waste." [page 8650, first column]

[from "Supplementary Information" to Draft Part 63, Section VIII]

SECTION VIII near the end, page 8650

"The proposed requirements will provide for a system of multiple barriers to ensure defense in depth and increase confidence that the postclosure performance objective will be achieved."

QUESTION ONE:

Will NRC use defense-in-depth as a decision criterion?

or, more directly,

Can DOE's license application "flunk" based on insufficient defense-in-depth, even if it would otherwise "pass"?

[The answer to this Question is apparently "yes".]

QUESTION TWO:

If so, how? How will the decision be framed and made?

Observation: The decision criteria need to be clear, fair, and technically logical.

QUESTION THREE

Perhaps, in practice - and despite NRC's words to the contrary --
- DOE will never actually be found to "flunk", but defense-in-depth will be used by NRC instead more like ALARA: "Do what you can, beyond meeting the bare regulations, whenever it's cost-effective".

How does NRC conceive that this would work in practice? Might NRC ask for more protection from one or another barrier in the name of defense-in-depth, even if the overall performance "passes"?

What if one barrier provides "90% of the total protection?"
Maybe DOE would "weaken" that barrier so that it would only provide 40%; if the entire repository still "passes", is this desirable?

[I am sorry to be sarcastic here - It is obviously undesirable. But this is related to a complaint that I've heard along the lines of "DOE's protection almost all comes from the canister; DOE is engineering their way around a poor site."]

OBSERVATION:

[from Budnitz letter of 25 June 1999]

"When I apply these ideas to Yucca Mountain, I stumble principally because the notion of so-called independent barriers (one of which can fail without compromising the overall system), which notion has been so useful conceptually for achieving and demonstrating power-reactor safety, seems not to apply to the Yucca Mountain repository system.

"As I understand the Yucca Mountain design concept, one cannot assume total failure of any of the so-called "barriers" without seriously compromising the overall performance!"

ASSUME PARTIAL FAILURE?

So perhaps NRC is not thinking about asking DOE to assume total failure --- perhaps DOE need only assume "partial" failure, for which the term "under-performance" is sometimes used.

What does that mean?

What analysis requirements (leading to some sort of decision criterion) will satisfy my three figures-of-merit: that the decision criterion must be clear, fair, and technically logical ?

ISSUES

- (1) If NRC lets DOE decide what "under-performance" means, what is to prevent the terrible problem known as "Bring me a rock --- sorry, wrong rock" ?
- (2) DOE will presumably not assume so much "under-performance" that the repository's overall ability to contain the waste is seriously compromised. But in fact, isn't that just what NRC's concern is, to look for combinations of "under-performance" that might lead to serious compromises?
- (3) So perhaps NRC needs to tell DOE how much "under-performance" to assume. Yet this leads to its own problems --- namely, NRC is trying not to be overly prescriptive!

ONE BASIC ISSUE: These are "sensitivity studies" that are always a good idea anyway. Why invoke them in the name of a philosophical notion like "defense-in-depth" that brings with it so much other baggage?

A Presentation for the Joint ACRS/ACNW Subcommittee
January 13, 2000

**DEFENSE-IN-DEPTH FOR RISK-INFORMED,
PERFORMANCE-BASED REGULATION:
A PROVISIONAL NMSS PERSPECTIVE**

Norman A. Eisenberg

(301) 415-7285
nae@nrc.gov

Senior Advisor for Performance Assessment
Division of Waste Management
Office of Nuclear Material Safety and Safeguards

OUTLINE

- 1. NMSS Motivations for Defense-in-Depth (DID)**
- 2. What is DID?**
- 3. How does DID differ from margin and other safety concepts?**
- 4. Provisional conclusions**
- 5. Residual issues**
- 6. Summary**

NMSS MOTIVATIONS FOR DEFENSE-IN-DEPTH

- **Risk-informing NMSS activities will include reexamination of regulatory approaches, including defense-in-depth (DID)**
- **Proposed Part 63 addresses DID with multiple barriers provision; many public comments on this subject**
- **Risk-informing regulation of interim spent fuel storage facilities**
- **ISA's for Fuel Cycle Facilities**
- **Risk-informing transportation regulations**

REGULATORY ENVIRONMENT IN NMSS

- **Wide range of licensees and systems regulated**
 - **Diverse systems**
 - **Complexity**
 - **Human interaction versus engineered aspects**
 - **Levels of hazard**
 - **Diverse capabilities for analysis among licensees**
 - **Diverse need/benefit/cost for risk-informing regulations**

- **Risk Considerations**
 - **individual risk to workers and public**
 - **normal and accident risk**
 - **perceived risk and actual risk**
 - **variety of initiators**
 - **mechanical failures**
 - **external events**
 - **human error**

PRINCIPAL FACTORS OF DID IN NMSS: CURRENT STATUS

- **Nature of licensees and activities regulated**
- **NMSS regulates systems with less hazard than nuclear power reactors**
- **NMSS regulations are a mix of performance-based and/or risk-informed and prescriptive, deterministic approach**
- **For some NMSS licensed activities, the hazard does not warrant very strong preventive measures of any type, performance-based or prescriptive**

NMSS SAFETY PHILOSOPHY

- Goal is reasonable assurance of protecting:
 - Public health and safety
 - Common defense and security
 - The environment

- Safety Concepts assist in achieving DID include:
 - Safety Margin
 - Diversity
 - Redundancy
 - No single point of failure
 - QA

- DID is a component of risk management

DEFINITION OF DEFENSE-IN-DEPTH

**(FROM THE COMMISSION WHITE PAPER ON
RISK-INFORMED PERFORMANCE-BASED REGULATION)**

- **Safety is not wholly dependent on any single element of the system**
- **Incorporation of DID produces a facility with greater tolerance of failures and external challenges**

STRUCTURALIST AND RATIONALIST APPROACHES TO DID

- **STRUCTURALIST APPROACH:**
 - The need for and extent of DID is related to the system structure
 - Many manifestations are based on knowledge and perspectives current when the systems were first developed or licensed
 - Some manifestations have an ad hoc basis

- **RATIONALIST APPROACH:**
 - The need for and extent of DID is related to the residual uncertainties in the system
 - The rationalist approach is just beginning to be applied in a risk-informed, performance-based regulatory environment

TYPES OF UNCERTAINTY IN SAFETY ASSESSMENTS

- **Parameter**
- **Model**
- **Scenario (including exposure scenario)**
- **Programmatic Factors (e.g., QA)**

TYPES OF RESIDUAL UNCERTAINTY

TYPE 1. (BEST AVAILABLE RISK ASSESSMENT)

A system for which a fairly complete risk analysis or safety analysis has been performed, so residual uncertainty relates to the confidence or lack of confidence in the analysis; i.e., the analysis does not represent all uncertainty, because the state of knowledge is incomplete.

TYPE 2. (LIMITED RISK ASSESSMENT)

A system for which the risk or safety analysis is somehow limited, e.g. by not being complete, or not quantifying certain types of uncertainty.

TYPE 1 LIMITATIONS OF RISK ANALYSES

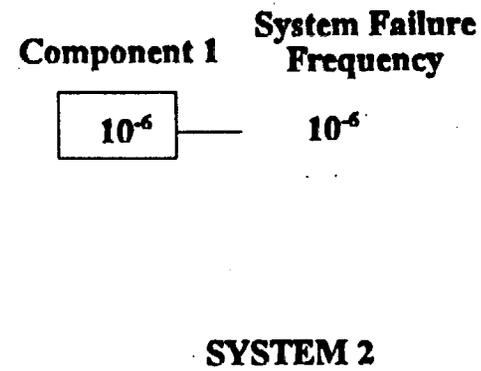
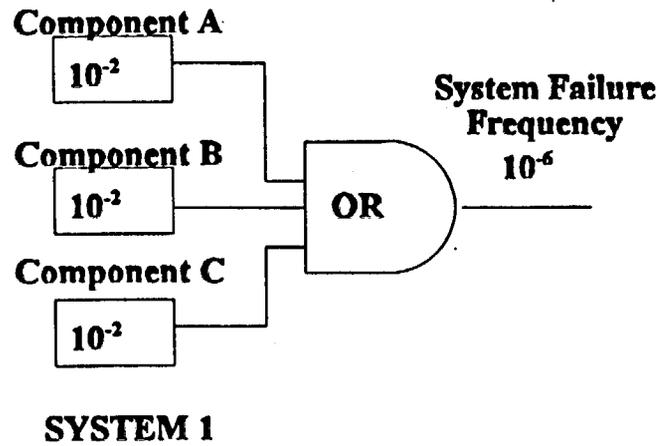
- **Risk Assessments are incomplete**
 - **Not all failure modes are included, because failure modes, not known now, are a threat to system performance**
 - **Currently unknown or unrecognized phenomena are not included in consequence models**
- **The range of variability in system parameters has been underestimated or biased**
- **Probabilities and consequences for rare events are based on sparse or non-existent data**
- **Models used to estimate consequences and probabilities in some cases cannot be validated**
- **Although systematic analyses can give great insights into the performance of new systems, some problems only come to light with experience**
- **The state of knowledge is evolving**

TYPE 2 LIMITATIONS OF RISK ANALYSES

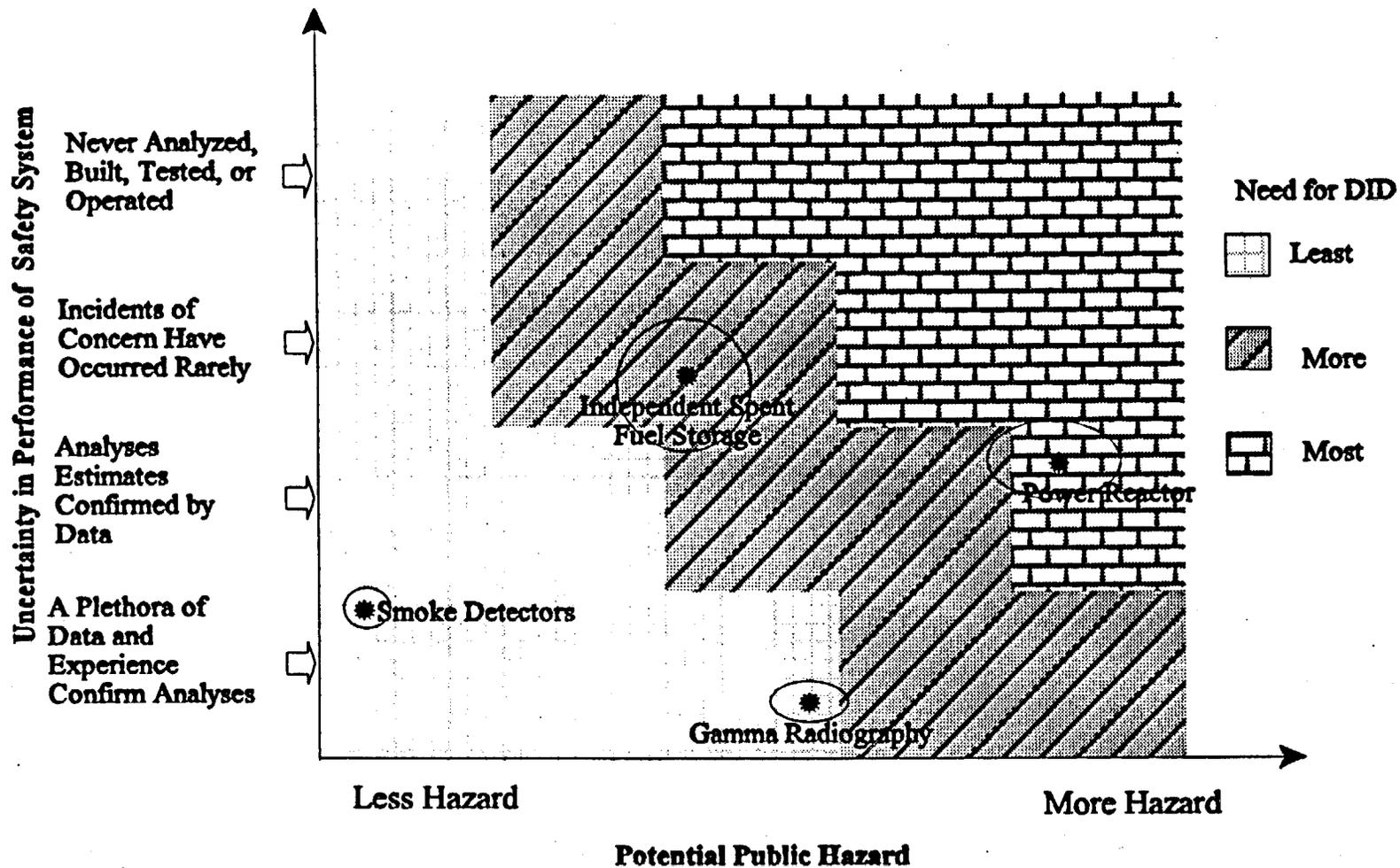
- **Risk Assessments are incomplete**
 - **Not all failure modes are included**
 - **Because of limitations on time and resources**
 - **Because procedures to enumerate all failure modes were misapplied and some failure modes were left out**
 - **Phenomena are not included in consequence models, because they are incorrectly considered unimportant or for reasons of economy**
- **Only certain kinds of uncertainty are explicitly represented in the risk assessment**
 - **Parameter uncertainty may or may not be propagated in consequence models**
 - **Model uncertainty may or may not be represented**
 - **Probabilities of various scenarios and uncertainty in the probabilities may or may not be represented**
 - **Not all quantifiable uncertainty may be quantified**
- **Models used to estimate consequences and probabilities have not been validated.**

DIFFERENCES BETWEEN DID AND MARGIN

- **Margin relates to the “cushion” between required performance and anticipated or predicted performance.**
- **DID relates to the characteristic of the system to: (1) not rely on any single element of the system and (2) be more robust to challenges**
- **Margin describes expected performance of a system versus the safety limit; DID describes the ability of the system to compensate for unanticipated performance, which results from limitations on knowledge.**
- **Increasing margin in a system that relies on a single component, does not necessarily increase DID.**
- **DID provides that if any component under-performs, the rest of the system compensates, so consequences are not unacceptable.**



Two different systems, both meeting the system risk goal of 10^{-4} , but exhibiting different DID characteristics.



Example of how need for defense-in-depth can be related to: (1) the uncertainty in the performance of the safety system and (2) the potential hazard posed by the system. Note: the positions of the various systems involves uncertainty on both axes.

PROVISIONAL CONCLUSIONS ABOUT DID

- 1. DID is related to, but different from, other safety concepts such as safety margin, redundancy, and diversity.**
- 2. DID is not necessarily equivalent to meeting a safety goal or the margin associated with meeting the goal.**
- 3. DID can be implemented in a risk-informed, performance-based regulatory context as a system requirement, rather than as a set of subsystem requirements.**
- 4. DID can be used to address residual uncertainties concerning the performance of a safety system.**
- 5. The need for DID depends on:**
 - a. Degree of residual uncertainty**
 - b. Degree of hazard**

PARTIAL LIST OF ISSUES TO BE RESOLVED

- **How to measure the degree of DID?**
- **How to measure the degree of uncertainty in performance of the safety system, encompassing quantified and unquantified uncertainty?**
- **How to measure the degree of potential hazard posed by a system?**
- **How to implement DID when the degree of uncertainty about different system components is not uniform?**
- **How to use current state of knowledge to make reasonable tests for a system to have sufficient DID, which allows for incomplete knowledge?**
- **How to explain to stakeholders the flexibility inherent in a risk-informed, performance-based approach to DID, which also provides reasonable assurance of safety?**

SUMMARY

- NMSS intends to consider implementation of DID in the context of risk-informed, performance-based regulation.
 - In ongoing regulatory activities
 - As part of the evolving risk-informed framework for NMSS
- As a general safety principle, the degree of DID needed to assure safety depends on several factors including:
 - Degree of residual uncertainty
 - Degree of hazard
- NMSS plans to implement DID as a system requirement, where feasible, rather than by prescriptive, subsystem requirements.
- NMSS needs flexibility in any overall approach in implementing DID to permit appropriate regulation for the range of systems regulated

BACKUP SLIDES

COMMISSION WHITE PAPER ON RISK-INFORMED PERFORMANCE-BASED REGULATION

“Defense-in-depth is an element of the NRC's Safety Philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility. The defense-in-depth philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility. The net effect of incorporating defense-in-depth into design, construction, maintenance, and operation is that the facility or system in question tends to be more tolerant of failures and external challenges.”

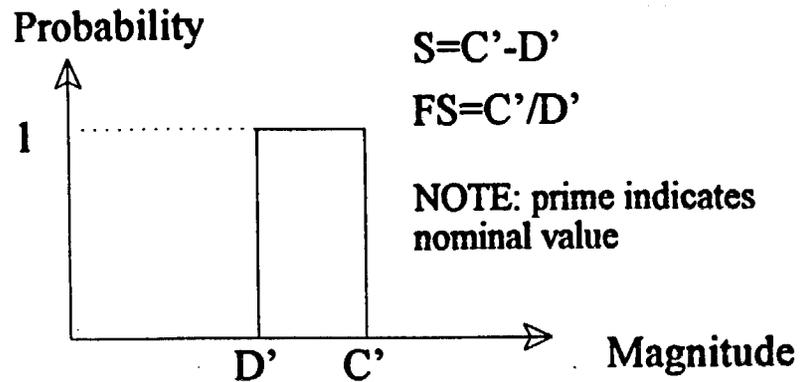


Figure (a) Deterministic System

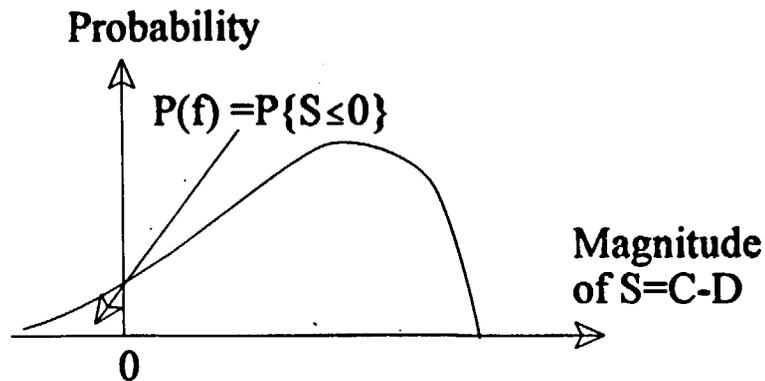


Figure (c) Safety Margin as a random variable.

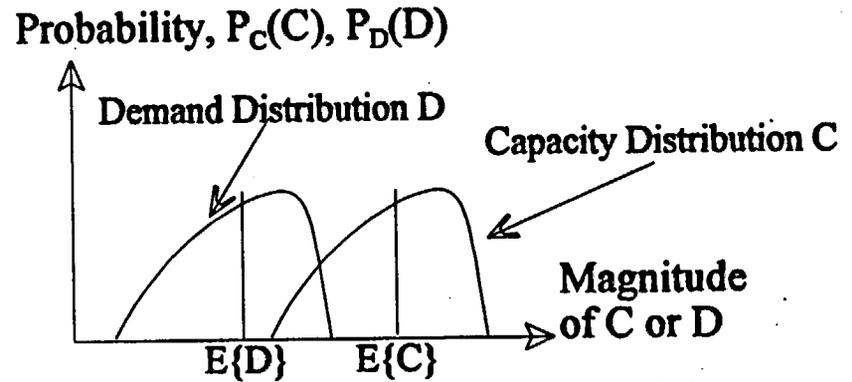


Figure (b) Capacity-Demand Model

D = Demand

C = Capacity

$S = C - D =$ Safety Margin

$FS = C/D =$ Factor of Safety

$CFS = E\{C\}/E\{D\} =$ Central Factor of Safety

THE CONCEPT OF MARGIN IN A PROBABILISTIC CONTEXT

Implementing the Multiple Barriers Requirement in a Geologic Repository for High-Level Waste: Current Thinking



Presentation to the Joint ACRS/ACNW Subcommittee

January 13, 2000

Christiana H. Lui

Division of Waste Management/NMSS

(301)415-6200/CXL@NRC.GOV



Introduction

- ◆ Extended public comment period on the proposed 10 CFR Part 63 ended on June 30, 1999; final rule to the Commission by March 31, 2000
- ◆ Work in progress
 - Objective is to share staff's best current thinking in clarifying the multiple barriers provision for postclosure safety evaluation
 - Defense in depth in preclosure safety evaluation is implemented through accident prevention, mitigation and intervention (e.g., emergency planning)



Intent Of Multiple Barriers

- ◆ Consistent with NRC's safety philosophy as stated in *Commission's White Paper on Risk-Informed and Performance-Based Regulation*
- ◆ Implemented as an assurance requirement in Part 63 to provide confidence that
 - ✓ Known uncertainties are appropriately captured in the compliance demonstration calculations
 - ✓ The repository system is sufficiently robust to account for imperfect knowledge



Consideration of Multiple Barriers Requirements in Part 63

- ◆ Assess all significant negative impacts on safety in the compliance demonstration calculations
- ◆ Identify all barriers in the above analysis
- ◆ Describe and quantify capabilities of the barriers
- ◆ Perform additional analyses to show **safety does not wholly dependent on any single barrier**
- ◆ Provide technical basis



Demonstration of Multiple Barriers

- ◆ Show balance of the repository system has the ability to compensate for an under-performing barrier so public health and safety are protected



Technical Issues For Multiple Barriers Analysis

- ◆ What should be the degree of barrier under-performance?
 - Performance-based
 - Prescriptive

- ◆ How should NRC evaluate the outcome of barrier under-performance analysis?



Demonstration of Multiple Barriers - Staff's Best Current Thinking

- ◆ Uses individual dose to evaluate the outcome of barrier under-performance analysis
- ◆ DOE quantifies the amount of under-performance for each barrier that can be compensated by the balance of the repository system to illustrate the extent of system resilience



Summary

- ◆ Multiple barrier is a system requirement for licensing a potential high-level waste repository at Yucca Mountain
- ◆ NRC will determine whether DOE has shown that the repository meets applicable regulations
 - ✓ Both geologic and engineered barriers contribute to safety
 - ✓ The repository system has the ability to compensate for under-performance of any one barrier
 - ✓ Not seeking complete redundancy



Summary (Continued)

- ◆ Extended public comment period on the proposed 10 CFR Part 63 ended on June 30, 1999; final rule to the Commission by March 31, 2000
 - Staff consideration of the public comments is well underway
 - Information received during this meeting will be available to the staff in preparing responses to the public comments, drafting the final rule and developing guidance in the Yucca Mountain Review Plan
 - Transcript of this meeting will be made available to the public on the rulemaking website



DEFENSE-IN-DEPTH: PERSPECTIVE FOR

RISK-INFORMING 10 CFR 50

presentation to

JOINT ACNW/ACRS SUBCOMMITTEE

T. L. King, RES

G. M. Holahan, NRR

January 13, 2000

BACKGROUND

- No formal regulation or agency policy statement on DID
- Commission White Paper on Risk-Informed Regulation (March 11, 1999):
“Defense-in-depth is an element of the NRC’s Safety Philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility. The defense-in-depth philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility. The net effect of incorporating defense-in-depth into design, construction, maintenance, and operation is that the facility or system in question tends to be more tolerant of failures and external challenges.”
- This philosophy is implemented in a number of ways depending on the specific program.

REACTOR PROGRAM
DEFENSE-IN-DEPTH

- Included in Reactor Regulation (e.g., GDC, SRP ...)
- Included in Licensing and License Amendment Process
- Included in Reactor Oversight Process

APPLICATION OF DID IN REACTOR REGULATION

- **Current Part 50 requirements include DID considerations:**
 - prevention and mitigation
 - single failure criterion
 - redundancy/diversity
 - barriers to FP release (cladding, RCS, containment)
 - EP
 - quality of design and operation

- **Application of DID varies:**
 - AOOs - DID in response to initiating events
 - DID preserves barrier integrity
 - DBAs - DID in response to and mitigation of initiating events
 - DID preserves mitigation
 - Severe Accidents - DID in mitigation

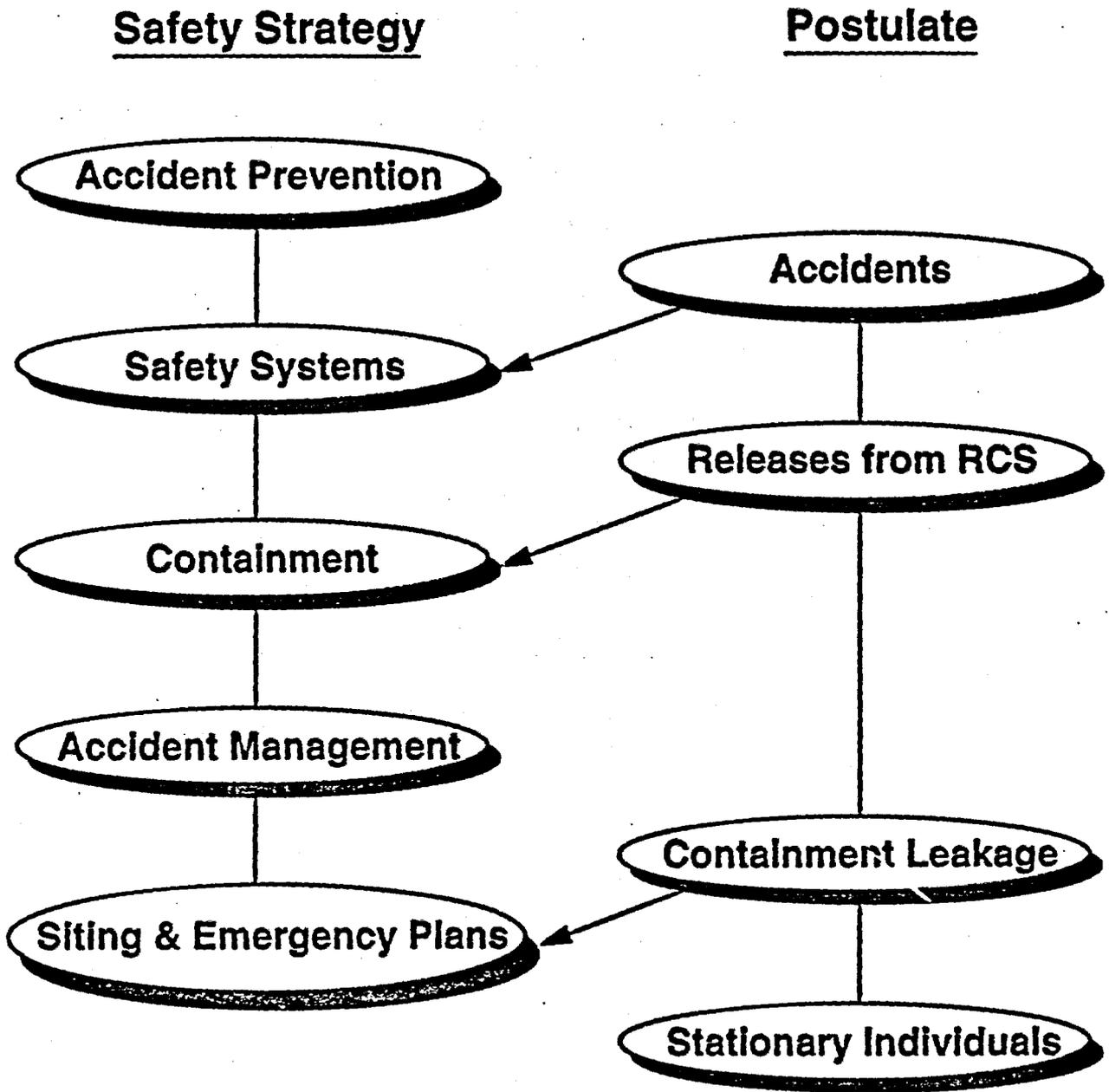


Figure 1.1-1 Defense in depth, safety strategies

**TABLE 1.1-1
DEFENSE IN DEPTH
MULTILAYER PROTECTION FROM FISSION PRODUCTS**

Barrier or Layer	Function
1. Ceramic fuel pellets	Only a fraction of the gaseous and volatile fission products is released from the pellets.
2. Metal cladding	The cladding tubes contain the fission products released from the pellets. During the life of the fuel, less than 0.5 percent of the tubes may develop pinhole sized leaks through which some fission products escape.
3. Reactor vessel and piping	The 8- to 10-inch (20- to 25-cm) thick steel vessel and 3- to 4-inch (7.6- to 10.2-cm) thick steel piping contain the reactor cooling water. A portion of the circulating water is continuously passed through filters to keep the radioactivity low.
4. Containment	The nuclear steam supply system is enclosed in a containment building strong enough to withstand the rupture of any pipe in the reactor coolant system.
5. Exclusion area	A designated area around each plant separates the plant from the public. Entrance is restricted.
6. Low population zone, evacuation plan	Residents in the low population zone are protected by emergency evacuation plans.
7. Population center distance	Plants are located at a distance from population centers.

REACTOR PROGRAM
DEFENSE-IN-DEPTH

General Design Criteria

- I. (GDC1-5) Overall Requirements
- II. (GDC 10-18) Protection by Multiple Fission Product Barriers
- III. (GDC 20-29) Protection and Reactivity Control Systems
- IV. (GDC 30-46) Fluid Systems
- V. (GDC 50-57) Reactor Containment
- VI. (GDC 60-64) Fuel and Radioactivity Control

REACTOR OVERSIGHT PROGRAM

DEFENSE-IN-DEPTH

- Reactor Oversight Process uses “cornerstones” as a central element in its formulation
- Cornerstones are a Defense-in-depth concept

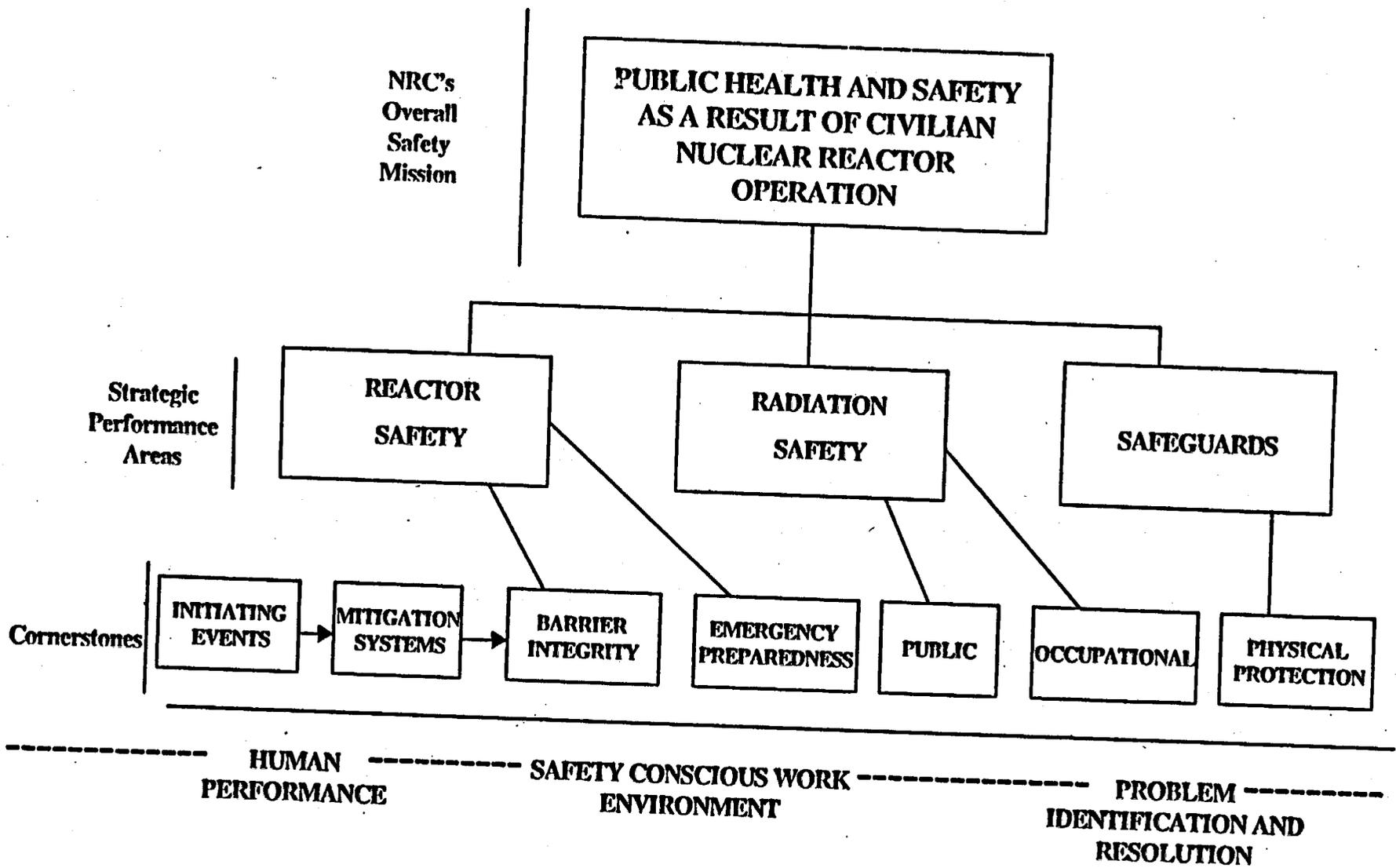


Figure 1- Cornerstones of Safety

Table 1 - PERFORMANCE INDICATORS

Cornerstone	Indicator		Thresholds		
			Increased Regulatory Response Band	Required Regulatory Response Band	Unacceptable Performance Band
Initiating Events	Unplanned scrams per 7000 critical hours (automatic and manual scrams)		>3	>6	>25
	Risk-significant scrams per 3 years		>4	>10	>20
	Transients per 7000 critical hours		>8	N/A	N/A
Mitigating Systems	Safety System Performance Indicator Unavailability	HPCI and RCIC	>0.04	>0.12	>0.5
		HPCS	>0.015	>0.04	>0.2
Emergency Power		>0.025	>0.05 (>2EDG >0.1)	>0.1 (>2EDG >0.2)	
RHR		>0.015	>0.05	TBD	
AFW		>0.02	>0.06	>0.12	
	HPSI	>0.015	>0.05	TBD	
	Safety System Failures		>5 - prior 4 qtrs	N/A	N/A
Barriers - Fuel Cladding - Reactor Coolant System - Containment	Reactor coolant system (RCS) specific activity		>50% of TS limit	>100% of TS limit	N/A
	RCS leak rate		>50% of TS limit	>100% of TS limit	N/A
	Containment leakage		>100% L _A	N/A	N/A
Emergency Preparedness	Emergency Response Organization (ERO) drill/exercise performance		<75% - prior 6 months; <90% - prior 2 years	<55% - prior 6 months; <70% - prior 2 years	N/A

Table 1 - PERFORMANCE INDICATORS

Cornerstone	Indicator	Thresholds		
		Increased Regulatory Response Band	Required Regulatory Response Band	Unacceptable Performance Band
	ERO readiness (percentage of ERO shift crews that have participated in a drill or exercise in the past 24 months)	<80% - prior 2 years; <90% - prior 3 years	<60% - prior 2 years; <70% - prior 3 years	N/A
	Alert and Notification System performance (percentage of availability time)	<94% per year	<90% per year	N/A
Occupational Radiation Safety	Occupational exposure control effectiveness (the number of non-compliances with 10 CFR 20 requirements for (1) high (greater than 1000 mRem/hour) and (2) very high radiation areas, and uncontrolled personnel exposures exceeding 10% of the stochastic or 2% of the non-stochastic limits)	6 or more occurrences in 3 years (rolling average); 3 or more in 1 year	12 or more occurrences in 3 years (rolling average); 6 or more in 1 year	N/A
Public Radiation Safety	Offsite release performance (number of effluent events that are reportable per 10 CFR 20, 10 CFR 50 Appendix I, Offsite Dose Calculation Manual, or Technical Specifications)	7 or more events in 3 years (rolling average); 4 or more events in 1 year	14 or more events in 3 years (rolling average); 8 or more events in 1 year	N/A
Physical Protection	Protected Area security equipment performance (availability of systems to perform their intended functions)	<95% per year	<85% per year	N/A
	Vital Area security equipment performance (availability of systems to perform their intended functions)	<95% per year	<85% per year	N/A
	Personnel screening process performance (acceptable implementation of the access authorization program)	3-5 reportable events	6 or more reportable events	N/A

LICENSEE PERFORMANCE INCREASING SAFETY SIGNIFICANCE ----->						
RESULTS		I. All Assessment Inputs (PIs and Cornerstone Inspection Areas) Green; Cornerstone Objectives Fully Met	II. One or Two Inputs White (In different cornerstones); Cornerstone Objectives Fully Met	III. One Degraded Cornerstone (2 Inputs White or 1 Input Yellow) or any 3 White Inputs; Cornerstone Objectives Met with Minimal Reduction in Safety Margin	IV. Repetitive Degraded Cornerstone, Multiple Degraded Cornerstones, or Multiple Yellow Inputs; Cornerstone Objectives Met with Significant Reduction in Safety Margin	V. Overall Red (Unacceptable) Performance; Plants Not Normally Permitted to Operate Within this Band, Unacceptable Margin to Safety
	RESPONSE	Management Meeting	Routine Resident Inspector Interaction	SRI/BC Meet with Licensee	DD/RA Meet with Licensee Management	EDO Meet with Senior Licensee Management
	Licensee Action	Licensee Corrective Action	Licensee Corrective Action with NRC Oversight	Licensee Self Assessment with NRC Oversight	Licensee Performance Improvement Plan with NRC Oversight	
	NRC Inspection	Risk-Informed Baseline Inspection Program	Inspection Follow-up	Inspection Focused on Cause of Degradation	Team Inspection Focused on Cause of Overall Degradation	
	Regulatory Actions	None	-Document Response to Degrading Area in Inspection Report	-Docket Response to Degrading Condition (Consider N+1 Inspection for 2 Consecutive Cycles in This Range)	-10 CFR 50.54(f) Letter - CAL/Order (Consider N+1 Inspection for 2 Consecutive Cycles in This Range)	Order to Modify, Suspend, or Revoke Licensed Activities
COMMUNICATION	Assessment Report	DD review/sign assessment report (w/ inspection plan)	DD review/sign assessment report (w/ inspection plan)	RA review/sign assessment report (w/ inspection plan)	RA review/sign assessment report (w/ inspection plan)	RA review/sign assessment report (w/ inspection plan)
	Public Assessment Meeting	SRI or Branch Chief Meet with Licensee	SRI or Branch Chief Meet with Licensee	RA Discuss Performance with Licensee	EDO Discuss Performance with Senior Licensee Management	Commission Meeting with Senior Licensee Management to Discuss Licensee Performance
----- Regional Review Agency Review ----->						

Table 5 - Action Matrix

ISSUES RELATED TO APPLICATION OF DID IN REACTOR RISK-INFORMED ACTIVITIES

- RI - License Amendments:
 - RG 1.174 guidance on DID.

- RG 1.174 - lists elements of DID
 - balance between prevention and mitigation
 - avoid over-reliance on programmatic activities
 - system redundancy, diversity, independence
 - defense against common cause failures
 - independence of barriers
 - defense against human errors
 - intent of GDCs

- RI - Part 50:
 - working definition of DID for:
 - OPTION 2 (scope)
 - OPTION 3 (technical requirements)

- Policy Issues:
 - is a definition of DID needed in the Safety Goal Policy?
 - is a separate policy statement needed on DID?

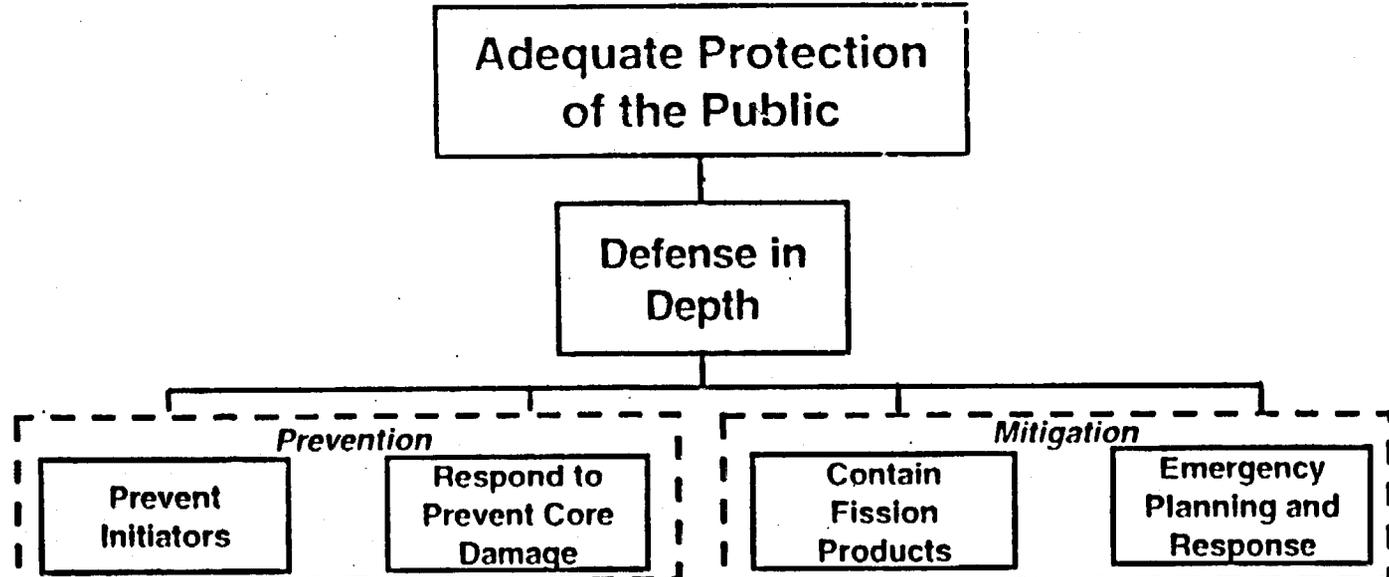
DEVELOPMENT OF A WORKING DEFINITION OF DID

- Purpose of Working Definition of DID:
 - establish an approach to be used in risk-informing 10 CFR Part 50 that provides:
 - multiple lines of defense
 - balance between prevention and mitigation
 - a framework to address uncertainties in accident scenarios:
 - likelihood
 - reliability
 - consequence (phenomena modeling)
 - success criteria
 - completeness
- Elements of Working Definition:
 - DID should consist of two parts:
 - fundamental elements that should be provided in all cases
 - implementation elements that may vary depending on uncertainty and reliability and risk goals.

WORKING DEFINITION OF DID FOR REACTORS

- Fundamental Elements:
 - build upon cornerstone concept:
 - initiating events
 - prevent core melt
 - contain fission products
 - EP & R
 - assure prevention and mitigation by providing:
 - reliable core melt prevention for all credible initiating events:
 - single failure criterion?
 - active vs. passive failure?
 - human performance?
 - redundancy/diversity?
 - ability to contain FP given a core melt
 - EP & R
 - assure balance between prevention and mitigation to achieve overall level of safety consistent with:
 - $\leq 10^{-4}/\text{RY CDF}$
 - $\leq 10^{-5}/\text{RY LERF}$

CONCEPTUAL FRAMEWORK FOR BALANCE BETWEEN PREVENTION AND MITIGATION



- Guidelines: (1) Consider the four cornerstones in pairs:
 Initiators and Responses $<1E-4$ and Containment and Emergency Planning $<.01$, OR
- (2) Consider the cornerstones individually, based on initiator frequency
- | | | | | |
|--------------------|--------|--|------|-----------|
| Anticipated | | | | |
| Initiators $<1/yr$ | $1E-4$ | | $.1$ | $\leq .1$ |
| Infrequent | | | | |
| Initiators $<.01$ | $1E-2$ | | $.1$ | $\leq .1$ |
| Rare | | | | |
| Events $<1E-6$ | 1 | | 1 | 1 |

Basis: The overall metric is frequency of significant dose to an offsite individual
 Each row results in $1E-6$ (summed over the events)

WORKING DEFINITION (CONT.)

- Implementation Elements:
 - use of redundancy, diversity, and safety margins would be variable, as necessary, to achieve reliability and risk goals and balance of prevention and mitigation
 - use of QA, EQ, IST, etc., would be variable, as necessary, to achieve reliability goals
 - use mean values in assessing risk
 - must consider full power and shutdown condition.

APPLICATION OF WORKING DEFINITION

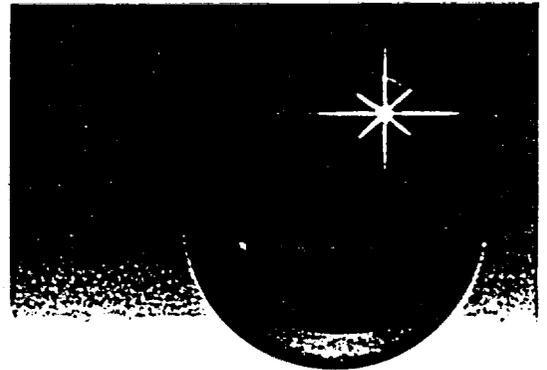
- Use for top down look at 10 CFR 50
- Apply to each credible initiating event.
- Do regulations, R.Gs., SRPs requirements result in achieving:
 - risk goals
 - balance between prevention and mitigation
 - lines of defense
- Do regulations, R.G. SRPs, adequately specify analysis methods and acceptance criteria?

EXECUTIVE

SUMMARY

EPRI

A L W R



**A D V A N C E D
L I G H T W A T E R R E A C T O R**

ADVANCED LIGHT WATER REACTOR
Utility Requirements Document

Issued 12/95

Introduction

The U.S. utilities are leading an industry wide effort to establish the technical foundation for the design of the Advanced Light Water Reactor (ALWR). This effort, the ALWR Program, is being managed for the U.S. electric utility industry by the Electric Power Research Institute (EPRI) and includes participation and sponsorship of several international utility companies and close cooperation with the U.S. Department of Energy (DOE). The cornerstone of the ALWR Program is a set of utility design requirements which are contained in the ALWR Utility Requirements Document.

Purpose of the Utility Requirements Document

The purpose of the Utility Requirements Document is to present a clear, complete statement of utility desires for their next generation of nuclear plants. The Utility Requirements Document consists of a comprehensive set of design requirements for future LWRs. The requirements are grounded in proven technology of 35 years of commercial U.S. and international LWR experience. Furthermore, the utility design requirements build on this LWR experience base, correcting problems which existed in operating plants and incorporating features which assure a simple, robust, more forgiving design.

The anticipated uses of the Utility Requirements Document are threefold:

- Establish a stabilized regulatory basis for future LWRs which includes the NRC's agreement on resolution of outstanding licensing issues and severe accident issues, and which provides high assurance of licensability;
- Provide a set of utility design requirements for a standardized plant which are reflected in individual reactor and plant supplier certification designs;
- Provide a set of utility technical requirements which are suitable for use in an ALWR investor bid package for eventual detailed design, licensing and construction, and which provide a basis for strong investor confidence that the risks associated with the initial investment to complete and operate the first ALWR are minimal.

Scope of Requirements Document

The Utility Requirements Document covers the entire plant up to the grid interface. It therefore is the basis for an integrated plant design, i.e., nuclear steam supply system and balance of plant, and it emphasizes those areas which are most important to the objective of achieving an ALWR which is excellent with respect to safety, performance, constructibility, and economics. The document applies to both Pressurized Water Reactors (PWRs) and Boiling Water Reactors (BWRs).

The Utility Requirements Document is organized in three volumes. Volume I summarizes ALWR Program policy statements and top-tier utility requirements.

Volumes II and III present the complete set of top-tier and detailed utility requirements for specific ALWR design concepts. Volume II covers Evolutionary ALWRs. These are simpler, much improved versions of existing LWRs, up to 1350 MWe, employing conventional but significantly improved, active safety systems. Volume III covers Passive ALWRs, greatly simplified, smaller (i.e., reference size 600 MWe) plants which employ primarily passive means (i.e., natural circulation, gravity drain, stored energy) for essential safety functions. Two passive design concepts are addressed in Volume III, the Passive BWR with pressure suppression containment and the loop-type Passive PWR with dry containment. While these Volume III concepts are not yet as completely developed as the Evolutionary ALWR, they extensively utilize existing LWR experience and Evolutionary ALWR utility requirements, and are expected to offer substantial advantages in constructibility and operability as well as the potential to surpass the very high ALWR safety standards.

In addition to the above Volume II and III ALWR concepts, there may be other design concepts which could be developed to meet ALWR Program objectives. Such design concepts are, however, not explicitly addressed in the Utility Requirements Document at this time.

ALWR Policies

The ALWR Program has formulated policies in a number of key areas in order to provide guidance for overall Utility Requirements Document development, and to provide guidance to the Plant Designer in applying the requirements. While not design requirements themselves, the policies cover fundamental ALWR principles which have a broad influence on the design requirements. A summary of key policy statements is as follows:

- Simplification -** Simplification is fundamental to ALWR success. Simplification opportunities are to be pursued with very high priority and assigned greater importance in design decisions than has been done in recent, operating plants; simplification is to be assessed primarily from the standpoint of the plant operator.
- Design Margin -** Like simplicity, design margin is considered to be of fundamental importance and is to be pursued with very high priority. It will be assigned greater importance in design decisions than has been done in recent, operating plants. Design margins which go beyond regulatory requirements are not to be traded off or eroded for regulatory purposes.
- Human Factors -** Human factors considerations will be incorporated into every step of the ALWR design process. Significant improvements will be made in the main control room design.
- Safety -** The ALWR design will achieve excellence in safety for protection of the public, on-site personnel safety, and investment protection. It places primary emphasis on accident prevention as well as significant additional emphasis on mitigation. Containment performance during severe accidents will be evaluated to assure that adequate containment margin exists.
- Design Basis Versus
Safety Margin -** The ALWR design will include both safety design and safety margin requirements. Safety design requirements (referred to as the Licensing Design Basis [LDB]) are necessary to meet the NRC's regulations with conservative, licensing-based methods. Safety margin requirements (referred to as the Safety Margin Basis [SMB]) are Plant Owner-initiated features which address investment protection and severe accident prevention and mitigation on a best estimate basis.
- Regulatory
Stabilization -** ALWR licensability is to be assured by resolving open licensing issues, appropriately updating regulatory requirements, establishing acceptable severe accident provisions, and achieving a design consistent with regulatory requirements.

E X E C U T I V E S U M M A R Y

- Standardization -** The ALWR utility requirements will form the technical foundation which leads the way to standardized, certified ALWR plant designs.
- Proven Technology -** Proven technology will be employed throughout the ALWR design in order to minimize investment risk to the plant owner, control costs, take advantage of existing LWR operating experience, and assure that a plant prototype is not required; proven technology is that which has been successfully and clearly demonstrated in LWRs or other applicable industries such as fossil power and process industries.
- Maintainability -** The ALWR will be designed for ease of maintenance to reduce operations and maintenance costs, reduce occupational exposure, and to facilitate repair and replacement of equipment.
- Constructibility -** The ALWR construction schedule will be substantially improved over existing plants and must provide a basis for investor confidence through use of a design-for-construction approach, and completed engineering prior to initiation of construction.
- Quality Assurance -** The responsibility for high quality design and construction work rests with the line management and personnel of the Plant Designer and Plant Constructor organizations.
- Economics -** The ALWR plant will be designed to have projected busbar costs that provide a sufficient cost advantage over the competing baseload electricity generation technologies to offset higher capital investment risk associated with nuclear plant utilization.
- Sabotage Protection -** The design will provide inherent resistance to sabotage and additional sabotage protection through plant security and through integration of plant arrangements and system configuration with plant security design.
- Good Neighbor -** The ALWR plant will be designed to be a good neighbor to its surrounding environment and population by minimizing radioactive and chemical releases.

ALWR Top-Tier Design Requirements

A brief summary of top-tier utility design requirements is provided in Table 1 for the ALWR. The top-tier utility design requirements are categorized by major functions, including safety and investment protection, performance, and design process and constructibility. There is also a set of general utility design requirements, such as simplification and proven technology, which apply broadly to the ALWR design, and a set of economic goals for the ALWR program. The top-tier utility design requirements are described further in Volume I and are formally invoked as utility requirements in Volumes II and III. These requirements reflect the ALWR Program policies described above and form the basis for developing the detailed system design requirements for specific ALWR concepts in Volumes II and III. Figure 1 shows the relationship of Volumes I, II, and III.

ALWR Implementation

Assuring that the role of the Utility Requirements Document is understood and is successfully carried out depends on an understanding of the relationship between the various activities which comprise ALWR implementation. Accordingly, implementation scenarios for the Evolutionary and Passive ALWRs have been developed. Though uncertainties still exist at this point, these scenarios are plausible enough to provide reasonable understanding of the relationships noted above. A key assumption in the implementation scenarios is that increasing demand for electricity in combination with concerns over the environment and greenhouse gas effects associated with fossil fuel burning will result in significant improvements in political and public acceptance of nuclear power in the U.S. The implementation scenarios are also based on the ALWR policy that a prototype plant is not required. Figure 2 shows the major milestones in the Evolutionary and Passive ALWR implementation scenarios.

Table 1. Summary of Top-Tier ALWR Plant Design Requirements

<i>Subject Area of Requirement</i>	<i>Statement of Requirement</i>
GENERAL UTILITY DESIGN REQUIREMENTS	
Plant type and size	PWR or BWR, applicable to a range of sizes up to 1350 MWe <ul style="list-style-type: none"> • Reference size for Evolutionary ALWR: 1200-1300 MWe per unit; • Reference size for Passive ALWR: 600 MWe per unit.

EXECUTIVE SUMMARY

Safety system concept	<p>Simplified safety system concepts:</p> <ul style="list-style-type: none">• Evolutionary ALWR - simplified, improved active systems;• Passive ALWR - primarily passive systems; safety-related ac electric power shall not be required.
Plant design life	60 years
Design philosophy	Simple, rugged, high design margin, based on proven technology; no power plant prototype required.
Plant siting envelope	Must be acceptable for most available sites in U.S.; 0.3g Safe Shutdown Earthquake (SSE).

SAFETY AND INVESTMENT PROTECTION

Accident resistance	<p>Design features that minimize the occurrence and severity of initiating events, such as:</p> <ul style="list-style-type: none">• Fuel thermal margin $\geq 15\%$;• Slower plant response to upset conditions through features such as increased coolant inventory;• Use of best available materials.
Core damage prevention	<p>Design features that prevent initiating events from progressing to the point of core damage.</p> <p>Demonstrate by PRA that core damage frequency is less</p> <ul style="list-style-type: none">• Core damage frequency than 10^{-5} per reactor year.• LOCA protection• Station blackout coping time for core cooling• Operator action
Mitigation	<p>No fuel damage for up to a 6-inch break</p> <p>8 hours minimum (indefinite for Passive ALWR)</p> <p>For passive ALWR, no core protection regulatory limits exceeded for at least 72 hours assuming no operator action for LDB events including loss of all power.</p> <p>Demonstrate by PRA that the whole body dose is less than 25 rem at the site boundary for severe accidents with cumulative frequency greater than 10^{-6} per year.</p>

- Equipment access Ready access to equipment.
- Equipment replacement Facilitate replacement of components, including steam generators.

Man-Machine Interface

- Instrumentation and control systems Advanced technology, including software based systems, alarm prioritization, fault tolerance, automatic testing, multiplexing, and computer driven displays.
- Operations simplicity A single operator able to control plants during normal power operation.
- Control stations Human engineered to enhance operator effectiveness, utilizing mockups, dynamic simulation, and operator input to design.

DESIGN PROCESS AND CONSTRUCTABILITY

Total time from owner commitment to construct to commercial operation 1300 MWe evolutionary plant designed for less than or equal to 72 months
600 MWe passive plant designed for less than or equal to 60 months

Construction time from first structural concrete to commercial operation 1300 MWe evolutionary plant designed for less than or equal to 54 months
600 MWe passive plant designed for less than or equal to 42 months

Design status at time of initiation of construction 90% complete

Design and plan for construction Design for simplicity and modularization to facilitate construction; develop an integrated construction plan through Plant Owner acceptance.

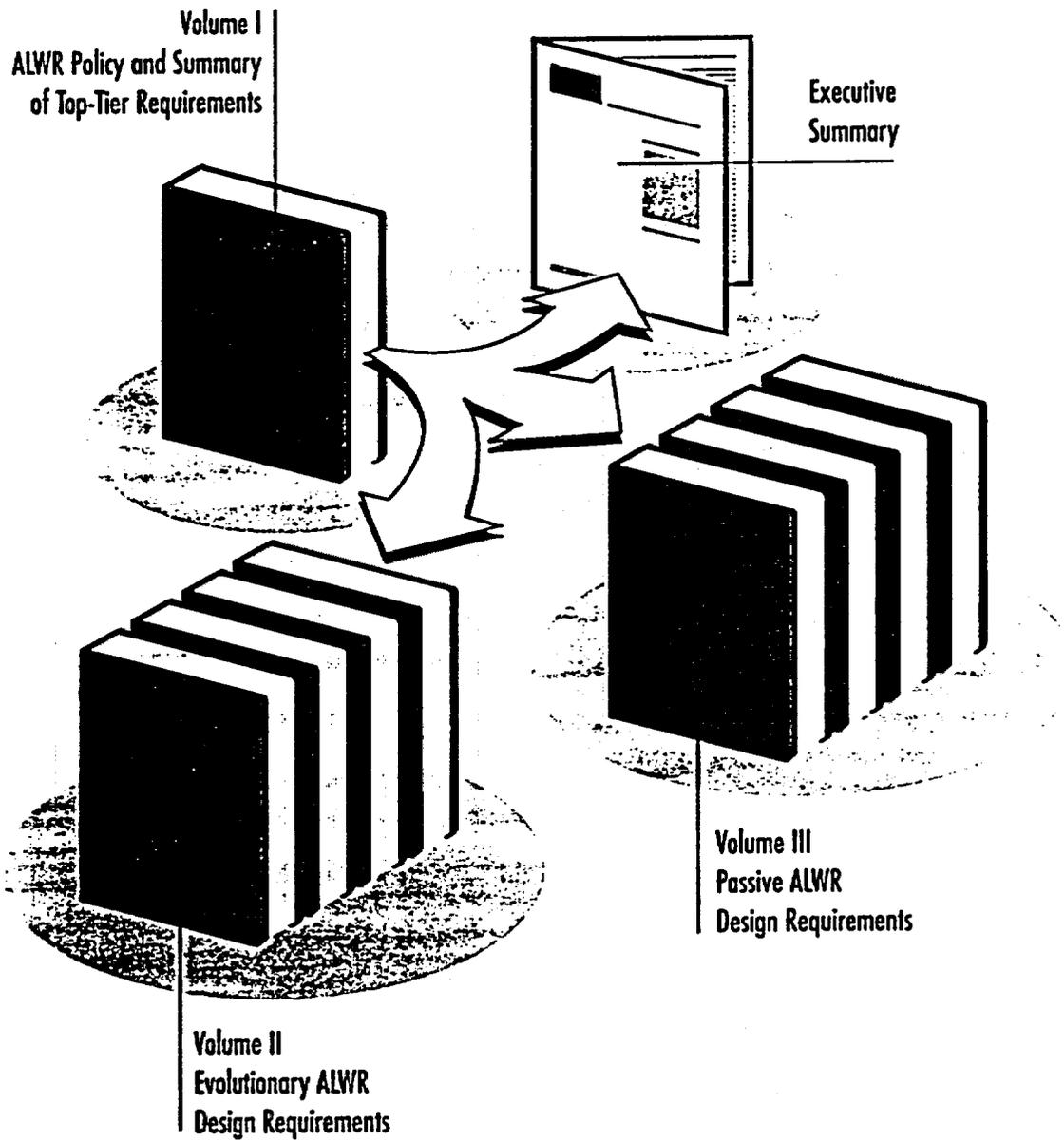
Design process

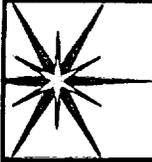
- Design integration Manage and execute design as a single, integrated process.
- Configuration management Comprehensive system to control plant design basis and installed equipment and structures.
- Information management Computerized system to generate and utilize an integrated plant information management system during design, construction, and operation.

ECONOMICS

- Cost goal** ALWR plants will have a sufficient cost advantage over competing baseload electricity generation technologies to offset a higher capital investment risk associated with nuclear plant utilization.
- Resulting quantified cost goals** Levelized January 1994 constant dollars for a 30-year capital amortization period, plant startup in 2005, and a mid-range-cost U.S. location (Kenosha, Wisconsin).
- **Median busbar cost** Sufficiently less than 43 mills/Kwh to offset the higher capital investment risk associated with nuclear plant utilization.
 - **Uncertainty** Projected 95th percentile non-exceedance cost substantially less than 53 mills/Kwh both to offset a higher capital investment risk associated with nuclear plant construction and to recognize that cost uncertainties with alternative generating technologies will decrease with time.

Figure 1. **RELATIONSHIP OF THE THREE VOLUMES OF
THE ALWR REQUIREMENTS DOCUMENT**





Defense-in-Depth Application to ALWR

**ACRS/ACNW Meeting
13 Jan. 2000**

**Gary Vine
Sr. Washington Representative**

EPRI



Overview

- > U.S. ALWR Program guided ALWR policies, design, development, & regulatory approval process from mid-'80s to late '90s**
 - > Broad participation: ind./govt.; international**
 - > ALWR Program embraced traditional D-in-D philosophy; drove designs to improved D-in-D**
 - > Primary approach followed "Structuralist Model"***
 - > Areas of effort toward "Rationalist Model"* (later)**
- (*as defined in ACRS paper by Sorensen et. al)

EPRI



ALWR Policies

- Simplification
- Design Margin
- Human Factors
- Safety
- Design Basis vs. Safety Margin
- Regulatory Stabilization
- Standardization
- Proven Technology
- Maintainability
- Constructibility
- Quality Assurance
- Economics
- Sabotage Protection
- Good Neighbor

EPRI



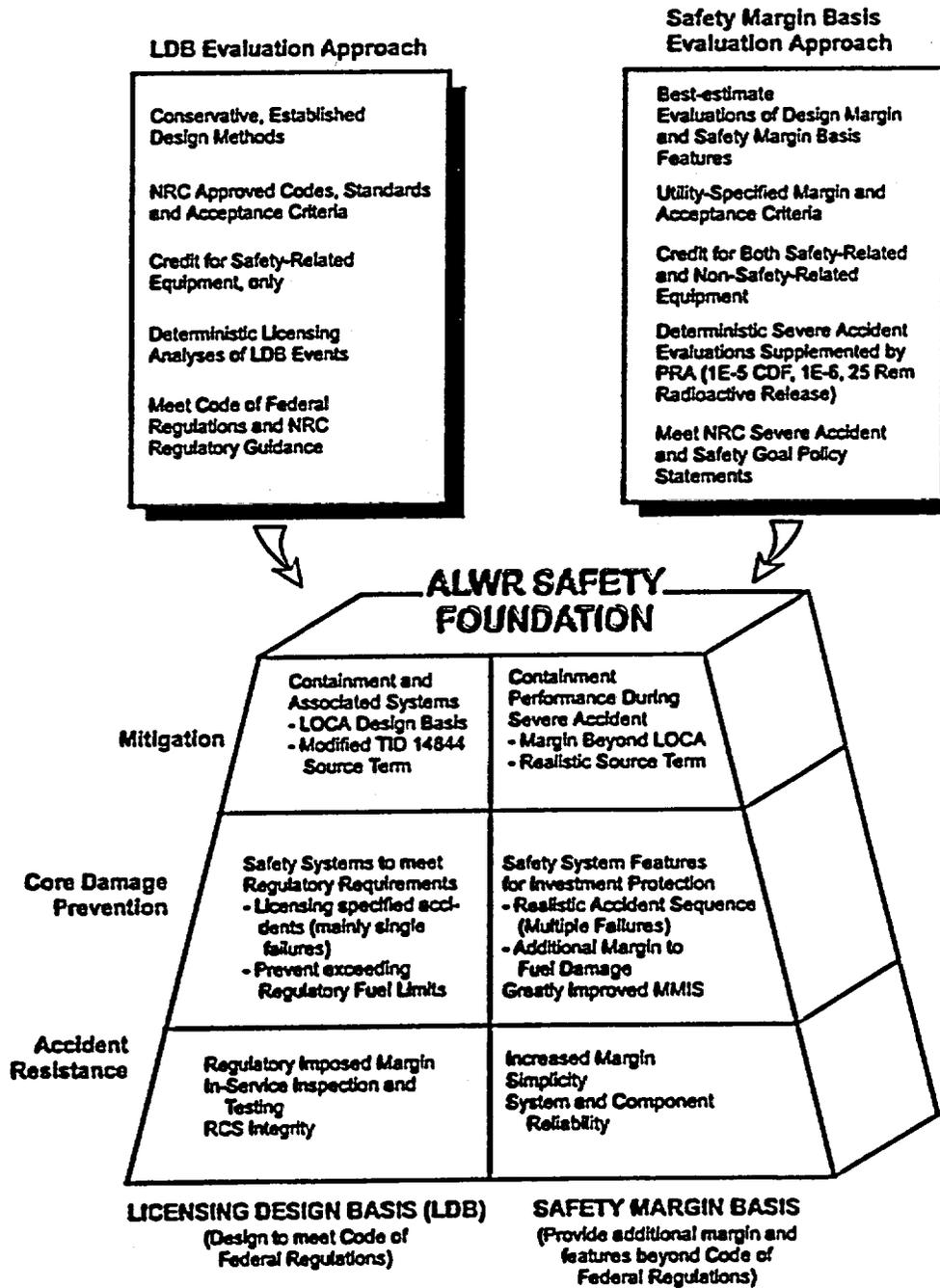
Areas of Emphasis Toward More Risk-Informed Approach

- Primary emphasis on accident resistance and prevention; balanced emphasis on mitigation
 - Safety is critical to BOTH owner & NRC
 - Investment protection also critical to owner
 - Cost-effective design typically favored prevention
 - Created some issues wrt "balance" in D-in-D
- Explicit consideration of severe accidents via Safety Margin Basis (best est., outside LDB)

EPRI

VOLUME I: POLICY AND TOP-TIER DESIGN REQUIREMENTS

FIGURE 2 - ALWR SAFETY FOUNDATION





Areas of Emphasis Toward More Risk-Informed Approach

- **Major reliance on PRA in design process**
 - Drove many URD and vendor design decisions
 - critically important use for passive plants: RTNSS
 - Regulatory use primarily confirmatory. Selective use to support new requirements (ex: approval of some “optimization issues” proposed by industry)
- **Industry’s quantitative safety requirements improved both prevention and mitigation**
 - CDF < 10 E-5; <25 Rem @ site boundary for sequences with cumulative frequency >10 E-6)
 - opposed numerical coupling of D-in-D reqts.

EPRI



Areas of Emphasis Toward More Risk-Informed Approach

- **Regulatory Stabilization; assured licensability**
 - generic resolution of issues in advance of DC
 - exceed regulations where feasible (provide margin to regulatory limits)
- **“Optimization Issues” -- proposed changes to regulations where needed, typically driven by risk-insights**
- **Economic policy necessitated smart choices**

EPRI



Concluding Remarks

- **Risk-informed Regulation essential for future of advanced reactor deployment**
- **Die is cast. “Rationalist Model” for D-in-D will become the future approach**
- **No downsides to Rationalist Model, if implemented properly. Major advantages**
- **Risk-Informed Regs by definition require consideration of D-in-D; use of eng. judgment**
- **US leadership on D-in-D issues important**

EPRI



DEFENSE IN DEPTH AND THE AP600

January 13, 2000

Brian A. McIntyre

Manager, Advanced Plant Safety and Licensing

WESTINGHOUSE ELECTRIC COMPANY

DEFENSE IN DEPTH DEFINITION / HISTORY



Traditionally a Part of the Prescriptive-Deterministic Regulatory Process

- **3 Barriers to Release**
- **Worst Single failure Assumption**
- **2 means of Providing Shutdown Capability**
- **Large Break LOCA**
- **10 CFR Appendix K**
- **Accident Mitigation by Only Safety Related Equipment**
- **Etc**

Invoked to Offset Perceived Uncertainties in Knowledge

Never Sure Exactly What it was

Never Sure When Enough was Enough

Now Appropriate to Strike a Balance with Risk Informed

DEFENSE IN DEPTH IN THE AP600



Unquantifiable Aspects (Applicable Beyond Nuclear Power Plants)

- Part of the Design Philosophy
- PRA Used as a Design Tool to Identify Potential Areas of Improvement
- Examined a Broad Range of Conditions
 - Shutdown and Low Power Operations
 - Single and Multiple Steam Generator Tube Rupture
 - With and Without Nonsafety-Related Systems
 - Common Mode Failures
 - Operator Errors
 - Hazards (Fire, Flood)
- Examined Broad Range of Initiating Events

Quantifiable Aspects

- Low Core Damage Frequency
 - Focused PRA Results
- Low Large Release Frequency
 - SAMDA

AP600 PRA RESULTS



	Core Damage Frequency			Large Release Frequency		
	At-Power	Shutdown	Total	At-Power	Shutdown	Total
Baseline PRA	1.7E-07	9.0E-08	2.6E-07	1.8E-08	1.5E-08	3.3E-08
Focused PRA	7.7E-06	4.1E-07	8.1E-06	5.5E-07	2.6E-07	8.1E-07
NRC Safety Goal			1E-04			1E-06

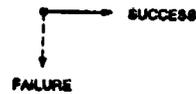
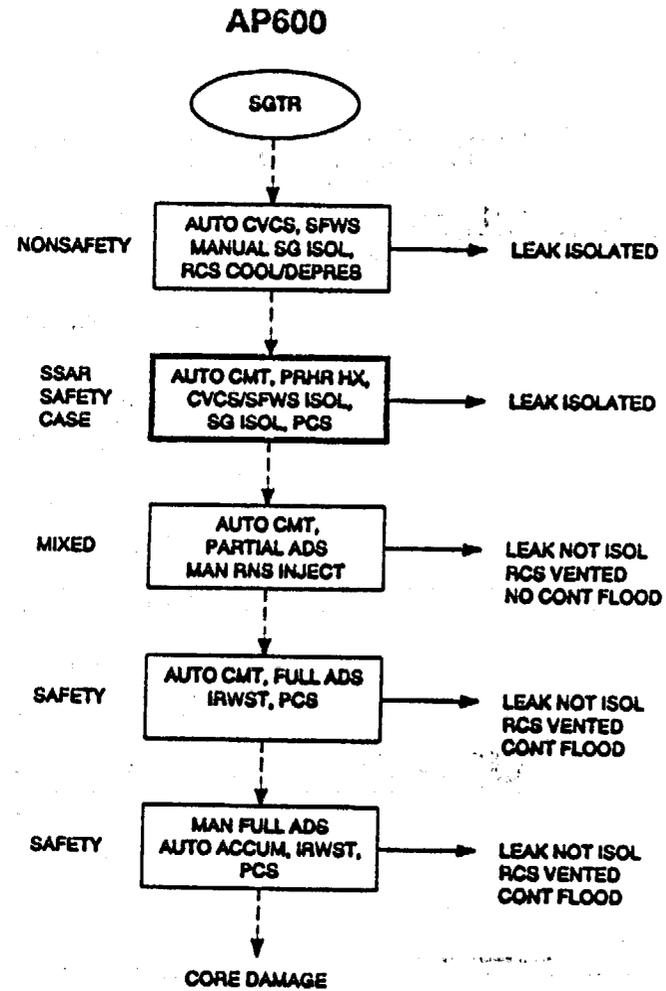
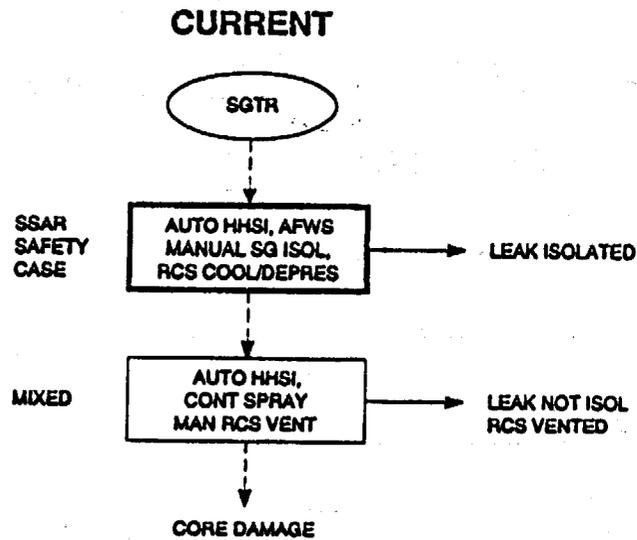
REF: AP600 Design Control Document

System Defense In Depth



- **AP600 Provides Multiple Levels of Defense**
 - First feature is usually nonsafety active feature
 - High quality industrial grade equipment
 - One feature is safety passive feature
 - Provides safety case for SSAR
 - Highest quality nuclear grade equipment
 - Other passive features provide additional defense-in-depth
 - Example; passive feed/bleed backs up PRHR HX
 - Available for all shutdown conditions as well as at power
 - More likely events have more levels of defense

SG Tube Rupture



AP600 PRA



- **PRA Used as Design and Licensing Tool**
 - 7 PRA iterations performed on AP600; first in 1987, final in 1997
 - Extensive NRC review / comment
 - Plant designers interacted with risk analysis
- **Each PRA / Design Iteration Included**
 - Plant design input and PRA model development
 - Quantification and sensitivity studies
 - Importance of nonsafety features, operators, etc.
 - Review / understanding of results
 - Improvement of PRA and plant
 - PRA analysis (event/fault trees, success criteria T/H analysis)
 - Plant operating procedures
 - Plant design
 - Subsequent PRA studies became more detailed
 - Internal/fire/flood events from at-power & shutdown conditions

AP600 PRHR HX FAILURE



- **Possible PRHR HX Failure Mechanisms**

- Failure of AOV to open
 - Mechanical failure
 - Actuation failure
- Isolation valves miss-positioned closed
- Plugging of flow path
- Inadequate IRWST water level
- Non-condensable gas binding
- Water hammer
- Inadequate heat transfer

IRWST WATER LEVEL



- **IRWST Water Required For PRHR HX Operation**
- **Means of Losing IRWST Water Quantified in PRA**
 - IRWST rupture following PRHR HX actuation
- **Means of Losing IRWST Water Not Quantified in PRA**
 - Leakage prior to PRHR HX actuation
 - Redundant (4) IRWST level instruments with alarms
 - Boil off due to PRHR HX operation
 - PRHR HX can operate >72 hr without water return
 - With water return can operate indefinitely

AP600 PRHR HX GAS BINDING



- **PRHR HX Gas Binding Is Prevented By AP600 Design**
- **Air from Shutdown Operations**
 - Procedures require venting
 - Level detectors alarm condition allowing operators to manually vent
- **H2 from RCS or Pressurizer**
 - H2 in RCS is saturated at 30 psig so it can not come out of solution
 - Level instruments would alarm condition
- **N2 from Accumulator Discharge**
 - Accumulators empty at very low pressures, about 100 psig
 - During transients RCS does not drop to such pressures
 - During LOCAs PRHR HX is assumed to fail when N2 enters RCS
- **Severe Core Damage**
 - PRHR HX is assumed to fail when H2 is generated by core damage

PRHR HX WATER HAMMER



- **Water Hammer Prevented By Design**
 - Inlet line to PRHR HX normally open
 - Pressure difference across isolation valve only 30 psi
 - No chance for low pressure void to exist downstream of isolation valve
 - Inlet line routed to maintain hot
 - Hot water prevents water hammer if HL becomes voided during accident
- **Water Hammer Not Included In PRA**

INADEQUATE HEAT TRANSFER

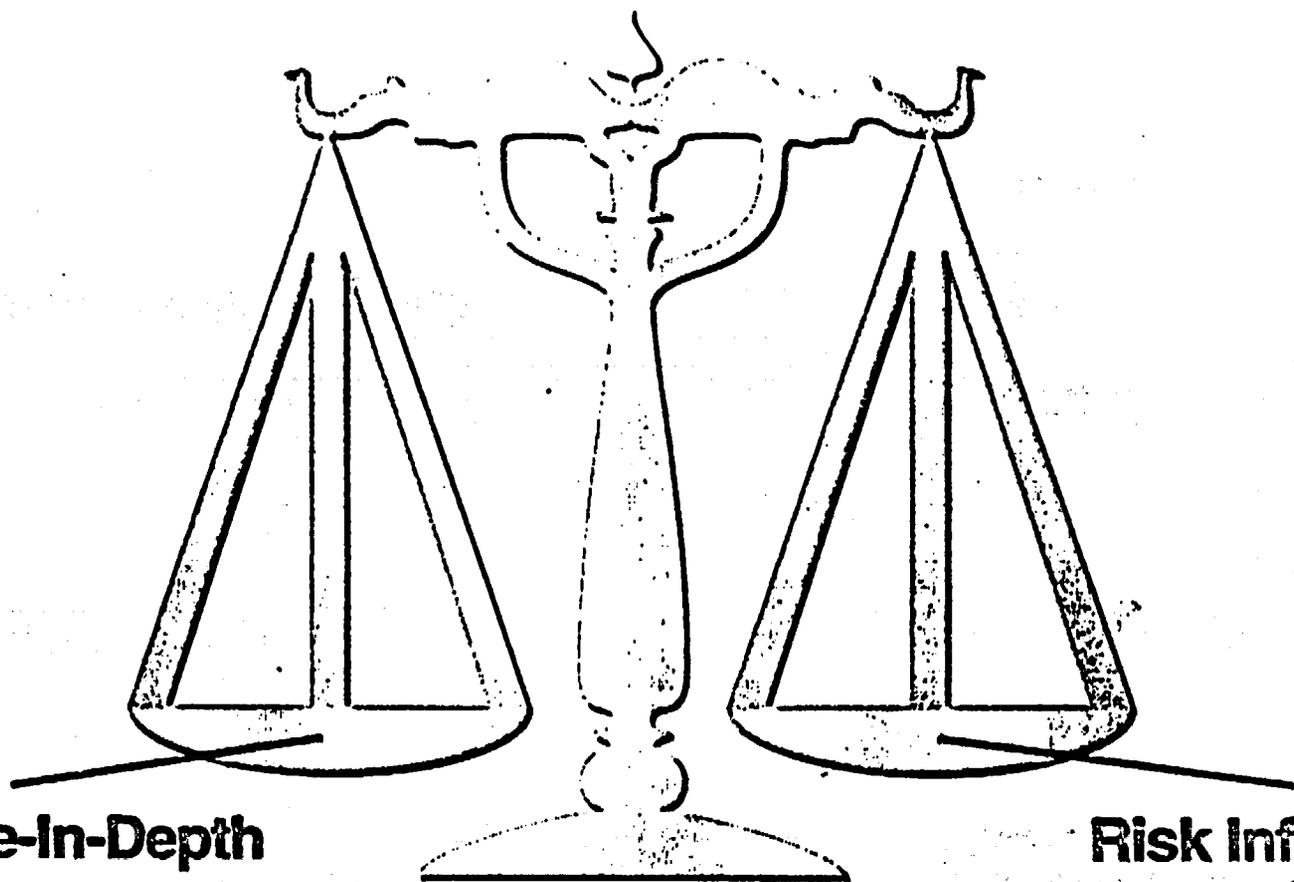


- **PRHR HX Sized On Data From AP600 Test**
 - Three full sized tubes tested at full pres/temp

- **PRHR HX Included In AP600 Integrated Tests**
 - SPES-2 and OSU

- **PRHR HX Will Be Tested In Each Plant**
 - Startup tests at full pres/temp
 - IST each refueling at reduced pres/temp

AP-600 CONTAINMENT SPRAY SYSTEM-?



RISK INFORMED PERSPECTIVE

<u>AP-600 Release Mode</u>	<u>Risk Contribution*</u>
Containment Isolation Failure	9.6-%
Early Containment Failure	83.9-%
Containment Bypass	5.8-%
Other	0.7-%

*population boundary dose risk -72 hr; PRA-Rev. 9

AP600 RISK SUMMARY



Release	Frequency (per year)	72 Hour Population TEDE Dose (man-rem)	Risk (man-rem/yr)
Early Failure	6.6E-9	1.0E6	6.8E-3
Intermediate Failure	1.3E-11	3.5E5	4.6E-6
Late Failure	1.5E-11	1.5E4	2.2E-7
Isolation Failure	3.6E-10	2.1E6	7.7E-4
Bypass	1.1E-8	4.2E4	4.7E-4
Totals			8.06E-3

AP600 RISK REDUCTION ESTIMATE LOW FLOW, NONSAFETY SPRAY



Release	Frequency (per year)	72 Hour Population TEDE Dose (man-rem)	Risk (man-rem/yr)	Reduced Risk Crediting Sprays (man-rem/yr)	Comment
Early Failure	6.6E-9	1.0E6	6.8E-3	3.8E-3	Approximately 2 hours between start of release and CF
Intermediate Failure	1.3E-11	3.5E5	4.6E-6	0.	Assumes tens of hours of spraying before CF
Late Failure	1.5E-11	1.5E4	2.2E-7	0.	Assumes tens of hours of spraying before CF
Isolation Failure	3.6E-10	2.1E6	7.7E-4	5.8E-5	Assumes 1 hour worth of spray decontamination
Bypass	1.1E-8	4.2E4	4.7E-4	4.7E-4	No spray reduction
Totals			8.06E-3	4.3E-3	

10 Sv (1000 Rem)

Certain death

1 Sv (100 Rem)

Floor for exposure threatening prompt death,
Clearly predictable proportion to threat of induced cancer,
Clinically detectable effects of radiation exposure,
Exposure limit for rescue workers in nuclear war or
emergency.

0.1 Sv (10 Rem)

Floor for clearly predictable proportion to threat of induced
cancer (based on bomb survivor data),
Typical standard for limit of public individual accident
exposure.

0.01 Sv (1 Rem)

Clearly acceptable annual exposure limit for radiation
workers,
Tolerable level of public exposure in recognized situations
which are difficult to change, e.g., radon in the home, high
natural background radiation,
Average total background radiation is below this level,
dominated by radon exposure which varies considerably.

1 mSv (100 mrem)

Clearly acceptable annual exposure to a member of the
public from all permitted sources,
Typical background radiation from terrestrial and cosmic
ray sources,
Additional cosmic ray exposure suffered by frequent flyers.

0.1 mSv (10 mrem)

Typical proposed limit for exposure of the public from
waste releases or a single permitted source,
Too small to be discerned as a change in background
radiation.

0.01 mSv (1 mrem)

Negligible individual exposure.

DEFENSE IN DEPTH

**JOINT SUBCOMMITTEE OF
ACRS AND ACNW**

JANUARY 13-14, 2000

ROBERT M. BERNERO

QUESTIONS TO BE ADDRESSED

- 1. What is defense in depth?**
- 2. Is there an overarching philosophy of defense in depth?**
- 3. Are current safety goals and objectives clear for general use?**
- 4. What is the role of defense in depth in risk-informed regulation of nuclear reactors?**
- 5. What is the role for defense in depth in risk-informed regulation of radioactive material processes and uses?**
- 6. What is the role for defense in depth in risk-informed regulation of radioactive waste disposal?**

WHAT IS DEFENSE IN DEPTH?

- **“Defense-in-depth is an element of the NRC’s Safety Philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility. The defense-in-depth philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance or operation of a nuclear facility. The net effect of incorporating defense-in-depth into design, construction, maintenance, and operation is that the facility or system in question tends to be more tolerant of failures and external challenges.”**
- **Defense in depth is not a formula for adequate protection; it is a part of the safety philosophy, a strategy for safety analysis.**

IS THERE AN OVERARCHING PHILOSOPHY OF DID?

- **Yes, as a strategy of safety analysis.**
- **Defense in depth: Prevent undue reliance on any single:**
 - **rarity of occurrence**
 - **design feature**
 - **barrier**
 - **performance model**
- **Not a formula for acceptability, defense in depth may not be enough defense.**
- **Risk-informed: Achieve a sufficient margin of safety, neither too close nor too far from the unacceptable.**

ARE CURRENT SAFETY GOALS AND OBJECTIVES CLEAR?

- **No, not for general use.**

- **The span of protection**
 - **Public safety**
 - **Worker safety**
 - **Patient safety**
 - **Environmental protection**

- **Range of authorized practices**
 - **Reactors**
 - **Fuel cycle facilities**
 - **Industrial and medical uses**
 - **Exempt distribution**
 - **Transportation**

WHAT IS THE ROLE OF DID IN REGULATION OF REACTORS?

- **Does not apply to routine releases.**
- **Basis for evaluating areas of heavy reliance in accident analysis, e.g.:**
 - **Seismic safety**
 - **RPV rupture**
 - **SG tube rupture**
 - **Human action**
- **Graded defense with graded goals.**

WHAT IS THE ROLE OF DID IN REGULATION OF MATERIALS?

- **May sometimes apply to routine releases, e.g., exempt products.**
- **Need graded goals for graded defenses.**
- **Think it through:**
 - **Potential consequences**
 - **Potential barriers**
 - **Potential actions**
 - **Balanced choice of defense**
- **Knotty problems, e.g., patient safety and medical QA**

WHAT IS THE ROLE OF DID IN REGULATION OF WASTE?

- **Definitely applies to release barriers.**
- **One fundamental basis of acceptability is the TSPA, with proper uncertainty analysis.**
- **Apparent confusion since DID analysis is a form of uncertainty analysis.**
- **Part 63 proposal is a sound approach to DID, develop the body of information for the exercise of judgement.**
- **Need graded goals for graded uncertainties: clearly acceptable, acceptable, clearly tolerable, tolerable, life-threatening, unacceptable.**