Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

ACRST-2066

Title: Advisory Committee on Reactor Safeguards Probabilistic Risk Assessment and Westinghouse Standard Plant Designs Subcommittees Joint Meeting

TR04 (ACRS)
RETURN ORIGINAL
TO BJWHITE
M/S T-2E26
415-7130
THANKS!

Docket Number: (not applicable)

Location: Rockville, Maryland

Date: Wednesday, June 5, 1996

ORIGINAL

Work Order No.: NRC-701 Pages 1-197

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

D I S C L A I M E R

PUBLIC NOTICE
BY THE
UNITED STATES NUCLEAR REGULATORY COMMISSION'S
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

JUNE 5, 1996

The contents of this transcript of the proceedings of the United States Nuclear Regulatory Commission's Advisory Committee on Reactor Safeguards on JUNE 5, 1996, as reported herein, is a record of the discussions recorded at the meeting held on the above date.

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

\+ + + + +

JOINT MEETING

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

PROBABILISTIC RISK ASSESSMENT (PRA) AND

WESTINGHOUSE STANDARD PLANT DESIGNS (WSPD) SUBCOMMITTEES

\+ + + + +

WEDNESDAY,

JUNE 5, 1996

\+ + + + +

ROCKVILLE, MARYLAND

\+ + + + +

The Subcommittee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B3, 11545 Rockville Pike, at 8:30 a.m., George E. Apostolakis, PRA Chairman, presiding.

MEMBERS PRESENT:

GEORGE E. APOSTOLAKIS, CHAIRMAN, PRA
WILLIAM J. LINDBLAD, CHAIRMAN, WSPD
IVAN CATTON, MEMBER
THOMAS S. KRESS, MEMBER
MARIO H. FONTANA, MEMBER
DANA A. POWERS, MEMBER

MEMBERS PRESENT: (CONTINUED)

ROBERT L. SEALE, MEMBER

CHARLES J. WYLIE, MEMBER

ACRS STAFF PRESENT:

NOEL DUDLEY

MIKE MARKLEY

PAUL BOEHNERT

AMARJIT SINGH

THERON BROWN

RICHARD P. SAVIO

ALSO PRESENT:

SELIM SANCAKTAR

TERRY SCHULZ

TIM BUETER

BRUCE MONTY

BRIAN McINTYRE

JOHN FLACK

NICK SALTOS

CYNTHIA HAAG

A-G-E-N-D-A

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

(8:33 a.m.)

CHAIRMAN APOSTOLAKIS: The meeting will now come to order. This is a joint meeting of the ACRS Joint Subcommittee on Probabilistic Risk Assessment and Westinghouse Standard Plant Designs.

I am George Apostolakis, Chairman of the Subcommittee on PRA.

Mr. William Lindblad is the Chairman of the Subcommittee of the Westinghouse Standard Plant Designs.

The ACRS Members in attendance are: Ivan Catton, Mario Fontana, Charles Wylie, William Lindblad, Robert Seale, Thomas Kress, William Shack and Dana Powers.

The purpose of this meeting is to hold discussions with representatives of Westinghouse Electric Corporation and the NRC staff as they choose to participate to gather information concerning the AP600 Level 1 and shutdown PRAs. The Subcommittee will gather information, analyze relevant issues and facts, and formulate proposed positions and actions as appropriate for deliberation by the full Committee.

Noel Dudley is the Cognizant ACRS Staff Engineer for 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 May 23, 1996.

A transcript of the meeting is being kept and will be made available as stated in the Federal Register Notice. 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 no written comments or requests for time to make oral statements from members of the public.

We will now proceed with the meeting. I call upon Chris Monty of Westinghouse to begin.

MR. MONTY: Good morning. My name is Bruce Monty and I'm from Westinghouse. I'm the manager of the Risk Assessment Services Group at Westinghouse and I'll provide some introductions this morning and then I'll turn it over to our technical experts on the PRA and design.

Just to start with introductions of who we have and who will be talking to you, Dr. Selim Sancaktar will be talking about the Level 1 at-power methodology and PRA results and insights. Mr. Tim Bueter, who is also a Westinghouse PRA engineer will be talking about the Level 1 insights and the shutdown PRA results and insights. Mr. Terry Schulz, who is the leader safety systems designer for the AP 600 will be talking about overview of the design as it pertains to some of the PRA sites.

The objection of the presentation is first to provide an overview of the AP600 design and since this is a PRA presentation, there will be an emphasis on defense-in-depth aspects in the safety systems in a design which will help you understand some of the results that we presented with respect to the Level 1 and shutdown.

We also will provide a technical summary of the AP600 here today which has been submitted in various revisions and I'll talk about that in a few minutes as part of the design process leading to the final design approval for the AP600.

The scope is limited to the plant core damage analysis for internal events at power and at shutdown events. We're currently working on a revision to the Level 2 and severe accident results that would include some of the work that recently has been completed by Dr. Thofanos on in vessel retention of core debris and in vessel hydrogen steam explosion. That work is still on-going and will not be talking about that today. In some future meetings we hope to come to share the work that we've done with you.

The next slide is an outline of the presentation. The first part will be Mr. Schulz will talk about an overview of the design, as I said, with an emphasis on the levels of defense. Dr. Sancaktar will talk about background and methodology and at power Level 1 analyses will include some insensitivity study results that we have on the analysis and Mr. Bueter will pick it up on PRA insights for Level 1 and the shutdown Level 1 analyses.

We also have other support personnel here as you have questions so we can try to answer them as quickly as we can. If not, if we do not have the answer, we have other experts back at Westinghouse. We have some material here that we can look for answers for the detailed analyses.

Talk about the background of the PRA for the AP600, we started doing the PRA in 1987 when we started the conceptual design. It was done initially to provide insights and to factor improvements into the design. Each revision of the PRA quantification included the following, design inputs, PRA model development and those things did evolve over the time since 1987 as we submitted our first formal PRA and then actually updated it several times. I'll talk about that in the stages below.

The sensitivity studies were done at each stage. We had review and understanding of results, both by the PRA analysts and the systems designers and we developed ideas to improve the plant analysis, the procedures and design. That was done primarily in two ways. One was obviously we documented the analyses at each stage, reports were generated, some were submitted to the NRC for NRC review. Another way was we had continuity of some personnel. For example, Mr. Schulz worked on the design and worked with the PRA analysts from the beginning in 1987 until today. We has worked continuously, so we do have personnel who have been involved throughout.

CHAIRMAN LINDBLAD: Excuse me, Bruce. When you speak of the PRA, what scope PRA were these and did it include shutdown during those periods or was it just at-power PRA?

MR. MONTY: Okay, as I go through the stages I can try to answer that question.

The first stage was in the 1987 and 1990, the first two stages. This was described in the report in detail, in the PRA report. It was in the 1987 time frame and that primarily consists of Level 1 and Level 2 PRA for internal events.

However, in Stage 3 what we call a base PRA which was completed in 1992, we did do the full Level 1, Level 2, Level 3 internal events and external events PRA, including a shutdown analyses. That was the first submittal for NRC review in 1992, along with the SSAR describing the plant design and other accident analyses.

Subsequent to that, in 1994, we had Revision 1 which consisted of primarily a revirion to the Level 2 severe accident modeling where we provided more detail on the containment event tree with respect to some of the severe accident analogy.

In Stage 5, revisions 2 through 6, which was picked primarily, revisions 2 through 6 is that we completed, as we completed sections we issued them to the NRC at that time.

In Stage 5, we addressed NRC comments on review of our base PRA and we also addressed some design changes that had been made in both the safety systems and some of the nonsafety systems.

Right now we are completing what we call the final PRA. We have completed the Level 1 and we have provided a markup of the previous revision 6 results to the NRC and we're anticipating a final cleaned up version of that Level 1, Level 2 by the end of June to be submitted to the NRC.

So that 's basically the history right now and we will have a discussion or a presentation of the total scope that we have completed and submitted to the NRC in one of the further talks.

CHAIRMAN APOSTOLAKIS: Why did you need so many revisions?

MR. MONTY: Well, the design has evolved continuously and while we did do a conceptual design, that initial PRA wasn't a simplified PRA relative to the PRA we have now and we learned things as we went along and unfortunately or fortunately when you change design features, new insights come out of each point and those were factored back into the design which required further update, as well as questions or agreements with the NRC to make changes to methodologies. I'll talk a little bit about that on the next slide. We did have peer reviews that we did factor into it to the study.

MEMBER SEALE: Would you think it fair to characterize that interaction between the development of the detailed design and the various stages in the PRA revisions as being the kind of activity that we might mean when we talk about a living PRA?

MR. MONTY: It's the same, but it's different in some ways. When we talk about a living PRA, the argument is once a plan is completed and as you move, go through plant lifetime and change things through the plant operation that you factor that back in.

MEMBER SEALE: But there's also a school of thought that says a PRA can be a useful learning device during the design.

MR. MONTY: Right, and in that sense it was to a large degree living. If I can just describe a little bit about the process of factoring in the design. We did these discrete updates that I showed on a previous slide. However, when a design change is proposed by the designer, there is a formal process of design change control where the PRA analyst can review the change before it happens versus actually happening and being put into the PRA after. So in that sense, yes, it was very much a living process.

In some cases, that change would result in an expert opinion by the PRA analyst if the change would be not a factor or might be a factor and that would be factored in the decision process where the changes could be done.

In other cases on major changes, a sensitivity study to the existing model might be done and then what we do, we primarily do is collet the changes in the various discrete points, made those changes at one time in the model. Because of the size of the model and the extent of the documentation, it's still a very difficult process to factor all the changes to have a consistent model with any design at any point in time.

So the formal configuration management process is used to try to keep a handle on the various changes and make it a sort of a living document.

Some other background, all stages of the PRA were done with the participation of the Westinghouse PRA group. This has been a group that we created in the early 1980s when PRA started to get a large amount of use in the industry and we have experience on other plant designs to advance PWR which was the Westinghouse evolutionary plant type that was designed in the early 1980s.

We did a PRA for that study and submitted it to the NRC in 1985. We did some preliminary PRA work on Sizewell for the British. The final PRA was completed by Nuclear Electric. I believe some of the upfront conceptual design PRA work and we have done extensive work on operating plants in the period from 1981 including numerous IPEs in support of some of our utility clients.

So we feel that that has helped us bring in some of the understanding of current plant issues, current safety issues that we could then factor into the design features to try to address them and some of the discussions later on, you'll see how some of those issues have been addressed with design features in the AP600.

In Stage 3, we did get support from PRA engineers from ENEL in Italy. They were a bit part of the first base PRA. That's why, if you look at the report you see at the bottom the ENEL logo, that's where that comes in. They have supported, in addition, to a smaller extent on future, subsequent revisions to the base PRA.

As far as peer review of the study, we've had two major peer reviews. One was sponsored by the advanced light water reactor utility steering committee group where they brought in utility PRA practitioners and operations experts to review the PRA and then more recently last year, the Department of Energy sponsored a peer review by NUS of the study and we reviewed their comments and some of those comments were factored into subsequent revisions.

Now the main objectives of the PRA itself, obviously, we wanted to satisfy the NRC requirements to do a design specific PRA for the application for design certification, the final design approval; and secondly, to provide a tool to investigate detailed design solutions and operational strategies. So what we have done, as I said, using a design process and we also used the output in various applications such as the development of emergency procedures, accident management strategies, technical specifications, reliability assessment programs and other applications.

We have the following quantitative goals, plant core damage frequency less than or equal to 1E-5 events per year total, excluding seismic and sabotage and a plant severe release frequency of less than or equal to 1E-6 events per year which is where a large release is defined as greater than 25 rem over 24 hours at one half mile over site 100. Th' is more stringent than the NRC safety goal of 10-4 for core damage frequency and we'll talk about the results that we have received and some of the reasons behind them in some of the discussions that we have today.

CHAIRMAN APOSTOLAKIS: Why are you excluding seismic?

MR. MONTY: By seismic, we use the seismic margins approach rather than a seismic PRA approach as specified in the ALWR utility requirements document.

CHAIRMAN APOSTOLAKIS: So that is a bounding technique?

MR. MONTY: Right. That was one of two options using the seismic PRA or seismic margins. We chose to go the same way as the previous advanced reactor designs and use the seismic margins approach.

CHAIRMAN APOSTOLAKIS: That guarantees that the contribution to core damage frequency is less than what, 10 to the -6 or -7?

MR. MONTY: Yeah.

MEMBER SEALE: These goals came out of the URD?

MR. MONTY: That's correct. We have committed to the goals that were in the URD requirements document.

Any other questions? Okay, with that I'd like to turn it over to Terry Schulz who will talk about the AP600 design aspects and the defense-in-depth in the design.

MR. SCHULZ: Okay, good morning. As Bruce mentioned, we have a little discussion here on the design aspects of the AP600. I hope to just concentrate on the -- to give you an overview of the design, but concentrate on the PRA-related aspects of it. We probably could spend a lot more than an hour on this, so I'll have to try to be careful with the discussion.

There are a number of features in the AP600 design that are key. In some cases, they vary from current plants and they have some importance related to the PRA. The plant has increased margins that's reflected in the low power density reactor operating temperatures, various factors like that and I'll touch on that a little bit more in the coming slides.

The reactor coolant system loop, we talk about it as a simplified loop. It has a lot to do with welds, section to pipe. The Canned reactor coolant pipes are a significant factor related to the reliability and avoidance of some accident sequences of seal failures. Passive safety features are very key element in the reliability and the PRA aspects of the design and I'll talk about a fair amount about the passive safety systems. The nonsafety systems or the defense-in-depth systems that we have I'll be mentioning, but we don't plan to show you any pictures or any specific discussions on those.

The instrumentation system and advanced control room is often an important factor in the PRA and the reliability of the plant and I have some information on that. The plant arrangement with its integration of the systems and operations is another important factor, but it relates more to at the Level 2 type PRA, so I won't really be talking any more about the layout of the plant today.

MEMBER CATTON: Do you use touch screens in your advanced control rooms?

MR. SCHULZ: There -- as I understand it, there is talk about soft controls. I don't know if the implementation will actually be touch screen or some other kind of control. I know there are dedicated switches in addition to any kind of soft control touch screens to give you system safety related system actuations of the safety system.

MEMBER CATTON: What did you assume in the PRA?

MR. SCHULZ: I don't --

MEMBER CATTON: Well, when we get to it we can talk about it.

MR. SCHULZ: Okay. Okay, so that is a list of the --

CHAIRMAN LINDBLAD: And in what way is plant arrangement construction enhanced? What is the objective of the enhancement, is it AP or cost?

MR. SCHULZ: Both. We have a number of different objectives. Cost, construction schedule, certainly are key elements to make the plant practical and of course, in all that we are integrating into the design the passive safety features which have interactions with the arrangement, fire separation was a factor from the very beginning since it was a new design, a new arrangement, the people that were working on the arrangement were aware of design issues like flooding, fire separation to optimize that in with the design.

CHAIRMAN LINDBLAD: And you're going to show us how modular construction enhances safety?

MR. SCHULZ: I'm not going to be talking about this any more today. Our judgment is that this is primarily an issue related to fire, flood, type of area events. Since we're talking about internal shutdown events that I was just mentioning this and I won't talk about it any more today.

CHAIRMAN LINDBLAD: Thank you.

MR. SCHULZ: This picture shows you the loop arrangement. It's a two loop plant. We do have four reactor coolant pumps that are canned motor pumps and as I mentioned it eliminates one of the small LOCA type sequences that you see in current PWRs because there are no seals in the pumps. The reactor vessel is basically a three loop sized reactor vessel in a two loop plant so the power density is lower.

There are no bottom penetrations below the loop level in-core instrumentation comes in through the top of the reactor so the reactor head is higher integrity. The fluence for the vessel is reduced. A number of changes like that make the vessel integrity much, much higher. The pressurizer is about 60 percent bigger than a typical two loop plant which gives more operating time, reduces challenges to safety valves. Steam generators have a number of design improvements in terms of materials of design which should reduce the chance of tube ruptures. All the major piping and most of the auxiliary piping is designed for leak before break which should reduce the chance of having a leak or a LOCA occur.

This is a fairly busy slide, but it tries to capture the architectural arrangement of the instrumentation system. This instrumentation system is a digital, microprocessor based system. You see on the right side here, this box, represents the protection and safety monitoring system. This is a system that trips the reactor and actuates the safety system and it's really four way redundant system all the way from the sensors through the processing through the actuation. It has interfaces with the main control room and remote shutdown station. As I mentioned there are dedicated controls in addition to soft type controls, dedicated controls provide system level actuation and reactor trip or safety injection actuation, those kind of functions. There are dedicated indications as well as qualified data displayed for the operators to guide them in taking manual actions when they are required.

There's also a control system. This is a nonsafety system that interfaces with the nonsafety active defense-in-depth type systems as well as the pure nonsafety systems in the plant. Similar design to the protection system, but not 4-way redundant and different kind of typically just soft control type interface for the operator.

On the right hand side, we have a smaller system which we call the diverse actuation system. Current Westinghouse plants have an AMSAC system which is dedicated to ATWS mitigation. This system does that, but we've added some functions to it based on the PRA results to actuate some of the other safety features to optimize the PRA results.

This system is diverse from the protection system that uses different kinds of hardware, software and it's completely separate. It's sensors are separate. It has its own set of dedicated controls separate from the protection system and some dedicated indications so the operators in case of complete loss of protection system can still take some limited action.

MEMBER WYLIE: Did you say single train or multi-train?

MR. SCHULZ: It's two out of two logic, so it's really two cabinets. Again, I think, that's consistent or similar to the AMSAC type system. It's not a safety system, so it's not really designed for single failure or two out of two logic minimizes the chance it will cause inadvertent actuations of things.

Most of the other functions are really not safety related. They're some administrative type of things and displays.

CHAIRMAN LINDBLAD: Terry, on this chart you show four boxes that are called dedicated controls and indication.

MR. SCHULZ: Yes.

CHAIRMAN LINDBLAD: Are these separate and independent from each other or are some of them shared?

MR. SCHULZ: The diverse actuation system is completely separate from everything else. And it's controls and indications and in fact, the whole processing and sensors is completely separate.

The protection system, of course, is separate from the diverse actuation system. In some cases, they have some sensor sharing, transfer of information from the protection down to the control system, so there may be some additional degree of sharing there, but when that's done, there's high integrity isolation devices from passing information.

Most of the protection system is, uses its own sensor and it's own processing hardware, software and display.

There are other displays like the wall panel information and CRT type displays which can display any kind of information, safety, nonsafety, except for diverse actuation. That's kept completely separate from everything else.

I would like to now get into --

MEMBER CATTON: What is the monitor buss?

MR. SCHULZ: It's a computer network that allows information to be shared between -- so basically anything that gets captured in the computer system, either the control or the safety system can be shared with various supervisor and maintenance, remote locations in the plant, remote shutdown station can see anything that's in this system.

MEMBER CATTON: Is it common to everything?

MR. SCHULZ: It shares information, okay. So I wouldn't say common per se, in that you see these isolation devices and anything that's coming out of the protection system is isolated before it gets on to here and the protection system doesn't take anything off of that bus.

MEMBER CATTON: Is it redundant?

MR. SCHULZ: I don't know whether the monitor bus is redundant or not.

MEMBER CATTON: When you see something like this you just wonder what happens if somebody puts an axe through it.

MR. SCHULZ: If you put an axe through it it first of all won't defect the protection system.

MEMBER CATTON: But it might affect you getting information about from the protection system.

MR. SCHULZ: It might in terms of these auxiliary functions, but not in terms of the qualified displays and dedicated indications.

MEMBER CATTON: Okay.

MR. SCHULZ: So within the protection system, there's a complete --

MEMBER CATTON: Within each one of those boxes is complete all the way to display and control?

MR. SCHULZ: Yes. All the way from sensors to control displays and back through control devices within these boxes and this is really more of an auxiliary type sharing.

MEMBER CATTON: If you lost it --

MR. BUETER: Terry, I have heard a little bit about the design. Tim Bueter. The design is currently conceptualized and it evolves, of course, with development of technology and time. It's currently conceptualized as a high redundant, very reliable computer network along the lines of which you would have in a critical type system today where you have switches and gateways that can find different paths and multiple paths to get through it. So in that respect it's redundant.

In the respect that Terry's talking about, I don't think it's redundant in terms of does one system have three pathways or something like that. The network itself is designed to be a critical pathway, along the lines of current computer technology.

MR. SCHULZ: Okay, uh, I'd like to move on and talk about primarily the passive safety systems. This slide gives you a brief overview of what the passive safety systems are -- what the role is in the plant versus the active nonsafety systems. The passive safety systems use passive processes like natural circulation, compressed gas, batteries. There is a one time alignment of valves. So strictly speaking not totally passive.

This one time alignment of valves, once that is accomplished no support systems are needed to continue operation of the system. The actuation initially is either fail safe and many of the applications and I'll point them out to you, are valves held in a position by air pressure or power and when you lose that support system, the valve goes to it safe position which actuates the system.

There are some applications where we want to power the valve to a safe position and in that case we use safety related DC power which is derived from batteries. We do not use AC power from diesels or offsite power, pumps, fans, rotating equipment that's required to operate for mitigation functions in the safety related systems.

These systems are designed to mitigate all the design basis accidents in the plant. So chapter 15 of the SSAR, this is what you'll see in terms of what systems are operating to remove the core decay heat or to provide safety injection.

They are designed to the full QA industry guidelines, NRC guidelines regulatory oversight.

They are sufficient -- designed to be sufficient to satisfy the safety goals, NRC safety goals by themselves and that gets into this issue of the regulatory treatment of nonsafety systems, though one of the objectives of the designs is to satisfy the safety goals by themselves.

There's reduced reliance on operators. Operators can still do things and you'll see when you see the PRA results that they can be effective, but on the other hand the need for them to do things in the AP600 has been reduced by the nature of the passive system designs and by some actuation signals we've provided.

There are also nonsafety systems in the plant. These systems typically assist in normal operation of the plant, but they do provide some risk reduction in our baseline PRA we do give credit for them. They typically have redundant equipment powered by both off-site and on-site, nonsafety supplies or power. Another function that they use is minimize the use of unnecessary use of the passive safety system.

They are not taken credit for in the Chapter 15 analysis. We do look at adverse interaction with the safety systems to make sure these systems don't somehow interfere with operation of the passive safety systems.

The QA requirements of regulatory oversight is what's called a graded approach and in some cases we do put some safety requirements on them. In most cases, they're nonsafety through the design.

The key passive safety features include a decay heat removal system connected directly to the reactor coolant system. The passive safety injection which is made up of several supplies of water, a core makeup tank which operates at full RCs pressure, accumulators which are fairly similar to the current plants; and a gravity injection from a refueling water storage tank that's located inside containment and that, of course, is like containment pressure, that's low pressure.

Those systems operating in conjunction with a depressurization system provide reactor coolant system makeup and safety injection.

The ultimate heat sink is provided by passive containment cooling system which basically uses the containment steel shell as a heat exchanger, water on the outside of the shell aids in cooling from the containment.

This is a very conceptual, simple slide which does show all the features I mentioned including the passive RHR which connects directly to the reactor coolant system, the accumulators, the makeup tanks, cooling water storage tank. Those all inject through two direct vessel injection lines.

The core makeup tank is connected with the pressure balance line so that it can gravity inject into the reactor coolant system, that any reactor cooling system pressure. In the long term, following an accident, the containment would flood up and there's recirculation, gravity recirculation available through some screens to go back into the reactor and I've got a better view later on to show you how that worked and again passive containment coolant aided by water drainage on the outside of containment provides effective cooling.

This picture gives you a little bit more idea of the sort of sectional arrangement of these features. The containment water storage tank is located on top of the concrete shield building so the water can drain by gravity on to the outside of the containment shell, in the case of an accident.

Air can circulate through open inlets down around the outside of the containment shell, basically above the operating deck and exhaust through a hole in the center. That air flow is not closed off during operations, so it's always open. And it by itself can provide effective cooling of the containment. It can't meet all of the design requirements in Chapter 15 by itself, but in PRA space it is adequate to prevent containment failure. The water flow and the evaporation of water into the air does allow the system to completely meet all the Chapter 15 and design requirements.

The refueling water storage tank is located basically below the operating deck, but above the reactor cooling system. The accumulators are located a bit lower and they are pressurized so the elevation is not so important with them. The core makeup which is filled with water and has gravity injection requirements is also located above the reactor.

I would like to go back a couple of pages and talk a little bit about the passive RHR next. It's about two pages back into your handout. This system is the system that's used to remove decay debris primarily in non-LOCA and accidents. So it replaces auxiliary feedwater systems in today's PRA.

It takes inlet from the hot leg side of the reactor and comes up into the inlet of the exchanger. The heat exchanger is located inside of this large or chilling water storage tank that we inside of containment. The outlet of the heat exchanger goes back to two normally closed valves, back into the cold leg side of the steam generator. That location was selected so that if the reactor coolant pumps are running, they actually force flow through the heat exchanger. If the reactor coolant pumps aren't running, then the flow will continue or would go in the same direction, taking hot water out of the reactor coolant system hot leg, flowing the water inside of the tubes and this gravity is head of cold water versus is head of hot water provides the natural circulation of the heat exchanger and the water enters into the cold leg downcomer into the core.

All that's needed to actuate the system is to open up one of these tube air operated valves. These valves are fail open so this is a case where we have fail safe operation. If we lose air or power, the cellinoids of these valves, they will open up and this system will start working.

The tank, as I mentioned,k is large. It will take in the range of 3 to 5 hours to start boiling in the tank following actuation of the tank system. The contents of the tank are sufficient so that the tank will last three days without any operator action to resupply water. In fact, there is a means of returning water to the tank. When this tank is boiling vents open up and the steam goes into the containment. That starts to heat up the containment and pressurize it and the containment coolant system starts condensing that steam. That steam tends to run down the walls of the containment that's collected in a gutter just above this tank and that condensate is normally returned to the tank.

That condensate return is not strictly a safety feature of the plant so it's not taking credit in safety analysis.

With that condensate return, the heat exchanger can operate indefinitely with minor losses of that condensate into the containment.

It's a very simple system. It again is designed primarily to deal with non-LOCA events, things like steamline breaks, feedwater breaks, loss of feedwater and provides an effective cooling of the system. It also plays a key role in steam generator tube rupture mitigation.

One of the very nice features of this design is that since it acts on the primary side, reactor side, once it catches up with decay heat it starts to cool the reactor down. It doesn't operate like the steam generator in terms of, at a fixed pressure temperature. Once its capability matches core decay heat and starts exceeding core decay heat, it starts bringing the pressure temperature of the reactor down which tends to automatically bring the temperature and pressure factor down to below the secondary site pressure. One of the things that our testing and analysis show is that this heat exchanger can terminate a tube rupture automatically without operator action. So it's a very effective feature and that's one of the important -- plays an important role in the PRA.

The passive safety injection system has a number of tanks as I mentioned. The accumulators are typically. They pressurize to about 700 psi. They sit behind several check valves. There's no actuation that has to be done to keep the system going. When the reactor pressure drops the check valve is forced to open by the pressure and accumulator and they provide injection.

The fact that they come in through the direct injection nozzle provides some additional redundancy of possibilities versus large break LOCA so if you break a cold leg or a hot leg pipe, this direct vessel injection line is arranged so that that piping cannot cause the breakage of the injection line so you do not spill an accumulator on a large break LOCA, so if you have a large break LOCA, you start out with two accumulators available and we've done some analyses that shows we only need one of those two in PRA space. We take credit for both in design basis space.

So the direct vessel injection model

arrangement helps us in terms of providing additional redundancy.

The core makeup tanks are filled with water. The volume of the massive water in the core makeup tanks is about the same as the water in the full reactor coolant system so they're fairly large tanks. They're designed for reactor coolant system, pressure and temperature condition and in fact, the inlet line in the cold leg is normally open and the outlet is normally isolated by two fail safe valves again, very similar to the passive RHR heat exchanger. We lose power or air with those valves open so it's a fail safe actuation.

The check valve for the outlet of this heat exchanger are special design that are biased open, so they don't have to open to initiate the design. The purpose of those valves is primarily in a large LOCA with reactor pressure drops rapidly and the accumulators inject rapidly. The check valves prevent accumulator bypass flow back through the core makeup tanks, so they have --

MEMBER WYLIE: The core makeup tanks, each tank has that volume in it?

MR. SCHULZ: Each tank is about half of the reactor coolant system. The two tanks together have the same massive water. They're actually slightly smaller volume, but because it's cold water versus hot water, the two tanks together have the massive reactor coolant system in them.

Accumulators are the same size so they have a lot of water in them too, but they also have some gas, so that the water in the accumulator is a little less than in the core makeup tanks.

The core makeup tanks, they can operate in two different modes. One of them is a natural circulation mode where water, hot water comes up and cold water is injected. That provides an effective boration and leakage makeup kind of capability. The boration capability is effective in steamline breaks and ATWS. The leakage makeup is fine for -- also for shrinkage in cool down events.

It's alsc efficient for tube rupture mitigation. If you have a loss of coolant accident and you start breeding your cold leg, then steam starts to come up to the top of the core makeup tank and allows the full content of the tank to be injected and it's injected at faster rates which you would like if you're voiding your cold leg and you have a loss of coolant. You would like a greater injection so the tank tends to have an automatic compensating slow injection if you don't have a LOCA, faster injection if you do have a LOCA.

Level instrumentation in that tank is what keys our automatic depressurization system. So if you start getting to about 2/3rds full in that tank, if you drain a significant amount of water out of the tank, then we start our depressurization system. That's staged into four stages either on the pressurizer and the fourth one is directly out of the hot legs. Those three stages go into a sparger inside the coolant water storage tank. That sparger is in there primarily to minimize the consequences of use of the system and not to really protect the containment. The containment is designed for double ended breaks of the hot leg, cold leg so that the sparger is not really safe from a steam condensing point of view.

The first three stages actually go off at different times which provides a more gradual control depressurizaton of the reactor. The fourth stage goes off on a separate, very low level signal in the core makeup tanks.

In fact, if we have a depressurization event, inadvertent or small LOCA type depressurization, we don't anticipate the fourth stage actually being necessary because we have a nonsafety pump system which can take water out of the refueling water storage tank and inject it through the direct vessel injection line and build up enough back pressure on the core make up tank that it slows down and stops before you get to the set point of the fourth stage.

This RNS system also provides some redundancy diversity to the gravity injection that comes in through the refueling water storage tank. If you are using just safety systems you will eventually get to the fourth stage opening and that will allow the refueling water storage tank to inject and the injection goes through two normally closed squib valves which provide a very leak-tight barrier between the reactor and the refueling water storage tank, check valve backup and squib valves.

These check valves sit in a normal no delta P environment which is a change from the original AP600 design. The squib valves take the delta P, the check valves just sit there with no delta P across them. They do have to open under low delta P, but that's a more similar environmental condition, operating condition to current operating plants.

The injection for refueling water storage tank, this is a very large tank. It's like half a million gallons of water, inside containment. So its injection will last a long time. Even with one of these -- there are two of these injection lines. Even with one of those lines broken and spilling, the injection will last six to eight hours. In other events, where you don't have a broken injection line, the injection tends to last longer, more like a day longer.

Eventually though, with no nonsafety systems, the tank will eventually drain down, tne containment will flood up and you'll go into a recirculation mode where again you open up some flow paths through the containment, either isolated with squib valves backed up witn an MOV and a check which allow water from the containment to go into the same lines, either the gravity injection or the pump injection to establish your long term cooling mode.

During one of these times, steam again which is generated through the ADS paths or through the break go into containment. The containment condenses that steam, drains it back down either through the tank itself or the containment which allows for its reuse in the injection.

CHAIRMAN LINDBLAD: Could you tell me what the elevation differences are with the gravity flow tankage?

MR. SCHULZ: I can touch on some of the key -- this line is about -- say 99 foot elevation. The bottom of the core makeup tank is about 107, so that's about 8 foot higher. The tank itself is 20 or so feet high. the bottom of this tank is about 103 -- now this tank normally doesn't empty completely. The recirc level, the final level that you get in the containment is about 107, 108 feet which is about 9 foot above the injection connection.

The top of this tank is about 133 foot, something like that. That's I think the water level above the bottom of the tank. So this tank -- you can get injection from this tank with a reactor pressure of about 10 pounds gauge, 10 to 12 pounds gauge.

CHAIRMAN LINDBLAD: What's the steam generator shell, excuse me, tube plate? What elevation is that? Higher or lower than normal two loop plants?

MR. SCHULZ: It's a little higher. Our cold leg, actually it's depicted here although this is not a dimensional drawing, the cold legs are elevated above the hot legs and they go into the pump discharge directly. There's no leak seal like in current plants. As a result that pushes the steam generator so the hot leg has a fairly significant rise to it getting into the steam generator. It should give us some benefits in mid-loop operations where we're not quite so sensitive to keeping a level at mid-loop. We can actually run it very close to the top of the hot leg.

CHAIRMAN LINDBLAD: Thank you. That's what I didn't know.

MR. SCHULZ: So the next slide I'd like to show you, just briefly touch on how the long term recirc works. I was going to color this in.

The picture on the left shows a post-LOCA situation that may be an hour into the event where the reactor is depressurized, the accumulators and core make up tanks are empty. You're getting injection from the refueling water storage tank through actually two separate DVI lines into the reactor. The core is covered. Steam with maybe some water is flowing out through the ADS flow path, some of them through the pressurizer, some of them directly from the fourth stage. There also may be a break. I showed here some water spilling out. So the water level in this case is relatively low.

Now in the next 8 to 24 hours or so, that water level will increase as the IRWST level drops. You'll finally get into the recirculation level. This is all water here and that water level as I mentioned before is 108 foot level in our elevation scheme. This injection nozzle is about 99 foot elevation, so about 9 foot elevation between the recirc level and this injection level. The key really is the level between here and the top of the core and this will primarily be steam in that case, above that level and that's the difference that's really available to drive water through the screens through the injection line into the reactor and then to push steam out the vent paths.

Again, we have done integrated testing in particular at OSU to demonstrate that this works to validate our codes that we also use to analyze this for Chapter 15 as well as PRA success criteria. So it is a key mode of operation that we have looked at very carefully to convince ourselves that it does work.

Passive containment cooling. Again, this is a simplified sketch. The key, of course, is using the steel shell with containment as a heat exchanger type device. The air going in and out is again always open, available for cooling of the containment. If the containment pressurizes due to a steamline break or LOCA, pressure instrumentation opens up to normally closed air operated valves.

These are again fail open, fail safe valves and if one of those opens, that allows water from the tank on top of the shield building to drain onto the top of the containment. There are some weird devices in there which are intended to roughly distribute the water around the containment. It doesn't have to be perfect. In fact, we've done a lot of sensitivity, showing that we can be off by quite a bit in terms of the coverage of the containment and still get very effective cooling in design basis space.

Hot water flows over the containment and evaporates then into the air which is flowing across the containment shell and that effectively cools the containment. The containment is designed for 45 pounds gauge. The peak pressure that you can get following a design basis accident is 40 to 42 or 43 pounds and that's due, of course, to the large mass-energy release. The passive containment cooling system is not involved in reducing that peak. It's pretty much expanded in the containment and passive heat sinks come into play.

Within a day, the passive containment coolant system with the water operating can bring the pressure down to about 10 to 12 pounds gauge. So it can effectively reduce the pressure.

MEMBER KRESS: What is the volume in your containment?

MR. SCHULZ: The volume of the containment? It's about 1.6 million cubic feet. That's a rough number.

MEMBER KRESS: It's about like PWRs now.

MR. SCHULZ: Yes, but this is a two loop plant. It's a little bit larger in a megawatt basis.

MEMBER KRESS: Per megawatt it's larger.

MR. SCHULZ: Yes. The water storage tank has got some standpipes in it which are designed to control the flow rate out of the tank so that initially we get fairly high flow rates, 200 gallons per minute or a little more and that is useful in reducing peak pressures should they exist in the containment. Then as the water drains down some, the flow rate slows down to more to be tailored more toward decay heat levels to maintain the level, the pressure in the containment at these lower levels.

The tank is designed to continue for at least three days following an accident. Following three days, we have made provisions for both water supplies in the plant, nonsafety water supplies, fire protection and normal makeup. We also have an alternate water supply where we can bring a fire truck up or something like that to pump up there. We've also done studies that even if we don't resupply water, the containment pressure would increase, but stay below design pressure following the three day supply of water.

CHAIRMAN LINDBLAD: The valve from the water storage tank and the like, is that all self-venting? If there's any air vortexing into one of those drains, will it clear itself?

MR. SCHULZ: Yes, it's all sloped down on here. There's also some vortex breakers on the inlets to those lines.

CHAIRMAN LINDBLAD: Thanks.

MR. SCHULZ: One final thing I wanted to mention in terms of the systems design aspect is related to this question of will these systems work? In the PRA, what's quantified is do you open the valves up, can a pipe break or can something plug, things that can be reasonably quantified, but if the valves open or sufficient number of valves open, they assume that -- we assume that the system works. And this picture is intended to give you an overview of the different things we have or will look at to convince ourselves and do all that, the systems will work.

It starts with what we call conservative design, so when I size the core makeup tank, I look at what the core requirements are and do a hand calculation that sets up the line resistances and the flow capabilities, so I do a very simplified analysis. It is conservative. I put a little margin on it.

Then that same system design is then tested in both what I call system tests which are like a core makeup tank test or passive RHR test, as well as integral tests, like at OSU and SPES where we put all the parts and pieces together and look at how they interact and how they operate during different size breaks.

That testing is then a very key element in input to the Chapter 15 type SSAR analysis where the codes are verified against the test information and then again in a conservative bounding type basis look at the different accidents with the single failure, with conservative acceptance criteria. We also do an AP600.

We have done and are continuing to do an extensive amount of T & H analysis to justify the assumptions made in the PRA in terms of how many valves are needed, how many tanks are needed. This is a more simplified analysis, but many more cases, because there's many different break [illegible]s, numbers of equipment. Conservative safety cases look at just a single failure.

But in PRA, we're looking at multiple failures, so there's many more culminations of things that we have to look at.

We learned a lot from doing this testing and analysis in terms of understanding how the plant works. And that's very key in terms of making sure those systems are reliable.

The Level 1, 2 and 3 PRA also gives us insight in terms of weak points in terms of the reliability of the systems. Common mode failure potentials and we've actually put some diversity into the system designs and valve selection based on the PRA.

Emergency procedures, we do additional analysis here to evaluate operator action strategies, interactions with nonsafety systems. In-plant activities, once the plant is built, there are additional things that will be done in terms of start-up testing or ITAACS that will verify the as-built initial condition of the system.

Once the plant is running it will be in-service testing and in-service inspection conducted to insure that during the life of the plant things continue to be operational. That will include things like checks on the passive RHR heat transfer rates.

Technical specifications assure that equipment is available, it's not failed. It's not out of service. Reliability insurance program will track failures rates and maintenance activities.

Another key aspect is conservative equipment design. The valves that we're going to use or the heat exchanger designs that we're going to use, we get as much out of operating experience as we can. Motor operated valve problems, we're factoring that into the specifications of a design of valves that we use. Equipment qualifications testing. Once we get to the point of vendor selection we eventually will do, before we start up the plant, equipment qualification testing and make sure that the valve that we build can meet our design requirements.

Okay, I'd like to now shift to kind of putting this all together a little bit in terms of the levels of defense in the plant. It's something that we have thought about, worried about, not only from a PRA point of view, but from a design point of view. Bruce Monty talked about the early involvement of PRA and design. There really have been a design interaction where we have learned from the PRA and taught the PRA about the plant design both ways.

The general philosophy that we have is that we have typically a nonsafety system that can provide mitigation of events. This -- if we have a more typical probable event like loss of off-site power, loss of mair feedwater, this is true and we get into like a large LOCA where there's a very low probability of event. We actually don't have a law and safety related protection scheme. It varies a little bit, but in the more probable events where additional reliability and redundancy and diversity is more beneficial, this is true.

These nonsafety systems again have -- they're reliable, they're designed to be reliable. They're not designed as safety systems, but they do have redundancy in on-site power connections. If we look strongly at operating experience, in particular, our normal RHR system, we put a lot of features in the normal RHR system.

We put a lot of features into the normal RHR system to minimize problems at mid-loop; special level instrumentation, better suction connection to the hot leg, no air traps so that if you do suck air into the system, you don't have to go down locally to vent air out to restart it. We can run the saturated water without throttling. Lots of things we've done to the normal RHR system as an example of learning from operating experience, making the system reliable.

We also have at least one and in most cases more than one passive safety related features that can deal with the accident. This system is what we would use in our safety analysis report. And as I mentioned we do have other defense-in-depth capabilities. In some cases, there are passive safety related and an example, the passive RHR as I mentioned is the safety related feature that removes core decay heat following loss of feedwater.

But backing that up is a passive feed and bleed. We use our safety injection in ADS capability, in fact, automatically safety, complete safety related backup to the passive RHR. It won't necessarily meet all the Chapter 15 requirements, but it can provide prevention of core damage in a PRA situation.

We also have multiple levels of defense during shutdowns. You'll hear in a little bit about our shutdown PRA and one of the things that has really benefitted the AP600 PRA is having not only the normally operating systems but a passive safety system backing that up and that provides -- it's not normally operating and that tends to separate common failure type scenarios, operational situations from those two levels of defense and we get a lot of our benefits in PRA reliability during shutdown by having these passive systems.

My last few slides --

CHAIRMAN LINDBLAD: Terry, with the larger steam generator at power -- excuse me, with the larger pressurizer power, what kind of transient that we see normally are you going to avoid? How much does it give you avoiding?

MR. SCHULZ: I'm not sure I can actually give you numbers. There's two kinds of things. One is if you're like pumping the system full due to a malfunction in a normal makeup system buys you time. Now it doesn't prevent you from eventually overfilling because that system can eventually just fill and we have some automatic trips that try to prevent that, but it does buy you some time here.

There are some events where when we look at a more realistic basis, if we have like a loss of main feedwater or loss of load or loss of condenser, we will not lift the safety valves. In current plants, we would lift the power operated relief valves, so that's an event where with a larger pressurizer, we would not open any valve during a clearly severe loss of heat sink type transient. In current plants, because of the small pressurizer and the presence of the power operated relief valve, those two combined, you actually will open vent valves on the pressurizer.

CHAIRMAN LINDBLAD: Thank you.

MR. SCHULZ: There's kind of two ways we've looked at defense-in-depth and tried to put in on paper. This slide has got a lot of stuff on it, but it primarily goes by function and shows you for that function the different things we have in the design to provide that function. It also shows a kind of a comparison to a typical Westinghouse PWR. For example, reactor shutdown, of course those designs rely primarily on control rods for shutdown; opening breakers to deenergize them. AP600 adds an additional feature that has come through the diverse actuation system to deenergize the motor generator sets to provide a different way of cutting power off to the rod to get them to go in.

Both designs provide what I call a ride out capability where the rods don't go in, but with our steam generator size, negative moderator temperature coefficient, we can ride out the transient and the pressure spike.

The decay heat removal was another example where we have several additional levels of defense due to the nature of the AP600 design. I think in some respects a little more interesting is if you look at a specific event, not all those features apply in every event. Two of them I have to show you this morning are loss of offsite power and steam generator tube rupture.

And what this tries to show is sort of blocks in groups of features in the design and you actually get into a PRA modeling this is broken up in even more detail looking at more individual tanks or components to provide a more accurate repenetration, but this does give you a more visual picture of what levels of defense we have.

In the case of loss of offsite power with the current PWR when that happens, of course, you lose your main feedwater system so the auxiliary feedwater system is automatically started. That is what I call the SSAR safety case which shows up in Chapter 15. If that works, of course, the plant is protected. If auxiliary feedwater system fails, then there is a feed and bleed type cooling capability where there is some automatic and some manual actions required, primarily the operator would be required to manually open the pressurizer venting capability. If that works, you can also successfully cool the reactor and if that fails typically you're into some kind of core damage scenario.

AP600 uses off-site power, the first thing that happens would tend to be start-up feedwater system.

That's like an aux. feed system, but it's a nonsafety related feature. It does start automatically, does load automatically onto our nonsafety diesels. If that doesn't work, then our passive RHR starts automatically and again that is kind of a fail safe feature of the design so it's very simple and reliable.

If that works, the core is cooled. That is our safety case which appears in Chapter 15. If that doesn't work, then we get into some variations of feed and bleed which rely on -- in this case here, for example, is fully automatic and involves only safety related equipment. This case here uses some manual initiation of the normal RHR system to provide an alternate injection recirc capability and I say partial ADS because it has greater injection pressure. You don't need as much ADS work, so you can tolerate more ADS failure.

We can also tolerate core makeup tank failures just using accumulators so we've got some diversity, redundancy within our passive feature.

Obviously, something that involves that much redundancy and diversity seems to be more reliable than an arrangement that has less.

In tube rupture, in current PWRs this is a very challenging event from a procedures point of view. It's not very challenging from a hydraulics point of view.

Things happen fairly slowly and are not nearly as exciting as a large LOCA.

But in the current plant, the safety case involves using safety injection auxiliary feedwater pumps, but then a lot of operator actions to control these pumps, to isolate the steam generator, to cool the RCS, to terminate the leak.

So there's a lot of operator action involved there. Now if, for example, the auxiliary feedwater system fails, you also can get into a feed and bleed type cooling mechanism. So there is some redundancy in hardware here.

In AP600, we've got basically an equivalent to this safety case using non-safety equipment, pumps, makeup operator action. If that works, we can isolate the leak. However, if the operators do nothing which we don't expect to happen, but as a limiting condition in our safety Chapter 15 case we looked at a situation where just core makeup tanks automatic, passive RHR, automatic, we have isolation of CVS start up feedwater if they malfunction. If they work normally, they actually control themselves to limit the injection to the volted generator and limit RCS makeup. But we have a backup of isolation to avoid adverse interactions.

Steam generator isolation is automatic.

You're just cutting off the turbine. And a passive RHR is mentioned can terminate this leak, without ADS, without operator action. If the passive RHR fails, then we can get into feed and bleed type cooling mechanisms which backup the passive RHR case.

Does anybody have any questions on anything I've talked about?

Okay. Thank you very much.

MR. POWERS: I'd just ask you a question about your defense-in-depth. It appears to me defense-in-depth, the things that you've talked about under the label of defense-in-depth struck me more as diversity, maybe redundancy, but a diversity rather than a defense-in-depth. Can you tell me more about how you're defining defense-in-depth?

MR. SCHULZ: You may be right in this case. There are different uses of that term. Sort of the classic light water reactor term, defense-in-depth, which relies more on the fuel cladding, the RCS pressuring boundary, the containment pressure boundary. That's all safety related. That's a part of the approach safety philosophy. This is a different use of the word and it is more general, small letters kind of thing. It does involve redundancy and diversity within systems, both mechanical and really I&C. I haven't talked much about the I&C, but earlier on when I talked about the protection control and diverse actuation systems, they all tie into the systems too and are an important part of the whole network of getting redundancy and diversity.

We use that term defense-in-depth in our SSAR in different ways and one of the ways is in this context it is more of a redundancy diversity. I don't disagree with what you said.

MR. POWERS: I prefer to use defense-in-depth to mean multiple independent barriers of increasing conservatism. And I'll reserve diversity and redundancy for more of what you've done here.

MR. SCHULZ: Any other questions?

CHAIRMAN APOSTOLAKIS: Thank you very much.

MR. SCHULZ: You're welcome.

CHAIRMAN APOSTOLAKIS: It's been suggested that we take a break now and then we'll start with PRA. So we'll be back in 15 minutes.

(Whereupon, the proceedings went off the record at 9:52 a.m. and resumed at 10:11 a.m.)

MR. SANCAKTAR: My name is Selim Sancaktar. It's written here just to make sure. I have worked for Westinghouse in the PRA group almost since its inception in 1981.

CHAIRMAN LINDBLAD: Is that PRA group specific too AP600 or is it a broad Westinghouse organization?

MR. SANCAKTAR: It's a broad Westinghouse organization. Actually, it works on various PRA projects nuclear or non-nuclear. This is only a project for us. It is one of the projects, one of the important projects we work on. It's only one of the projects.

CHAIRMAN LINDBLAD: But is it within the nuclear group?

MR. SANCAKTAR: Yes. Originally, the PRA group was part of the nuclear safety department. After various reorganizations, it was under some other division but yes.

MEMBER KRESS: Does it make use of Fauske and Associates?

MR. SANCAKTAR: Yes. Fauske and Associates actually used to report to Monty directly.

CHAIRMAN APOSTOLAKIS: And now? It used to.

MR. MONTY: This is Bruce Monty. They report to a different organization now since the volume of severe accident PRA work has declined over time.

MR. SANCAKTAR: Just as a tidbit, Terry Schultz, the redesign engineer, we worked with him since 1982 time frame, originally on APWR advanced PWR design project where the PRA was submitted to the NRC. Probably Terry can hold his own in a PRA meeting since that time.

I believe that there's a lot of interaction that's real, not on paper only, but it's also real between PRA and design.

Just to put this back in perspective, I'll go to this original slide for a second. We colored basically these three areas. Now I'm going to say a few things about background and methodology of the whole PRA just to put things in perspective. Then we will go directly to at power level I analysis.

What I will be telling you about are the results of the final PRA level I. You may have seen the one that I submitted to the NRC which includes 1995 results. So what I will show you will be slightly different.

CHAIRMAN LINDBLAD: And when will it be submitted if we haven't seen it yet?

MR. SANCAKTAR: As Bruce Monty mentioned, markups have already been submitted to the NRC. The formal documentation will be submitted by the end of this month, by the end of June.

So I'm basically picking up from here. Scope and methodology of the whole PRA. You can see some of the PRA covers the extent of the level I, level II, level III analysis. Level I referring to core damage analysis. Level II referring to containment response analysis, and level III referring to severe release.

MEMBER KRESS: Do you use a MACCS code for level III?

MR. SANCAKTAR: I think so, yes.

To show you the scope of the events analyzed, we analyzed the internal events. We refer to them as at power, but they are also known as internal initiating events.

We have done an equally in-depth modeling for shutdown events. We have studied internal flooding, fire, and we studied seismic events and then other initiating events that may be applicable to typical sites like the winds and external flooding.

Again, just to give you a brief sense of what is included, in level I analysis scope, we include all the standard analysis. We start with initiating events, categorize them into various manageable sets so far, challenges to the plant safety systems. We develop event tree models for each initiating event category. We at that time generate success criteria for core damage as well as each system that responds to the events.

Terry already mentioned this tree, but I will repeat it. There is an extensive thermal hydraulics analysis done to support the success criteria. We think that that's rather comfortable in that sense that our analysis are robust.

Once we establish event tree models for each system that will respond to an event, we generate plant systems models which are mostly fault trees. If something is simple, it might be as simple as a hand calculation, but usually they are fault trees.

In doing that, common cause failures are given special attention, especially in redundant plants like this. You have to give additional attention to common cause because that's probably what is going to get you random failure of many many different levels of -- I don't want to say defense in depth, but levels of available success paths.

Human reliability is --

CHAIRMAN APOSTOLAKIS: Excuse me. How can you do this though without knowing the actual plant layout. Do you know that? Do you know where the various components are?

MR. SANCAKTAR: We know what the design is today because we have access to designers and drawings. So we do whatever is available as much as possible at this point.

If there is any need after the construction stage is done, of course the models should be revisited and --

CHAIRMAN APOSTOLAKIS: And you are using generic models such as the multiple Greek letter?

MR. SANCAKTAR: Right. For common cause modeling, we are using multiple Greek letter method. Sometimes we just defer to data and assume a little bit more conservative. We don't even go into taking for certain. Twos, threes, and fours, if not necessary.

We try to minimize the gymnastics in the common cause, avoid later changes or effects.

Human reliability, we basically use that methodology. The operator actions are all rule-based, procedure-based. There are very few local actions, local action meaning actions outside of the control room. They are of no consequence. I'll mention that later on.

CHAIRMAN APOSTOLAKIS: You will come back to each one of these issues or this is it?

MR. SANCAKTAR: I will not go into details of them later on, but at any point as we go ahead, if you have questions, I will be happy to elaborate as we go into other areas. I don't have like a slide on common cause or human reliability that is formally in the package.

However, I will be happy to try to give you more information at the points you request.

CHAIRMAN APOSTOLAKIS: Well, I do have -- I'm sorry, do you have a comment?

CHAIRMAN LINDBLAD: Yes. Dr. Sancaktar, if that's the case, let me ask about the extensive thermal hydraulic analysis to support success criteria.

MR. SANCAKTAR: Yes.

CHAIRMAN LINDBLAD: This was done by people outside the PRA group, is that right?

MR. SANCAKTAR: We have basically two types of analysis. There are some analysts who are in the PRA group. They basically run the MAAP code. Then we have other groups that normally do chapter 15 analysis, who run codes like NOTRUMP. They are outside of our group. We use extensively both MAAP and other accepted codes. So the answer to your question is we have some of them in our group, some of them outside of our group.

CHAIRMAN LINDBLAD: So how do those extensive analysis affect the practioners' judgement as to what uncertainty lies with the actuation of systems?

MR. SANCAKTAR: That subject was actually brought up by the NRC, the thermal hydraulic uncertainties. So what we have done is we have generated a separate program to address it.

CHAIRMAN LINDBLAD: Separate from what?

MR. SANCAKTAR: From the PRA. So at the present time, it's being wrapped up. We would like to finish it soon and present it as a report by itself, as a project by itself. But at this point, the thermal hydraulic uncertainty is not a quantified aspect of the PRA.

MEMBER CATTON: Now I'd like to continue a follow-up question for Bill. There has been some controversy about the differences in success criteria achieved with MAAP and other thermal hydraulic codes that are more robust. Have you -- what do you do about this? Given there's a difference, what do you choose?

MR. SANCAKTAR: Let me tell you what I know and then maybe if I say something that's not complete, it can be supplemented.

The only what I would call a controversy I heard was an original version, version three of MAAP was used originally a few years back by others to make some calculations. We are using MAAP four, which is adequate -- which we believe is adequate for these calculations. We are backing up our major calculations by NOTRUMP also.

MEMBER CATTON: Have you made comparisons, a sufficient number of comparisons between the two codes?

MR. SANCAKTAR: Yes. In fact, that will be part of the report I mentioned that will come out about thermal hydraulic uncertainties. It will be --

MEMBER CATTON: Well, this has nothing to do with thermal hydraulic uncertainties. It has to do with code error.

MR. SANCAKTAR: It's combined in there. There were two projects.

MEMBER CATTON: So you were going to treat that as an uncertainty?

MR. SANCAKTAR: No. There were going to be two projects, one is benchmarking of codes. The other one is uncertainties. But they are not really separate. As you make one set of runs, they feed each other. So this is being combined.

MEMBER CATTON: I would hope the differences in the two codes don't feed each other.

MR. SANCAKTAR: Okay. Do you want to say something?

MR. MONTY: Okay. Just to make a comment. We understand the issues with respect to some differences between MAAP cases and MAAP predictions and other code predictions. That is one of the reasons we moved to supplement the MAAP cases that we originally did for success criteria using the MAAP four code with more detail codes like NOTRUMP, which we are currently doing comparisons of the two, so that we show that we understand the plant better.

What basically happens is we are looking at failures beyond the design basis cases. For example, in a design basis, we may be assuming a core make-up tank and an accumulator is available to respond to a loss of coolant accident. In our success criteria, we are assuming either of those two makeup sources is enough.

Originally, we justified that using MAAP or determined that using a MAAP code. Now we are supplementing that with NOTRUMP cases, which is the small break LOCA design code, which has been compared to test results and so forth. So that in the end, we will have success criteria that have a basis both in MAAP for certain sensitivities to determine what is the most limiting set of conditions. That will be supplemented by NOTRUMP runs for the most limited condition.

MEMBER CATTON: And at some point, this will be documented so one can trace it from --

MR. SANCAKTAR: Yes. It's coming out. When is the report scheduled to come out?

MR. MONTY: The report will be done later this summer at the end of July for the MAAP comparison.

MEMBER CATTON: Okay. I mean you know about the Crisco controversy, the Crisco plant? No?

MR. SANCAKTAR: Would you --

MEMBER CATTON: That's where they had made the success criteria in the Crisco plant PRA, which I believe was done by Westinghouse, was quite different than when they used the RELAP5 something or other. I guess the Westinghouse defended very strongly the MAAP results, which was surprising. That's why I raised the issue. I look forward to seeing your report.

MR. SANCAKTAR: Okay. I hope that it will be satisfactory to you and to the NRC. It's basically, the intent is to put this to bed.

MEMBER CATTON: Good, good.

CHAIRMAN APOSTOLAKIS: I have a couple of comments.

MR. SANCAKTAR: Sure.

CHAIRMAN APOSTOLAKIS: I was looking randomly at some of the documents we received. There is a letter from Mr. McIntyre to the NRC, Mr. Quay, I hope I pronounced it right, dated April 1 of this year, which provides information in response to questions from the NRC staff.

It gives calculations for human error rates, for LPM-MAN01, which is the diagnosing the need for RCS depressurization. Figure A-1 is a typical THERP diagram. It says diagnose failure within 25 minutes. It's assigned an error rate of 4 x 10 to the minus three. Then that's followed by a failure to respond to two alarms, which also has 8 x 10 to the minus four. Therefore, the product has negligible probability.

Then I went to chapter 30. On page 30-4, it says the generic procedures are based on the philosophy of symptomatic responses to an emergency operating situation, and therefore reduces the diagnosis of an event to responding to cues such as alarms, annunciators and indicators.

So chapter 30 says that diagnosis really means responding to the alarms, and yet in the actual analysis, you have two pieces. One is failure to diagnose, which is 4 x 10 to the minus three, and the other one is failure to respond to the alarms, another 10 to the minus four.

It seems to me according to what chapter 30 says, you should not be using the failure to diagnose within 25 minutes, in which case the probability would be 8 x 10 to the minus four for the total.

MR. SANCAKTAR: Yes. I can answer that to make it very clear. The report that you are referring to, chapter 30, is what we are standing behind. The letter is a sensitivity analysis to show that what we have done is at least conservative and does not introduce anything new. If we have taken credit for the standard process of you first have to respond, you can diagnose something in a certain amount of time. Then if you have cues, actually that helps even more.

In the report, we did not take credit for the first part. So yes, we have 10 to the minus four. We don't have 10 to the minus four times something. That's just an example to show that we are okay.

CHAIRMAN APOSTOLAKIS: So let me understand this. The probability that you actually use is on the page here, page 10, current AP600 HEPs, LPM-MAN01, 1.34 x 10 to the minus three.

MR. SANCAKTAR: Right.

CHAIRMAN APOSTOLAKIS: So that includes the failure to respond to the two alarms? It's not really this figure A-1?

MR. SANCAKTAR: Right. The figure is a sensitivity analysis to respond to the question that what we have done is bounding.

CHAIRMAN APOSTOLAKIS: Well, I mean the assumption here of independence of these two actions and multiplying them is questionable. So I don't know -- I mean you reported a higher number, but that doesn't prove that this is bounded.

MR. SANCAKTAR: What you are looking at currently is a direct counterpart of an example in therp 1278 for large loca. Exactly the same concept. You are welcome to --

CHAIRMAN APOSTOLAKIS: Yes, but you are arguing that this diagnosis is no different from recognizing the alarms?

MR. SANCAKTAR: Right. We still have that position.

CHAIRMAN APOSTOLAKIS: Okay. So this figure then is not what you are using.

MR. SANCAKTAR: Right.

CHAIRMAN APOSTOLAKIS: Okay. Now the next question. In chapter 30 you say it is advisable not to use table 20-3 of the Therp handbook. But here you are using that. So again, that's in the spirit of doing sensitivity analysis?

MR. SANCAKTAR: To show by a numerical means where we stand, just to end the discussion on whether this is conservative or not conservative or whatever.

CHAIRMAN APOSTOLAKIS: Is that clearly stated in this letter that this a sensitivity thing? Mainly I didn't read it in detail.

MR. BUETER: The context of the report is a response to a request for additional information.

CHAIRMAN APOSTOLAKIS: Right.

MR. BUETER: That response along with our reply I think would give you a clear picture of what's presented there.

I believe the RAI, and correct me if I'm wrong, was along the lines of -- I see John getting up, are you going to offer --

MR. FLACK: Yes. Excuse me. This is John Flack from Office of NRR. We requested that information to follow up some questions on the HRA. They performed these analyses that you see in response to that question that was raised. It was not as part of the PRA itself.

CHAIRMAN APOSTOLAKIS: So this is really going against the main assumptions that were made. Okay.

MR. SANCAKTAR: It's just another way of calculating the number to show that it is less than or equal to what we calculated.

CHAIRMAN APOSTOLAKIS: And what you calculate is in chapter 30?

MR. SANCAKTAR: Right.

CHAIRMAN APOSTOLAKIS: Okay. I will look at it later.

Now also in chapter 30 you have a statement that needs to be discussed. Although the use of symptom based procedures may not eliminate all knowledge-based behaviors by the operators, the scope of the AP600 human reliability analysis covers only the modeling of rule-based activities. Therefore, no credit is taken for knowledge based recovery actions efforts.

Is that a credit? It seems to me that if you assume that it is knowledge-based behavior, things only can get worse.

MR. SANCAKTAR: If you are only in a knowledge-based situation, things will get worse. But if you are in a rule-based situation --

CHAIRMAN APOSTOLAKIS: They are better.

MR. SANCAKTAR: They can be better. It may be better, but we didn't get into those areas. We didn't say that somebody will think of this and take care of it. If it's not in the rules, we didn't take credit for --

CHAIRMAN APOSTOLAKIS: But basically what you are saying here is that there is no knowledge-based behavior. You assume there is no knowledge-based behavior. It's only rule-based, which automatically eliminates the possibility of knowledge-based mistakes. So how can you call that a credit?

MR. SANCAKTAR: No, no. That's not the intent. What you are referring to is cognitive errors.

CHAIRMAN APOSTOLAKIS: Right.

MR. SANCAKTAR: That statement does not address that issue.

CHAIRMAN APOSTOLAKIS: So what you are saying here is that you assume rule-based behavior, but only the consider the possibility of deviating from the procedure?

MR. SANCAKTAR: Right.

CHAIRMAN APOSTOLAKIS: And you are saying that things may get better because someone may behave differently and use his brain and do something clever?

MR. SANCAKTAR: Could have been, right.

CHAIRMAN APOSTOLAKIS: That says you don't take credit.

MR. SANCAKTAR: Right.

CHAIRMAN APOSTOLAKIS: But at the same time, that person may screw up.

MR. SANCAKTAR: They may.

CHAIRMAN APOSTOLAKIS: So we do not really know, not looking at knowledge-based behavior is credit or --

MR. SANCAKTAR: I understand.

CHAIRMAN APOSTOLAKIS: The words need to be changed. Is it really true that there will be no knowledge-based behavior at all, I mean this reactor, that everything is rule-based?

MR. SANCAKTAR: No. There might be, but we have not gone into any credit taking for knowledge-based behavior, credit taking, because we don't have to. I mean this plant has so much margin, we don't have to worry about operator actions that much.

If we had to, if we were in a different plant, had to have other operator actions, recovery for example, then we would have been pushing the boundary of rule-basis and might have gone into knowledge-based. But we didn't feel the need for this plant, because we already had automatic systems lots of credits, in which some rule-based operator actions we get enough so that we don't feel any urge to take one more credit for some recovery action at the last minute which actually might be a realistic.

CHAIRMAN APOSTOLAKIS: Yes. But it is not the credit that I'm worried about.

MR. SANCAKTAR: If you are asking about how cognitive failures are factored into it?

CHAIRMAN APOSTOLAKIS: Yes.

MR. SANCAKTAR: Okay. Now that, I don't think it's any different than how they are handled with the present state of the art. If we can identify things that we can put our hands on, we tried to address them.

CHAIRMAN APOSTOLAKIS: But you say you are not able to identify.

MR. SANCAKTAR: Right. We have not seen anything yet that we can put our hands on and say there it is.

Now once a plant is built and you can actually visit and see things and so on, this may change. But at the current design stage, whatever we can see, we try to address. If there are questions, we try to address. But we do not have anything we can put our hands on and say here is an obvious pitfall for cognitive behavior.

However, our human factor group receives these operator actions remodel. They will be looking into those to see which ones they should look for human factors point of view dealing with man machine interface designers. There is a power program to address possibilities like that. But we didn't put any numbers for things that we couldn't observe yet, but we are open. I mean, if we find anything, we'll model it. Or if anybody else asks or points out something, we'll look into it.

CHAIRMAN APOSTOLAKIS: As part of this response, you said that you have raised all human error probabilities to one.

MR. SANCAKTAR: The sensitivity analysis.

CHAIRMAN APOSTOLAKIS: Yes.

MR. SANCAKTAR: Yes. I have that.

CHAIRMAN APOSTOLAKIS: And the resulting core damage frequency became 2.78 x 10 to the minus five. So it went up by what, by two orders of magnitude?

MR. SANCAKTAR: Yes. I will talk about it when the sensitivity analysis comes, if you don't mind.

CHAIRMAN APOSTOLAKIS: No, that's fine.

MR. SANCAKTAR: If you want, we can do it now.

CHAIRMAN APOSTOLAKIS: That's fine. Okay, thank you.

MR. SANCAKTAR: So in modeling the plant systems, we have also separately taken care of common cause failures, human reliability. We have specialists who deal with these. Data analysis is also handled in a central manner.

Fault trees and event trees are quantified. Afterwards, importance and sensitivity studies are formed. One of which is termed the focus PRA. That's the only credit is given for circulated systems for mitigation of accidents. This is the subject for what is referred to as RTNSS, regulatory treatment of non-safety systems. We have some preliminary results that I would like to show you briefly later on.

CHAIRMAN APOSTOLAKIS: Have you done uncertainty analysis on all this?

MR. SANCAKTAR: As we speak, we are in the process of doing quantitative uncertainty analysis on level I.

CHAIRMAN APOSTOLAKIS: And the goal of 10 to the minus five for core damage frequency is interpreted as a mean value?

MR. SANCAKTAR: Yes. I'm not going to talk about the next two slides. They will just give you a sense of what subject matters were covered in the PRA. It's just a duplication of the contents of the PRA report.

CHAIRMAN APOSTOLAKIS: I suggest that you go to the slide that says plant features important to the reduction of risk. Do you think that's a good idea? I think we're going to run out of time. I really want to discuss the results.

MEMBER KRESS: I know this is a level I discussion. You did do some level III work?

MR. SANCAKTAR: Yes.

MEMBER KRESS: What did you use for a site, some sort of a hypothetical standard site?

MR. SANCAKTAR: You want to know about that?

MR. BUETER: Yes. The short answer is yes. It's kind of a generic --

MEMBER KRESS: Some generic kind of site.

MR. SANCAKTAR: You want me to skip methods and so on?

CHAIRMAN APOSTOLAKIS: Yes. See slide 12. Only if you agree, of course.

MR. SANCAKTAR: I'm here to report information, whichever you like.

Before I go into the results, I want to just point out a few items here. This is not a complete or exhaustive list.

In current PWRs, station blackout, which is defined as the loss of all AC power, appears to appear as the dominant risk contributor in many plants. AP600, it almost wipes it out as a threat to the plant core damage risk. It's basically safety systems are not dependent on AC power. We still have some credit for non-safety systems. We still have diesel generators. We still have startup feedwater and so on.

Terry already showed you a slide where he pointed out the defense in that in quotes. More diversity and redundancy that's provided.

So looking at this PRA issue, this was actually, it was an attempt to deal with --

MEMBER POWERS: Can I ask a question about terminology on the slide?

MR. SANCAKTAR: Yes.

MEMBER POWERS: You distinguish between a dominant risk contributor and a dominant fission product contributor to release from fission product.

MR. SANCAKTAR: Right.

MEMBER POWERS: Would I be correct in assuming that when you say risk contributor, what you mean is core damage frequency contributor, and when you say fission product release, contributor fission product release, you are talking about what the rest of us would call risk?

MR. SANCAKTAR: Yes. Actually, this basically, this discussion refers to core damage frequency. I couldn't resist saying something about steam generator tube ruptures. I can not say that it's necessarily a core damage --

MEMBER POWERS: It tends to be low on the frequency list and high on the risk?

MR. SANCAKTAR: Right. But it doesn't necessarily mean -- yes, absolutely true what you said, absolutely true.

Again, reactor coolant pump, seal LOCA, which is coupled with either station blackout or loss of cooling systems like component cooling water, service water, or just random failures appears to be dominant again in many plants. Again, the AP600 addresses it by having canned motors, which avoids this kind of a failure mode.

Loss of support system events, again, this actually ties back into this. Also it ties into cooling of SI pumps or recirculation pumps. It may or may not be an important contributor, depending upon the plant, but again, AP600 safety systems do not rely on cooling support or AC power for the loss of support system events which appear as plant specific events in many plants, are not very important as we will see in the next slides.

Steam generator tube rupture, again, Terry Schultz has shown you the slide which has various ways, success paths out of it. Here are three of them. The two and three are actually automatic with manual backup. The first one is actually from how it will develop, if you follow the procedures.

One may discuss the philosophy is better just not to touch it maybe, because two and three are good enough, are pretty reliable. But this is the way it will go. This is why this is up front, not because it's more important or anything like that.

Interfacing systems LOCA, again, this is a bypass potential. The frequency may not be a high contributor, but it might be in core damage, but it might be important for severe release. Basically, normal RHR paths in AP600 are able to withstand RCS pressure and also we have more valves in the interface boundary between the high pressure and the low pressure side. We try to make the valves different whenever possible, more and different. Not just more.

For example, in the current plants, there is always the two MOV situations in one of the paths. We don't have any two MOVs. We have more than two valves, up to five. They usually have different types of valves. So we tried to reduce this one --

CHAIRMAN LINDBLAD: Before you leave that --

MR. SANCAKTAR: Sure.

CHAIRMAN LINDBLAD: It may be a matter of definition, but it seems to me that in existing plants, the station blackout is really loss of safety electric systems rather than just AC power. It just happens that AC power is a safety electric system. But you have defined it as the problem goes away because you don't use AC power but in fact, station blackout for an AP600 may mean loss of some of your DC.

MR. SANCAKTAR: Sure. That's addressed. I try to keep this terminology kind of parallel or consistent with the current plants. But once you get into the AP600 modeling, after this happens, you asked a question whether you have DC failing or not, old batteries common cause failure. It's in there, yes. It's also in there.

MR. SCHULZ: Selim, let me add -- this is Terry Schultz, that in case of loss of DC power, we have a level of defense involving passive RHR, passive containment cooling which is fail safe. It doesn't need DC power.

Now if you get into LOCA situation, we do need DC power. But if you are really starting from a loss of power situation, you presumably wouldn't couple that with a loss of coolant accident. We can't actually deal with that better than the current plants can deal with that also.

That was not what Selim was talking about, but to answer your question.

CHAIRMAN LINDBLAD: Thank you.

MR. SANCAKTAR: Some other items that I thought might be of interest. In current plants, there are certain operator action that you have to do like in steam generator tube rupture. There is no way around it without operator action.

AP600 minimizes the importance of operator actions to mitigate accidents. There is no single operator action that you have to do to get out of a situation. Everything is automatic design basis sequence of response.

But as Dr. Apostolakis pointed out, there is a lot of impact of the operator action which we will revisit in a few minutes hopefully, which doesn't mean that it's not any -- of no consequence. They help a lot.

ATWS is a subject matter that is discussed a lot in PRA. It may or may not have high program frequency. In AP600, Terry mentioned there's a diverse actuation system introduced to reduce ATWS challenges for AP600, because we can not tolerate even the existing low frequency of ATWS since our overall plant frequency is low. So this has to be taken into account.

In some older plants, switchover to

recirculation might be a dominant contributor, especially if it is a manual action and you have to stop, close valves, open valves, et cetera, restart pumps.

Again, this has been discussed in detail by Terry. I think AP600 tried to address the injection and recirculation switchover process being very simple, fail safe, et cetera.

Just a couple of things about shutdown. The first one is about RHR and support systems. There are certain simplifications and improvements introduced. However, the most important one is actually this bullet with respect to shutdown. We have passive IRWST injection providing backup to RNS automatically. If the normal RHR fails during shutdown, IRWST would take over automatically, no operator action. Tim will be discussing the shutdown process in more detail.

CHAIRMAN LINDBLAD: If I wanted to add a PRA issue of reliability of digital software, how would you answer the other block over there, how the design addresses the issue?

MR. SANCAKTAR: Well, the I&C system was modeled in detail. Its reliability is at this point to our satisfaction. Now is it much better, is it equal or is it -- I don't know whether I can make a strong statement about it because there are different points of view. But I&C system has been modeled with a card level. Common cause of software and similar concerns have been addressed at different levels.

CHAIRMAN LINDBLAD: But there isn't a unique approach that AP600 takes?

MR. SANCAKTAR: No. There isn't.

MR. SCHULZ: Selim, it's Terry Schultz. The U&V of the protection system will be a thing we will rely on. We also, diverse actuation system are making commitments that that software will be different than the software in the protection system. So the diverse actuation system will help answer that question.

CHAIRMAN LINDBLAD: Thank you.

CHAIRMAN APOSTOLAKIS: Well, you didn't actually quantify the reliability of the IRSS, did you?

MR. SANCAKTAR: We did. Our PMS and PLS is quantified in excruciating detail to capture the potential failure that would defeat the redundancy. Since it's highly redundant, it was captured at the card level so that we could introduce common cause failures of card groups or software at different levels, whether it's at the highest level for example, the software error that will knock out PMS and PLS.

CHAIRMAN APOSTOLAKIS: How did you model that?

MR. SANCAKTAR: As a basic event. Is that what you are asking?

CHAIRMAN APOSTOLAKIS: Yes.

MR. SANCAKTAR: Or how did you get a number for it?

CHAIRMAN APOSTOLAKIS: What software error, I mean you just assumed the rate?

MR. SANCAKTAR: Yes. A model has been defined and introduced. It basically caps the reliability you can get for PMS and PLS as a product. It saturates it so that you don't go 10 to the minus nine to 10 with them.

Again, what that value is can be discussed too, whatever.

MEMBER WYLIE: The diverse actuation system, is that located in the main control center?

MR. SANCAKTAR: You mean the manipulation of it?

MEMBER WYLIE: Yes.

MR. SANCAKTAR: Yes.

MEMBER WYLIE: Okay. Is there a separate center outside the main control center?

MR. SANCAKTAR: Terry?

MR. SCHULZ: I'm Terry Schulz. Diverse actuation system controls, manual controls are only located in the main control room.

MEMBER WYLIE: There's no external shutdown panel?

MR. SCHULZ: No. There is.

MR. SANCAKTAR: That's the difference.

MR. SCHULZ: There is a very complete remote shutdown station. It basically can control all of the safety and non-safety equipment in the plant. But it does it through the protection and control system, not through diverse actuation.

MR. SANCAKTAR: Diverse actuation is additional to what normally exists as a control room and panel outside.

Okay. Finally we come to level I at-power after all this digression. We try to give you some overview. We went through the normal processes of trying to determine what kind of initiating event categories are appropriate for AP600 other than usual LOCAs and transients. Basically we ended up with 26 initiating event categories. Eleven of them are LOCA coolant accidents in a general sense. They include situations where you have some sort of a LOCA RCS inventory. Twelve categories of transients and now we categorize the ATWS even into three different categories.

This is the trickiest part, the next is the trickiest part. What plant-specific initiating events can be introduced in this plant that may not be present in current plants. We looked at things like the direct vessel injection line. Terry has shown on his slides this line. If any one of these lines has a LOCA, we assume that every water source that feeds it is lost. That includes CMT, accumulator, IRWST injection, IRWST recirculation.

In fact, that probably should be one of the dominant contributors for damage frequency, because you are knocking out half of your safety trains in a two loop plant. So one should really expect this to show up somewhere.

Then core makeup tank line break, is that really a special case of this. It has much less in consequence than the first one. Then passive residual heat removal systems introduced into this plant, of course brings in its own possibility of tube ruptures. So that's addressed.

So this spectrum of events are shown on the next slide in two columns. We tried to put everything on one page, so actually this is a continuation of the first column.

You'll see the LOCAs here. By the way, the way these are ordered here the same order as they will appear in the next slides in contribution to core damage frequency.

So this is reactor vessel rupture. This is SI line break, is the same as DVI line break. Any acronyms here. Passive RHR tube rupture. Loss of component cooling service water. So this is the spectrum of events. So we have a total of 2.4 events postulated per year. It's coming basically from transients with main feedwater available, 1.4 per year. Looking for loss of on-site power about one every eight years.

CHAIRMAN APOSTOLAKIS: Is that kind of a generic number or what?

MR. SANCAKTAR: It is a generic num... It is a little bit higher than what typical plant would have used today because we have only one line coming in. Currently plants have two lines that they take credit for. So a current plant today, there's an IPE, it's being used generic. They would have probably used a lower number than this.

CHAIRMAN APOSTOLAKIS: Most of these numbers are calculated, right?

MR. SANCAKTAR: Yes, they are calculated. They are taken from the URD whenever possible, like this 1.2 and -1 is taken from the URD document.

CHAIRMAN APOSTOLAKIS: And how do they find their way into the URD document? I mean they were calculated at some point?

MR. SANCAKTAR: It is calculated from the existing data, but looking at one line coming in instead of two lines. So there is a penalty taken for that.

CHAIRMAN APOSTOLAKIS: So for example, CMT line break, 8.9 to the minus five.

MR. SANCAKTAR: Okay, sorry. I might have --

CHAIRMAN APOSTOLAKIS: Yes. You were referring to the --

MR. SANCAKTAR: Right. I was referring to this. How are these numbers calculated, okay.

CHAIRMAN APOSTOLAKIS: Let's take the CMT line, which is a new event.

MR. SANCAKTAR: Let me explain that. Whenever possible, we try to take the numbers from existing data, like transients. We sift through the data available and try to group them into what is applicable to the AP600. All are basically transients.

Now with LOCAs and lower less likely events, we either use what's available or suggested in the literature or calculate them from raw data or lower level data.

So for example, the LOCAs were calculated using a number of segments and points of welding and so on rather than assigning a generic number. But the sums almost adopt what you would have obtained if you had a generic number suggested by URD.

If you take some of the large LOCAs, intermediate, medium and small, and add them up, that's pretty much very close to what is in the URD. But we've partitioned them to reflect what's in this plant. It is back to the type of size of piping, and also we claim and we would like to reflect that the PRA, that this plant has less number of pipes, less welds as Terry mentioned before. So that should also factor into it.

MEMBER CATTON: Just looking at your numbers, you have large LOCA and small LOCA the same.

MR. SANCAKTAR: Yes. I knew that that question would come, so I had to answer that. Actually, we had to introduce this intermediate LOCA because of our thermal hydraulic analysis after we made hundreds of them. We broke small LOCA, intermediate LOCA. Actually you can think of this as a standard small LOCA, which is more like 10 to the minus three. Until all this rigorous analysis, the results didn't matter, you know, the conditional core melt frequency wasn't justified to all this detail.

But the success criteria pointed out that intermediate LOCA and small LOCA have a little bit.

MEMBER CATTON: And CMT line break, isn't that a small LOCA? Right underneath small LOCA.

MR. SANCAKTAR: Here?

MEMBER CATTON: Yes.

MR. SANCAKTAR: Well, it might be different types of LOCAs, it depends upon the size of the break. It might be small LOCA.

CHAIRMAN APOSTOLAKIS: It's almost the same anyway.

MEMBER CATTON: Yes, but they broke it up so much you can't tell. You sort of develop numbers in your head for things.

MR. SANCAKTAR: Yes, yes, I realize that.

MEMBER CATTON: You are just foxing us.

MR. SANCAKTAR: Not really. The thing was, we didn't know. I mean we have to look at CMT line breaks. We didn't know what will come out of it. We have to look at it. It might come out to be insignificant or not, but it's something special --

MEMBER CATTON: What is an RCS leak? Is that a hole in the vessel?

MR. SANCAKTAR: RCS leaks are LOCAs from what is in tech specs up to three-eighths of an inch break.

MEMBER CATTON: Oh, so an instrument line or something like that.

MR. SANCAKTAR: Right. They can be normally handled by CVCS. However, if CVCS also fails and you are going to shut down, then they will create eventually a SI signal. It's a smaller end of small LOCAs, if you want.

MR. MONTY: Selim, this is Bruce. I just want to make a comment that the definition of the LOCAs here were set up based on an evaluation of the equipment that would be available in each one. Like you mentioned on the DVI line break, disabled certain equipment. Similarly, the CMT line break disabled certain equipment. That is why we have to break them differently.

The definitions have the same names as you traditionally see in the design base analysis, but they are not the same. They are not common with sizes. So I think the intermediate, the medium and the small go up to approximately a nine inch equivalent diameter size. Then large LOCA is anything bigger than that.

MEMBER CATTON: Actually, I like this better.

CHAIRMAN LINDBLAD: Is there any initiating event frequency associated with the reactor coolant pump seal? Granted it's a canned rotor, but you say it's incredible that it can fail?

MR. SANCAKTAR: Right. We didn't assign a number to it. If you think of it as buried in one of these LOCAs, small LOCA.

MEMBER CATTON: Is there somewhere that --

MR. SANCAKTAR: But we didn't assign a number for it, to answer your question. There is no number assigned to it. Not even epsilon.

MEMBER CATTON: I don't know much about canned rotor pumps, except everybody says they are so good. Is there somewhere I could see a cross-section of one? I'd like to see why it's incredible that it could leak.

MR. SCHULZ: Basically a three, four inch thick steel pressure vessel that surrounds all the rotating parts. So the shaft does not go through the pressure boundary.

MEMBER CATTON: But the picture that you showed before shows a door on it.

MR. SCHULZ: That's the electrical door on the outside of the pump. I also have one. It will take me -- if you want to see it.

MEMBER CATTON: The electrical motor drives a shaft, so there's got to be seals.

MR. SCHULZ: No. The motor isn't -- (inaudible) -- in the water.

MEMBER CATTON: Oh, it is. So it's just the door. What's the failure probability of the door, wherever it is. I can't see it here.

MEMBER WYLIE: It's at the bottom there on the right.

MEMBER CATTON: Bottom right.

MR. SCHULZ: I think this is the door you were talking about. The electricity is really going into part of the figure that's outside the pressure point.

MEMBER CATTON: Can you hear him?

MR. SCHULZ: The key is that the electricity that comes in goes into a stator which is outside, while it actually penetrates the pressure boundary here. This thick steel surrounds everything else so it's really a pressure thick steel pressure vessel.

MEMBER CATTON: And then it's bolted up against that flange?

MR. SCHULZ: Right. There's a bolt closure which is very similar to current plants, though in current plants, it doesn't encompass the motor. It just encompasses the seals. There is a way of taking apart the current pumps to get the empeller out.

MEMBER CATTON: You can see the nuts. What's the probability of failure of those bolts?

MR. SCHULZ: Very small. If these bolts fail, presumably that's like a large LOCA.

MEMBER CATTON: It's a large LOCA in a rather awkward place, isn't it?

MR. SCHULZ: It's not any worse than a pump failure. I mean this bolted closure exists in current plants. A very similar diameter, that it encloses just the seal package in current plants, but there is a similar diameter bolted closure in pumps in current plants. So it's presumably a similar risk that's encompassed in large LOCA type numbers.

MEMBER CATTON: So it would fit into the 10 to the minus four for the large LOCA. Okay.

MR. MONTY: This is Bruce Monty. Just one more comment on the initiating event on the pumps. The treatment is similar, the mechanical failure for the reactor coolant pump in the current initiating events on current plants is subsumed in the small LOCA, large LOCA initiating event frequency. The only thing that's additionally modeled is the dependent failure from the loss of AC, and then a coincident or a causal failure of the seal after the loss of AC or the cooling system, which we don't have in this situation. The only thing we have in this situation is the same mechanical failure that's present in current plants, which is always subsumed into the initiating event frequency for LOCA.

CHAIRMAN LINDBLAD: And is there any casualty associated with a seizing of the pump or a loss of power -- excuse me, loss of electric power at full load? There is no requirement for coast down?

MR. SCHULZ: If I understood the question, there was a loss of coolant flow?

CHAIRMAN LINDBLAD: Yes.

MR. SCHULZ: These pumps, if anything, the reliability data that I think exists indicates that they are equal to or more reliable than the shaft seal pumps in terms of functioning. There is an initiating event which is a loss of coolant flow.

I guess I'm not sure how that was calculated or gotten.

MR. SANCAKTAR: That's a transient pump existing, derived from the existing data.

CHAIRMAN LINDBLAD: And is that with a motor coming to stop immediately or does it coast down?

MR. SCHULZ: The event would assume a reasonable coast down. These canned motor pumps do have a high inertia piece inside of them. It was specially developed for AP600 to provide some necessary coast down. So the pumps that operate equivalently from that point of view, if you turn the power off, it provides sufficient coast time to insert the rods to prevent any core damage.

CHAIRMAN LINDBLAD: And so it doesn't contemplate a pump motor combination seizing, coming to stop?

MR. SCHULZ: The particular event I think is more --

CHAIRMAN LINDBLAD: Loss of power?

MR. SCHULZ: Loss of power or loss of somehow to the pumps. Of course in chapter 15 analysis, we do look at a single pump shaft, pump stopping and looking at the safety consequences of that.

CHAIRMAN LINDBLAD: Okay. Thank you.

CHAIRMAN APOSTOLAKIS: So let's move on.

MR. SANCAKTAR: Okay. Next slide jumps to the results. First on this slide, we see the dominant initiating event contributors to core damage frequency, which show large LOCA as the first one.

I always look for this one as kind of a break point. If everything is below that, it's act of god type of thing. These are also act of god kind of numbers.

But total this, 2 X 10 to the minus seven. The dominant contributors are listed here. We'll see about nine of them or so make up almost 94 percent of the risk with respect to core damage frequency.

CHAIRMAN LINDBLAD: I'm not sure I understand what your introductory statement was, below reactor vessel rupture. What did you mean by that? That small LOCA is an act of god and other things aren't?

MR. SANCAKTAR: No. Reactor vessel rupture is basically a very low probability event. It has been every design and operational precaution is taken to keep it low. So in general, it's not, at least in my mind, it's not a major contributor to core damage.

If I can keep everything below that, I feel pretty much -- well, I have a warm feeling that CDF is small. So if you look here, you'll see that these three LOCAs show up higher than that. If you are looking for some sort of an anchor point, you don't have to see it that way, I mean that's how I try to present it, the way I see it.

CHAIRMAN APOSTOLAKIS: So what you are saying is god acts only below the reactor vessel rupture frequency?

[Laughter.]

MR. SANCAKTAR: In this plant. In other plants, it's at higher levels.

CHAIRMAN LINDBLAD: And you are saying that the events are ordered with respect to CDF?

MR. SANCAKTAR: In this case.

CHAIRMAN LINDBLAD: Yes, thank you.

MR. SANCAKTAR: Large LOCA is first.

CHAIRMAN APOSTOLAKIS: Now let's talk about it. The initiating event frequency for the large LOCA is 10 to the minus four.

MR. SANCAKTAR: Right.

CHAIRMAN APOSTOLAKIS: And your sequence that leads to core damage is 5 x 10 to the minus eight. So you have a multiplier there of 5 x 10 to the minus four. Can you tell us where that comes from?

MR. SANCAKTAR: Sure. Actually, I don't have a slide for it, but I can tell you what the dominant contributor for that is.

CHAIRMAN APOSTOLAKIS: Sure.

MR. SANCAKTAR: This information is available of course.

Okay. Large LOCA initiating event occurs. I'm talking about the cut sets at component level.

CHAIRMAN APOSTOLAKIS: No. The sequence, the accident sequence.

MR. SANCAKTAR: Oh, the sequence.

CHAIRMAN APOSTOLAKIS: Yes.

MR. SANCAKTAR: We have a slide for that actually. The sequence would be a large LOCA initiating event occurs, success of one of two or two of two accumulators, and failure of IRWST or CMT.

CHAIRMAN APOSTOLAKIS: Or, either one? If either one fails, so the frequency then that one of them will fail is roughly 2 or 3 x 10 to the minus four?

MR. SANCAKTAR: Yes.

CHAIRMAN APOSTOLAKIS: That frequency comes from where?

MR. SANCAKTAR: It comes from fault tree modeling.

CHAIRMAN APOSTOLAKIS: But these are essentially passive systems, aren't they?

MR. SANCAKTAR: Yes.

CHAIRMAN APOSTOLAKIS: So what kind of failure does the 10 to the minus four represent in that case?

MR. SANCAKTAR: It represents failure of for example, for CMT actuation, I&C actuation, the failure of valves, if there are strainers like in IRWST there are strainers, mostly common cause failures.

CHAIRMAN APOSTOLAKIS: Of what? Common cause failures of what?

MR. SANCAKTAR: Of valves or actuation logic. It's applicable to actuation logic, it's applicable.

CHAIRMAN APOSTOLAKIS: So if all these things work, then you assume that the system has a probability of one, of doing its job?

MR. SANCAKTAR: Yes, yes.

CHAIRMAN APOSTOLAKIS: So essentially what you are saying is that these passive systems have a reliability of one?

MR. SANCAKTAR: These passive systems have -- in the way you are asking is they have the same reliability as what you would model today as SI pump system or whatever, not any different in modeling. It's the same model.

CHAIRMAN APOSTOLAKIS: It is the same model in what way?

MR. SANCAKTAR: If today we were to take an SI injection, and somebody said what's the reliability of it, we calculate it.

CHAIRMAN APOSTOLAKIS: Yes, but that --

MR. SANCAKTAR: This does exactly the same thing to it. There is nothing different.

CHAIRMAN APOSTOLAKIS: The unreliability though of today's systems is dominated by failures of active components. So you are saying that basically the valve not opening is the dominant contributor to risk here?

MEMBER KRESS: These numbers have active components in them. You have your whole active system that's non-safety. They are in the PRA.

CHAIRMAN APOSTOLAKIS: No, no. He said CMT. That's a passive system.

MEMBER KRESS: I know, but if it doesn't work, your active system still are assumed turned on.

MR. SANCAKTAR: Right, but they don't do anything to large LOCA.

MEMBER KRESS: They don't do anything to a large LOCA?

CHAIRMAN APOSTOLAKIS: No. It's only the

IRWST.

MR. SANCAKTAR: Let's make sure that we have the same terminology on active, passive, because the concept might be --

CHAIRMAN APOSTOLAKIS: Maybe we can go back to the diagram that we saw earlier with the CMT?

MR. SANCAKTAR: Yes. The drawing.

CHAIRMAN APOSTOLAKIS: The drawing, yes.

MR. SANCAKTAR: Terry has that.

MR. MONTY: Selim, this is Bruce Monty. I think a better example of how it is modeled in the existing PRA is the SI accumulator. They are present in both plants. They are both passive systems.

Once the check valve operates on current plants, you assume injection. We have modeled the passive system similarly, including the accumulators, which is one of the passive systems.

CHAIRMAN APOSTOLAKIS: So the large LOCA sequence includes the failure of the core makeup tanks, both of them? Failure of both is needed?

MR. SANCAKTAR: No. One of two.

CHAIRMAN APOSTOLAKIS: Failure of both. The IRWST, will have one of them.

MR. SANCAKTAR: Only one is needed.

CHAIRMAN APOSTOLAKIS: How many IRWSTs do we have?

MR. SANCAKTAR: We have two tanks.

CHAIRMAN APOSTOLAKIS: Oh, we do have two?

MR. SANCAKTAR: Right. There is another tank on the other side.

CHAIRMAN APOSTOLAKIS: I thought there was one.

MR. SANCAKTAR: I'm sorry. There's another line on the other side.

CHAIRMAN APOSTOLAKIS: Yes. There is one IRWST and two CMTs.

MR. SANCAKTAR: In fact, the failure, the dominant component failure is the sump screen. There are so many valves.

CHAIRMAN APOSTOLAKIS: So let's look at the core makeup tanks. You are saying the failure is only failure of these two valves to open?

MR. SANCAKTAR: Right. This valve is open. These valves --

CHAIRMAN APOSTOLAKIS: Have to open.

MR. SANCAKTAR: Open, and then these have to open.

MR. SCHULZ: The check valves, they are normally open. Those are special biased open check valves.

MR. SANCAKTAR: There is a failure associated with them.

CHAIRMAN APOSTOLAKIS: And that's where the 10 to the minus four comes from?

MR. SANCAKTAR: Right. But IRWST failure comes from the sump screen plugging basically, the highest number. Then the rest of them come from valves opening and not opening and so on. So really sump screen -- the IRWST screen is the only one, tank screen is the only one that's single in there at this point. Then there's another one on the other side.

CHAIRMAN APOSTOLAKIS: Okay.

MEMBER CATTON: Do you have the capability to backflush that sump screen that plugs your dead in the water?

MR. SCHULZ: This is Terry Schulz. We do not have the ability to backflush that screen. There are two separate screens in different parts of the tank. We do pump through that screen during shutdown normal operations so we can detect degradations. The screens are enormous size. The tank is a stainless steel tank with reactor grade water in it. So we don't see any mechanism to clog that screen like you've seen in BWRs.

MEMBER CATTON: Well, when you are in the final stages, the water is the result of condensation in the containment. Right? It sort of follows various paths back to the sump and then into the reactor.

MR. SCHULZ: Well, there's two different flow paths back from the containment. One of them is through the gutters into the tank directly. That flow path basically stays above the operating deck so there's very little chance that it's going to pick up debris. The flow cross section into the tank is relatively small, but the gutter down spout several inches across, and it will also have some screens on it.

There are flow paths down through the sump screens as labeled there, which do come from the containment. Now those are again, very generously sized. They are also unique in AP600 in that they start like a foot off the floor and they go up about 15 feet.

MEMBER CATTON: Are you familiar with the recent problems with the BWR screens?

MR. SCHULZ: Yes. I am.

MEMBER CATTON: Similar types of requirements in the design of the sump screens, or does it matter?

MR. SCHULZ: We address those problems in some different ways in that we have inherently better chemistry in these tanks and better materials, stainless steel.

MEMBER CATTON: I am not sure that's what I am addressing.

MEMBER SHACK: But he has much bigger screens, because he hasn't had to design them for the dynamic loads that you get in the BWR. So you have huge screens compared to what a BWR would have, right?

MR. SCHULZ: Yes.

CHAIRMAN LINDBLAD: And what are you protecting, what are you screening out? What is the smallest size that can flow through or the largest size that can flow through?

MR. SCHULZ: I think it's approximately a quarter inch pipe.

CHAIRMAN LINDBLAD: What is it that you are protecting from?

MR. SCHULZ: There are no pumps to protect.

CHAIRMAN LINDBLAD: So it's fuel passages?

MR. SCHULZ: Primarily fuel passages.

MEMBER CATTON: So over time, anything that's laying around will wind up in the core?

MR. SCHULZ: No. It won't.

MEMBER CATTON: I don't know if that's that.

CHAIRMAN LINDBLAD: On these gutters that collect containment condensate, is there a settling area so that if paint strips off the containment, it settles out?

MR. SCHULZ: There are large settling areas.

The refueling water storage tank is a big tank. It has a lot of surface area in it. The paint that's on the containment is primarily a type of paint that will -- it's not an apoxy. It will not flake off. It will come off in small particles which are dense and tend to settle.

CHAIRMAN LINDBLAD: I know that that's what it says, but what's the velocity in the gutters?

MR. SCHULZ: The gutter would -- are not designed to be settling areas. So if paint does get into gutter areas, it could get presumably swept along to the like down spout into the tank. The tank has settling areas in it. It has little curves next to the screens to prevent minimize -- movement of particles to the screens.

Now there are some screens that have additional potential challenges in that they are down lower in the containment and there is apoxy paint around those areas. So there is more chance of getting bigger things that might come up to those screens. But those screens won't come into play until at least six hours after an accident. So you've had a long time for things to settle. There is large settling areas down in those.

Those screens are also very tall vertically, because of the design of AP600, the flood up level is fairly high from the loop compartment areas which will mean that again, things will tend to settle out and minimize the chance of getting to the screens.

MEMBER CATTON: Did you have a question?

MEMBER SEALE: No. I don't want to have to redesign the thing right here.

MR. SANCAKTAR: Actually, if you look at -- if you have seen the previous submittal, this is not here. SI line break is number one. This large LOCA came up due to a design change in the most recent phase. So you may not recognize this particular distribution of risk with respect to core damage frequency.

The reason why large LOCA is up here is IRWST explosive valves have to open automatically when CMT level goes down. That's why CMT is creeping in here. Otherwise, CMT is of no importance with respect to providing water alone. The important thing is that CMT is coming in, because it's level actuates the IRWST gravity injection explosive valves. That's how CMT is creeping in. We take no credit for operator actions to manually activate IRWST.

CHAIRMAN APOSTOLAKIS: Which of these sequences do take credit for operator?

MR. SANCAKTAR: Any sequence which does not develop fast takes credit for operator actions. I would say this doesn't, this would.

CHAIRMAN APOSTOLAKIS: Fast means what?

MR. SANCAKTAR: Let's say 10 minutes or so. Almost any would take credit for operator actions as long as there is sufficient time determined by success criteria that the operator can do something and it's in the procedure, and it's in the right part of the procedure so operator can get there in an amount of time. But sometimes it's a very simple thing, but he may not get there because he has to go through the procedures.

If you ignore the procedures, he can get there, but he's not allowed to get there. So we don't give him credit in that case.

That's what I was, you know, when you mentioned knowledge-based before. That's the type of thing. You may observe the thing and just actually take credit for it by pressing a button.

CHAIRMAN APOSTOLAKIS: So later on when you do the sensitivity analysis, which one of these sequences do we expect to rise?

MR. SANCAKTAR: With respect to operator actions? I can not answer that without looking at the section on sensitivity. Can we skip it while he is looking in the sensitivity analysis section. There should be a table which shows which sequence becomes number one when operator actions are turned off.

This is the DVI line break. We expect this to be here because we lost basically by definition of the initiating event, we lost one set of safety trains of injection and recirculation.

Intermediate LOCA comes in because of its initiating event frequency. It's almost 10 to the minus three. Reactor vessel and then ATWS with no main feedwater available. That's a standard ATWS definition comes in, and then it's followed by a medium LOCA, small LOCA, et cetera.

Just to show you the same thing actually on a histogram, so you can see here where transients and loss of offsite power is showing up.

CHAIRMAN APOSTOLAKIS: What is NLOCA?

MR. SANCAKTAR: That's the intermediate LOCA from two to six inches. It's the same information, different presentation.

MR. MONTY: You have an acronym list there on the next.

MR. SANCAKTAR: The next page is acronyms.

CHAIRMAN APOSTOLAKIS: Oh, okay.

MR. MONTY: That's the key to the histogram.

MR. SANCAKTAR: Here is actually the whole list of 26 of them on pages 20 and 21. We couldn't put them on one slide.

Basically transients, loss of off-site power, loss of support systems, are all at the lower end of the spectrum.

CHAIRMAN LINDBLAD: While they may not have any visibility on CDF, what is the thought as to the frequency of inadvertent safety injection compared with conventional existing plants? With these passive systems do you think you are going to have more or fewer inadvertent actuation?

MR. SANCAKTAR: I think Terry would --

MR. SCHULZ: Yes, this is Terry Schulz. There are several aspects to that, ways you can get that. One of them is the I&C failures. We were using two out of four logic with improved testing, which should reduce the chance of crossing wires and screwing up the I&C.

Another aspect is margins to setpoints, where you can bump into set points inadvertently. There, we're using basically the same kind of set points, low pressurizer pressure, a high containment pressure to actuate the systems. So from that aspect, we think we're going to be as good as good plants are today.

There's another aspect where we have a transient and you'd normally actuate SI today or you'd actuate aux feedwater, and we have our non-safety systems as a first level of defense. So that would reduce the challenge rates to the passive systems from that point of view.

CHAIRMAN LINDBLAD: And so when you integrate all that, what do you think?

MR. SCHULZ: I think that the challenge rate to the passive systems will be less. It will be less often actuated than in current plants.

MR. SANCAKTAR: I have the answer to your previous question about how the order is influenced when operator actions are assumed to have failed. All operator actions are set failures, no credit for operator actions. I'll just write down a few of them.

This is on page 50-32 of the report. I'll have to point out to you though that what I'm talking about is what's submitted as Rev. 6 previous stage. So there might be some changes, but I don't think it will be terribly different.

Steam generator tube rupture, 43.3 percent. ATWS with main feedwater, 19 percent. ATWS is 14 percent. NLOCA is seven percent. PRHR tube rupture is six percent. And so on. That should be a lot.

CHAIRMAN APOSTOLAKIS: So the major change is the steam generator tube rupture.

MR. SANCAKTAR: Tube rupture, yes.

CHAIRMAN APOSTOLAKIS: Goes from 3.6 percent to 43 percent.

MR. SANCAKTAR: Yes.

CHAIRMAN APOSTOLAKIS: So when you do an uncertainty analysis I guess, we're going to see some input to that, right? Because the human error has to --

MR. SANCAKTAR: Right. It's my opinion that steam generator tube rupture was somewhat conservatively modeled at the great objections of Terry Schulz. So if a fairer representation of it would probably change this somewhat in a positive manner.

CHAIRMAN LINDBLAD: With the larger pressurizer, will an operator be able to recognize the steam generator tube rupture easier or more difficult, thicker or slower?

MR. SANCAKTAR: You expect them to have a few more minutes or something like that. But we didn't really take any credit for it.

CHAIRMAN LINDBLAD: But also it may not be so obvious that it's a steam generator tube rupture.

MR. SCHULZ: I think that -- this is Terry Schulz. The clues that distinguish between a general leak or an RCS leak versus a tube rupture are not depressurizer behavior, but radiation levels on the secondary side, levels on the secondary side.

We do have some better radiation level instrumentation on the steam generators to help us.

CHAIRMAN LINDBLAD: Are they safety instruments? Are they safety grade?

MR. SCHULZ: I think they are.

MR. SANCAKTAR: I think they are.

MR. SCHULZ: I'm not 100 percent sure of that.

MR. SANCAKTAR: Again, in my opinion, steam generator tube rupture is actually in some sense self-correcting in the sense that if it is hard to diagnose, it means that it's smaller rupture. Then you have more time. If it's bigger, it's easier to diagnose.

So when we try to assign a delta time for operator action, we usually stay on the conservative side. But in reality, both conditions can not exist. Either if it's on the larger end of the spectrum, in which case it's easier to diagnose, but less time. Or it's on the lower end of the spectrum, in which case you have much more time. But we assume the worst at each end and end up with a rather I think conservative estimate of at least operator response to it.

MR. MONTY: Selim, this is Bruce Monty. One comment to make. Because of the automatic systems that we have in response to tube rupture, there isn't as much dependence on the operator as in current plants where the operator must diagnose which generator and take actions to isolate it and cool down and depressurize.

In this plant, the operator doesn't do anything. There's still two levels of response. One of the passive RHR, which basically takes the heat now and allows you to get off the generators. Then the backup to that is the ADS actuation.

MR. SANCAKTAR: Just to give a sense of these numbers with respect to some other results, the current four loop Westinghouse PWR, 1.2 to the minus five for an IPE. Evolutionary PWR 1.7 to the minus six. This is where AP600 adds up to. So we see an order of magnitude here, and two orders of magnitude there.

Loss of off-site power and transients are basically beaten to death here. A lot of improvement in steam generator tube rupture. This ATWS, some improvement, but not orders of magnitude. LOCAs, again, order of magnitude here, and close to an order of magnitude there.

CHAIRMAN LINDBLAD: Okay, I'll acknowledge the calculations show that. Of course the current four loop PWR is based on operating experience. The AP600 is based on conceptual designs.

MR. SANCAKTAR: Absolutely. In that sense.

CHAIRMAN LINDBLAD: There's a credibility that goes along with these as well, but granted --

MR. SANCAKTAR: I won't dispute your

statement. This is just what numbers looked like as calculated.

MR. BUETER: Selim, would it be fair to say -- this is Tim Bueter. Would it be fair to say though that these numbers were calculated with data that is based on many of the current plants. Many of these numbers that were used for initiating events, et cetera, come from "generic" data. Granted there are some calculated based on AP600, but --

MR. MONTY: Yes. This is Bruce Monty. The point here I think is the valves and the I&C and some of the systems are what are used in some plants, the same type of equipment is used on plants today which we then have used that data. So it's not totally conceptual. There is a lot of actual operating history that goes into the data.

What we did was looked at the data and said is it applicable to this plant. In many cases it is. In some cases it's not. In those cases, we had to generate new data for new systems.

CHAIRMAN LINDBLAD: Well I suspect though that when we were doing the conceptual design of a four loop Westinghouse PWR, we really didn't look at reactor coolant pump seal as being a problem. It was only with operating experience that we found out about it.

Now with your AP600, you say well, we've designed that out. But we don't know what we have designed in. So --

MR. SANCAKTAR: This number for things that were looked at and covered is representative of that number. The point I think you are saying is what else has come out. We try to pick it up as much as possible, but we will never guarantee -- I don't think any PRA analyst will say that I covered everything.

Tomorrow a new event will happen and we will all look and say oops, we didn't really think about it in any sense. Then we will add it to the list and continue.

MEMBER KRESS: That's one reason you have defense in depth.

MR. SANCAKTAR: Yes, yes. So that's part of the game. I don't think any PRA analyst should go and say "This is it, I calculated it, I'm finished, this is the bottom line."

But we dug up as much as possible to try to dig up. NRC really asked us questions to go and search even more. In the future, I'm sure there will be other aspects to be covered, but as of today, it's our belief that this is what we can represent with today's information and knowledge.

CHAIRMAN LINDBLAD: Now the IPEs for the

current four loop Westinghouse PWRs have substantial variance in those numbers. We think that the AP600, when we have 100 of them installed will have similar variants?

MR. SANCAKTAR: It's hard to say because first of all I don't know what substantial in your mind means. Is a factor of two substantial, or are we talking about 10?

CHAIRMAN LINDBLAD: Ten.

MR. SANCAKTAR: Ten, okay. Thank you. At least we are in the same ballpark.

This is like a Snupps type of plant. We try to choose something that this system exists, you know, what was the most recent one built. There are so many different design variations on plants and then how they are put together.

This plant is on one, a singleton on a site. If there were one more on the same site, this would have really really gone down. This is like loss of service water and component cooling water type of things creeping up and causing trouble.

MR. MONTY: Selim --

MR. SANCAKTAR: So there are so many variations and it's hard to generalize because of the existing plants being of different generations. whether the site has one or two units, whether support systems were designed one way or the other --

MR. SCHULZ: Selim, there are two factors I think in some of the variations. Some of the variation is who is doing the PRA.

We chose this particular plant, Westinghouse, because we had some of the same people perform the PRA using the same methods. We're not looking at a PRA performed by another organization versus us.

The second thing is some of the variation is created by the plant-specific variation in the support systems, service water, component cooling water, AC power and so forth. In the AP600, we have reduced the dependence on that so we'd expect a spread due to that to be small. So that we would expect that that number would be a smaller band over -- if you built 100 AP600s which we hope to do at some point in the future, but we'd expect the band to be smaller. Plus, it's a standardized plant, and we're not going to vary the systems as much.

CHAIRMAN LINDBLAD: But it's interesting that the scope of the PRA with operating experience, all others represents 30 percent of the total contribution. Whereas you are saying for the plant that we just have conceptual design on, all others represents less than one one-thousandth of the total contribution.

So it kind of suggests to me that that 8 x 10 is going to grow with time.

MR. SANCAKTAR: Maybe, but what Bruce said is very important. That this all others is an unfortunate categorization. There are things in there. Ninety percent of all others is what Bruce mentioned, and I mentioned too, loss of service water, component cooling water going to RCP seal LOCA. It's a single unit. So if you don't' have a sister unit to help it.

So actually, it's an unfortunate group. If you broke this into support systems or something like that, and all others, maybe that would have been a little bit more informative.

CHAIRMAN LINDBLAD: But one of our previous members of the committee focused on interdependencies of systems and educated all of us how a plant arrangement and unique site facility design had a lot to do with introducing other problems.

MR. SANCAKTAR: Basically this shows us that we try to respond to what exists now, what kind of concerns have been identified. The design, it had a model, the design has addressed them so that the model reflected them. We tried to find out other challenges to the plant, but all we could identify we put them in.

If there is more, eventually -- if there is more we will find them. Not they are very unlikely, and again, it might come up one day and we'll address them.

CHAIRMAN APOSTOLAKIS: Didn't Idaho National Laboratory have a contract to review of PRA?

MR. SANCAKTAR: For the NRC?

CHAIRMAN APOSTOLAKIS: Did they come up with any different issues, sources of contribute to core damage significant?

MR. SALTOS: Well, we've had -- okay. I'm Nick Saltos, with Safety Assessment branch. We have some differences in the initiating event frequencies, which would have been worked out with Westinghouse.

And we -- several numbers have been adjusted since then. We still have some open items, especially regarding the steam generator tube rupture event trees, the passive RHR tube rupture event tree. But, basically, we don't have any completely new categories of accident frequency.

CHAIRMAN APOSTOLAKIS: Okay. I guess your next major contributor, unexpected failure, probably would come from the combination of I and C failures, and some operator action, or something we have not seen yet.

MR. SANCAKTAR: Possibly.

CHAIRMAN LINDBLAD: Now, how do you handle reliance on, let's say, valves that are normally held open by air, and the air being supplied by a non-safety system, and worrying whether oil carryover from the air compressor might freeze the spool valve, or the pilot, or whatever is going to lock the valve into position?

MR. SANCAKTAR: So, it won't open?

CHAIRMAN LINDBLAD: Yes.

MR. SCHULZ: Selim, let me. This is Terry Schulz. We do several things. One, we design the air system to prevent that. We also try to design the valves so that they are not susceptible to materials used, and are not susceptible to that problem.

And we also test the valves. So, every three months, we stroke the valve open and closed, and time it, and make sure we don't see any degradation.

CHAIRMAN LINDBLAD: And so what does the PRE practitioner use then, for the reliability for that fail to open, fail on loss of air? Fail open, loss of air?

MR. SANCAKTAR: We use the number that was suggested by the URD document, which basically came from current operating data, sifted through current operating data. So there is no special treatment.

MR. SCHULZ: And what about -- is the reliability that you build your rate between the failure rate that we use?

MR. SANCAKTAR: Failure to --

MR. SCHULZ: Failure to operate.

MR. SANCAKTAR: -- open.

MR. SCHULZ: To go to the fail position. I don't think it's that extraordinarily high, I guess is the reason I was asking the question.

CHAIRMAN LINDBLAD: Okay. Why don't you go on, and tell me later.

MR. SCHULZ: Okay.

CHAIRMAN LINDBLAD: Thank you.

CHAIRMAN APOSTOLAKIS: You have about 12 minutes.

MR. SANCAKTAR: Okay. In 12 minutes --

CHAIRMAN APOSTOLAKIS: What are the major points you want to make? Because I looked at your viewgraphs, and it seems to me some of them have been gone through already.

MR. SANCAKTAR: Yes. This slide is definitely a repeat.

CHAIRMAN APOSTOLAKIS: Okay. So let's go to what you think --

MR. SANCAKTAR: Yes.

CHAIRMAN APOSTOLAKIS: -- is important.

MR. SANCAKTAR: Okay. But let me capture the meaning of the slide that I skipped. The slide is going to give you an idea that the number we obtained is a reflection of the plant result on purpose, things that the designers do, to address the current issues. It's not a number that has somehow randomly appeared out of nowhere. Anyway.

This is a -- these are system importances. Namely, take one system and set it for failure, and see what the core damage frequency would be, to see its importance. But --

CHAIRMAN APOSTOLAKIS: So this is not -- you're not using any of the standard importance measures?

MR. SANCAKTAR: This is -- this increased.

CHAIRMAN APOSTOLAKIS: Well, I mean, to zero.

MR. SANCAKTAR: Well, here --

CHAIRMAN APOSTOLAKIS: You're not using Fussel-Vesselly, or --

MR. SANCAKTAR: This is risk increase. This is.

CHAIRMAN APOSTOLAKIS: Risk achievement worth, and whatever?

MR. SANCAKTAR: Right. Risk achievement worth, or risk increase for this system. Not the basic again, but for the whole system.

CHAIRMAN APOSTOLAKIS: Yes.

MR. SANCAKTAR: But. And for purposes of CMT, you rip it out, or set it to failure. The core damage frequency goes to N times ten minus four, whatever the significant figure is.

And we will -- the number is, it may not be standard. We just assign some adjectives to discuss it. So, this showed that safety systems are, of course, important.

And here, we see some medium importance, like DAS, and we see here that basically, support systems are alone. Failure of each one does not really affect the core melt that much.

If you want to ask a question, why are these here? I mean, I will explain it, if somebody will ask this.

CHAIRMAN APOSTOLAKIS: No, we don't.

(Laughter.)

MR. SANCAKTAR: Okay. Failure to operate to de-energized position, for air-operated valve, is ten to minus six per hour, from the URD. So, if you assume a thousand hour surveillance interval, it will be ten to minus four, fourish number. You asked the question.

CHAIRMAN LINDBLAD: Yes. Thank you.

MR. SANCAKTAR: Here are a few system analyses. Not all of them, just a few. The first one was set all the operator actions to one. And you -- before you go to set this here, as someone was saying, you will touch base again, so you may want to probe it now.

But the core melt goes from one point minus seven to about two factors, or maybe higher. And, from this, what we can conclude is that you don't need operator actions to maintain the core damage frequency of at the order of ten to the minus five.

And then, if you do if for internal, it still -- the core damage frequency for internal initiating events is ten to the minus five. And, of course, we also see the other side of the coin. Namely, if you want to maintain a low -- very, very low core damage frequency, operator actions help.

The explosive valves. They are not open with the basic event or failure probabilities are ten times larger than what we have here.

And the core damage frequency goes to 6.3 to the ten minus seven, which is like a factor of almost four. So, there is some sensitivity to explosive valves, which are used in ADS, and also in IRWST.

Check valves. What if the safety-related check valve were an automatically, or likely to fail across the board? Then core melt increases to almost three to four. With the four, yes, there is some sensitivity to that function.

And this is the focussed PRA result for regulatory treatment of non-safety systems. So, if we assume that only safety systems are used to respond to an initiating event, the core damage frequency goes to 6.2 times ten to the minus six. So this is a pretty favorable -- I think it's a pretty favorable result.

MEMBER KRESS: From that, you would conclude that none of your non-safety systems are?

MR. SANCAKTAR: Together. Right. Right. Even if you -- the previous slide points that out, because, it was, you know, one a time, you know, in here.

MEMBER KRESS: Yes.

MR. SANCAKTAR: But now, this shows you the effect of basically ripping out all these.

CHAIRMAN LINDBLAD: Do any of these issues change at 72 hours?

MR. SANCAKTAR: Our qualitative arguments point out that it doesn't.

CHAIRMAN LINDBLAD: That sounds like there's another answer.

MR. SANCAKTAR: What?

CHAIRMAN LINDBLAD: That sounds to me like there's another answer.

MR. SANCAKTAR: No. We don't have quantitative models for it.

CHAIRMAN LINDBLAD: I see.

MR. SANCAKTAR: But our current assessment is that our results are good, throughout the period of interest, from 24 to 72 hours. But there is no quantitative model for it. No quantitative.

MEMBER POWERS: On your previous slide, where you destroyed human actions.

MR. SANCAKTAR: Yes.

MEMBER POWERS: And took no credit for human actions. That result is extraordinarily interesting. And I wonder, does it imply that your system is particularly vulnerable to internal sabotage events?

MR. SANCAKTAR: Not -- I don't see the relation really, because not respond, afraid of not responding on that point. I don't see the connection.

MEMBER POWERS: Well, if the operator's acting, you get 1.7 times ten to the minus seventh. If the operator's not acting, you get 1.7 times ten to the minus fifth. Now, operators acting in a deleterious fashion -- I mean, if I just draw the straight line, I'm getting big numbers, I think.

MR. SANCAKTAR: I think you would get big numbers with any plant. I don't think that this plant -- this plant is especially different from any other plant.

If somebody wants to do something on purpose, I don't see that there is a place here that is going to be any different, or much worse than a current plant, or any other existing installation.

MEMBER POWERS: In other words, the -- that possibility --

CHAIRMAN LINDBLAD: Excuse me, Dana, but let me follow up on that. It seems to me that the location of systems that are essential to safety are within the containment, as compared to the current plants, where things outside the containment can give you lots of trouble with internal sabotage. Is that not true?

MR. SANCAKTAR: That's true. If you are dealing with --

CHAIRMAN LINDBLAD: If we can control containment access.

MR. SANCAKTAR: If the question is equipment damage, then that is an absolutely correct statement. It's actually an improvement in this plant.

But, if your answer is within the control, you know, somebody does something on purpose, in the control room, I don't see any -- I don't have any good answer to tell you.

You know, it's better, worse. I can't think of any. I mean, what can you do? I don't see how it follows from this. I don't see the power. Maybe there is, but I don't see it.

MR. BUETER: This is Tim Bueter again. If you're in the control room, you'd have to have access to the controls, on the computer, so that would reduce it down to people with access to that.

So, in that respect, you're saying "well, this is the person that's already been cleared for operations." And he has, you know -- he decides "today's Thursday. I'm going to do something."

CHAIRMAN LINDBLAD: I understood him to qualify that to be insiders.

MEMBER POWERS: That's usually what internal sabotage means. I guess what I'm asking -- I just drew the straight line. I'm asking if there a reason not to draw the straight line? Has internal sabotage been a consideration in the design of this plant?

MR. SCHULZ: This is Terry Schulz. Sabotage has been a consideration, in some respects. It's something that we've thought about.

But it hasn't directly affected the design, because we think that the -- having the multiple levels of defense, things located different places, a lot of the protection coming from inside containment, being fail-safe, gives us, inherently, a lot of sabotage protection.

With the insider manipulating things. He has to defeat a lot of things, to cause a problem. Safety things, non-safety things, different instrumentation systems, to really completely void the protection of the plant.

So, we think that it's going to be more difficult to cause problems with this plant, from a sabotage point of view, than current plants.

And we think that that core damage frequency, without operator action, is really an indication of the multiple levels of defense. It's not all coming from one system.

It's not all coming from things located in one place. So, it is, we think, difficult to block all the different safety features in this plant. So that, inherently, that gives you better protection.

Yes, given enough time and effort, and people, you know, you probably could show that you could defeat everything. But we think it's more difficult.

MR. MCINTYRE: This is Brian McIntyre. In answer to your question, yes, we're looking at that, as part of the security analysis, and vulnerability studies, and all that stuff that we do for Chapter 13.6.

We are looking at the effect of insider sabotage, and the way the plant is designed. That's not part of, obviously, this presentation. That's another discussion.

MEMBER POWERS: Is it a quantitative

examination, or is it more like Mr. Schulz said, this feeling? In a sense.

MR. MCINTYRE: It's more qualitative. It looks at the types of things that you would have to do to disable the plant. Where things are located.

And, as Mr. Lindblad said, basically -- things we have done to do -- to improve the design, are move more things inside the containment. Much more restrictive access to components.

MEMBER POWERS: Do you have quantitative aspirations, for the output of that?

MR. MCINTYRE: Do I have a quantitative aspirations? No. I don't believe that's something that we would -- I don't believe anybody has ever really done that, to the best of my knowledge.

MR. SCHULZ: Your point is well taken. You know, there's certainly, we've made considerations for sabotage, and we certainly could limit the people that have -- that are susceptible to such things, through the design of the plant.

But I think one of the things we're trying to show here is the plant does pretty well without operator actions. That's true. But you've still got a couple of orders of magnitude of difference. So, the operators are important, and that's pretty common with current plants.

Now, you know, I think I would think that, if one person of this select group should decide to do something, as Terry pointed out, you'd have to defeat many diffe- nt things, and it's hard for me to conceive of a conspiracy between this select group, so the other people would be there, too.

MEMBER POWERS: I guess I'm familiar with a number of incidents where a group, not maliciously, succeeded in defeating an enormous number of systems.

(Laughter.)

MR. SCHULZ: Certainly, it's possible. I agree with you.

MEMBER POWERS: Walked themselves right into it.

MR. MCINTYRE: Yes. It certainly is possible.

MEMBER POWERS: I mean, it seems to happen about once a year, that we get multiple systems defeated.

CHAIRMAN LINDBLAD: But also, I think one of the things that Dana and I were pursuing was that there are NRC staff people who say that plant security is not susceptible to PRA analysis, and we were trying to see what your views were. Or, I was trying to see what your views were.

MEMBER POWERS: Yes. And I think we concluded that they don't think it's susceptible to PRA analysis either.

CHAIRMAN LINDBLAD: Yes. But I don't know that -- well, we'll find out.

MEMBER CATTON: Hal would not agree with you.

CHAIRMAN LINDBLAD: Yes.

MEMBER POWERS: I wouldn't agree with him.

CHAIRMAN LINDBLAD: Wouldn't agree with Hal.

CHAIRMAN APOSTOLAKIS: Moving right along.

CHAIRMAN LINDBLAD: Okay.

CHAIRMAN APOSTOLAKIS: I understand that you would like to talk about the insights after lunch.

MR. SANCAKTAR: Yes. Okay.

CHAIRMAN APOSTOLAKIS: So this is a good time to break. Okay. We'll see you in one hour.

MR. SANCAKTAR: Okay.

(Whereupon, the foregoing matter went off the record at 12:03 p.m., and went back on the record at 1:04 p.m.)

A-F-T-E-R-N-O-O-N S-E-S-S-I-O-N

(1:04 p.m.)

CHAIRMAN APOSTOLAKIS: We have to start exactly at one? Okay. I have to use this? So, we're talking about insights, right?

MR. BUETER: Right.

CHAIRMAN APOSTOLAKIS: Okay.

MR. BUETER: I'm Tim Bueter. I'm the last member of this triad, I guess you could say. But, as you mentioned, we're going to talk about insights. So, we're going to go back to our outline, and we'll start out with the level one insights, and then we'll do it again for shutdown.

Sorry. The switch is on. So, we did this PRA analysis, this level one analysis, then we got a result. I think the important thing to ask is what insights are there to be gained from this? What things are important in this plant?

Why is the number so low? There's another question. There are several reasons for that. Probably one of the more important ones is the redundancy and diversity in our passive safety systems. That makes the safety systems reliable.

We have -- compared to current plants, we have several things that we feel are more reliable, because they are passive. We have passive CMTs, instead of high pressure safety injection pumps.

We have IRWST injection, instead of a low pressure set of pumps. So, again, we have passive components, instead of an active pump system.

For high pressure events, we have a depressurization system, along with the injection system so we don't have to worry about how do you get the pressure down low enough to get your low pressure injection system. You have this tremendous volume of water. We can put it back into the DRCS.

We also have the passive containment, for a longer term recirculation. It essentially provides an alternate heat sink. So that gives you a long term cooling without, again, active pumps.

The operator, while still important, is certainly not as important as in current plants. Our systems operate monthly, automatically.

There are no single operator actions that can lead to a core damage. The automatic systems are expected to operate as the first line of defense, with the operators backing up the automatic system.

The -- my references to active pumps. Generally, what I'm getting at is the passive systems don't rely on support systems. Like AC power or cooling water. Whereas, the pump, you've got to keep it cool, and you've got to power going to it.

Yes, we need DC power, to address somebody's comment earlier. But, again, we covered that in the analyses, and we do have redundancy and diversity in our DC power supply.

Our I and C systems are obviously important because of all the automatic actuation. We're saying we have automatic actuations, so we make our protection system redundant.

We have diversity within the sensors, and then we provide a diverse actuation system on top of that, to give not only diverse reactor trip, but actuation of the safety systems.

IS LOCA. As Selim pointed out, IS LOCA is a concern. In our plants, we tried to at least reduce the concern, if not entirely eliminate it, by designing our normal RHR system with multiple valves in the interface connections, in the connections, and make the system able to withstand design pressure.

So, you don't guarantee a pipe rupture, just because you do break these multiple barriers. Our seal LOCA is eliminated by canned motor pumps. As Mr. Schulz pointed out, a big pressure vessel, so you don't have the seal to worry about.

And last but not least is these safety systems that are more simple than an active pumping system. They don't require a lot of maintenance.

And, on top of that, when we do do the maintenance, it's periods when they're not required. We plan the maintenance for these systems when they're not required to perform their function. Yes?

CHAIRMAN LINDBLAD: When you say safety -- simple safety systems, are you speaking of bricks and mortar, or are you talking about I and C as well?

MR. BUETER: No, I'm referring -- this is referring to the big tank of water with a single valve, or two valves, or something like that. You're right. The I and C --

CHAIRMAN LINDBLAD: You're talking about bricks and mortar is more detailed than the?

MR. BUETER: Yes. The I and C. The I and C, I think, you could probably characterize as more detailed, given current technology, but. Now, as far as --

CHAIRMAN LINDBLAD: Would the maintenance be done when the systems are not required?

MR. BUETER: The I and C is designed to have a lot of its own -- I don't want to say maintenance. But it does a lot of its own checking.

And the maintenance is planned into it, in that we have a lot of redundancy into it. So, Terry has a lot to say on this subject. I could certainly defer to you on that.

MR. SCHULZ: The tech specs do allow one of the divisions to be taken out of service for testing or maintenance at-power, so it's more of a designed-in capability to test and maintain that, at-power.

MR. BUETER: So you still have multiple channels of -- multiple, redundant channels, even if you do maintenance on it. And the system allows you to plan for that.

CHAIRMAN LINDBLAD: But I, I don't know. Probably the insight comes from the safety systems where you spend a lot of time analyzing them, probably have been improved.

But the I and C is still kind of a desert for studying its reliability, and you're not sure where you stand with that, I would think.

MR. BUETER: Certainly, I and C includes software, and software reliability has been a source of debate in the software industry, for quite a period of time. It's becoming more of a substantive debate in the nuclear industry.

Digital technology is relatively new, so that can be debated as well. We have modelled in things like software common cause, common cause failure in cards, etcetera, and we account for some of that in our diversity, through the DAS.

And, in some conversations we've had about diversity, yes, we're talking about, like, having several groups of people do the software development, with different compilers, you know, things like that. But you're right. That's a good point.

This is bringing up the defense-in-depth phrase again. But nonetheless, we'll call it multiple levels of core protection, alluding to some of the things that have been said before.

Our passive features are backed up, in many cases, by additional passive features. And then, we take the passive features, and back them up by active features. So you get multiple levels, and the redundancy and the diversity in your mitigation of transients.

As I mentioned before, containment cooling is an alternate heat sink. We don't have to worry about active pump systems there, long term, which certainly can be a problem. Air circulates just due to physics.

We've eliminated a lot of operator actions. The plant experience, over the past decades, has shown that some operators actions are very important, and reduce the possibility of error, if you provide automatic functions, or eliminate them entirely.

Automatic feed and bleed. We've made it simpler. And we hav· automatic actuation of the valves. Switch over to recirc is the same type of thing.

Our tube rupture. Again, we have two automatic paths for mitigation, followed by the operators can come in and back that up. And then, for ATWS type situations, we have a different -- a diverse reactor trip function. So, all those things come together.

CHAIRMAN LINDBLAD: Can I ask --

MR. BUETER: Certainly.

CHAIRMAN LINDBLAD: -- a question. It would seem to me that, with this heading, I would have seen issues about low power density, and large volume pressurizer reducing transients, and the effect of transients.

MR. BUETER: Certainly true.

CHAIRMAN LINDBLAD: And I don't. And is there some reason why it is not an insight to this, it hasn't given you much?

MR. BUETER: No. Just, a lot of this is a matter of brevity, and a lot of it is, in the PRA, we didn't take credit for the fact that the larger pressurizer. We didn't take credit for the fact that you have a lower power density, necessarily. Now --

CHAIRMAN LINDBLAD: Well, yes you do, don't you? In terms of a transient?

MR. BUETER: In your transient analysis, we do indirectly. But is there something in the PRA model that says we have larger pressurizers, so this is less likely to fail? No.

But, in the running of the simulations for whatever transient -- you know, ATWS, for instance, yes, there's a counter-flow, because the computer model has that bigger pressurizer, if you will, in there.

And you're right. Those are certainly important features, and we had this discussion. What's an insight, what's a feature, etcetera, etcetera. And, you know, these are just -- we're trying to hit some of the highlights. There are certainly others. You can go into the larger pressurizer.

CHAIRMAN LINDBLAD: I also think your close coupling of your loops cuts down the exposure to LOCA, and the elevation to the steam generator helped. But that -- you don't think those are significant, compared with these?

MR. BUETER: Yes, sir. They're certainly significant. Again, we were just trying to hit some of the --

CHAIRMAN LINDBLAD: All right.

MR. BUETER: -- hit some of the highlights. We can go on for quite a bit of time on those. But you're, you're certainly right there. We probably should mention those.

I was going to stop at-power. Anybody want to go back to that?

(No response.)

We'll make references to it, because the shutdown is done in a similar manner, but we're going to stop on that one.

CHAIRMAN LINDBLAD: When are we going to deal with fire?

MR. BUETER: Fire is in a subsequent meeting, because that analysis is still being performed, and we're not prepared to discuss it.

CHAIRMAN LINDBLAD: Thank you. That's fine.

MR. BUETER: Okay. Shutdown. Again, this is level one shutdown. For AP600, we -- I'll call it a different tact. And obviously, it was required, but not too many shutdown analyses have been done in the past. And the URD actually says a qualitative assessment in shutdown is acceptable.

We did a full scope PRA. We went the full range of conditions, from Mode Two all the way down to Mode Six. We looked at each of them, and evaluated them in some fashion.

We did a level one and a level two PRA for shutdown. We're in the process of revising it. So, we basically have level one results available.

We did look at all the various conditions from, again, Mode Two down to Mode Six. We looked at -- for instance, we looked, in Mode Two, to hot shutdown. And, in that case, we said "well, there's a lot of the same initiating events."

And, in fact, we just assumed they're all there. Obviously, some of them are a little ridiculous. You don't have an ATWS, if your rods are in. But we said "okay, if you assume that they're all available."

And we have basically the same number of systems to mitigate it, and you're only in there for about 22 hours, the risk was obviously very low. And we felt it was bounded by the power analysis. So, we didn't build models and quantify it per se.

Then shutdown from hot shutdown to cold shutdown, with the RCS intact. We said, "well there's a lot of specific things going on here. You're in a lot of specific maintenance operations, you spend a significant amount of time there."

We built models for it, and did specific quantifications for that. We call it -- I don't want to call it a mode, because. A stage of shutdown, let's say. And we'll call this -- in later discussions, we'll call this non-drain conditions.

A lower mode of cooler operations, if you will. You go into the mid-loop, Modes Five and Six. And we lumped in several operations. Draining and filling of the RCS, the refueling cavity, and mid-loop, where they do a lot of maintenance and other activities.

That's certainly an important condition, as, I think, history has shown. So, we did the valve models, and did a specific quantification. And they'll be calling that drain conditions later on.

Another stage of shutdown is where you have the cavity filled up with basically half a million gallons of water. And the head may be off, or at least loosened up. And we looked at that, and said "well, you know, you can lose your normal RHR, you can lose your spent fuel cooling."

So, you have to have two barriers. And, if those do happen, you have to have a long time before you even get to core uncovery. We're talking days. Certainly, there's a very low risk.

We went through, and evaluated that risk, and said "this is not worth the effort to build very large models and quantify specifically." So, we did not quantify that.

Again, going back to the evaluation of all the various stages of shutdown. As I said, we looked at a lot of the same initiating events. We said, "well, is this bounded by the at-power events?" And, in Mode Two, or Mode Four, we said "yes, it is."

Are the conditions -- the temperature and pressure of the RCS, significantly reduced by the use it? Is it not a credible event, because there's no pressure there?

An example of that might be a large pipe break. You're not going to have a large pipe break, if it's not pressurized. Then, we screened out some initiating events, for the models we did build.

And this is an example of them. Then, we said "well, there's initiating events that are particular to shutdown, certainly, and particular to this plant." So, we looked at them.

Boron dilution. Can the rod be pulled out again? Is there anything unique to the passive systems? In a spurious ADS, that's important. Rupture of the -- excuse me, I mean, of the IRWST tank. Things like that, that would be credible. And we looked at all those things.

So we ended up with several initiating events we modelled. Loss of normal decay heat removal, as you would expect. This is normal RHR, component cooling water and service water. Loss of off-site power. And then loss of the coolant, a leak of some kind.

Using the same methcds that we had at-power, we developed fault trees for these various modes, and event trees. We modelled equipment failures, common cause, and human errors, and the same methods, sometimes using a lot of the same data.

We looked at the refueling schedule to say, "okay, what are the activities that need to be performed, and how long do they take?"

We wanted to make sure to account for all of the potential activities that we could think of, all the possibilities. You know, how long do they take? What would the operators be doing?

So we went through and looked at all the various operations that we would expect to be performed, and then we quantified them, again, using the fault tree, event tree methods that we used in the at-power analyses.

We finally get to some numbers. We come up with these initiating events. They're divided into draining conditions and non-draining conditions. So, you could have a loss of off-site power, you know, with the mid-loop or at -- with the RCS intact, etcetera.

CHAIRMAN LINDBLAD: What are the units of frequency per year? Which year is this? The calendar year, or the year you're in the drain condition?

MR. BUETER: It's normalized per year, I believe.

CHAIRMAN LINDBLAD: Per calendar year?

MR. BUETER: Per calendar year. Yes. It's normalized to a calendar year, but we're in shutdown for 340 total days, is the time used.

MR. SCHULZ: Hours.

MR. BUETER: Excuse me. Hours. Good point. In this case, we got not applicable, because we're calling the over-draining, you know, while you're draining. We just called it -- we just defined that to be drain conditions.

In this case, we're saying that, if you're in mid-loop, you're not going to get a pipe rupture of the RNS. It's not pressurized.

I mean, we can talk about the numbers. I don't know if you want to get into that or not. There's a better number. I have another slide that gives you a little more on this.

But, basically, our results are almost an order of magnitude -- well, maybe half an order of magnitude, I guess less than that, power. And, again, this is per calendar year, so we're comparing apples and apples.

And, as you would expect, with current-day plants, and in this plant, 90 percent of that is due to drain down conditions in mid-loop. Why is that? Well, it's because, at mid-loop, you don't have as much to back you up. You have less inventory.

You can look at it another way. How do the various commissioning events contribute? We've got a little acronym list I can put up, to solve that problem. Loss of decay heat removal, at drained down conditions, as you would expect, becomes the dominant one.

This is loss of support to the RNS. It includes component cooling and service water, so it's kind of a lumped category. So, and it almost distorts it. But, and you've got lots of RNS down here.

Loss of off-site power becomes important, just because it makes you lose RNS, if nothing else. Now, we do have the diesel generators to back it up, so that helps.

But, again, you're taking out decay heat removal, so that makes it less functional, since it makes it important. The non-drained conditions have lesser importance, if you will, contribute a lesser fraction.

CHAIRMAN LINDBLAD: In doing your loss of component cooling systems, or cooling systems, in the drained condition, how many hours after full power was the event postulated? Or days?

MR. BUETER: Don't know exactly. Isaac? Terry? Okay. How many hours did we get, after we got in -- after we shut down, did we take to get the thing up?

MR. SCHULZ: If you're in non-drained condition, of course, you get into that essentially right away. For the drained condition, I think it's about 28 hours or something is the earliest.

MR. BUETER: Wow.

MR. SCHULZ: That you can get into a drain condition.

CHAIRMAN LINDBLAD: From at-power, or just from?

MR. SCHULZ: From at-power.

CHAIRMAN LINDBLAD: Okay.

MR. BUETER: The earliest?

MR. SCHULZ: The earliest. And then, of course, there's another -- on the start-up end of it, there's one that, a drain condition that occurs much later.

CHAIRMAN LINDBLAD: Is that one of the objectives, from the URD as well, to have a system that one can open up quickly? In the overall design?

MR. BUETER: I don't believe so.

MR. SCHULZ: Well, they have a -- not specifically. But they do have a breaker to breaker refueling time of about 17 days. That's if they want the plant to be in check.

CHAIRMAN LINDBLAD: Yes.

MR. SCHULZ: They don't break it down into individual activities.

CHAIRMAN LINDBLAD: Right.

MEMBER SEALE: Do they include things like goals, on how rapidly one can do the steam generator tube inspection, something like that?

MR. SCHULZ: Is that a question?

MEMBER SEALE: Yes.

MR. SCHULZ: Not specifically. But they have looked at a refueling outage plan --

MEMBER SEALE: Yes.

MR. SCHULZ: -- in detail, and questioned the times that we've assumed for all the different activities, like steam generator inspection, to make sure that they were not overly optimistic, and we had adequate windows of time to do those things, and still be consistent with the overall.

MEMBER SEALE: I meant in the URD, is there any comment about that?

MR. SCHULZ: Not that I'm aware of.

MEMBER SEALE: Okay.

MR. BUETER: I can put the picture up again, if you like. But this just basically says it in numbers.

And, again, if you look at the drain conditions, most of the -- this is another drain condition, but most of the, 97 percent of the risk is due to drain conditions. But, even at that, it's relatively low. Loss of decay heat removal is your major factor.

Now, we do have a passive system, at mid-loop, namely the IRWST injection that backs up the RNS. So that's one of the reasons we can keep the CDF so low, even at drain conditions.

MEMBER POWERS: You say that the risk is quite low, yet, between operation and shutdown conditions, if we look at it on a per hour basis, there's roughly a factor of seven increase in the riskiness of shutdown operations. And I wondered why that would be tolerable to a design engineer.

MR. BUETER: We were just talking about this last night.

MR. SCHULZ: There's always a question of how low is low enough. From a design perspective, what I guess I think I was looking at was what the overall risk on a yearly basis was. And --

MEMBER POWERS: But you're designing a system that people are operating. And why would you set, find tolerable a design objective in which this -- this is a paper, this is plant on paper. As a design objective, that necessarily becomes riskier.

I mean, just on the outset. I mean, you might have to accept that, once you start operating, but I think, as a design engineer, you'd say "gee, I don't want my risk per hour of human activity to go up."

MR. SCHULZ: Well, that's not the way we looked at it. The way we looked at it was the absolute numbers being extremely low, a ten to the minus eight kind of number.

And some people would question that as being we don't really know it that well, to start with. How can we expect it to be that way?

MEMBER POWERS: Well --

MR. SCHULZ: We have done things that improve the situation versus today's plant. But you're looking at it on a ratio to the at-power risk.

The other way of looking at it is the kind of numbers that Tim has up there now, which is how does this compare with current plants? And the absolute numbers are orders of magnitude better than current plants.

So that was more our perspective. That we did do real things, to provide more levels of defense than current plants have. We did significantly reduce the absolute risk, and we felt that that was appropriate.

MEMBER POWERS: That's fair.

CHAIRMAN LINDBLAD: But it also -- pursuing that, suggests that the motivation for this AP600 passive design was a number of years ago, when the perception was that the risks existed at-power, and that shutdown risk was rather, very modest, in normal operating plants.

But since -- and you kind of wonder. If you started with a clean sheet of paper again, recognizing some of the shutdown risks that are apparent in existing plants, would there have been other features that the URD perhaps would have looked for, or that you would have actually turned to, to minimize the shutdown risk?

MR. BUETER: Would there be other features?

MR. SCHULZ: I think that we have only quantified AP600 shutdown risks since 1991, '92 time frame. But that is a few years ago.

CHAIRMAN LINDBLAD: Yes.

MR. SCHULZ: And we had been worrying somewhat, from a design perspective, even before then. And it is very speculative. Could we have come up with other designs? Sure. Could we now come up with other designs? Sure.

But I think we also feel very comfortable with where we are. We think that we do have a much-improved design, that not only improves the normal operations of the plant, in terms of how the shutdown systems, the normal systems work, and how they dealt with figurative problems that have existed.

Better mid-loop level instrumentation, better drain controls, automatic isolation of drains. There have been a lot of things. Some of which came out of the PRAs, some of which we just thought up on our own, as we designed the systems, as well as the passive feature that provides the back-up.

How far is far enough is a very philosophical question. In our -- I guess, fairly comfortable, and fairly proud of where we've gotten to in this design, and the shutdown in this area.

CHAIRMAN LINDBLAD: Let me ask you this question. And it follows up on Dana's question to you. If this AP600 is sited in the Gulf of Mexico, and a hurricane is expected in the next six hours, will you run the plant, or shut it down?

MR. SCHULZ: We would shut it down, but we wouldn't put it in mid-loop. As Tim suggested, the mid-loop condition is where the risk is coming from. So we would put it in a hot standby condition, very much like

Turkey Point did.

And I think they did the right thing there, and that the same kind f conclusion would come out of AP600. If you would shut it down, but you keep it in a hot standby, where you have the most options, and levels of defense.

MEMBER SEALE: I guess I have -- I'd say I do understand the problem. You have gone into this operational design, and applied an awful lot of passive features that were available to you, simply because the operational modes were pretty well-defined.

When you get into the shutdown mode, there are an awful lot of other things that happen. I mean, the menu is pretty -- is a lot larger, it seems to me anyway. The things that you do, the extent to which you rely on operator action and all.

And I guess I'm not surprised that, on a per hour basis, you wind up with a bigger set of options, when you're in the operational mode -- I mean, when you're in the shutdown mode.

So I guess I'm not as surprised. But the point's well-taken, you know. And so that's a hell of a good place to be.

CHAIRMAN APOSTOLAKIS: So, basically, the message from all of this is what will dominate will be external events. Is that correct?

MR. BUETER: I don't see why external -- what do you mean by external?

CHAIRMAN APOSTOLAKIS: Seismic, fires. I mean, ten to the minus eight. They can easily overrun that.

MR. BUETER: Certainly it can be easily overrun. We haven't done the other analyses, we haven't completed them yet, so I don't know if I can tell you that.

But the same types of things that helped us achieve this low core damage frequency work to our benefit, and work to the plant's benefit, in external events.

We have many other mitigation possibilities, as Mr. Schulz and Selim have mentioned. Certainly, if a fire affects one of them, you have to deal with the ones that are left, but we have multiples compared to current plants.

So, you know, maybe that will be what comes out of it. But it's going to be more of a result of -- maybe the other numbers will be on the same order of magnitude. That's conceivable, because then we'll have a bounding analysis, or something like that.

I don't think we're going to see it along the same magnitude as current plants, though. Certainly not that. And I can conceive of a fire maybe being an E minus eight or something. That depends on how conservative and how bounding we deal with the analysis.

CHAIRMAN APOSTOLAKIS: All day long, we were told that you would be using the seismic margins --

MR. BUETER: Yes, sir.

CHAIRMAN APOSTOLAKIS: -- approach?

MR. BUETER: Yes, sir.

CHAIRMAN APOSTOLAKIS: Now that does not quantify risk, does it?

MR. BUETER: I don't believe so.

CHAIRMAN APOSTOLAKIS: It's a bounding kind of.

MR. BUETER: Yes. It's a bounding analysis. You know, Cindy does the method better than I do, in this respect.

CHAIRMAN APOSTOLAKIS: Well, there must be some criteria for bounding the frequencies, is that right? The seismic.

MS. HAAG: This is Cindy Haag, from Westinghouse. For those seismic margins, you don't come out with an absolute risk number, you know, like a core damage frequency type number. What you come out with is the -- you use the HCLFP values.

CHAIRMAN APOSTOLAKIS: A little better.

MS. HAAG: Okay. And you come out to say can the plant withstand -- the HCLFP is about .5 g. Can your equipment withstand something, at least to a .5 g? And are there any operator actions that might be needed to be taken, in order to be able to withstand a .5 g earthquake?

That's sort of the criteria you're trying to meet. You're not trying to come out with core damage frequency numbers. You're coming out with more of a HCLFP evaluation.

CHAIRMAN APOSTOLAKIS: But, given that there is a very good suspicion that seismic risk will dominate, shouldn't you be doing a natural seismic analysis? Or, you cannot do it, because you don't have a site? Is that correct?

MS. HAAG: That's correct.

CHAIRMAN APOSTOLAKIS: Okay.

MS. HAAG: You don't have the site characteristics to be able to calculate that.

CHAIRMAN APOSTOLAKIS: So, after the site is selected, then you would expect -- well, we would expect seismic?

MS. HAAG: I don't believe that the criteria is that you must do a seismic PRA. Seismic margins. You can do further seismic margin evaluations.

CHAIRMAN APOSTOLAKIS: The criteria. Whose criteria are these?

MS. HAAG: From the URD. That criteria is stated there. And what's accepted under the IPEEE is a seismic margin. And for other design certifications as well.

CHAIRMAN APOSTOLAKIS: I'm not so sure. I mean, if we have safety goals to meet. I mean, the bounding analysis -- oh, okay. I see.

If the bounding analysis shows that it's less than ten to the minus four, you are okay, even though it may be ten to the minus six, and dominates this. That's strange. This must be the first time we're doing something strange.

MEMBER KRESS: We ought to fix that.

CHAIRMAN APOSTOLAKIS: We ought to fix it.

MEMBER KRESS: We'll have full scope, level three PRAs.

CHAIRMAN APOSTOLAKIS: With uncertainty analysis.

MEMBER KRESS: Thank you.

MEMBER SEALE: And a bonus every year for PRAs.

MR. BUETER: Okay. I think, as has been alluded to, the number's relatively low, compared to other plants, other studies that have been done.

And, as I said, there are not a whole lot of them out there. But we selected these, and tried to make some kind of comparison.

So there's a little bit of subjectivity in how these are grouped. Believe me, I didn't do it to be, you know, advantageous to anybody. I just kind of put it together the best way it would fit.

But you can see the AP600 is a couple of orders of magnitude smaller in core damage frequency than, say, current generation type plants. And about one or more less than an evolutionary PWR, for the various types of events, and in total number, at shutdown.

Now, I think -- I don't claim to be real familiar with all the details of these studies. But I think, if we looked at it, we would say that they're all dominated by mid-loop conditions. So, you know, the comparison holds true there, too.

MEMBER POWERS: If I look at the comparison carefully, how much of the reduction have you achieved by design improvements, and how much actual hardware changes, and how much have you achieved because you're in shutdown for fewer hours than these other plants?

MR. BUETER: Certainly the mission time, or the time has an impact. You can't argue that, because the arithmetic is pretty straightforward.

But I think that the important thing is -- and I was, I'll touch on this a little bit. The AP600 has a mitigation system. And I'll talk about it at mid-loop, because that's, again, where most of the risk is.

What's the concern at mid-loop? Well, mid-loop loss of decay heat removal. Okay, you're, you lose your RNS. Well, in current plants, your RNS, you have redundancy in trains --

MR. MONTY: I think we can get through this one fairly easily.

MR. BUETER: Okay.

MR. MONTY: If you look at a few slides back, when we did the sensitivity. You look at the sensitivity to the no credit for IRWST injections, you see a very large increase by not having that feature.

So, we would argue that a large part of the benefit is in having that feature in the plant. The path of IRWST injection. There is some change in the time spent, but it would probably be dominated by that feature in the design.

MR. BUETER: So there's your question. It's hardware, is a big factor. I think another aspect of that is we've tried to design to present loss of RNS, loss of decay heat removal, or, at a minimum, the ability to regain it.

Another important thing, I think, is well, the normal RHR at other plants as redundant as it is in the AP600? We have the IRWST as a back-up. It's not an operation. It's just there.

And it's been assured to be functional, before you go to mid-loop. So we've said "yes, this is functional, and it's there as a back-up, and we're not using it."

MEMBER POWERS: I bring the question up, because I would suspect the time in shutdown is an extraordinarily uncertain number for a new plant. So, as the other ones, you presumably had some data on the actual time.

MR. BUETER: Certainly, you could argue that. I don't think the time was going to be the dominant factor. The time has some kind of an impact, but it's certainly not going to be dominant. And you could plug in a larger number, and still come up with comparable results.

CHAIRMAN LINDBLAD: Tim, all of your shutdown assessments were done with fuel in the reactor vessel, is that right?

MR. BUETER: I --

CHAIRMAN LINDBLAD: Did you do a spent fuel pool assessment?

MR. BUETER: I don't believe so. Isaac?

(No audible response.)

Okay.

CHAIRMAN LINDBLAD: And because of cooling systems not all being safety grade, is it likely that the spent fuel assessment for an AP600 will give risks per hour, perhaps higher than that of a current level plant? With safety grade cooling systems and electric systems?

MR. BUETER: This is Schulz's.

MR. SCHULZ: We don't think so. The most reliable mechanism of cooling, we would think, would be the water that's already in the pool.

CHAIRMAN LINDBLAD: Passive cooling, you're calling it?

MR. SCHULZ: Passive cooling.

CHAIRMAN LINDBLAD: Okay.

MR. SCHULZ: And we've done evaluations on AP600. And, anytime you're operating the plant, you have at least seven days worth of water at pool. There are some specific --

CHAIRMAN LINDBLAD: Those are the same times that apply to existing operating plants.

MR. SCHULZ: I don't know if they have quite the same times, but I imagine they would be very similar.

The pools are fully loaded, of course.

CHAIRMAN LINDBLAD: Yes. But you don't know of any features that would actually bring your pool risk assessment below that of existing plants?

MR. SCHULZ: The only things that we have that current plants don't have would be designed in make-up connections that can be -- you don't have to get into the pit area, to squirt water into there. We've got a designed in connection that we can get temporary water supplies to very easily.

And the other thing is use of other passive water supplies, such as the passive containment cooling water. We've got about 350,000 gallons of water sitting on top of the containment area there.

And, if you have removed all the fuel -- and that's probably your biggest heat load situation, is a core offload into the pit, then all that other water could be made use, brought to bear on the pit point.

CHAIRMAN LINDBLAD: Through pipes, or through the transfer tube?

MR. SCHULZ: Not through the transfer tube. It would be through pipes. And right now, it may even take some temporary connections.

CHAIRMAN LINDBLAD: Okay. And, on the other hand, the operating plants have a safety grade diesel electric system?

MR. SCHULZ: That's right.

CHAIRMAN LINDBLAD: And this plant does not?

MR. SCHULZ: That's right.

CHAIRMAN LINDBLAD: And so that's a trade-off of sorts?

MR. SCHULZ: Yes. Now, and we can debate it. Is the safety-related system more reliable than our non-safety-related system, which starts in two minutes, and we do less rapid start testing on? There's other trade-offs there that you -- we think we've made, too.

CHAIRMAN LINDBLAD: All right.

MR. BUETER: The same discussion I mentioned at-power. You do all this work, and you want to see, well what are the results of this? What insights are to be gained? Why is the number so low? What's important to this plant?

And I said most of them. Shutdown risk is certainly relevant at power. On an hourly basis, at mid-loop, not necessarily true. I don't think that's anything unknown.

The dominant risk, again, is loss of heat decay removal at mid-loop. But we have -- because of the passive systems, and the passive systems of back-up, the normal RHR we have, you have the ability to have a lower core damage frequency.

Again, the IRWST injection is not being used. Its operation, operability is assured, before you get to mid-loop. It backs up the RNS. The IRWST is multiple and diverse. We have multiple flow paths from the IRWST, through more than one strainer.

We also have a diverse flow path that goes through -- again, it's passive, but it goes through an RNS line, and it's got a different set type of valve in it. So you eliminate common cause in that respect.

We don't rely on AC power for the passive IRWST injection. As Bruce pointed out, it's a very important function, but if we don't -- if you have a loop, and you're in shutdown, it's just not going to hurt you. You still have the DC batteries to activate the IRWST injection.

And, on top of all that, if you do have a loss of off-site power, we do have our generators. Again, they're not safety-related, as we mentioned before. But we feel they're certainly relatively reliable. Argue which is better or not.

Another very important thing that current plants don't have is automatic isolation of the drains. One of the problems at mid-loop, of course, is what happens if you overdrain? How do you know if you're overdrainirg?

Well, we designed in hot leg level instrumentation, reliability and diversity into that, and gave it automatic signals to isolate these drain valve. So, it should --

MR. SCHULZ: The level of instrumentation is redundant, but --

MR. BUETER: Not diverse?

MR. SCHULZ: Not really diverse, no.

MR. BUETER: Okay.

CHAIRMAN LINDBLAD: What's the -- what's the design of the level of instrumentation? What is so reliable that it's?

MR. SCHULZ: Well, current plants did not have -- at least, originally designed in systems, the temporary tag-on tubing.

CHAIRMAN LINDBLAD: Right.

MR. SCHULZ: And video cameras, and things.

CHAIRMAN LINDBLAD: Right.

MR. SCHULZ: We have added to the AP600 redundant DP cells that, with our narrow range, basically hot leg plus a little bit, up to the steam generator inlet, give a very accurate indication of what's going on in the hot leg.

We do have a small element of diversity in that we have a wide range pressurizer level, down to the bottom of the hot leg. So that covers the transition into the mid-loop level instruments.

And so you can get some assurance that, when you're bringing it into the hot leg, that you're -- you've been tracking this wide range instrument into the other range. So you do have a third level instrument there, that you do have some.

CHAIRMAN LINDBLAD: Is there some kind of level sensor, in the reactor vessel itself?

MR. SCHULZ: No, there isn't.

CHAIRMAN LINDBLAD: Thank you.

MR. BUETER: We also did sensitivity analyses for the shutdown. As Mr. Monty mentioned, we suspected the IRWST was very important, and I think this sensitivity shows that.

If we take out the IRWST injection, at shutdown, you're core damage frequency rises significantly. That would be expected, I think. It is our back-up to RNS.

Human actions are important. So, we say "well, what happens if we make the operators unreliable, if you will, to a good degree?"

This is a couple of orders of magnitude higher, a larger number than is normally used. So, it represents a one out of two failure, if you will. The operators. And, again the operators are important, but it's still a very low number.

So the automatic functions of the plant certainly give us a lot of margin. But we can't say the operators are useless, because they may help a lot, too. Go back to the --

MEMBER POWERS: You didn't take that completely to zero reliability the way you did on your power reactor?

MR. BUETER: No, we did do that. The operators, the backup to the operator to the automatic is more important at shutdown than it is at risk. Yes.

MEMBER SEALE: That sort of goes along with what I said earlier.

MR. BUETER: Yes. The focus PRA where again we only take credit for the mitigation from the safety systems causes the CDF to go up a little bit. That's still very low. Again, I think that shows the margin we have with our safety systems only. It doesn't take credit for duplicity of trains in RS or CCW or anything like that. I said shutdown, anybody? Entertain anything?

Well, we are trying to present highlights. Mr. Monty is going to give you the -- you can go ahead.

MR. MONTY: I'm just going to provide a quick wrap up. In conclusion -- here we go, I'll turn it on. In conclusion what we intended this presentation to tell you is that we have performed a detailed PRA of the AP600 design. We talked about the AP power and the shutdown material. In the future we hope to talk about the level 2 analysis and the external events. As I said before the Level 2 analysis includes credit for in vessel retention as part of the flooding up near the vessel and that we have used the work done, sponsored by DOE Advanced Reactors Reaction Program, fed that into our Level 2 analysis that's ongoing now, the revision that we are doing now. And we would expect to discuss that with you in the future. We also did a Level 2 for shutdown and that will also be discussed in the future.

From what we've shown you, we think we are well on the way of meeting the AP600 design goals. Obviously we didn't show you the external events. And the design goals include addressing some of the external events like internal flooding and fire. But the numbers that we show you today show that we are on the way to meeting those goals.

It demonstrates a significant core damage frequency improvement over current plants. We've done a lot of things over the seven year or eight year period of doing PRA and design to improve the core damage frequency by adding in features. And as I said, an iterative PRA application has allowed some designer enhancements. And it also provides input into the emergency response guidelines that we have developed for the plant, and as well, the, some accident management insights that will go into the future accident management guidelines when the plant is sited and built.

So, with that, I'd like to thank you for having us here today to go through this material and we are looking forward to future discussions.

CHAIRMAN APOSTOLAKIS: Thank you very much.

MR. MONTY: Thank you.

CHAIRMAN LINDBLAD: If the passive plant features reliance on "natural" forces, Westinghouse and your partners must have done extensive studies about what affects natural forces. Now I won't deny that gravity is always there, but friction works against natural forces. What have you determined needs to be done to keep the natural forces free of friction?

MR. MONTY: Terry? As far as design?

MR. SCHULZ: I think the keys to that are --

CHAIRMAN LINDBLAD: And has this been looked at in some detail?

MR. SCHULZ: I believe so. We start with what we think are conservative calculations for estimating the friction losses in the design phase and in using that in the accident analysis. The testing that we have done at SPES and OSU use similar analytical techniques which I think verified, or have verified that our approach is conservative and reasonable.

The other thing, of course, that will eventually happen is that when the plant is built there will be start up tests which will verify that the friction factors are within the safety limits that we set for our current analysis. And following on that, the in service testing that will verify that the friction factors stay within bounds over the life of the plant.

CHAIRMAN LINDBLAD: Now here you are, I think you are talking about piping hydraulic friction, are you not?

MR. SCHULZ: Yes, were you thinking something?

CHAIRMAN LINDBLAD: I was thinking about that, but also components and valves such as spool valves and the air operated valves and check valve hinge pins.

MR. SCHULZ: Well, the check valves will have, what I would call enhanced service testing, we will be exercising them with flow on a regular basis. And if, in monitoring their performance with non-intrusive diagnostic instrumentation so we can tell whether the valve is degrading. I think that coupled with system flow tests which would include the valves would cover not only the piping resistance but the valve resistance.

CHAIRMAN LINDBLAD: Do you see any suggestion that the water treatment needs to be controlled any differently from the current range of plant?

MR. SCHULZ: Not in the reactor coolant system. Now we do have the passive containment cooling system which is a different animal and we are providing what we think is appropriate chemistry control of that tank, that storage tank on top of the shield building.

It doesn't enter, water doesn't enter the reactor, so we don't have reactor compatibility issues, but we do have to flow the chemistry there sufficient so it doesn't somehow foul up the system and the valves that are associated with it. And we have placed some controls on that water. A means of sampling and adding chemicals to the water.

CHAIRMAN LINDBLAD: And I ask this out of ignorance, do you believe that that water treatment is important to maintaining low friction or does it turn out that it's not that important. There aren't many challenges to friction growth in either piping hydraulic friction or components of control systems from water treatment issues.

MR. SCHULZ: With the use of stainless steel piping and the types of water chemistry that we are using, I don't believe that we really have a concern with friction of a pipe of the valves changing. And if we were using carbon steel equipment, yes, that would be certainly more of a concern, but --

CHAIRMAN LINDBLAD: Is biological growth an issue in any of these systems?

MR. SCHULZ: That is more of a question I think with the passive containment cooling tank. It is more of a stagnant tank and I think we are taking some of the concerns that we are trying to address with our chemistry controls and sampling capabilities relate to that. But, again, doing a system flow test showing that when we open the valve, the flow out of the tank onto the containment is within the design limits I think is also an ultimate check.

CHAIRMAN LINDBLAD: Okay, slightly different from friction, I haven't done many natural forced systems. All my systems have been pumped in the past in which NPSH was very important on the section of my pump. Tell me, does NPSH get to be an issue in the CMT tank? Maybe Ivan already has asked you this but, can the tank heat up to the point where the flow is reduced?

MR. SCHULZ: Not in the same sense that a pump system can ultimately degrade and possibly fail. The density of the water within the tank is the, is a strong element to the driving force. So as long as you account for that in your calculations, then --

CHAIRMAN LINDBLAD: But there is an upper limit in the temperature that the water cannot exceed to maintain your circumstances?

MR. SCHULZ: We put a limit on the normal standby temperature, like most plants do. Because the subcooling of the water in the tank does play a role in heat removal. So, we place a limit on the initial standby.

CHAIRMAN LINDBLAD: So it's a heat capacity rather than the flow characteristic.

MR. SCHULZ: There's both, there is both. But during an accident the tank can and does heat up to reactor temperatures and that's not a problem. And it does affect or reduce the flow rate, but again is, doesn't seem to be a lead to inadequate cooling.

CHAIRMAN LINDBLAD: Shifting the emphasis for a minute. If the existing plants have a safety grade accelerate feedwater system and we still have transients associated with losing level and steam generators, if we build new plants without safety grade feedwater systems are we going to have more steam generator level transients or less?

Loss of feedwater is a problem in existing plants, and even with safety grade components. And now we are going to go to non-safety grade components. Are we going to have more or less problems?

MR. SCHULZ: I'm not sure, is your question more related to the initiating event of loss of, are we going to have more losses of main feedwater, or more losses of main feedwater and auxiliary/start-up?

CHAIRMAN LINDBLAD: I guess the latter.

MR. SCHULZ: Okay, because we are doing a number of things that are unique to AP600 to improve the main feedwater system, including its response during a reactor trip. Now, obviously that only helps if the main feedwater wasn't the source of the problem. So, what --

CHAIRMAN LINDBLAD: -- has a reliable power supply.

MR. SCHULZ: Right. Now, obviously, we are not putting that on the diesels, those are huge pumps. So if you are talking about a loss of offsite power, then we are solely dependent on the start-up feedwater pumps.

Now, there is only two of those pumps. A typical aux feed system has three pumps and probably one turbine driven pump. So I wouldn't claim that our start-up feedwater is as reliable as an aux feed system. But we do think it will be very reliable.

Now, where does that end up? Probably would have a few more losses of feedwater. But of course backing all that up is our passive RHR. So if we lose all source of steam generator feed, we won't dry out the steam generators. The passive RHR will come on and will take over decay heat and will cool the reactor that way. It depends on what your concern is.

CHAIRMAN LINDBLAD: Thank you, sir.

CHAIRMAN APOSTOLAKIS: Well, are we ready to move on to the discussion? Well, in terms of future activities.

CHAIRMAN LINDBLAD: And could I ask --

CHAIRMAN APOSTOLAKIS: Sure, sure.

CHAIRMAN LINDBLAD: Generally, when we listen to other PRAs, particularly by reactor designers, we are interested in where did the operating experience and the review, you spoke of two reviews having been made of your PRA, are those available documents? Have I -- are they submitted?

MR. MONTY: No, they were not submitted.

CHAIRMAN LINDBLAD: They were not submitted.

MR. MONTY: They were independent reviews done for us that we factored into our work. But we did not submit those reviews. They are not formal reviews for the submittal process.

CHAIRMAN LINDBLAD: And presumably they had substantial operating experienced people involved in making those reviews.

MR. MONTY: I believe, especially the ALWR Utility Steering Group Committee did have actual operators, or people with operating plant history that reviewed, or had been active in doing PRAs on operating plants.

CHAIRMAN LINDBLAD: Well, can you tell me, were any of those issues raised by people with operating experience not closed with your organization, or do you think you satisfied them all?

MR. SCHULZ: Cindy, do you remember what the status of the, of all the comments were that we received?

MS. HAAG: I believe we've addressed those all within the update of the PRA. Those, that review was done prior to the submittal of the 1995 work. So that would have been factored into what you received in 1995 and have available for you right now.

CHAIRMAN LINDBLAD: And this, this most recent PRA, is that going to be reviewed by the same group?

MR. MONTY: No, the changes are very minor, relatively minor responding to some, a limited set of design changes. So we are not anticipating, the changes were not significant we would not anticipate another peer review per say as we had before. So I don't believe that there are any plans to do any additional independent review other than the NRC review being done.

CHAIRMAN APOSTOLAKIS: Okay, so thank you very much again, and let's see if the members have any --

MEMBER SEALE: Now you have a fire PRA that you are in the process of or fire a PRA or a five?

MR. BUETER: Fire analysis.

CHAIRMAN APOSTOLAKIS: It's not five. It's not a boundary.

MS. HAAG: It does five methodology. I wouldn't call it a true five. There is some exceptions to it. But it goes beyond five, because five I believe only goes to evaluation. I don't believe they necessarily go on to doing quantification. And we have done some quantification. So I, they are calling it a fire assessment.

CHAIRMAN APOSTOLAKIS: So --

MEMBER SEALE: I was going to say one of the things that strikes me about this design is that from the very beginning it seems to me there is a lot more discipline in the context of the plant layout and things like that. And I think most of us understand that fire mitigation, which is really the problem in a plant like this. I mean, you are going to have occasional flash point, but you want to make sure you don't feed it.

But fire mitigation is very much a matter of discipline and so I would be very surprised if you don't see some significant reductions in fire as well whenever you do it. I mean, if you apply the same level of discipline in what goes into the plant and how you control it, and so on. I'd be surprised. It's a guess.

CHAIRMAN LINDBLAD: Is there greater or less discipline in areas where non-safety grade equipment is used?

MEMBER SEALE: Now that's a good question.

CHAIRMAN LINDBLAD: Yes, and one might think that with a cut back in the amount of safety grade power supplies, there might be exposure to greater fire risk.

MEMBER SEALE: More ignition, certainly. But then that's where the discipline comes in in terms of what is available to feed it.

CHAIRMAN LINDBLAD: Yes but it comes down to what is non-safety.

MEMBER SEALE: Yes.

MEMBER CATTON: And fire systems are usually non-safety.

MEMBER SEALE: Yes.

MEMBER CATTON: So you have to wonder if the discipline carries over.

MEMBER SEALE: Well, that's kind of the challenge I think in what I said.

CHAIRMAN APOSTOLAKIS: Comments from Westinghouse on this?

MR. SCHULZ: We were thinking about it. No -- not enough discipline is the right word for more or less. Made some conscious decisions in the non-safety areas to not, for example, train separate the start-up feedwater pumps. They aren't safety equipment. They don't design that system for all the same kind of failures that an aux feed system would be designed for.

So that was kind of a conscious decision. So there is some of that involved. And when we go to non-safety areas, we don't apply the same rigor in separation. Now, we have two diesels and we put those into fire zones, they are side by side, but --

MEMBER SEALE: But separated.

MR. SCHULZ: But separated. So that was from a practical, reasonable approach. But we haven't vigorously applied separation in the non-safety areas. That was a conscious decision because they are not non-safety. They are non-safety.

But in the safety areas, we've tried to be, as you alluded to, very rigorous in the clean sheet of paper, and to keep things where practical behind walls, separated in different areas, to have a very clean fire separation.

CHAIRMAN LINDBLAD: Terry, as I remember the current class of operating plants went to diesels because of start-up times for emergency power supplies. And you speak of non-safety generators as always being diesel engines. What happened to turbines? Why don't you make those anymore?

MR. SCHULZ: That wasn't fair. We do, we do still make them.

CHAIRMAN LINDBLAD: What is the time requirement aside from non-safety grade engine generators at start-up?

MR. SCHULZ: We have established, I think it's about two minutes is our initial load point. We did have some discussions on gas turbines, or turbine type devices. And there were some questions about them being able to start even that fast.

CHAIRMAN LINDBLAD: So you still have a time window.

MR. SCHULZ: Yes, there was a time issue --

CHAIRMAN LINDBLAD: That is what you have.

MR. SCHULZ: Yes. And it was felt that diesel generators starting that slowly that we could avoid some of the cracked cylinder type issues that they get into with the real fast start diesels. But the diesel would actually have a chance to warm up a little bit before we actually loaded it.

CHAIRMAN LINDBLAD: What generates the two minute requirement?

MR. SCHULZ: It's, it's not a real strict requirement. We did some evaluations on start-up feedwater, and I think that's probably the limiting factor in our design in terms of we were just comfortable with waiting that long. We started to get uncomfortable with longer times, although it wasn't really a cliff.

MEMBER WYLIE: Is the chemical volume and control system safety very --

MR. SCHULZ: It's function of pumping water is not safety related. It does have some containment penetration, some RCS pressure boundary isolation which is safety related. But the stuff that's outside of containment in terms of boric acid storage tank and the make-up pumps are non-safety related.

MEMBER WYLIE: I believe they are the back-up safety injection system?

MR. SCHULZ: They provide what we called earlier, I called earlier a defense in depth capability of terms of borating and making up for a certain amount of leakage and under the core cooling system I think Tim Bueter said something with the PRA, the RCS leak initiating event which is a tech spec leakage up to instrument line break can be made up for with the CVS make-up pumps. So they are a high head, low capacity pump that provide some defense in depth to our passive core cooling system.

MEMBER WYLIE: I believe he actually indicated it is back-up high head injection and --

MR. SCHULZ: Although it doesn't have recirc capability and it really can't deal with small LOCAs by itself. If you operate it in conjunction with normal RHR which does have some recirc capability, together you can provide some protection. But by itself, it's really only capable of dealing with leaks that you can basically shut down, depressurize and pretty much get rid of the problem that way.

MR. BUETER: It buys you some time. In a lot of cases it just buys you some time.

MR. SCHULZ: But it is considered a defense in-depth. It is loaded on the diesels automatically. It will do some extra things in our graded QA approach on the CVS.

MEMBER WYLIE: But now that injection line goes outside to the pump right?

MR. SCHULZ: Right, pumps are outside containment.

MEMBER WYLIE: And so, is that covered in the PRA by the safety injection line break? Is that the same?

MR. BUETER: No, there, there is not a real connection, no. SI line break, I don't think CVS is really a factor. The line break is greater than the flow of the CVS so --

MR. SCHULZ: The consequences of breaking the CVS line, like active reactor core cooling system would be fairly minor in comparison with breaking the passive core cooling system direct vessel injection line.

MEMBER WYLIE: Where is it covered in your PRA? I mean you list it as an internal event, the CVCS system.

MR. BUETER: I'm confused with the question. You are saying where is the breakage in the CVCS line?

MEMBER WYLIE: No, where are you covered in your analysis in your PRA?

MR. BUETER: The breakage of the CVCS line? Or loss of CVCS?

MEMBER WYLIE: The breakage of the CVCS line.

MR. SCHULZ: It would be considered, I would think Tim, with one of your LOCA line segments.

MR. BUETER: I was trying to decide which LOCA, trying to think how big that line is. It would be a LOCA sequence.

MEMBER WYLIE: I beg your pardon?

MR. BUETER: It would be a LOCA sequence. Off the top of my head, I'm not sure which one. It would be --

MEMBER WYLIE: You show a safety injection line break, is it encompassed in that or --

MR. BUETER: Oh, the SI line break, no not necessarily, the SI line break is a specific line --

MEMBER WYLIE: Oh, okay.

MR. BUETER: -- and the plant response to that is different because you lose a lot of your injection ability. So, that's why the SI line break is culled out. It's not because of its size, necessarily.

MEMBER WYLIE: Okay.

MR. BUETER: It's because the plant response is significantly different.

MEMBER WYLIE: So you list it as an event, but you didn't show it anywhere. That's what I'm curious about.

MR. MONTY: Do you know what page you are referring to, that we can take a look at?

MEMBER WYLIE: It's listed, there is no page on this thing, under the content of the APR, you show it as item 15.

MR. MONTY: That's on the table of contents?

MEMBER WYLIE: Yes, and then, let's see --

MR. BUETER: Okay, you are referring to the chapter that discusses the model for the CVS?

MEMBER WYLIE: Yes.

MR. BUETER: Okay. That's not necessarily saying that this is a, loss of CVS is an internal event. What that chapter is saying, we built this model of CVS so we can use it in our event trees. And this is a chapter that says, here is the CVS model and how it's described.

MEMBER WYLIE: But under the function, you list that there is a safety injection, don't you?

MR. BUETER: Cindy --

MS. HAAG: Excuse me, this is Cindy Haag. In the PRA report the failure of the CVS pipeline, loss of the CVS piping is factored into the intermediate LOCA event. So it's factored into the LOCA frequency.

MR. BUETER: Yes, so I'm not sure what size, it's in on the LOCAs, but --

MEMBER WYLIE: Okay, so it's covered there.

MR. BUETER: It could also be small LOCA.

MEMBER WYLIE: But it's outside containment, is that right? Well, he says it's not.

MR. MONTY: Okay, it's a different line, but now his question then is, I think his question is is there a part of the CVS system that is outside containment and is there protection there against having outside containment loss of cooling accident.

MEMBER WYLIE: That's right.

MR. MONTY: Harry, do you understand that question? How do we protect the CVCS system from a loss of coolant accident outside containment since the pumps are located outside containment?

MR. SCHULZ: Okay, if you break that line, for it to be a LOCA, it has to be inside containment, the pipe break. Because there are RCS pressure bound reisolation valves, containment isolation valves. There is probably five or six valves that separate the reactor from the piping outside of containment.

So, in order for there to be a LOCA, it has to be something that you don't, or can't isolate. So that would be a pipe break inside containment.

If you broke the line outside containment, I mean that could happen, a hydrogen line break or something, and the system is not protected against that. I mean, it's not a safety system. It's located in a non-safety building. If the pipe breaks, the pipe breaks and it disables the system because the isorcore cooling system is completely located inside containment, we don't see any possibility of adverse interactions between that CVS hydrogen line break and our protection safety shut down equipment, or whatever, inside containment. I don't know if I'm really answering your question, but --

MEMBER WYLIE: Well, I'm not sure, I mean if it goes outside containment, the line does, then suppose it breaks.

MEMBER CATTON: If it breaks just outside containment.

MEMBER WYLIE: Yes.

MR. SCHULZ: There is no, there is no accident.

MR. BUETER: It's multiple levels of separation in valves between that line break if you will and the RCS pressure boundary. But --

MR. SCHULZ: Including a check valve just inside containment.

MR. BUETER: So, if the line broke and if several valves failed, yes, you would --

MEMBER WYLIE: You are relying on check valves shutting it off.

MR. SCHULZ: Well, check valve and three or four other valves.

MEMBER WYLIE: You didn't show it so I couldn't --

MR. MONTY: What I think he is saying is on the schematic that we showed, the simplified schematic, we did not show the valves that would be available to isolate the break if it occurred outside containment. To isolate the inside containment equipment from outside containment. Well you have to go more detailed design drawing to see those valves.

CHAIRMAN APOSTOLAKIS: Any other questions?

CHAIRMAN LINDBLAD: Today, when you showed a schematic of the plant arrangement, like you showed the reservoir above the containment for the passive containment cooling system as having a normal make-up. Now, is there some other secondary make-up to the reservoir other than the normal make-up?

MR. MONTY: Terry?

MR. SCHULZ: The, what I call the temporary make-up, the fire truck type make-up only goes directly to the containment.

CHAIRMAN LINDBLAD: Directly to the shell, not to the reservoir.

MR. SCHULZ: Right. I don't know if there is like a fire make-up connection to the tank itself --

CHAIRMAN LINDBLAD: Okay.

MR. SCHULZ: There might be, but I'm not sure.

CHAIRMAN LINDBLAD: Okay.

CHAIRMAN APOSTOLAKIS: Any other questions?

MEMBER FONTANA: Well, a little different, slightly different subject. This is a 600 megawatt plant. If a utility says I want a bigger plant, but I want to use as much of these passive features as possible. I know you can't use the direct heating out of the contain -- direct cooling from the containment. But is there something like that would obviate the use of gravity drain, for example, if you have a higher power density in the core or something like thac.

Have you looked at what limits, what would, what limits you could reach and still use some of these passive features?

MR. BUETER: I think we have looked at some of that stuff, and Terry can address it.

MR. SCHULZ: Yes, this is Terry Schulz. We have a program with some Japanese utilities that is really, a thousand megawatt version using all of the passive features, including passive containment cooling. And it's feasible. That design is not nearly as progressed as the AP600, but it seems to be feasible.

MR. POWERS: Does the containment volume change?

MR. SCHULZ: Versus AP600?

MR. POWERS: Right.

MR. SCHULZ: Yes. Yes, it gets bigger and that's part of the challenge there in terms of trying to avoid heat treating the steel in containment because it gets too thick and stuff like that.

MR. POWERS: Do you scale volume according to the power or to the cooling surface area?

MR. SCHULZ: It's more to the cooling surface area. We need a certain diameter to get all the stuff in there, in terms of the generators and the storage tanks and things like that. And then you need a certain surface area in order to get the heat transfer and dealing with seismic issues in Japan is a special challenge. And so, but, the version seems feasible.

CHAIRMAN LINDBLAD: Same power density, or did, was that an increase in power density as well?

MR. SCHULZ: It's similar. It was a like four loop reactor, like a Snoupps-type four loop reactor vessel with a thousand megawatt power, so it was reduced power density. I don't know if it's exactly the same as AP600 or maybe a touch higher, but similar.

MEMBER KRESS: Will the ex-vessel flooding feature still work at that power level?

MR. SCHULZ: I don't know.

MEMBER KRESS: It probably hasn't been looked at.

MR. SCHULZ: I don't think that they have looked at that, yet.

MEMBER FONTANA: When do we hear about Level 2?

CHAIRMAN APOSTOLAKIS: Well, that's the next subject. Follow-up actions. What, we are talking about follow-up actions. Noel, what are we going to do next?

MR. DUDLEY: What I foresee doing next is once the Level 2 PRAs and external events are available, a month to six weeks after receiving those we could schedule another meeting.

MEMBER SEALE: When is that?

CHAIRMAN APOSTOLAKIS: When do you think that will be?

MR. MONTY: That's, what a month to six weeks after June 28, which is when we are scheduled to submit the Level 2.

MEMBER CATTON: So it's August.

MR. MONTY: In the August time frame.

CHAIRMAN APOSTOLAKIS: Now, the Level 1 PRAs will be submitted in final form at the end of this month.

MR. MONTY: At the end of this month, also.

CHAIRMAN APOSTOLAKIS: Then what happens? Are we done with ACRS review?

CHAIRMAN LINDBLAD: On PRA?

CHAIRMAN APOSTOLAKIS: Level 1.

MEMBER KRESS: Presumably these would be an

SER.

CHAIRMAN APOSTOLAKIS: So the -- are we getting -- oh, okay. So the staff will write something and then we get involved. But we will not interact with Westinghouse again.

MEMBER KRESS: Not necessarily.

MEMBER CATTON: It probably depends on what the staff has to say.

CHAIRMAN APOSTOLAKIS: Westinghouse?

MEMBER CATTON: Or the staff.

CHAIRMAN APOSTOLAKIS: Because that's a fairly sizeable document. I mean, I haven't really had the chance to --

MEMBER CATTON: Maybe you ought to start reading it now.

MEMBER KRESS: We are relying on you to reading that.

CHAIRMAN APOSTOLAKIS: I have already. I have already started. When you took away human actions, it's no fun anymore.

MEMBER CATTON: Wait til we get to Level 2 and fire, and these other things. It will liven up.

CHAIRMAN APOSTOLAKIS: Well, we still have the uncertainty analysis now. We will have to see a good distinction on aliatory and abstemious.

Okay, so then it seems that an external, on Level 2 not external events. Only Level 2 we may be meeting sometime in October, November?

MR. DUDLEY: We will need to talk about that, whether we, whether the Committee will want to review that immediately after its issued by Westinghouse or after the staff has had a chance to review and comment on it. It depends on how the Committee wants to proceed with that.

CHAIRMAN APOSTOLAKIS: And so that's for Level 2. External events will come later? Or at the same time?

MR. MONTY: We could potentially do that all at the same time.

CHAIRMAN APOSTOLAKIS: And uncertainly analysis is in progress now.

MR. MONTY: Yes.

CHAIRMAN APOSTOLAKIS: Level 1.

MR. MONTY: Yes.

MEMBER SEALE: Sounds like it would be fun, George.

CHAIRMAN APOSTOLAKIS: Naturally, we are going back to Level 1. Anything else that anybody wants to raise? Any other members? Requests, recommendations? No?

MEMBER FONTANA: I have a --

CHAIRMAN APOSTOLAKIS: Sure.

MEMBER FONTANA: A little bit off the wall, but I remember two years ago, there used to be an argument between two camps. One said you can't do a PRA until you have a complete design. If you remember that. And then the other camp was saying you can use our risk assessment approach as to help guide the design. And I think you've shown the latter as feasible.

Let's take leap of faith here. In the future, some future kind of risk based regulation, is it feasible to design a plant to what the plant is supposed to do plus expected off design conditions, and do away with arbitrary design basis accidents and determine what the design basis accidents ought to be on a basis of feeding back to risk assessment.

I think eventually, this is a great leap forward, do you understand? We are not talking about tomorrow or anything like that. You guys design plant. Is that feasible?

MR. BUETER: My feeling is it's feasible.

MR. MONTY: There is some benefit in the guidance that the design requirements give you. And then it makes it easier to then model, you've got to start with something.

MEMBER FONTANA: You've got to start somewhere.

MR. MONTY: Right, and it helps you start somewhere. And then you get into an iterative process. And as you can see, we've done a number of revisions. Those were not, speaking from a designer, those were not inexpensive PRA exercises. With respect to manhours and calendar time.

So, if you went to just PRA and then have to feed back to designers and so forth, it would probably increase the cost. While, starting with the design requirement helps get you to a good point and then you get into the PRA process and feedback into the design. So --

MEMBER FONTANA: One question that comes up. Would you then use a large break LOCA on your containment system? For example, very low probably.

Well, anyway that's a great leap forward and it's not anything we can discuss here in a few minutes. I was just wondering what your feeling was.

MEMBER SEALE: Out of the box again.

MEMBER FONTANA: Sorry about that.

MEMBER SEALE: No.

MR. MONTY: I was going to let Terry, if Terry wanted to make a comment. He is a designer and he has come to know PRA a lot more in the last few years.

MR. SCHULZ: Too well, I think. I guess, I'm not sure that it would, in terms of getting to where we are now, that it would cost any more because of all the PRAs we've done.

But the real challenge I would think would be more in, we see this some already in terms of regulatory comfort with the PRA. We are using PRA already a little bit more than previous plants in terms of regulatory treatment of non-safety systems, tech specs. As a result, the PRAs come under more scrutiny. Things are being questioned. The success criteria all needs to be calculated, and the codes we use, and the margins in the codes.

It all becomes more important at a higher level as we start to approach design basis kind of scrutiny. And that's a real challenge in the PRA. How do you know that the valve reliability is right? We are using it as your design basis, would you then have to add a QA test to determine valve reliability? Those are the things where you need a lot of discipline in a regulatory process --

CHAIRMAN APOSTOLAKIS: Yes.

MR. SCHULZ: -- to deal with. Now, theoretically it's quite possible. I think the design aspect of it, I think we've essentially done it. But how you get to closure on licensing and regulatory issues that way take up a lot of time.

CHAIRMAN LINDBLAD: I'm kind of disappointed that we didn't get into fire today because I'm trying to look ahead to issues of why don't we have containment spray? Or why don't we have a fire sprinkler system that looks like containment spray. And --

MEMBER CATTON: Use it for both.

CHAIRMAN LINDBLAD: Use it for both, yes. And, I'm kind of impressed that with canned motor pumps, we've avoided a lot of the fire issues associated with reactor pump lube oil fires. I think we still probably have air cooling systems inside the containment, normally, is that right? With filtration and filter elements that are --

MR. SCHULZ: No filter elements, but there is fan coolers to take heat out of the containment normally.

CHAIRMAN LINDBLAD: And those are big motors with a lube oil system?

MR. SCHULZ: Well, they are electric motors. They are not that huge. A couple hundred horsepower or something like that. But they may have some lube oil, I don't know.

CHAIRMAN LINDBLAD: But I'm really kind of interested, is there any rationale for having a sprinklered containment before you get to the fission product cleanup issue of Level 2 or Level 3 issues? And, it would be a shame if you have avoided all of these ignition sources and then still thought you needed a fire system in there. I think we will see that later.

CHAIRMAN APOSTOLAKIS: Anything else?

(No response.)

CHAIRMAN APOSTOLAKIS: Well, I'd like to thank the Westinghouse team for an excellent presentation and this meeting is adjourned.

(Whereupon, the above meeting was concluded at 2:35 p.m.)

C E R T I F I C A T E

This is to certify that the attached proceedings before the United States Nuclear Regulatory Commission in the matter of:

Name of Proceeding: ACRS PROBABALISTIC RISK ASSESSMENT AND WESTINGHOUSE STANDARD PLANT DESIGNS JOINT MEETING

Docket Number: N/A

Place of Proceeding: ROCKVILLE, MARYLAND

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.

Corbett Riner

CORBETT RINER
Official Reporter
Neal R. Gross and Co., Inc.

INTRODUCTORY STATEMENT BY THE CHAIRMAN OF THE PROBABILISTIC RISK ASSESSMENT AND WESTINGHOUSE STANDARD PLANT DESIGNS JOINT SUBCOMMITTEE
11545 ROCKVILLE PIKE, ROOM T-2B3
ROCKVILLE, MARYLAND
JUNE 5, 1996

The meeting will now come to order. This is a meeting of the ACRS Joint Subcommittee on Probabilistic Risk Assessment and Westinghouse Standard Plant Designs.

I am George Apostolakis, Chairman of the Subcommittee.

The ACRS Members in attendance are:

William Lindblad, Ivan Catton, Mario Fontana, Thomas Kress, Don Miller, Dana Powers, Robert Seale, William Shack, and Charles Wylie.

The purpose of this meeting is to hold discussions with representatives of Westinghouse Electric Corporation and the NRC staff to gather information concerning the AP600 Level 1 and shutdown PRAs. The Subcommittee will gather information, analyze relevant issues and facts, and formulate proposed positions and actions as appropriate, for deliberation by the full Committee.

Noel Dudley is the Cognizant ACRS Staff Engineer for 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 May 23, 1996.

A transcript of the meeting is being kept and will be made available as stated in the Federal Register Notice. 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 no written comments or requests for time to make oral statements from members of the public.

(Chairman's Comments-if any)

We will proceed with the meeting and I call upon Brian McIntyre of Westinghouse to begin.

Westinghouse Electric Corporation

PRESENTATION TO

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

AP600 PROBABILISTIC RISK ASSESSMENT

Dr. Selim Sancaktar
W PRA Engineer
412-374-5983

Mr. Terry Schulz
W Design Engineer
412-374-5120

Mr. Tim Bueter
W PRA Engineer
412-374-5854

June 5, 1996

Objective of Presentation

Objective: - To provide an overview of the AP600 design.

- To provide a technical summary of the AP600 PRA submitted to the NRC as a part of the design certification process.

Scope: Plant core damage analysis for internal events at power and shutdown conditions.

Outline of Presentation

AP600

INTRODUCTION

OVERVIEW OF AP600

- AP600 Levels of Defense

BACKGROUND AND METHODOLOGY

- AP600 PRA Scope
- AP600 PRA Methods
- Plant Features Important to Reduction of Risk

AT POWER LEVEL 1 ANALYSES

- Results for At-Power Internal Events
- Sensitivity Studies
- PRA Insights

SHUTDOWN LEVEL 1 ANALYSES

- Results for Shutdown Events
- Sensitivity Studies
- PRA Insights

AP600 PRA Background

The AP600 PRA has been used since 1987 to provide insights into improvement of the design.

Each revision of the PRA quantification included:

- Plant design input and PRA model development
- Sensitivity studies
- Review and understanding of results
- Development of ideas to improve the plant analysis, procedures and design

STAGES 1/2:	Use of the PRA during the early design stage and preliminary PRA analyses (1987- 1990)
STAGE 3:	Base PRA (1992)
STAGE 4:	Revision 1 (1994)
STAGE 5:	Revisions 2 - 6 (1995)
STAGE 6:	Final PRA (1996)

AP600 PRA Background

All stages were done by the Westinghouse PRA group. The PRA group has been together since 1981 and its experience has included the following studies:

- Advanced PWR PRA submitted to the NRC in 1985
- Preliminary Sizewell PRA for the British
- More than 20 domestic and foreign IPE/PRA studies

In stage 3, the analysis effort was supported by PRA engineers from ENEL (Italy).

AP600 PRA Objectives

The main objectives of the AP600 PRA are:

- Satisfy the NRC regulatory requirements that a design-specific PRA be conducted as part of the application for design certification
- Provide a tool to investigate detailed design solutions and operational strategies to optimize AP600 plant safety

The AP600 PRA has the following quantitative goals:

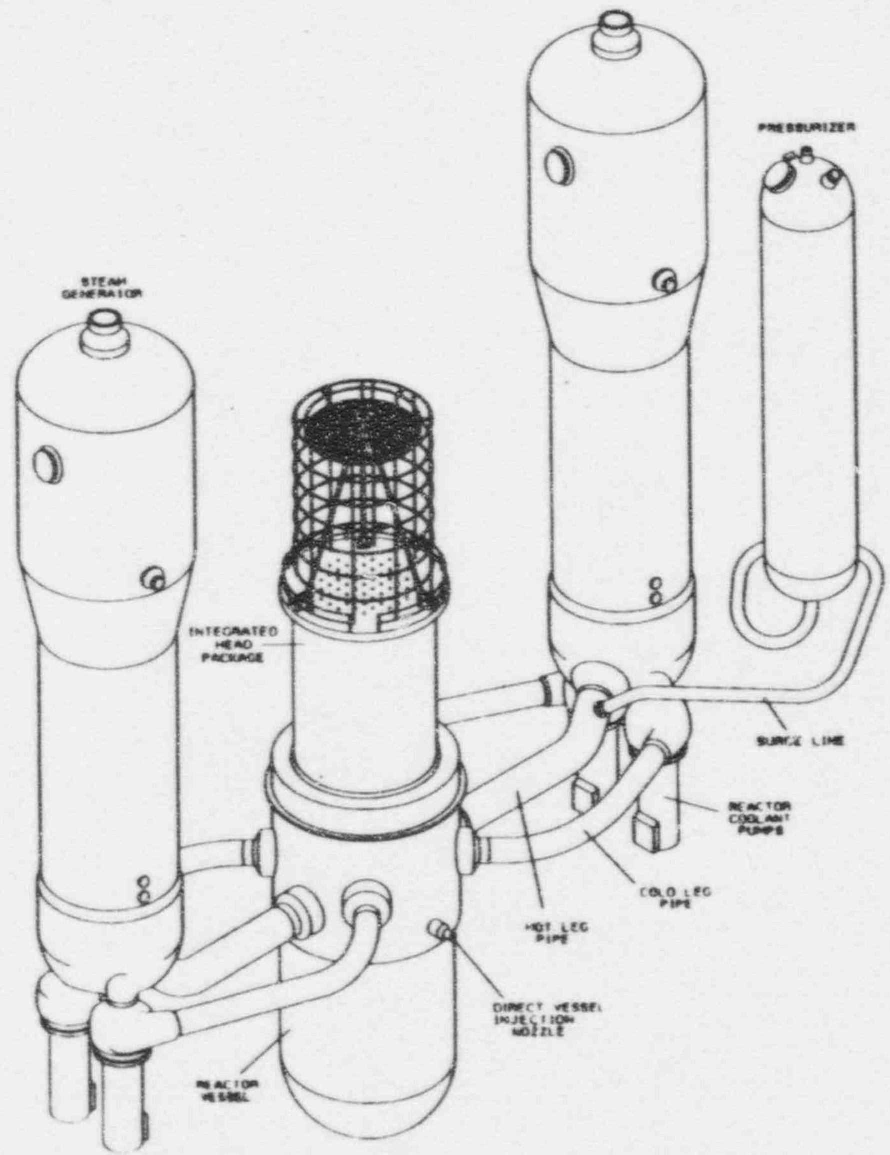
- Plant core damage frequency is less than or equal to 1.0E-05 events per year
- Plant severe release frequency is less than or equal to 1.0E-06 events per year (greater than 25 rem whole-body dose over 24 hours at one-half mile)

AP600
DESIGN OVERVIEW

AP600 PLANT FEATURES

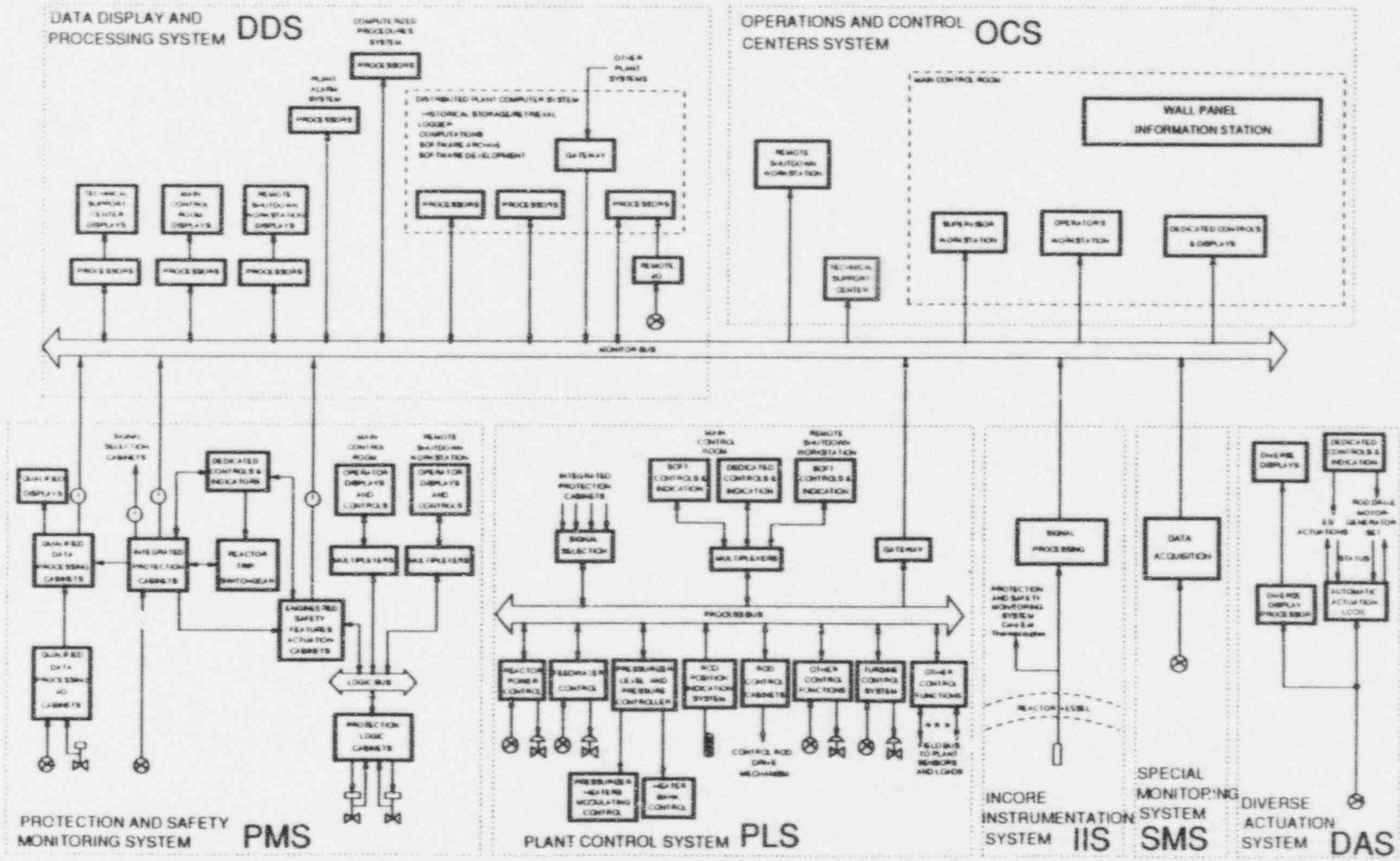
- **Increased Margins**
  - Lower reactor power density
  - Larger pressurizer
- **Simplified Loop Configuration With Canned Pumps**
- **Passive Safety Systems**
- **Simplified Non-Safety Systems**
- **Digital Instrumentation and Control Systems**
  - Advanced control room
- **Enhanced Plant Arrangement and Construction**
  - Integration of cost / construction / operation / maintenance
  - Extensive use of modular construction

AP600 RCS LOOP



SSAR Sec. 5.1

AP600 I&C ARCHITECTURE



SSAR Sec. 7.1

AP600 SYSTEMS DESIGN APPROACH

- **Provide Simple Passive Safety Systems**
  - Use "natural" driving forces only
  - One-time alignment of active valves
  - No support systems after actuation
    - Actuation is fail safe or powered by safety DC
    - No safety AC power, pumps, fans, diesels
  - No operator actions required to cool core / containment
  - Satisfy NRC safety goals
  - Mitigate design basis accidents
  - Full safety design and regulatory oversight

- **Provide Simple Active Non-Safety Systems**
  - Use active equipment with lessons learned from operating plants
  - Redundant active equipment powered by nonsafety diesels
  - Minimize unnecessary use of passive safety systems
  - Not required to mitigate design basis accidents
  - Reduce risk to utility & public
  - Graded design and regulatory oversight

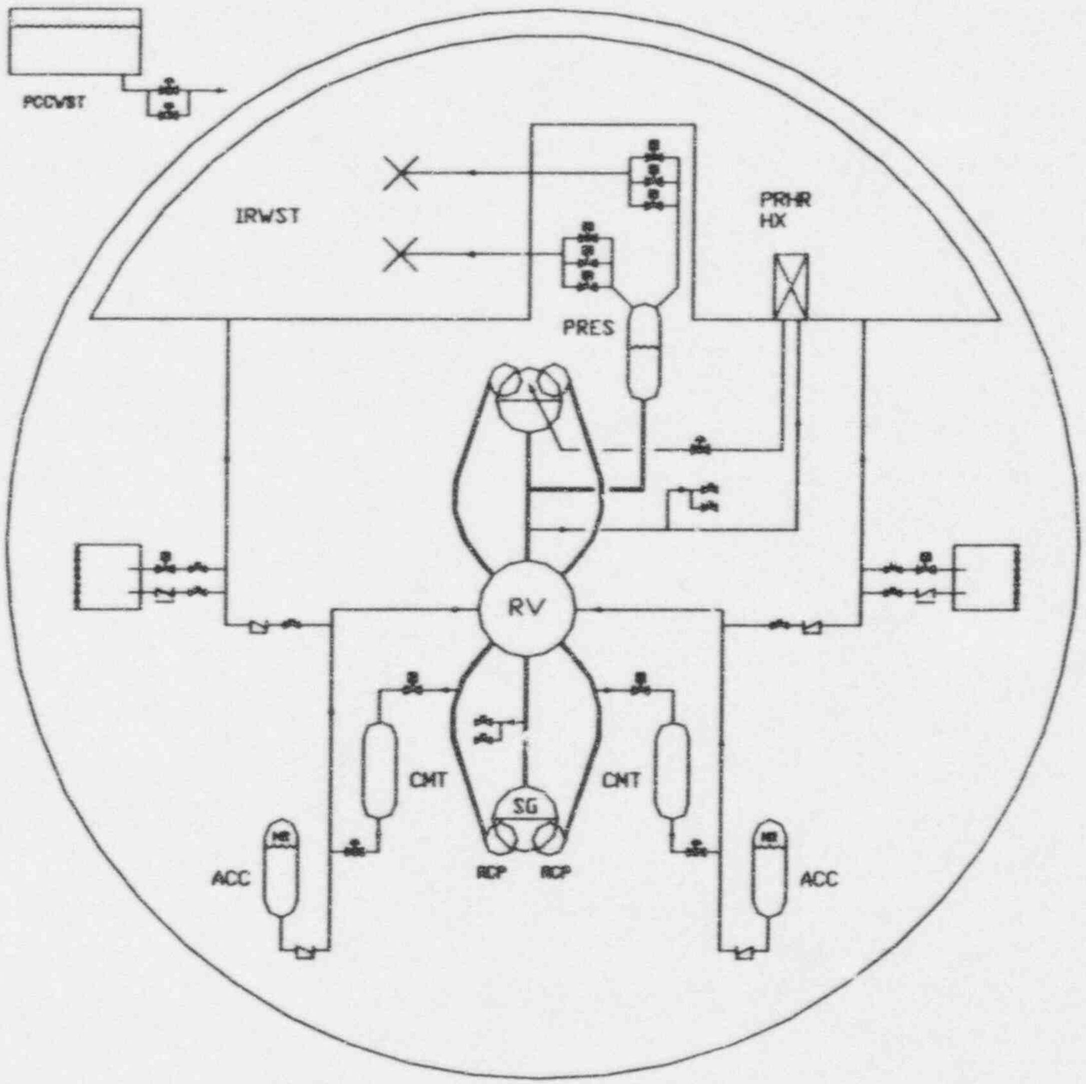
AP600 PASSIVE SAFETY FEATURES

- **Passive Decay Heat Removal**
  - Natural circulation HX connected to RCS

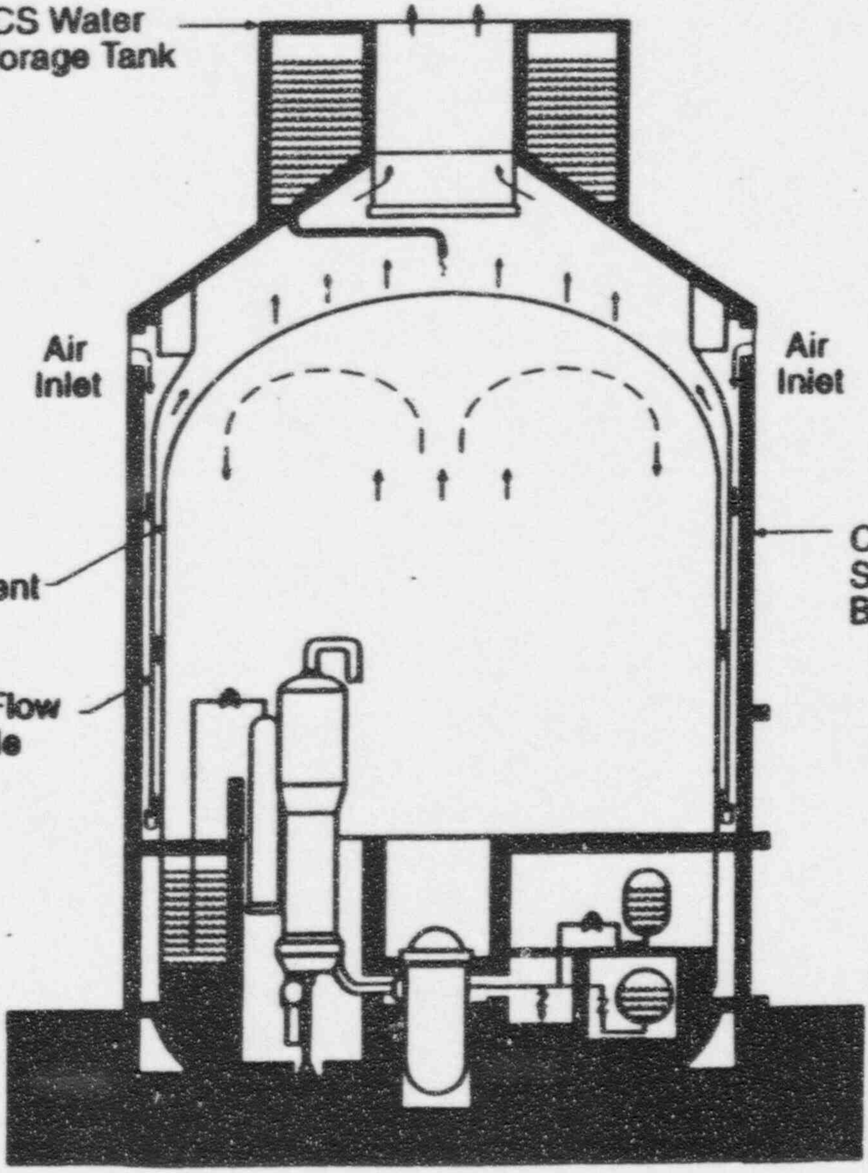
- **Passive Safety Injection**
  - Gravity drain core makeup tanks (at RCS pressure)
  - N2 pressurized accumulators (at 700 psig)
  - Gravity drain refueling water storage tank (at containment pressure)
  - Automatic RCS depressurization

- **Passive Containment Cooling**
  - Steel containment shell transfers heat to natural circulation of air and evaporation of water drained by gravity

AP600 PASSIVE SAFETY FEATURES

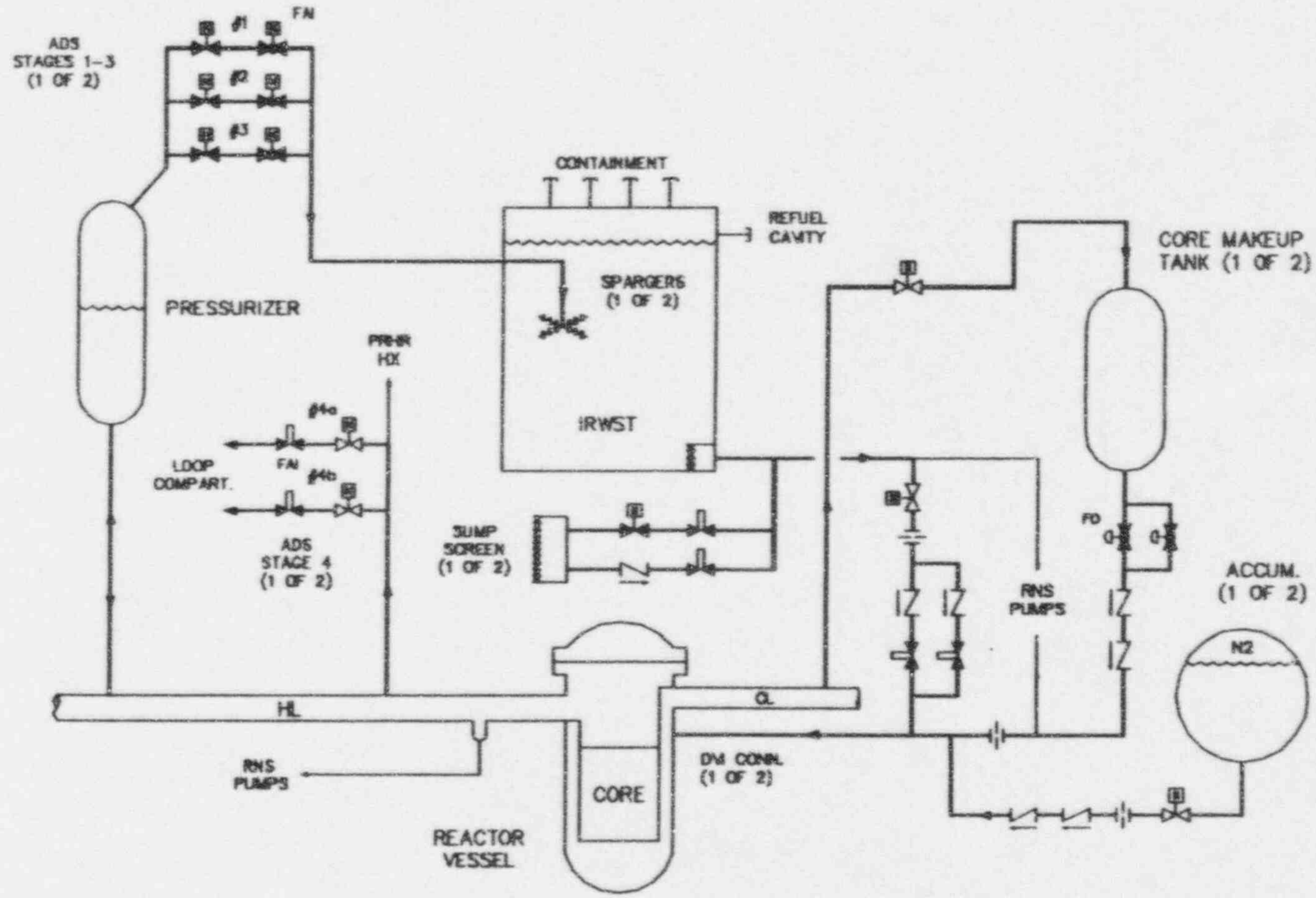


AP600 ARRANGEMENT



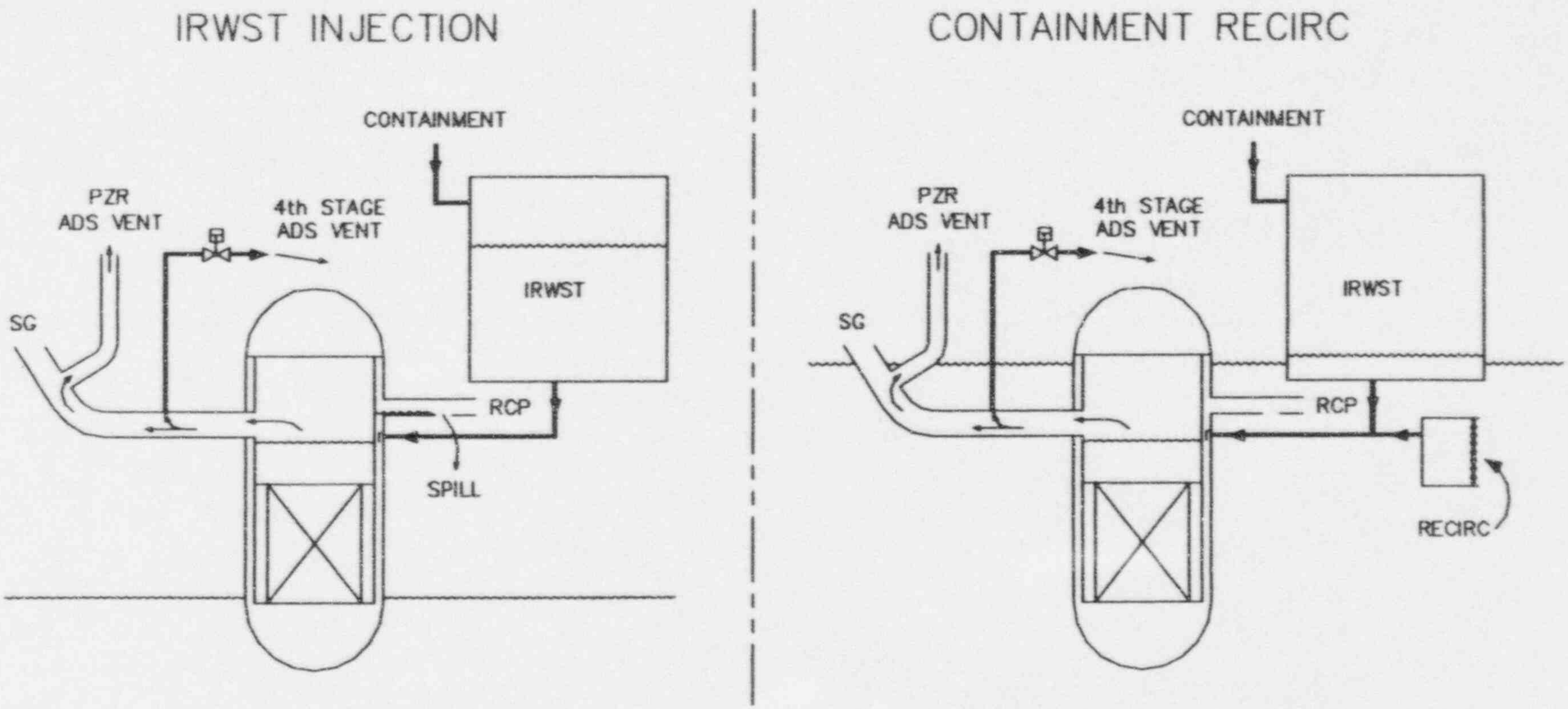
SSAR Sec. 1.2

AP600 PASSIVE SI SYSTEM



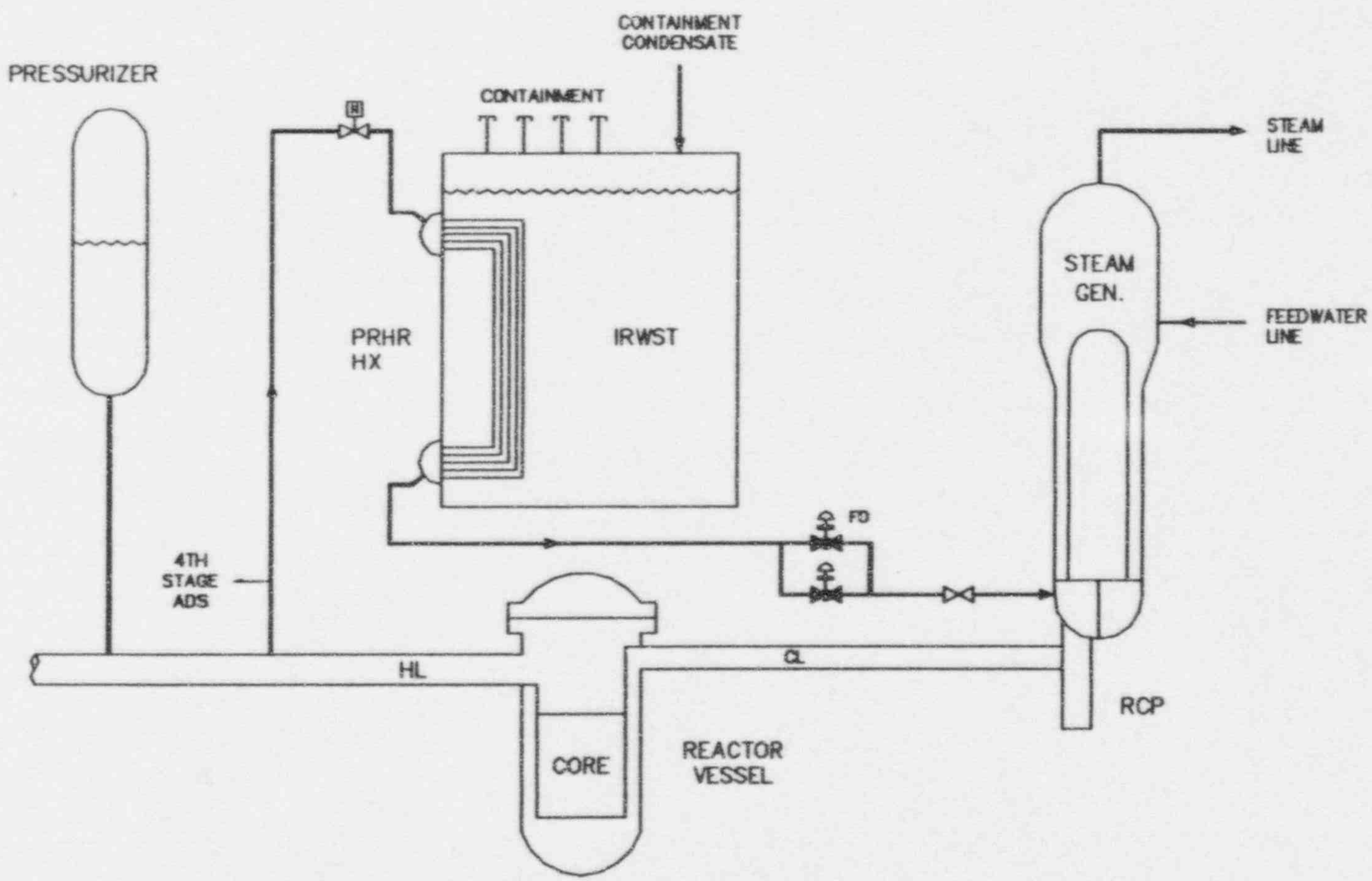
SSAR Sec. 6.3

LONG TERM PASSIVE SI OPERATION



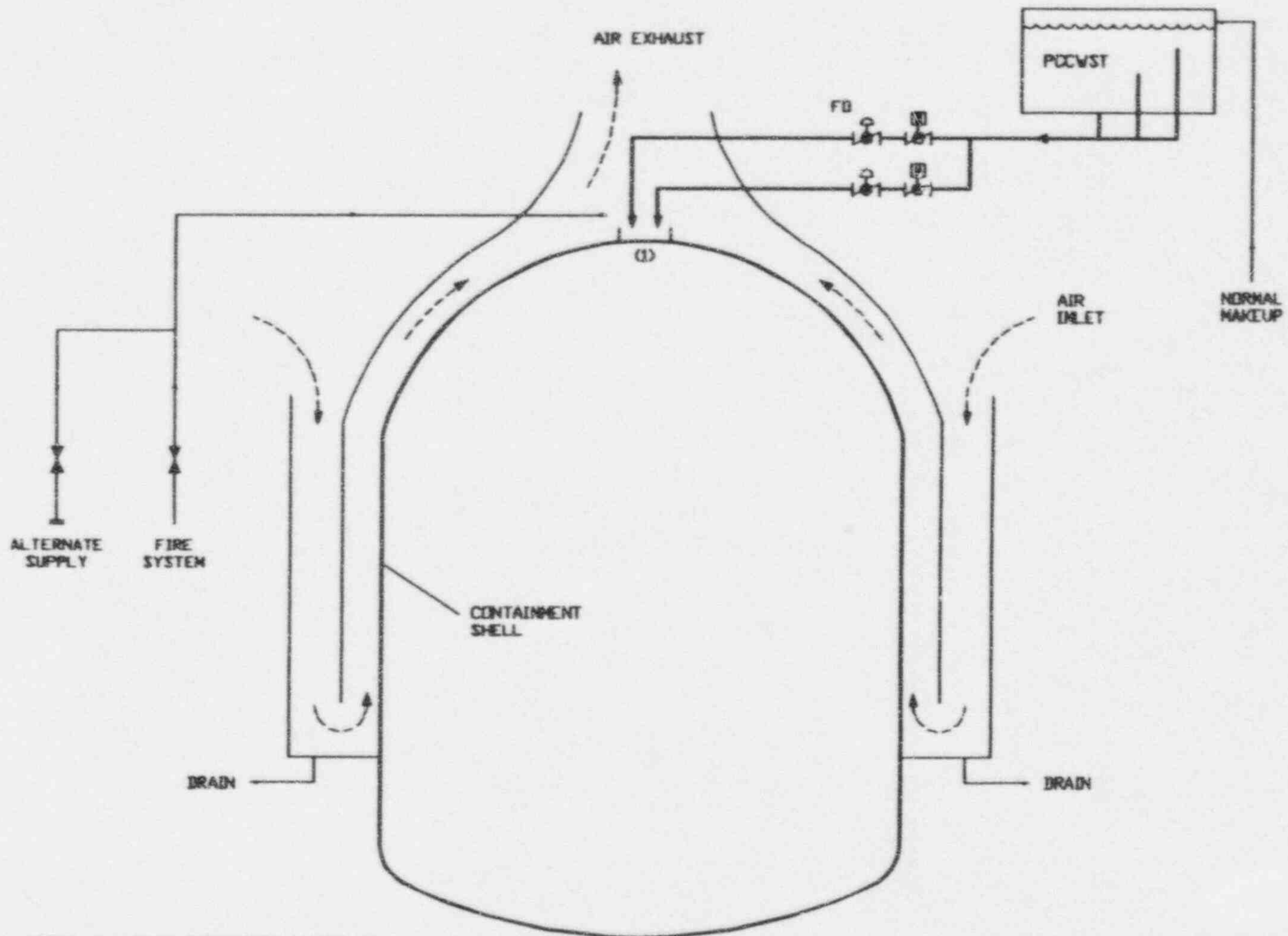
SSAR Sec. 6.3

AP600 PRHR HX SYSTEM



SSAR Sec. 6.3

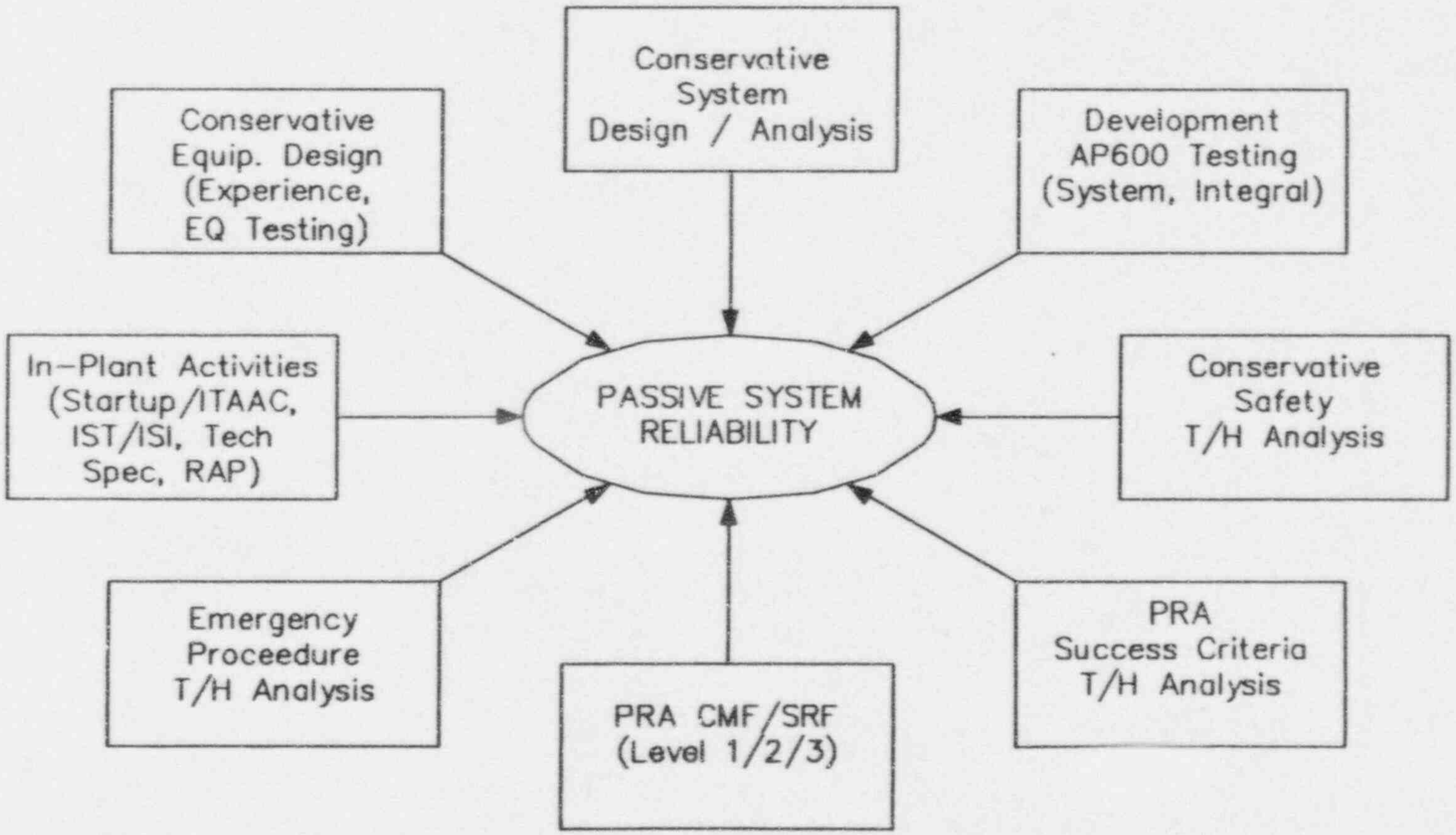
AP600 PASSIVE CONT COOLING



NOTES: (1) WEIRS DISTRIBUTE WATER FILM

SSAR Sec. 6.2

AP600 PASSIVE SYSTEM RELIABILITY



AP600
DEFENSE-IN-DEPTH

AP600 DEFENSE-IN-DEPTH

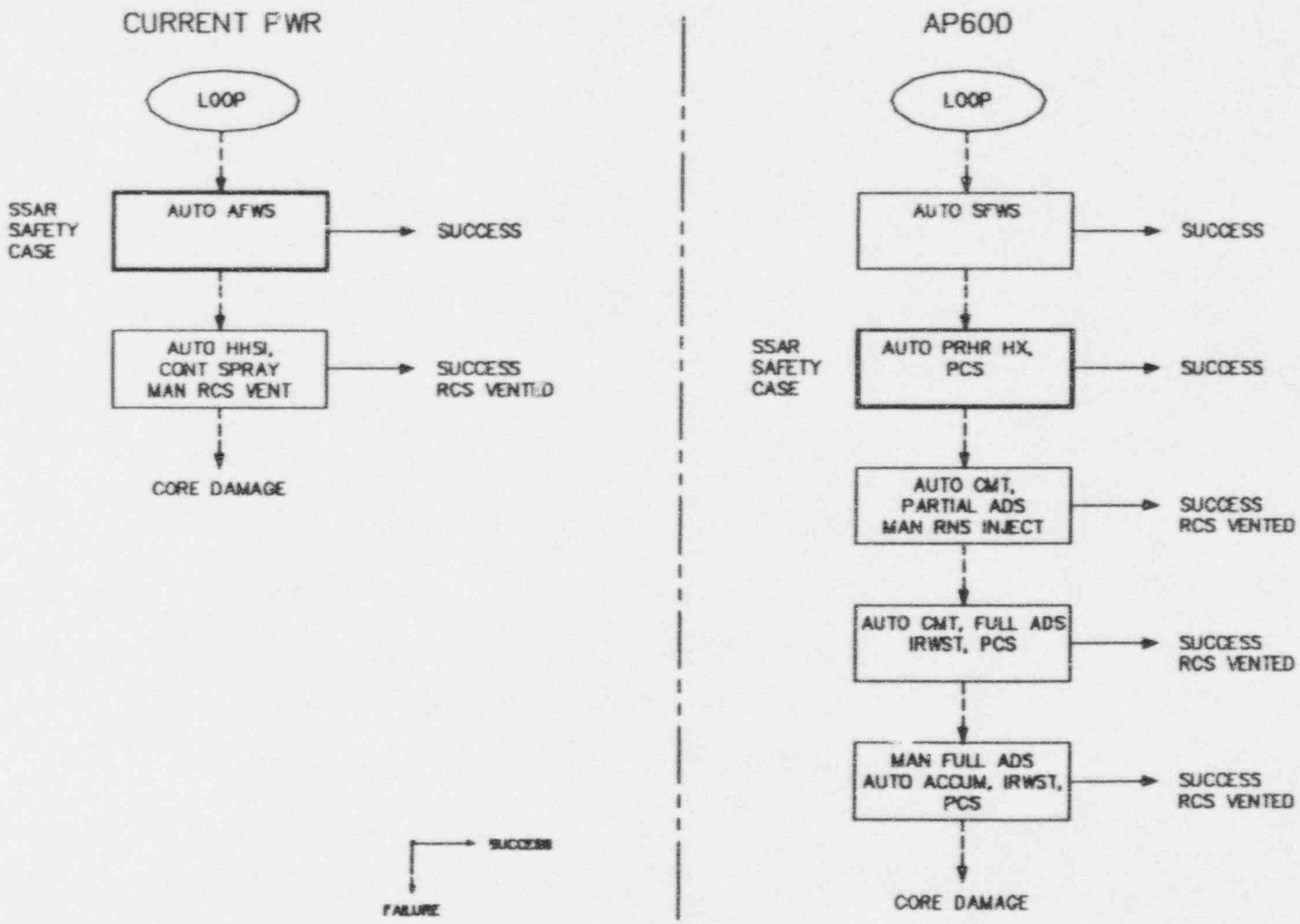
- **AP600 Provides Multiple Levels of Defense**
  - First is usually nonsafety-related active system
    - Reliable (redundant active components, onsite power)
    - Lessons learned from operating plants
    - Not required for safety case in SSAR
  - At least one is safety-related passive system
    - Provides safety case in SSAR
  - Other passive features provide additional defense-in-depth
    - Example - passive feed-bleed backs up PRHR HX

- **Multiple Levels of Defense Available During Shutdowns**
  - Available during hot standby through refueling shutdown
  - One is nonsafety-related active system
    - May be in operation (RNS, CCS, SWS)
  - At least one passive safety-related system also available
    - Not used for normal operation

CORE COOLING DEFENSE-IN-DEPTH

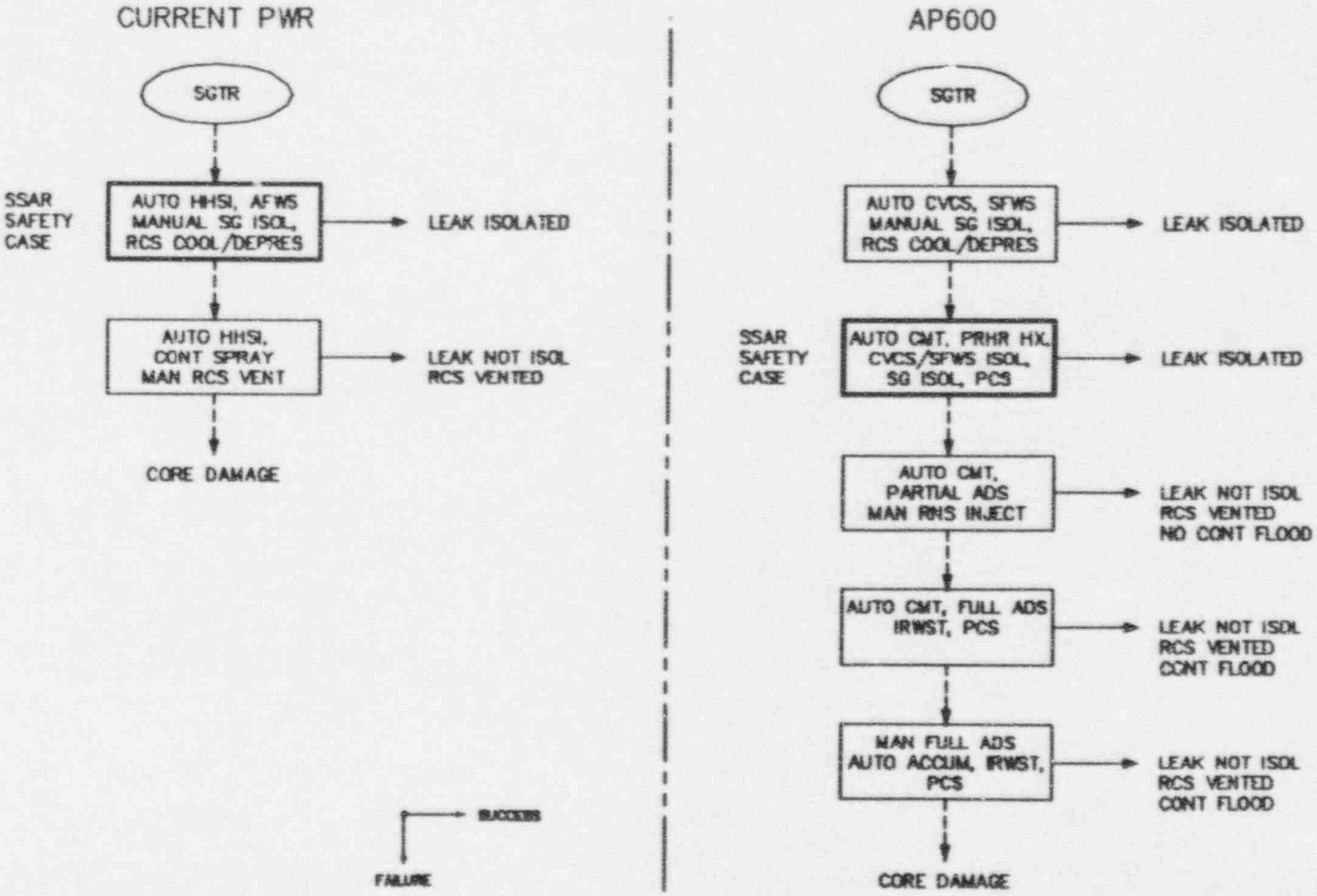
FUNCTION	CURRENT PWR	AP600
REACTOR SHUTDOWN	- CONTROL RODS (BREAKERS) - RIDEOUT (NEG MTC, AMSAC, AFWS, CVCS)	- CONTROL RODS (BREAKERS) - CONTROL RODS (MG SETS) - RIDEOUT (MORE NEG MTC, DAS, PRHRS/SFWS, CMT/CVCS)
RCS OVERPRESSURE PROTECTION	- PZR PORV - HIGH PRES TRIP - PZR SAFETY VALVES	- LARGER PZR - HIGH PRES TRIP - PZR SAFETY VALVES
RCS HEAT REMOVAL	- MAIN FEEDWATER SYS - AUX FEEDWATER SYS - MANUAL FEED/BLEED (PZR PORV, HHSI)	- MAIN FEEDWATER SYS - STARTUP FEEDWATER SYS - PRHR HX - AUTO FEED/BLEED (CMT / IRWST, ADS) - MANUAL FEED/BLEED (ACCUM / RNS, ADS)
HIGH PRESSURE INJECTION	- CVCS PUMPS - HHSI PUMPS	- CVCS PUMPS - CMT - ACCUM / IRWST (ADS) - ACCUM / RNS (ADS)
LOW PRESSURE INJECTION	- ACCUM - LHSI PUMPS	- ACCUM - IRWST (ADS) - RNS PUMPS
LONG TERM RECIRC	- LHSI PUMPS FEEDING HHSI PUMPS	- CONTAINMENT SUMP (ADS) - RNS PUMPS
CONTAINMENT HEAT REMOVAL	- FAN COOLERS - CONT SPRAY PUMPS / HX	- FAN COOLERS - EXTERNAL AIR + WATER DRAIN - EXTERNAL AIR ONLY COOLING

LOSS OFFSITE POWER



WCAP 13793

SG TUBE RUPTURE



WCAP 13793

AP600 PRA Scope and Methodology

AP600 PRA Scope

- Level of PRA Performed

  Level I
  Level II
  Level III

- Events Analyzed

  - At-power Internal Events
  - Shutdown
  - Internal Flooding
  - Seismic Margins
  - Other External Events

AP600 PRA Scope

Level 1 analysis scope includes

- Initiating events
- Event trees and success criteria
  - Extensive T/H analyses to support success criteria
- Plant systems analyses
- Common cause failures
- Human reliability
- Data analysis
- Fault tree and event tree quantification
- Importance and sensitivity studies
  - "Focused PRA" - mitigation credit is taken only for safety-related systems

CONTENTS OF AP600 PRA

CONTENTS OF AP600 PRA

CONTENTS OF AP600 PRA

EXTERNAL EVENTS

ANALYSIS SUMMARY

APPENDICES

AP600 PRA Methods

- Scope and methods are defined according to Revision 5/6 of the ALWR Utility Requirements Document (URD). Exceptions are justified in the PRA.

- PRA methods used are standard quantitative methods such as described in NUREG-2300.

- Data used are mean values

- Success criteria derived from extensive T/H analyses

AP600 PRA Methods

- Fault tree linking (small event tree/large fault tree) method used to quantify core damage sequence frequencies.

- Fault trees include:

  - system component failures
  - common cause faults
  - test & maintenance unavailability
  - human errors

- Detailed I&C models developed for PMS and PLS

- Reliability goal assigned for DAS

Plant Features Important to Reduction of Risk

Based on insights obtained from Sizewell, APWR, IPEs, and other PRAs, the AP600 design addressed PRA-related issues that dominate PWR plant CDF.

PRA Issue	How AP600 Design Addresses the Issue
Station Blackout (loss of all ac power). Dominant risk contributor in typical plants.	Safety systems are not dependent on ac power
Reactor coolant pump (RCP) seal LOCA (coupled with station blackout, or loss of cooling support systems events). Dominant risk contributor in typical plants.	RCPs have canned motors which cannot have a seal LOCA
Loss of support system events, such as ac power, component cooling, service water.	Safety systems do not rely on ac power and cooling support systems
Steam generator tube rupture (SGTR) events. Contributor to fission product release, although may not be dominant in core damage frequency.	Three levels of defense for mitigation of SGTR: 1) active systems and operator actions 2) automatic passive RHR (PRHR) 3) automatic ADS and passive injection
Interfacing systems LOCA. Contributor to fission product release.	The RNS path will be able to withstand RCS pressure. Multiple, diverse valves are placed along the RCS/RNS interface path.

Plant Features Important to Reduction of Risk

PRA Issue	How AP600 Design Addresses the Issue
Susceptibility to human errors. Operator actions required to mitigate some accidents.	The design minimizes the importance of operator actions to mitigate accidents.
ATWS	Diverse actuation system (DAS) for reactor trip is introduced as a nonsafety-related backup to PMS. This allows reduction in the ATWS challenges for AP600.
LOCA events and switchover to recirculation. Can be a dominant contributor	Injection and recirculation pumps are replaced with more reliable passive systems. The injection-to-recirculation switchover process is simplified.
Reliability of RHR and its support systems for decay heat removal during shutdown	Administrative guidelines require the maintenance and testing of the RNS and its support systems before going to shutdown. Design of hot leg nozzles and RNS pumps prevents cavitation at the pump suction. Remote hot leg level instrumentation added. Remote operation of RCS drains added.
Loss of decay heat removal during shutdown	Passive IRWST injection provides backup to RNS.

AP600 Level 1 At-Power PRA

At-Power Initiating Events

Twenty-six initiating event categories defined to represent the AP600 design:

- 11 are loss of coolant accidents (LOCAs)
- 12 are transients
- 3 are anticipated transients without scram (ATWS) precursors

Plant-specific initiating event categories defined and evaluated include:

- direct vessel injection line break
- core makeup tank (CMT) line break
- passive residual heat removal (PRHR) tube rupture

At-Power Initiating Event Frequencies

AP600

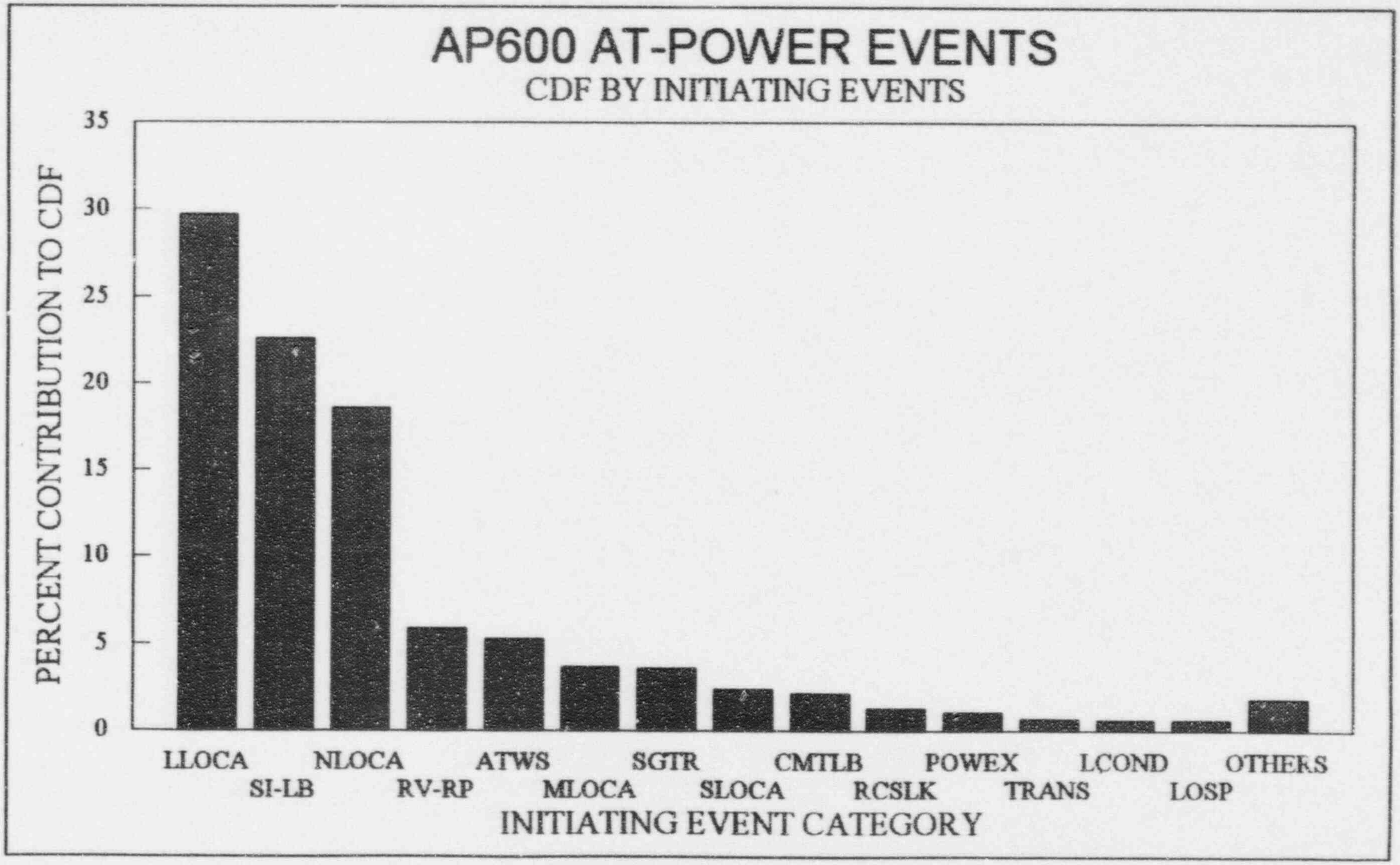
Initiating Event	Frequency (per year)	Initiating Event	Frequency (per year)
Large LOCA	1.0E-04	Loss of Offsite Power	1.2E-01
SI Line Break	1.0E-04	ATWS with MFW	– *
Intermediate LOCA	7.7E-04	PRHR Tube Rupture	2.5E-04
RV Rupture	1.0E-08	Main Steam Line Stuck Open	1.2E-03
ATWS with No MFW	– *	ATWS with SI	– *
Medium LOCA	1.6E-04	Loss of MFW to 2 SGs	3.4E-01
SGTR	5.2E-03	Loss of MFW to 1 SG	1.9E-01
Small LOCA	1.0E-04	Loss of Compressed Air	3.5E-02
CMT Line Break	8.9E-05	Steam Line Break Upstream of MSIV	3.7E-04
RCS Leak	1.2E-02	Loss of CCS/SWS	1.4E-01
Core Power Excursion	4.5E-03	Interfacing Systems LOCA	5.0E-11
Transient with MFW	1.4	Loss of RCS Flow	1.8E-02
Loss of Condenser	1.1E-01	Steam Line Break Downstream of MSIV	6.0E-04
		Total	2.4

* = ATWS precursor frequencies are accounted for in other initiating event categories.

Dominant Initiating Events

Initiating Event	Core Damage Frequency (CDF)	Percent Contribution to CDF	Cumulative Percent Contribution to CDF
Large LOCA	5.0E-08	29.7	29.7
SI line break	3.8E-08	22.6	52.3
Intermediate LOCA	3.2E-08	18.6	70.9
Reactor vessel rupture	1.0E-08	5.9	76.8
ATWS with no MFW	9.0E-09	5.3	82.1
Medium LOCA	6.2E-09	3.7	85.8
SGTR	6.1E-09	3.6	89.4
Small LOCA	4.1E-09	2.4	91.8
CMT line break	3.5E-09	2.1	93.9
All others	1.0E-08	6.1	100
Total	1.7E-07	100	

At-Power CDF by Initiating Event



Initiating Event Category Acronym Definition

AP600

LLOCA	→	Large LOCA
SI-LB	→	SI Line Break
NLOCA	→	Intermediate LOCA
RV-RP	→	Reactor Vessel Rupture
ATWS	→	ATWS with no MFW
MLOCA	→	Medium LOCA
SGTR	→	Steam Generator Tube Rupture
SLOCA	→	Small LOCA
CMTLB	→	CMT Line Break
RCSLK	→	RCS Leak
POWEX	→	Power Excursion
TRANS	→	Transient with MFW
LCOND	→	Loss of Condenser
LOSP	→	Loss of Offsite Power

CDF Results for At-Power Events

Initiating Event	Core Damage Frequency (CDF)	Percent Contributio n to CDF	Initiating Event Frequency (per year)
Large LOCA	5.0E-08	29.7	1.0E-04
SI line break	3.8E-08	22.6	1.0E-04
Intermediate LOCA	3.2E-08	18.6	7.7E-04
Reactor vessel rupture	1.0E-08	5.9	1.0E-08
ATWS with no MFW	9.0E-09	5.3	— *
Medium LOCA	6.2E-09	3.7	1.6E-04
SGTR	6.1E-09	3.6	5.2E-03
Small LOCA	4.1E-09	2.4	1.0E-04
CMT line break	3.5E-09	2.1	8.9E-05
RCS leak	2.3E-09	1.3	1.2E-02
Core power excursion	1.8E-09	1.1	4.5E-03
Transient with MFW	1.1E-09	0.7	1.4
Loss of condenser	1.0E-09	0.6	1.1E-01
Loss of offsite power	1.0E-09	0.6	1.2E-01
ATWS with MFW	7.1E-10	0.4	— *

Notes:
* ATWS precursor frequencies are accounted for in other initiating event categories.

CDF Results for At-Power Events

Initiating Event	Core Damage Frequency (CDF)	Percent Contributio n to CDF	Initiating Event Frequency (per year)
PRHR tube rupture	5.6E-10	0.3	2.5E-04
Main steam line stuck open valve	4.8E-10	0.3	1.2E-03
ATWS with SI	3.8E-10	0.3	— *
Loss of MFW to 2 SGs	3.0E-10	0.2	3.4E-01
Loss of MFW to 1 SG	1.8E-10	0.1	1.9E-01
Loss of compressed air	1.7E-10	0.1	3.5E-02
Steam line break upstream of MSIV	1.2E-10	0.1	3.7E-04
Loss of CCS/SWS	1.2E10	0.1	1.4E-01
Interfacing systems LOCA	5.0E-11	<0.1	5.0E-11
Loss of RCS flow	1.3E-11	<0.1	1.8E-02
Steam line break downstream of MSIV	9.5E-12	<0.1	6.0E-04
Total	1.7E-07	100	2.4

Notes:

* ATWS precursor frequencies are accounted for in other initiating event categories.

Comparison to Other Plant PRA Results

Initiating Event	AP600 CDF	Evolutionary PWR CDF	Current 4-Loop Westinghouse PWR CDF
LOCA	1.5E-07	7.0E-07	4.2E-06
ATWS	1.0E-08	5.0E-08	3.3E-08
SGTR	6.1E-09	3.0E-07	6.3E-07
Transients	2.1E-09	6.0E-07	3.9E-07
LOOP	1.0E-09	4.0E-08	2.4E-05
All Others	8.0E-10	1.0E-08	1.3E-05
Total	1.7E-07	1.7E-6	4.2E-05

Design Features That Reduce Typical CDF Contributors

Transients:

- Core cooling following transients is available from main feedwater, startup feedwater, PRHR, and feed and bleed.

Loss of offsite power:

- PRHR provides decay heat removal (no ac or dc power)
- Feed and bleed cooling provides backup to PRHR
  - requires power provided by 1E dc batteries

SGTR:

- PRHR (automatic)
- Feed and bleed (automatic)
- Nonsafety active systems and operator actions

Sensitivity Studies for At-Power Analysis

SYSTEM IMPORTANCES
(CDF when the system is assumed to have failed)

Important			Medium Importance(*)	Marginally Important	
1 E-02	1 E-03	1 E-04	1 E-05	1 E-06	1 E-07
PMS	**ADS**	**CMT**	**IWRST-INJ**	PLS	**SG OVERFILL PROTECTION**
DC -1E	**IRWST-REC**	**ACC**	**PRHR**	RNS	MFW
			DAS	AC POWER	SFW
			NON 1E DC	SWS	DG
				CCS	
				CAS	

* Core damage values greater than 5.0E-06 /year are conservatively classified in this column, since this column contains transition from marginally important category to important category.

Safety systems are shown in bold.

Sensitivity Studies

AP600

Sensitivity	New CDF	Comments
No credit for operator actions	1.8E-05/yr	Operator actions are not needed to maintain CDF at better than most current plants AP600 meets NRC safety goal without operator actions
Increase failure probability of squib valve basic events by a factor of 10	6.3E-07/yr	The CDF has some sensitivity to the squib valve failure probability.
Increase the failure probability of safety system check valve basic events by a factor of 10	5.3E-07/yr	The CDF has some sensitivity to the safety system check valve failure probability.
Credit taken only for safety-related systems mitigation (focused PRA)	6.2E-06/yr*	The plant CDF can be maintained at the E-05/year range with only safety systems; Credit taken only for safety-related system mitigation.

*under final Westinghouse review

At-Power Events Insights and Features

- Insights gained from previous PRA stages have been factored into the design. Features important to the at-power CDF reduction are discussed below.

- Reliable passive safety systems (redundant/diverse)

  - Passive CMTs replace high pressure safety injection pumps

  - Passive IRWST injection replaces low pressure injection pumps

  - Automatic depressurization system (ADS) and CMT/IRWST replaces manual feed and bleed operations

  - ADS mitigates high pressure events and allows low pressure injection to occur

  - Passive containment recirculation replaces low pressure recirculation pumps

At-Power Events Insights and Features

AP600

- Automatic actuation capabilities reduce the dependency on operator actions compared to current plants
- Operator action to prevent core damage is only required in cases of multiple failures
- Passive systems do not rely on support systems such as AC power and cooling water
- Reliable I&C systems
  - PMS highly redundant with sensor diversity
  - DAS provides diverse actuation of safety systems and provides a diverse reactor trip function

At-Power Events Insights and Features

- Interfacing systems LOCA event frequency reduced by RNS valve arrangement / design pressure
- RCP seal LOCA eliminated by canned motor pump
- Simple safety systems require less planned maintenance
  - Performed during periods when system not required

At-Power Events Insights and Features

AP600

- Increased core protection defense-in-depth
  - Passive features backed up by additional passive features (ex: passive feed and bleed backing up PRHR; accumulators backing up CMTs)
  - Passive features backed up by active features (ex: SFW backs up PRHR; RNS injection backs up IRWST injection)

- Passive containment cooling provides reliable ultimate heat sink
  - No reliance on active pumped systems
  - Natural circulation air cooling of containment sufficient for heat removal

- Important operator actions eliminated
  - Automatic feed and bleed
  - Switchover to recirculation
  - Tube rupture mitigation
  - Diverse reactor trip via DAS

HO
5

AP600 Level 1 PRA Shutdown Analyses

Shutdown PRA

Full scope Level 1 and 2 PRA performed for shutdown assessment (Chapter 54 of PRA)

Shutdown conditions evaluated:

- **Startup (Mode 2) to Hot Shutdown (Mode 4) with steam generator cooling**
  - **not quantified; risk < 1% of power operation**

- **Hot Shutdown (Mode 4) to Cold Shutdown (Mode 5) with RCS intact**
  - **specific quantification performed**
  - **referred to as "nondrained condition"**

- **Reduced RCS inventory (Modes 5 & 6)**
  - **includes drain/fill RCS, drain/fill refueling cavity, mid-loop**
  - **specific quantification performed**
  - **referred to as "drained condition"**

- **Refueling with flooded cavity (Mode 6)**
  - **not quantified; large water inventory**

Shutdown Initiating Events

- First considered at-power initiating events (IEs)
  - Initiating event bounded by at-power event
  - Conditions of RCS significantly reduced during shutdown
  - Initiating event precluded by system alignment during shutdown
  - Examples of IEs inappropriate to reactor shutdown include:
    - Turbine trip, loss of main feedwater
    - ATWS
    - Breach in RCS pressure boundary

- Then considered and evaluated additional shutdown IEs
  - Reactivity accidents (boron dilution, rod withdrawal)
  - Events unique to passive systems

- Shutdown IEs modeled using event trees
  - Loss of normal decay heat removal (RNS, CCS, SWS)
  - Loss of offsite power
  - Loss of reactor coolant (RNS pipe break, inadvertent drains)

Shutdown PRA Quantification Process

AP600

- Unavailabilities modeled in fault trees
  - Random equipment failures
  - Common cause failures
  - Human errors

- Use refueling outage schedule to determine system mission times
  - Includes allowances for maintenance activities
  - Mid-loop time for nozzle dam installation/removal
  - Reduced RCS inventory time for vessel head removal & re-installation

- Fault tree / event tree quantification
  - Same process as used for at-power quantification

Shutdown Initiating Event Frequencies

Shutdown Initiating Event	Shutdown Initiating Event Frequency (per year)	
	Drained Conditions	Nondrained Conditions
Loss of offsite power	1.5E-03	8.1E-03
Loss of decay heat removal due to RNS failure	8.2E-05	9.6E-04
Loss of decay heat removal due to CCS or SWS failure	4.2E-04	3.2E-03
LOCA due to RNS pipe rupture	ϵ	1.5E-05
LOCA due to inadvertent drains	1.1E-05	1.7E-05
RCS overdraining during drain-down conditions	4.4E-06	N/A

N/A = not applicable

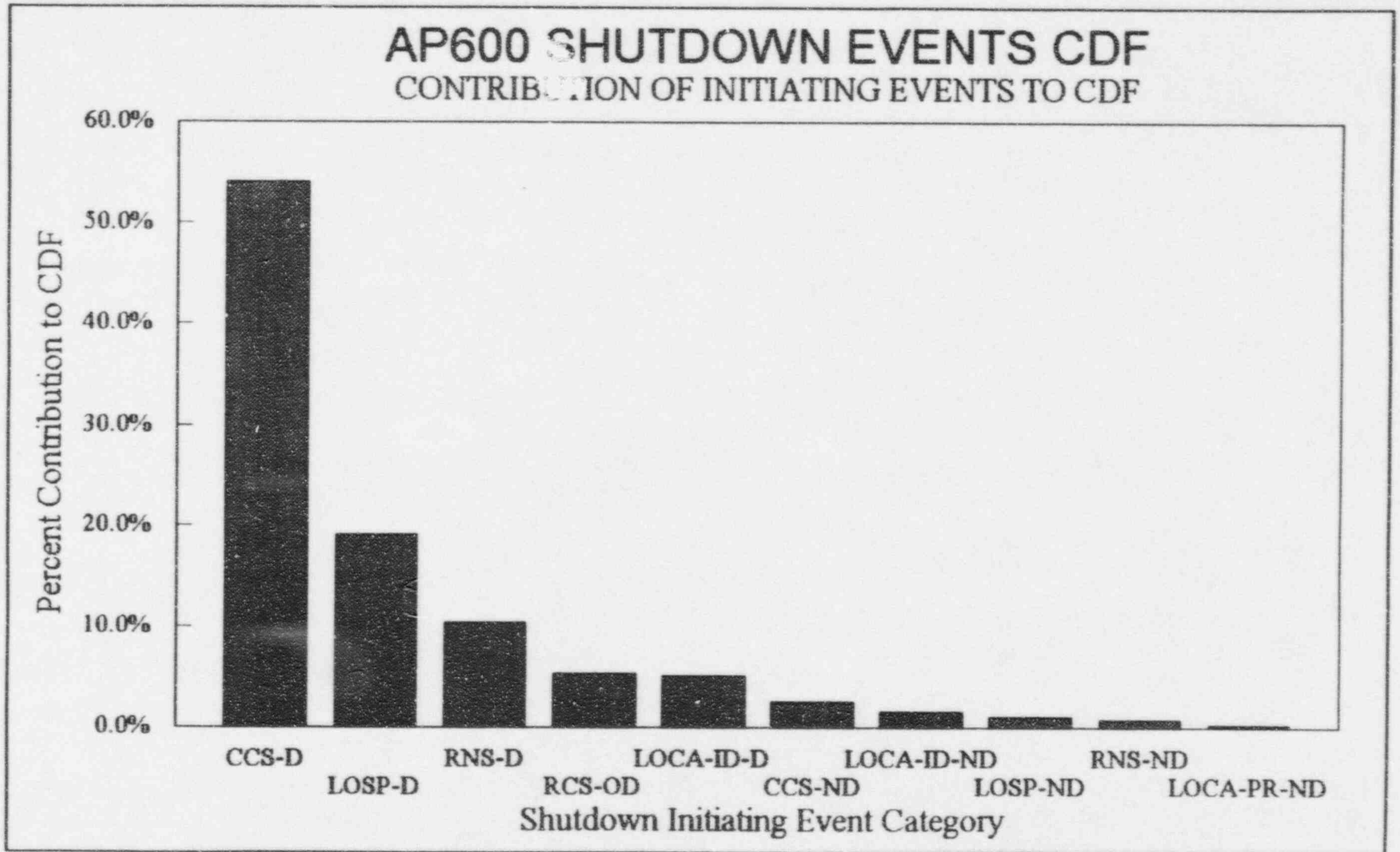
Shutdown PRA Results

- Shutdown CDF

  5.5E-08 per year (compared to 1.7E-07/yr at power)

- 90% of CDF occurs during drained or reduced inventory conditions

Shutdown CDF by Initiating Events



Shutdown Initiating Events

AP600

CCS-D → Loss of decay heat removal due to CCS or SWS failure for drained conditions

LOSP-D → Loss of offsite power for drained conditions

RNS-D → Loss of decay heat removal due to RNS failure for drained conditions

RCS-OD → RCS overdraining during drain-down conditions

LOCA-ID-D → LOCA due to inadvertent drains for drained conditions

CCS-ND → Loss of decay heat removal due to CCS or SWS failure for nondrained conditions

LOCA-ID-ND → LOCA due to inadvertent drains for nondrained conditions

LOSP-ND → Loss of offsite power for nondrained conditions

RNS-ND → Loss of decay heat removal due to RNS failure for nondrained conditions

LOCA-PR-ND → LOCA due to RNS pipe rupture for nondrained conditions

Shutdown PRA Results

Initiating Event	Core Damage Frequency (CDF)	Percent Contribution to CDF	Cumulative Percent Contribution to CDF
Loss of CCS/SWS - drained	3.0E-08	54.1	54.1
LOOP - drained	1.0E-08	19.0	73.1
Loss of RNS - drained	5.7E-09	10.4	83.6
RCS overdrain - drain-down to mid-loop	3.0E-09	5.4	88.9
LOCA (Inadvertent drains) - nondrained	2.8E-09	5.1	94.0
Loss CCS/SWS) - nondrained	1.4E-09	2.5	96.5
LOCA (Inadvertent drains) - drained	8.0E-10	1.5	98.0
LOOP - nondrained	5.4E-10	1.0	99.0
Loss RNS - nondrained	4.1E-10	0.7	99.7
LOCA (RNS pipe rupture) - nondrained	1.4E-10	0.3	100
TOTALS	5.5E-08	100	

Comparison of Shutdown Assessments

(Internal Events)

Event	AP600	Evolutionary PWR	NSAC-84	NUREG/CR-5015	Seabrook
Loss of Decay Heat Removal	3.7E-08	2.0E-07	1.3E-05	4.3E-05	2.6E-05
LOCA	3.8E-09	1.0E-07	1.8E-06	4.2E-06	7.8E-06
LOOP	1.1E-08	2.0E-07	1.3E-07	5.2E-06	2.6E-06
Other	3.0E-09	N/A	3.2E-06	N/A	4.8E-06
Total*	5.5E-08	5.0E-07	1.8E-05	5.2E-05	4.5E-05

* Totals are not exact due to rounding

Shutdown PRA Insights

- Shutdown risk less than at power
- Dominant shutdown risk due to loss of decay heat removal during drained conditions
- Features Important to Shutdown CDF Reduction
  - Passive safety systems back up normal decay heat removal functions
  - Passive IRWST injection has redundant and diverse flowpaths
  - LOOP coincident with shutdown is not significant
    - Passive IRWST injection does not require AC power
      - RNS, CCS train supported by diesel generators
  - Automatic RCS drain isolation

Key Shutdown Sensitivity Analyses

AP600

Sensitivity	New CDF	Comments
No credit for IRWST injection flowpaths (4 IRWST + 1 RNS path)	6.4E-04/yr.	IRWST injection flowpaths are very important to mitigate accidents at shutdown
Set all operator mitigation HEPs to 0.5	3.0E-06/yr.	CDF still at E-06 with very little credit for operator mitigative actions
Credit taken only for safety-related systems mitigation (focused PRA)	4.1E-07/yr.	The plant CDF can be maintained at the E-06/yr. range with only safety systems. Credit taken only for safety-related system mitigation.

CONCLUSION

- Performed a detailed PRA of the AP600 design.
  - At-power and shutdown
- AP600 design meets both the NRC and industry core damage frequency goals.
- Demonstrates a significant core damage frequency improvement over current operating plants.
- Iterative PRA application has allowed design enhancements that address the significant PRA issues.