Official Transcript of Proceedings ACRST-3405

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards Reliability and Probability Risk Assessment Subcommittee

Docket Number: (n/a)

PROCESS USING ADAMS
TEMPLATE: ACRS/ACNW-005

SUNSI REVIEW COMPLETE

Location: Rockville, Maryland

Date: Tuesday, October 2, 2007

Work Order No.: NRC-1798

Pages 1-171

ORIGINAL

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

TR04

DISCLAIMER

UNITED STATES NUCLEAR REGULATORY COMMISSION'S

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

October 2, 2007

The contents of this transcript of the proceeding of the United States Nuclear Regulatory Commission Advisory Committee on Reactor Safeguards, taken on October 2, 2007, 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

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS (ACRS)

SUBCOMMITTEE ON RELIABILITY AND PROBABILISTIC RISK ASSESSMENT

+ + + + +

TUESDAY,

OCTOBER 2, 2007

+ + + + +

The meeting was convened in Room T-2B3 of Two White Flint North, 11545 Rockville Pike, Rockville, Maryland, at 8:30 a.m., Dr. George Apostolakis, Chairman, presiding.

<u>MEMBERS PRESENT:</u>

GEORGE E. APOSTOLAKIS	Chairman
OTTO L. MAYNARD	ACRS Member
DENNIS C. BLEY	ACRS Member
JOHN W. STETKAR	ACRS Member
WILLIAM J. SHACK	ACRS Member
SAID ABDEL-KHALIK	ACRS Member
DANA A. POWERS	ACRS Member

ALSO PRESENT:

SERGIO GUARRO
TOM KRESS
STEVE EPSTEIN
KEN CANAVAN
ANTOINE RAUZY
MARK REINHARDT

TABLE OF CONTENTS

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

8:31 a.m.

CHAIR APOSTOLAKIS: The meeting will now come to order. This is a meeting of the Reliability and Probability Risk Assessment Subcommittee of the ACRS.

I am George Apostolakis, Chairman of the Subcommittee.

Members in attendance are Said Abdel-Khalik, Dennis Bley, Otto Maynard, Dana Powers, John Stetkar and Bill Shack.

Also in attendance are ACRS consultants Sergio Guarro and Tom Kress.

The purpose of this meeting is to discuss the next generation PSA software and modern representation standards.

The Subcommittee will gather information, analyze relevant issues and facts and formulate proposed positions and actions as appropriate for deliberation by the full Committee.

Dr. Hossein Nourbakhsh was the designated Federal Official 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 September 21, 2007.

A transcript of the meeting is being kept and will be made available as stated in the *Federal Register* notice. It is requested the speakers first identify themselves, use one of the microphones 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 regarding today's meeting.

We will now proceed with the meeting, and I call up Mr. Steve Epstein of ABC Consulting to begin.

DR. EPSTEIN: Good morning. My name is Steve Epstein. I'm from ABS Consulting, but also I'm a member of Open PSA, which is a small group of PSA researchers that just began.

We don't have a lot of time. I have a lot of material to cover. Some of the things I'll go through quickly. Some of the mathematical demonstrations I won't spend too much time on. However, after the meeting or perhaps later with a cup of coffee I can go over some of the calculations in detail.

CHAIR APOSTOLAKIS: Please introduce

your colleagues.

DR. EPSTEIN: Oh, my colleagues. This is Dr. Antoine Rauzy from the Institut de Mathematique de Luminy in Marsaeilles. And also --

CHAIR APOSTOLAKIS: Is that in France?

DR. EPSTEIN: Yes. And in the audience Dr. Olivier Nushaumer, who is also on the Board of the Open PSA. A researcher from KKL in Switzerland.

The purpose of this meeting, Dr. Apostolakis sent us a letter asking us to cover these issues. I hope we can. I'll go back to at the end and if I haven't, I'll try to make things clearer.

Twenty-one years ago during the heady days of the IPP and the PRA risk software boldly stepped out where no risk software had gone before to the PC. Before that it had all been on mainframes. And here's a group photo of some of the old people. All when we began the IPEs, we were very excited. And in this time over the 21 years our abilities and the demands of PSA have completely grown. Now we have safety monitors, model size is of a size that no one ever imagined when they started thinking of fault trees and event trees.

We want to do on run maintenance. We

want to do risk-informed applications. There's lots of work now being done in seismic analysis, fire analysis, BOP analysis balance of plant, flood analysis which are really taxing the way that we have been doing PSA from our viewpoint.

And we've made strides in computer software as well. Of course, all of you have heard of the famous BDD, which is really just one of the directed acyclic the graph. Here's a small one from Dr. Nushaumer's thesis. It only has 37,000 nodes but it does encode ten to the ninth cutsets which is a lot of cutsets, hard to review.

And we've had coding breakthroughs. Just recently Dr. Nusbaumer solved a very large full tree model of the Leibstadt PSA. He solved it exactly with no truncation using BDD. And his Ph.D thesis you can buy from him afterwards for about .50 cents.

CHAIR APOSTOLAKIS: Are you going to explain, you know not all members are familiar with things like truncation and all that.

DR. EPSTEIN: I hope we can.

CHAIR APOSTOLAKIS: You will, or you are doing it now?

DR. EPSTEIN: I hope we will, yes.

CHAIR APOSTOLAKIS: I'm just informing you that you shouldn't assume that the jargon of PSA is known to everyone.

DR. EPSTEIN: I will do my best.

CHAIR APOSTOLAKIS: Okay.

DR. EPSTEIN: Also we have new ways of visually visualizing data. This is an example of being able to visualize data that was created in Stockholm at the University of Polinska. It's an exciting new way of visualizing many, many axes of data all at the same time moving across the screen.

And because of these successes we've heard lots of rumblings and rumors about creating PRA software of the next generation. We, however, a small group of computer scientists who have been working in this, and mathematicians, we became focused on some other key issues not necessarily writing new software per se and new engines. And I would like to go over some of these.

The little checkmarks I click and they'll show me a deeper presentation, but they're not lined up right.

Let me start just by going over them.

Quality assurance by comparison. Right now it's very difficult to take models done in two different softwares: A model done in one software and move it to another to check its results and to understand it better.

The assurance of the model completeness as quantified. Right now because of the size of the models it is necessary to truncate, to throw away large parts of the problem whose probability is quite low. However, when doing this it raises a whole other set of issues that I'll talk more about in depth.

Peer review of algorithms. Right now when one of us decides we're going to write a new program or have a new method, we do not go out and ask others in our group to check it. And we feel that this is a grave mistake.

Portability of the models between different softwares. As I said, with quality assurance by comparison, there's no way it can be easily done at this moment.

CHAIR APOSTOLAKIS: What exactly do you mean "by comparing models?" Can't I say that what I really care about is the top 100 minimal cutsets?

DR. EPSTEIN: Yes, I think so. But let me --

CHAIR APOSTOLAKIS: And I can look at

it--

DR. EPSTEIN: -- show you what I mean here.

Quality assurance by comparison. Are the minimal cutsets results a good result? So what we did, which we took a full PSA model from loss off offsite power of Japanese nuclear plant. There were 181 sequences, 171 which have led to core damage. Some of them, their biggest sequences here were not big by American standards. 1128 gates and 1700 basic events per sequence. More details are available in our paper published in 2004.

What we did was we compared the BDD solution to the minimum cutset solution that was done with RiskSpectrum. And here are our results.

The minimum cutset solution was less than the BDD solution 53 times. And those are the number of sequences in which there were under estimation. Over estimations there were 128 that were over estimated. And the order of the sequences was not the same as the order of the sequences using minimum cutsets.

So what this showed us was with success branches, which most minimum cutset codes do not handle well, there was a big difference in sequence ranking and in sequence value.

Now there are also issues with importance, but I'll get to those later. This is what we discovered.

CHAIR APOSTOLAKIS: So let me see if I understand the table. Let's take that row that says between 50 percent and 100 percent.

DR. EPSTEIN: This one here?

CHAIR APOSTOLAKIS: Yes. So you say that you found 9 sequences in which the probability of each sequence, right?

DR. EPSTEIN: Yes, each of the nine sequences.

CHAIR APOSTOLAKIS: Of the each of the line sequences was 50 percent to 100 percent lower?

DR. EPSTEIN: Yes, then the true exact value of the sequence.

CHAIR APOSTOLAKIS: And you assumed that the B

CHAIR APOSTOLAKIS:

CHAIR APOSTOLAKIS: BDD solution is the true exact value?

DR. EPSTEIN: We're hoping that it is. Mathematically it should be. And the proofs and the benchmarks of the computer code show it to be correct.

CHAIR APOSTOLAKIS: And you will tell us why, I assume?

DR. EPSTEIN: Why what?

CHAIR APOSTOLAKIS: Why this happens?

DR. EPSTEIN: You know, we're not sure why this happens. What we're finding, and I don't want to get too much off this, but what we're finding is that the solution accuracy is highly dependent upon the model. Some models have terrible importance results when compared minimum cutsets to BDD. Other models have no difference in the importance. And we have some ideas of why this happens. But they're really not for talking or publication at the moment.

CHAIR APOSTOLAKIS: But these results, as I understand it, have nothing to do with truncation.

DR. EPSTEIN: Yes, some of them for sure. And also, that there aren't any success branches.

Sure, the minimum cutsets was truncated. Absolutely.

CHAIR APOSTOLAKIS: How can that be? I mean if I have sequence --

MEMBER STETKAR: George?

CHAIR APOSTOLAKIS: Yes, John?

MEMBER STETKAR: Let me.

I'm going to hold you to details because you skipped over something pretty quick.

DR. EPSTEIN: Yes.

MEMBER STETKAR: You mentioned this comparison was done comparing to RiskSpectrum?

DR. EPSTEIN: Right.

MEMBER STETKAR: Was it done with the minimum cutoff internally generated in RiskSpectrum?

DR. EPSTEIN: No, no, no, no, no.

MEMBER STETKAR: Oh, okay. So that would make a big difference in the top part of that table.

DR. EPSTEIN: No. This is with absolute cutoff.

MEMBER STETKAR: This is a lot of detail to some of the members and anybody in the audience who doesn't know RiskSpectrum.

DR. EPSTEIN: No. This is absolute cutoff.

MEMBER STETKAR: Which absolute cutoff in RiskSpectrum, though? User --

DR. EPSTEIN: Not the one that changes.

MEMBER STETKAR: Not the one that changes?

DR. EPSTEIN: Right.

MEMBER STETKAR: The internally generated cutoff?

DR. EPSTEIN: Ah, yes, yes.

MEMBER STETKAR: What I call the internally generated cutoff.

DR. EPSTEIN: Oh, okay, yes.

MEMBER STETKAR: Okay.

DR. EPSTEIN: The absolute cutoff.

CHAIR APOSTOLAKIS: Let's see if --

MEMBER STETKAR: Then it is truncation.

CHAIR APOSTOLAKIS: -- the rest of us can understand a little bit. The events that constitute a sequence are the same in both solutions?

DR. EPSTEIN: Yes. The top events in the sequence. But --

CHAIR APOSTOLAKIS: No, no, no. You're talking about individual sequences here.

DR. EPSTEIN: Okay. Yes.

CHAIR APOSTOLAKIS: All the events are the same?

DR. EPSTEIN: That's right. The basic

events are the same.

CHAIR APOSTOLAKIS: Right. It has A,B,C,D?

DR. EPSTEIN: Right.

CHAIR APOSTOLAKIS: So where is the cutoff when I do, say, the RiskSpectrum?

DR. EPSTEIN: Maybe this was ten to the eleven, ten to the negative 12.

MEMBER STETKAR: It's a numerical cutoff that throws away cutsets as it --

CHAIR APOSTOLAKIS: But you're throwing in--it's a minimal cutset itself. You're not throwing away cutsets. So that's what I don't understand. Where is the cutoff?

MEMBER STETKAR: They are throwing away. They do throw away cutsets.

DR. EPSTEIN: Well, presumed cutsets.

MEMBER STETKAR: Presumed minimal. I mean it's --

MEMBER POWERS: May I ask a question, because I'm really having a little trouble following this? Would you define what you're calling a sequence in terms of the minimal cutsets that are part of that sequence?

DR. EPSTEIN: Yes.

CHAIR APOSTOLAKIS: Oh.

DR. EPSTEIN: I'm sorry, George. Yes.

CHAIR APOSTOLAKIS: So it's not just the five events that constitute --

DR. EPSTEIN: No, no, no.

CHAIR APOSTOLAKIS: Each event has a fault tree hung in there?

DR. EPSTEIN: Each sequence has a fault tree, for example, yes.

CHAIR APOSTOLAKIS: Each event in the sequence has a fault -- oh.

MEMBER BLEY: But not all have the minimal cutsets?

DR. EPSTEIN: No.

CHAIR APOSTOLAKIS: There is not minimal cutsets.

MR. GUARRO: You said something before I would like to have a clarification on.

DR. EPSTEIN: Okay.

MR. GUARRO: You said that the difference in importance measure, et cetera, et cetera you get from -- depends on the model. Certain models agree with the BDD, certain models do not.

When you say "models," you mean the same way of representing -- I mean different ways of representing the same events and sequences?

DR. EPSTEIN: No, no. The same model. The same physical fault trees in basic events if they're physical.

MR. GUARRO: Yes, but you say that different models --

DR. EPSTEIN: By different organization.

MR. GUARRO: So you're modeling different sequences and some come out good and some come out bad, is that what you said?

DR. EPSTEIN: Sergio, I really don't want to go into that too much right now. It's a new thing that we're just finding. I was just answering a question from --

MEMBER BLEY: I'm sorry. You brought this up a couple of times.

DR. EPSTEIN: Okay.

MEMBER BLEY: When you speak of a model--

DR. EPSTEIN: Right.

MEMBER BLEY: -- you're speaking of what we used to call a structure function; the actual fault tree where the angates --

DR. EPSTEIN: Yes. That's right.

MEMBER BLEY: And when you say a different model I think you're meaning one that has maybe a lot of angates in a certain area or not?

DR. EPSTEIN: No.

MEMBER BLEY: That's not what you mean by a different model?

DR. EPSTEIN: Okay. When I mean a different model, I mean there's a model from Power Plant A, there's a model from Power Plant B. Those are two different models.

MEMBER BLEY: Of not even the same --

DR. EPSTEIN: Of not even the same --

MEMBER BLEY: Okay. That's what I was trying to understand.

DR. EPSTEIN: Okay.

MEMBER BLEY: I'm still -- but the thing that makes them different is the structure?

DR. EPSTEIN: That's right. The way the modeler made a structure.

MEMBER BLEY: Not the model? It's the structure. It's where the gates and how many --

DR. EPSTEIN: Right. It's how he represented it.

MEMBER BLEY: And in what way? It's the structure function.

DR. EPSTEIN: That's right.

MEMBER BLEY: That's important.

DR. EPSTEIN: Okay.

MEMBER STETKAR: Just when you say you're changing the frequencies by a 100 to 300 percent, are we talking about frequencies that are a couple of times the truncation frequency? What's the frequency of the sequence that I'm missing by 300 percent compared to the truncation frequency?

DR. EPSTEIN: You know, I don't have it right here. I have the paper. I can give it to you. Wherever --

MEMBER STETKAR: I mean, are those 15 very, very low frequency sequences that I'm effecting no dramatically?

DR. EPSTEIN: You know, I just can't remember. It was three years ago. And we could go over the paper together. But this was published in the journal that Dr. Apostolakis is an editor of. And everything is very detailed there.

CHAIR APOSTOLAKIS: So the truth here is that you're talking about accident sequences?

DR. EPSTEIN: Yes.

CHAIR APOSTOLAKIS: And then each event typically has a fault tree hanging there and there was a cutoff frequency that was used --

DR. EPSTEIN: Yes.

CHAIR APOSTOLAKIS: Okay. Good. Now I understand.

DR. EPSTEIN: Okay.

CHAIR APOSTOLAKIS: You're overestimating, too? I mean your minimal cutsets overestimate?

DR. EPSTEIN: Yes. Yes. That can happen.

CHAIR APOSTOLAKIS: And you are investigating why?

DR. EPSTEIN: One of the reasons that it overestimates is because where event approximation. One of the reasons it underestimates is because of truncation.

CHAIR APOSTOLAKIS: I see. And sometimes--

DR. EPSTEIN: Sometimes it gets mixed up and the order of which are important sequences completely changes.

CHAIR APOSTOLAKIS: Okay.

DR. EPSTEIN: Yes. It's --

CHAIR APOSTOLAKIS: Do all the codes now that people use employ the rare event approximation?

DR. EPSTEIN: Well, all the min. cut

upper bound. But sometimes the min. cut upper bound is employed incorrectly when there is negation or high frequencies in which the min. cut upper bound should never be applied.

CHAIR APOSTOLAKIS: Okay.

DR. EPSTEIN: We also think that in our studies of looking at the models the clarity of the model, especially models that have been done over several years by many different analysts have a certain lack of clarity.

Formal verification of calculation methods. Many times people ask us, and we'll show you examples of this, to review a new idea they have for calculation. And we find that they don't go into detail trying to prove that this method is correct.

We also have problems with the way uncertainty calculations and importance calculations are done. And we have some results here -- well, I'll show you right now from Dr. Duflot's recent study of importance measures in chaos.

Last year's paper look at RAW, risk achievement worth, as one of the measures. But all of the measures suffer from this same problem because they use here a conditional probability. And all importance measures are built on conditional probabilities. They are calculated from the minimum cutsets generated for S, but with any sufficiently large and interesting system, the cutsets are truncated. And I'll show you a very simple example of what this can do.

Here we have a very simple system. It only has tow cutsets; A and P and B and Q. And let's say that A was 1E negative 3 and P was 1E negative 9. Truncation limit is negative 13. So this one gets thrown away. So there's no recalculation of the minimum cutset when we do a calculation that given A has failed, and given A is a success. And when we get through this we see that the RAW for B with respect to the system is 1 and the RAW for A is 1 negative 3. However, if we had regenerated the cutsets, then the RAW of B has a value that's actually interesting.

Now this can happen in a real PRA when a given basic event has maybe hundreds of different combinations with other basic events and it falls bellow a cutoff.

Now what Nicolov found also is that a given truncation when it may be good for calculating core damage frequency, but the order and the value of importance measures may be chaotic at the same truncation value. His Ph.D. thesis shows this using one of the French reference PRAs, which is like a SPAR model.

CHAIR APOSTOLAKIS: What's chaotic in this context?

DR. EPSTEIN: At one truncation level that's a negative -- yes. But at each truncation level the values change and the order changes. So just because you're getting closure, perhaps, with core damage, that doesn't mean you're getting the same thing. And it's because of the conditional probability being so high.

For cutsets we are not using conditions.

Here's an interesting thing. Peer review of algorithms. Last year after PSAM a development group from Europe asked me to review this idea. Generate the minimum cutsets with truncation, create a BDD from the minimum cutsets. Calculate the exact value of the cutsets by making a BDD. They felt that this would be better because they would have the exact value of the cutsets.

This is called CBDDs. CBDD they call it.

Well, let's take a look at their idea.

Let's say we have all the minimum

cutsets. Of course, that's just a representation of the fault tree with no redundant paths.

We know for sure that if the probabilities are low enough, that the relevant approximation, the min. cut upper bound and the BDD will all be ordered like this: The BDD will be the smallest and the rare event will be the largest, min. cut upper bound will be in the middle. This is because all three of them -- excuse me -- are in a sense are Sylvester-Poincarè expansions and they have to be in this order.

But we truncate, we discharge the minimal cutsets because they fall below a probability. So we have a set of retained cutsets and we have all of the cutsets. So our question is when we're calculating the retained cutsets how do these measures match up against these? Who is the best estimator?

Well, if there's no truncation, we know that they're the same. However, with just a teeny weeny bit of truncation, the retained cutset measure start slipping down to the left. In fact, you're guaranteed that the BDD solution of the cutsets is the worst answer you could have. It's absolutely the least conservative. And as it grows, perhaps the mim. cut upper bound is the best estimator. And as it really grows the rare event approximation falls below the true value of the system. With any large system we don't the exact value, so we don't know which case we have. So in no way can this method be useful to us.

The Seabrook example, the service water system. There's a 101 cutsets which are retained. When they did the rare event approximation, that's what they got. The true binary decision diagram is this. The rare event is an underestimation.

CHAIR APOSTOLAKIS: So the difference is what?

DR. EPSTEIN: A factor of ten.

Here is a small backup cooling system that I made just to get a good sense of the idea. You can see that with the truncation these are well-ordered. However, the true value of the system is this and the rare event approximately is the best estimator.

In that way of thinking whoever thought of the rare event approximation to use for PRA wasn't so much of an idiot. Because with all the things that are changing; high/low, high/low this may absorb. We have seen that we can generate -- we have BDD'ed all the sequences, use minimum cutsets with all the sequence. The sequence values and rankings are completely different but the core damage is the same. It's like your mother; right for the wrong reasons but it works.

So the important thing here is to know what problem you're trying to solve. We're not interested in the exact value of the retained cutsets. We're interested in the exact value of the system and the best approximation of that value.

CHAIR APOSTOLAKIS: Is this happening because the rare event approximation is applied to individual cutsets but ignores how many of those you have?

DR. EPSTEIN: Oh, sure. That's one reason for sure. But what I want to say is that willy-nilly to invent new methods without peer review is not a good idea. RISKMAN hasn't ever been peer reviewed. I'm embarrassed by that, my own code. Nobody's ever, ever looked at it and said this is right, this is wrong. It's probably a big mistake.

CHAIR APOSTOLAKIS: Well, that's an interesting statement because many times and in various context in this room we've asked the Staff whether a model whose results they accept has been peer reviewed. And the answer is we don't peer review everything.

DR. EPSTEIN: Well, I'm talking just about the program. I'm talking about the software and the algorithms.

CHAIR APOSTOLAKIS: I know.

DR. EPSTEIN: I don't know so much about PRA outside of my area of work. I really don't. I'm sorry.

CHAIR APOSTOLAKIS: And the human reliability models of EPRI have never been reviewed by the Staff, yet we accept the results.

MEMBER BLEY: That's correct.

CHAIR APOSTOLAKIS: That's correct.

MEMBER POWERS: Staff review and peer review I think are two different things.

DR. EPSTEIN: It probably is.

CHAIR APOSTOLAKIS: I would prefer to have a Staff review, though.

MEMBER POWERS: Oh, yes. Me, too.

CHAIR APOSTOLAKIS: Yes. The Staff review is usually, many times it includes a peer review.

MEMBER POWERS: It could well, but it is

clearly a large order thing. I mean, peer review is here portrayed as some great thing and it comes under tremendous fire in other contexts.

CHAIR APOSTOLAKIS: Why?

MEMBER POWERS: Because peers are biased.

CHAIR APOSTOLAKIS: Well, I mean you're opening up a new area, but --

DR. EPSTEIN: Okay. But also --

CHAIR APOSTOLAKIS: But the issue of review is the general issue you are addressing?

DR. EPSTEIN: Yes. Here's another interesting study, what I call assurance of model completeness as quantified. What you see is not what you get. Here is the model. It was a full PSA from loss of offsite power at an American power plant. A 136 sequences, 95 led to core damage. Core damage was modeled as one large fault tree. You can see the other kinds of measures.

What we did? What we did was we choose the largest core damage sequence and we pruned this huge fault tree to only include this sequence. We calculated all initiators simultaneously and we obtained the cutsets generated by the fault tree linking engine on the side. Then we generated the cutsets with ZBDD, which is a different algorithm than the Mockus algorithm which is used in most cutset codes. And we generated it going down the tree at different levels until we have the same cutsets.

We found 462 cutsets, the same as with the fault tree linking tool. But the depth of the solution was only to level 4. Remember this had a 133 levels deep this fault tree. A huge fault tree. However, only to level 4 had anything to do with the solution. Ninety-five percent of the modeled gates were not used. Ninety-six percent of the modeled basic events weren't used, though we quantified the fault tree to level 4 and we created a BDD. We ignored success branches, so we'd be comparing apples and apples.

We found that the minimum cutset rare event quantified frequency was seven eight negative six, but the BDD quantified frequency was four E negative six. It's a big difference considering we did not consider success branches.

We calculated the truncation upper bound, in other words what is the highest possible value of all the cutsets you've thrown away and the truncation upper bound is larger than the BDD solution.

And we're pretty sure this drove Shakespeare to say the fault is not in the tree, my dear Horatio, but in the models themselves. And this is what I meant by different models compute in different ways.

Correct uncertainty. I did that.

Ah. Formal verification of calculation methods. Two months ago I was approached by a develop group from Asia and they asked Dr. Rauzy, Dr. Nusbaumer and I to please take a look at what they called the destructive truth table method with truncation to tell us if we could come up with any counter examples.

This is pretty complex. I only want to go over it briefly. It's tangential to the main point. But if anyone is really interested, I'll go over this one in depth.

So much correspondence in examples. This is what we discovered that these researchers were telling us they wanted to do. They wanted to start at the bottom of the tree with an empty truth table. At each gate add inputs to the truth table, fill out a full truth table, collapse the gates. And the code was that the top event calculated would always be less than the exact value which would always be less than an upper bound. However, with one example they sent to us, I actually calculated the example and then I built a BDD to compare it, and it was wrong.

In this example P-exact lies outside the upper bound. Then Antoine, he made another one with the same example by just making a negation. And he got the exact value to drop below the two bounds.

Why does it happen? Well, mathematically this is why it does happen. And, of course, it's possible to detect this case, these two cases. It's very difficult. One has to follow what I call the gate collapse rule, which is something that Antoine wrote about in 2000 in one of his first BDD papers. It says that you can't do this collapsing/expanding thing unless all other gates would share at least in putter in the truth table. Gate G has all inputs resolved and all other gates which share inputs fulfilled these two.

It ends up mathematically that this is exactly the same problem as solving a BDD so that if the truth table method could work, it would mean the BDD could work. And right now we don't know how to make either of those two work efficiently.

We don't present this to trash anybody's algorithm. But what surprised me that there has never been an attempt to prove that this algorithm was correct or to search out counter examples. And for 40 years our discipline of computer science has had methods to demonstrate formally algorithm correctness. Floyd in '67, Hoare in '69, the Scott & Strachey Denotational Semantics, a landmark in '72. We've already used these for the help of what we're all doing here, and maybe this is the first time software engineers and mathematicians have said, "Look, we can help. We see problems." To us, this is one of them.

CHAIR APOSTOLAKIS: Is that the same as PRA review?

DR. EPSTEIN: I don't know. I've done a PRA review. George, you know that what we've always been asked to do is to build tools for everyone. But nobody has ever asked us to join in --

CHAIR APOSTOLAKIS: But if I gave you Saphire and we asked you to review it as a peer --

DR. EPSTEIN: Oh, yes.

CHAIR APOSTOLAKIS: You're certainly a peer? You will have biases, but I will accept that.

DR. EPSTEIN: Well, you know --

CHAIR APOSTOLAKIS: I'll give that. Would you go and use these methods to check Saphire's correctness --

DR. EPSTEIN: Oh, absolutely. Absolutely.

CHAIR APOSTOLAKIS: -- or whatever would--

DR. EPSTEIN: Sure. We'd sit down within quantum loops and build loop invariance and make sure that these loop invariance would hold. That's the things we do.

CHAIR APOSTOLAKIS: But do these methods, though, check the self-consistency of the code? They can't really check whether it's accurate, do they?

DR. EPSTEIN: To completely do a proof on a whole code is beyond anybody's ability right now.

CHAIR APOSTOLAKIS: So a PI review much more?

DR. EPSTEIN: What is very important, though, is to look at the key algorithms and the way they're encoded to see if we can show formally that they're correct or to quickly make counter examples to show that they're not. In that we're lucky. If we do a counter example we're home. We don't have to do anymore work.

This is something that Antoine always says to me. He says "We must concern ourselves our accuracy and proof." And I have to say there is very little that he does that does not contain this.

And speed isn't everything. We all want our solutions really fast, people go after speed. But good cooking takes the time it takes. You can make things go fast necessarily and get right answers.

CHAIR APOSTOLAKIS: But, Steve, accuracy has to be looked at in the context of PRA. I mean if you by accuracy you mean the exact result is 3.2 ten to the minus five and somebody finds three, we don't care.

DR. EPSTEIN: No, no. I mean accuracy of the code. I mean the accuracy of the code. You don't want a code that on the same inputs gives you negative four one time and negative ten the next. Accuracy of the code.

CHAIR APOSTOLAKIS: Has accuracy of model?

DR. EPSTEIN: Huh?

CHAIR APOSTOLAKIS: Okay. Okay.

DR. EPSTEIN: Yes. I'm not talking about approximations or heuristics, though heuristics are rules of thumb to be able to make good methods, they also should be studied for their limits; when they're efficient and when they can't be used. There are some people that don't know minimum upper cut bound, which is a heuristic, should not be used with probabilities that are large. The answer will be wrong, and people don't know that.

So what we think is really needed before we develop new methods, new software, new user interfaces is take a look at what we have right now and to realize there's no free lunch. Model size is complex. Model is huge. The problems are mathematically extraordinarily complex. And they all boil down and are isomorphic really to truth table solutions. And we know how hard those are.

MEMBER BLEY: Steve?

DR. EPSTEIN: Yes?

MEMBER BLEY: Would it be fair to rephrase what you just said, as you see the first step, and understanding what these various codes do well, what they do poorly and when?

DR. EPSTEIN: Yes, yes, yes.

MEMBER BLEY: That's what you're after?

DR. EPSTEIN: Yes, that's a great first step. That's how we started this in PSA, and I'll try to get there. So we think that before we get in the next generation, no matter how nice this vision is, no matter how much we want it and to avoid the dreaded second systems effect -- whenever you have great first systems everyone gets these wonderful ideas how we can make everything new and fit together and do everything for everybody, and they always fail. We don't want that.

What we want is a PSA software architecture. Clean like a Frank Lloyd Wright house that's open, not owned my any one company, that's extensible, that's adaptable to new ideas that can be extended by new discoveries and separates the data, what we call the model, and the software.

This last one has been the watchword of good computer science now since structure programming began in the '70s. Separate the data and the code. And this way we could allow the greatest interconnectivity and portability between--

CHAIR APOSTOLAKIS: Has this code been peer reviewed?

DR. EPSTEIN: This is not my computer.

MEMBER BLEY: All the computers do it. And there are peer reviews on that.

DR. EPSTEIN: I always turn all those things off on my computer.

You know if a car worked like a computer, so you'd be driving to work and it'd slow down and suddenly stop and you'd run around it a couple of times, clap your hands, do this with the key and it'd restart. Talk about unreliability.

MEMBER BLEY: Well, can you say some more about where you're headed while this things--

DR. EPSTEIN: Yes. Where I'm headed is right here. We are proposing a PSA software architecture. The foundation is a standard for representing a PSA model, therefore facilitating independence between model representations in software. Each risk application would generate a model in this standard from whatever its own internal representation would be.

It'll be fine.

MEMBER BLEY: It's okay. It's fine. We can read. We can read it. That's fine.

DR. EPSTEIN: Okay. Viewers and calculation engines could interface with these models via the standard representation. Let me show what I mean like a true engineer.

This is my Lego model of the PRA architecture. First the foundation. The standard representation format, what we call surf, catch the wave. This is what we think has to be in place first. And then we assemble the risk applications and the data. So here we have risk applications like CAFTA, like RISKMAN, safety monitors, PSA viewers and reviewers that don't do calculation, but just like they look. Industry data, calculation engines. Next generation tools. They're all here and then you can just build upon the foundation.

For example, here you could use RiskSpectrum as the user interface, FTRex is the engine. And what if the NRC wanted to make their own PRA reviewer? A piece of software that went over any model and checked certain things out? The standard format could take that.

Here's another one. Industry common data. The RSAT engine from RiskSpectrum, the CAFTA user interface and maybe even RISKMAN right in there, or a full blown system where you're using RiskSpectrum, FTRex, RDAT from, RSAT engine from RiskSpectrum, RISKMAN, new generation tool like Luke Tree Walker; altogether, all interconnected through this standard representation format. This isn't just imagination. We've done research and prototypes in this and we've been using XML as the representation format, which is a public domain. It's called Extensible Markup Language. It's very easy to use this to incorporate data. It's owned by no one. It's well agreed upon in the computing world right now and many next generation applications in other areas including the World Wide Web have been using this.

Here's an example. One, three different fault tree linking models from three different U.S. organization. We hook CAFTA, FTRex, the BDD engine Aralia up and MS Excel, which also reads and writes XML to be able to sort and mix and match.

We did another one with a Japanese core damage model, same kind of idea.

We investigated the SPAR model using this.

CHAIR APOSTOLAKIS: And what do you conclude?

DR. EPSTEIN: We concluded that the sequences were different, but the core damage was the same.

CHAIR APOSTOLAKIS: The sequences were

different from what?

DR. EPSTEIN: The sequences which were generated by Saphire where in a different order than the sequences generated by BDD and some of the sequences, a lot of them, have different values. Sometimes high, sometimes low. But when you added the whole thing together to get core damage, it was so close it might as well have been the same.

CHAIR APOSTOLAKIS: So it's the prioritization that would be effected?

DR. EPSTEIN: Well, we're pretty sure. We didn't important studies. We didn't do a lot of different studies. But there's no mathematical reason why the rare event in BDD should have come out the same. It was fortuitous. But a good estimator.

CHAIR APOSTOLAKIS: But you showed us earlier if one could run the service water system that you showed earlier --

DR. EPSTEIN: Yes.

CHAIR APOSTOLAKIS: The 100,000 cutsets on a SPAR -- I mean on Saphire.

DR. EPSTEIN: Yes.

CHAIR APOSTOLAKIS: And run it with BDD, would you still expect the --

DR. EPSTEIN: No. Because the SWS system has no sequences. It's just a system. So there aren't sequences involved.

Also, it's modeled in a different way and by a different person. It seems -- and we've looked maybe at 50 or 60 models now pretty closely. And the ability to calculate well completely depends on the model.

We also did a sanity check on the Mars exploration rover for NASA. This information I cannot give out. I'm just now allowed to. However, there were big differences.

So what have we been doing to bring these benefits into existence? What is our main thrust? Well, there were enough of us talking on the telephone and visiting each other and doing some projects together, we got this idea of open -- well, it wasn't yet Open PSA. We said let's get a bunch of people together and let's talk about this.

And Dr. Kluegel from Goesgen, he offered to host the meeting. And we did this in June.

And from this we created the Open PSA Initiative. And these are the names of the companies at that first meeting who wanted to joint. We don't know how we're going to make this organization, under what blanket it falls, but wanting to work together to do these things.

And we wrote a statement to purpose and we created a website to show our ideas. And this is really the heart of what I want to say. We want to provide an open and transparent public forum to disseminate information, independently review new ideas and spread the word. We want to emphasize an openness, which is not always by any company interest or political interest and worldwide. And we believe this openness will lead to methods in software with a higher quality and lead to better understanding of PSA models, encourage peer review and allow transportability. That's what we think we as mathematicians and computer scientists involved in this assessment can do. This is how we can make things better.

And we made our first working group. We got the people who were really interested in making a standard, we got them together. We had a meeting at ABS. And Antoine will later present what we did there.

And then Ken Canavan kindly has offered to have another workshop in this area, which will be tomorrow at the NEI.

We approached ASME to see if they were interested in our work in standards and perhaps wanted to incorporate it with their work. And we wanted to create an open standards working group which had Open PSA members and ASME members and anybody else who had a good mind who wanted to engage in this.

What can we do now? Well, here's an example test case. Arizona Power and Light uses RiskSpectrum. Most other models in this country are CAFTA models. The NRC would like to review both models easily with Saphire. So, let's create a prototype representation. Let's create a model closure. In other words, everything you need in the model to be able to calculate and let's attempt to exchange these models using the format, see what happens.

This can't be done without experimentation. This is science.

And how can you? Well, we're hoping that the individuals here that are listening to us, some of you may get excited about this idea. You want to support it. What we're seeing right now is that the Open PSA group would be the guardians of a model of a standard format. It would be independent from any one company.

You know, my bosses are croaking about this, but I told them in the beginning when they allotted time and money to pursue this, I said "What we discovered here is not owned by ABS. Not at all." We don't think any company that sells software should be in charge of this idea.

We should do quantification research and verification. We should measure degrees of standardization. We could provide a pool of professionals from all over the world who can do software testing, benchmarking, peer review. And we want to solicit people to be members. And maybe we'll even get companies to give us support a half year or so. We'd love to be able to have internships for university students to get a younger generation of PRA analysts who also understand the mathematics. And that's what we want to do. That's where we see the state of affairs right now.

We're making great strides in solving the whole problem. But we're not going to get there without working together.

CHAIR APOSTOLAKIS: You done?

DR. EPSTEIN: We're not going to arrive here if we don't all work together. And not isolated, and not worry about commercial interests. This is an important problem.

And that's what I have to say.

CHAIR APOSTOLAKIS: Okay. Thank you, Steve.

The next presentation is by Mr. Canavan of EPRI.

And we are ahead of schedule, so that's great.

MEMBER BLEY: Unusual.

CHAIR APOSTOLAKIS: You will correct that, Ken?

MR. CANAVAN: I'll try and take care of that for you. Actually, I should be brief.

Forgot my handouts, but your staff was kind enough to make some handouts for us. And you'll have something in front of you to read.

Well, good morning. My name is Ken Canavan and I'm from EPRI. Always a pleasure to talk to you, George, and your Subcommittee.

This morning I'm going to talk a little bit about the next generation of tools, and my intent was to give you a project status.

The next generation of tools is a project that began several years ago. EPRI is the purveyor of one of the software tools that's quite heavily used and sponsors a users group that has about 100 different participants both in the nuclear industry and the aerospace industry, and they provide CAFTA, in a more broader term the R&R workstation with CAFTA which is a fault tree modeling code along with all these supporting tools.

And I'm going to talk about we've been involved in a constant update process that we've been participating in to keep the tool current for all the users. And as part of that several years ago we began to develop what we call the next generation of tools. It doesn't so much change the way we do things, but to keep it current and to modify it.

And here are some of the issues. You've heard some of this from Dr. Epstein. I'll weigh in in a couple of different spots, providing a slightly different perspective on some things, but in general our fault tree and eventually approach to PRA modeling began way back in the '70s. Actually probably backwards even earlier than that. And over time models have increased in their scope and their complexity, which you've heard before. And our technology has, indeed, improved.

And while we realize the PRAs is really a simplified estimate of the risk, way to estimate the risk, most of those simplifications we've introduced. So things like truncation, rare event approximation, minimum cut upper bound are all items that we've used to make the calculation run quicker or run at all. Basically back in the '70s it was run at all.

We also have an issue now where we use the PRA a lot more. We do risk-informed applications. Those effect a lot of the decisions that we make at the plant. While they are only informed, we do want to be accurately informed. And therefore, the documentation becomes important. So there's another element of this where we look at the need to control the PRA model, its documentation, its applications and to demonstrate the questions that's asked most frequently in RAIs, which is does the PRA reflect the as-built and as-operated plan.

Well those are some of our issues. Some of our solutions are to start developing the next generation of tools which consists of new and improved items, three items that we've listed. One is the logic modeling. The second one is the quantification techniques which were discussed in the previous presentation by Dr. Epstein. And the last is a documentation techniques.

But the common elements of all the next generation of tools is they must be evolutionary as opposed to revolutionary. The reason why I say that is people die in revolutions, and we don't want that. People have a large stake in their models. Their models go way back. They have many, many millions of dollars invested. And to simply throw those out and to start again would be an issue. So we need to be evolutionary. We need to be able to build on those tools.

They need to be easy to develop, maintain, verify and review. Whatever we do must comport with that. The reason is manpower. It's just a simple matter, manpower.

And the last part is we will talk about some visual interfaces, some connectivity. It's necessary, but we're not going to talk about much about that here today.

So this is one vision of the next generation of tools. And several years ago EPRI began several projects to look at these three things: To improve modeling, improve quantification, improve documentation. And the areas were researched carefully and these items were picked. And in the case of modeling, we'll talk a little bit about declarative modeling. And I'll get into what declarative modeling is. And then we're going to talk a little bit about quantification techniques. And we'll talk a little bit about BDD, minimal cutset BDD and what we call direct probability calculation.

And then we'll talk a little bit about PRA documentation assistant, which is another tool that EPRI is developing for handling the documents.

So let's start by talking about declarative modeling. Declarative modeling allows attributes to be assigned to fault tree elements. As a matter of fact, it could be event tree elements, but we focus on fault tree elements. And those attributes include things like probability and frequency or conditional values, or settings under various conditions. So if you think about the fault tree model right now, it's a big logic model representation. In that we always associate with each basic event, we associate a value which usually is a frequency or a probability depending on the basic type so if it's initiator, it could actually be a frequency. But we can go beyond that now. If we can associate that piece of data with that element in the tree, perhaps we can associate other elements with that item in the tree, such as a note why the value is the value, or beyond a note perhaps we can say when you run an initiator like loss of offsite power, turn this part of the logic, turn these events to false, they can't occur. And by doing this and by assigning this act as a basic event when we run the loss of offsite power tree the model becomes a different: Things turn on, things turn off and the model starts looking different in structure. These are things that we can do, that we have done in some limited fashion now that we're working on.

CHAIR APOSTOLAKIS: But when a PRA is done now, surely people do that. Maybe it's not built into the code.

MR. CANAVAN: Right, it's not built into the code.

CHAIR APOSTOLAKIS: But they do that?

MR. CANAVAN: That's correct.

CHAIR APOSTOLAKIS: Okay.

MR. CANAVAN: We actually can go beyond that. We'll talk a little bit more about exactly what we can do. Because we can assign multiple probabilities to the same basic event. We'll talk a little bit more about that.

So those are the attributes. And then the elements are well we can do this with basic events, gates or initiating events or any element in the fault tree.

And as George pointed out, we do this in a basic level for just about everything. We assign a database value and we have a separate file for turning on and off events to make them look different. So these are in a bunch of different places. What declarative modeling is it starts pulling it together and it adds another level to it.

For example, these are some of the declarative modeling capabilities. The first one is to simplify recovery in post processing. So right now in post processing we might look at a cutset that has a number of human actions in it. We might say well those three human actions aren't really independent, they have dependencies in them. So let's go back and model it depending human action. We usually do that at the end and appended to the cutset. But declarative modeling would allow us to go back to the fault tree and put it in the tree where it belongs. So we could take a dependent event that's in a recovery file and we can move it back into the tree.

We can specify mutually exclusive events within the fault tree rather than at the end, as George pointed out. We normally do that. Usually exclusives are items like, for example, train 1 of a safety system and train 2 of the safety system are under maintenance at the same time. Those normally appear in cutsets and then are removed because the model doesn't recognize they can't occur together. But with declarative modeling we can say when one event has occurred, don't allow the second event to occur. So what this does is it sort of starts slimming down the model, slimming down the quantification to just what's important.

We can also now handle phased mission times with loss of offsite power recovery. If you can specify, for example, different values for the same event given how you arrive at that event in the fault tree, you can now start making the logic a little bit more compact. And as an example I'll give you seal LOCA. Seal LOCA is a curve with a different frequency and a different timing depending on if they lose cooling or if they lose injection, or if they lose both. And one of the things that we can do is since we can assign one event, such as seal failure, in the model with various probabilities depending on how it's arrived at in the tree, we now can specify several probabilities to the same basic event depending on how that even is arrived at.

MEMBER BLEY: Excuse me, Ken.

MR. CANAVAN: Yes.

MEMBER BLEY: I kind of get what you're talking about, but this idea of declarative modeling is this software you're talking about that edits the model or is it a new way to build the model?

MR. CANAVAN: This is a software that allows this capability to be entered into the model. So you would choose --

MEMBER BLEY: After you've --

MR. CANAVAN: Yes.

MEMBER BLEY: -- entered your fault tree and now you put in some kind of statements --

MR. CANAVAN: Yes.

MEMBER BLEY: -- that tell it to do these things?

MR. CANAVAN: Yes.

MEMBER BLEY: Okay.

MR. CANAVAN: If you're familiar with

the operations of some other codes, some other codes border on declarative modeling or use declarative statements.

What this allows you to do is it's a capability. It's a modeling capability and it adds a level of what I always look at as depth to the model. The model right now is two dimensional. You have a fault tree; what you see is what you get, it's on the piece of paper. Now it would have a sort of another dimension where you'd have to actually look at the attributes if there were attributes assigned. And look at those and see that you get depth to the model, which means you can model things like phased mission times much more accurately because you can assign the various probabilities at various times in the model. It can be time dependent, it could be phased, it could be any reason for assigning those values.

CHAIR APOSTOLAKIS: But let's pursue this a little bit.

MR. CANAVAN: Sure.

CHAIR APOSTOLAKIS: I mean if you do what Dennis said, then you still rely on the goodness of the analyst, right? I mean --

MR. CANAVAN: Yes.

CHAIR APOSTOLAKIS: -- you're building your model and then you put all these declarative statements in the code.

MR. CANAVAN: Yes.

CHAIR APOSTOLAKIS: I thought you were coming from another direction that by having those things in the -- is the code going to ask the analyst, you know, is this mutually exclusive then from something else and so on? Then I can see the value because it's helping the analyst. But if it's just a matter of me doing the fault tree and then putting it in the code and then putting statements, I'm not sure that's very valuable.

MR. CANAVAN: Actually, I think I'll bring you full circle.

CHAIR APOSTOLAKIS: If you got a prompt, I think that will be really --

MR. CANAVAN: Never even thought of that. That's a very interesting idea of putting in the prompts.

What we would do now is, for example, in the mutually exclusives we have a file of mutually exclusive events that appears at the end of the tree. We would now be able to take that and put it into the tree. And then later if you wanted to see it back as a table, it could put it back as a table. Literally, it's a toggle switch in the computer that says I want to import these things into the tree.

What it does in that particular case it would make the quantification more accurate because those events wouldn't appear in the results. But it would also be still reviewable because if you wanted to see it as a table, you could indeed see it as a table. So it allows you to do the same thing you were doing, but more efficiently in the code.

MEMBER KRESS: Could you explain to me what a mutually exclusive event is? I thought they were all mutually exclusive; if you went down one path, you don't go down another.

MR. CANAVAN: In this particular case mutually exclusive refers to the case where, for example, if you model train 1 of a safety system and you model train 2 of a safety system and in both trains you model then being in maintenance, tech specs forbids you from entering that condition. But the fault tree doesn't know that, so it produces that as a cutset. So it says, for example, failure of the --

MEMBER KRESS: And it's not taken care of by the probability assigns --

MR. CANAVAN: Well, it appears in the cutset as train 1 has failed due to maintenance, train 2 has failed due to -- unavailable due to maintenance.

CHAIR APOSTOLAKIS: It's down. On failure. It down.

MR. CANAVAN: Right. Is down.

MEMBER KRESS: I understand that.

MR. CANAVAN: And what we normally do is remove those at the end. But this would prevent them from even appearing.

It sort of goes beyond this. It simplifies the model in that if you look at current models due to the complexity, we have a light of alignments going on by using additional events. For example, there are very complicated ways of excluding events by using nangates and house events and specifying series of conditions that get quite complicate. So you can have pages and pages of logic devoted into saying that when a loss of offsite power occurs this pump trips and then it has to restart. And you can write a very complicated piece of logic for the cases where that occurs.

With declarative modeling you would simply just say when this initiating event is running the code starts to look a little bit -- it would go in and turn off those events rather than having separate events that function in the role as turning them off.

And the last part is documentation and reviewability, and this is where I'll get back to some of what George was saying well you got to make it better, not just more capability but you want to make it less error proof. And one of the things that we've been talking about is you can view the fault tree by the attributes now. So instead of looking at this very large linked fault tree that's thousands and thousands of gates and thousands and thousands of events we can now, for example, say we want to look at the large LOCA initiator and it would show us just the large LOCA model.

We could now say we want to look at specific conditions, and they could be highlighted in various colors to show us paths through the tree, which make the tree and the logic smaller, which means it's more easily reviewable, bite size chunks if you will, and then you can search paths if you wanted to see them.

For example, what are the three ways that I get seal LOCA. You could trace back through the tree and see the way that it filters down to that element.

You could also add notes in the logic to qualify it so when you're looking at the fault tree and you now mouse over an event, we're all familiar with the annoying Microsoft mouse over thing where a little description comes up, but we can now make little descriptions come up when you mouse over the event. Because that event has several attributes, one of which is a note that says "I'm here because..."

So if you have an event that's an angate, you could actually refer it back to the success criteria notebook which says both of these trains must work for there to be success of this system, and there could be a reference.

So this is one of the more parts of the modeling that we're looking at improving.

CHAIR APOSTOLAKIS: It seems to me that the issue of reviewability is the most important one as far as this agency is concerned. When we get applications for whatever and they risk-informed, the Staff has to review the models. And if you make their life much easier than it is today, then I think that that would be a very useful thing.

MR. CANAVAN: Absolutely.

CHAIR APOSTOLAKIS: And that brings something else in mind, Dana. We're supposed to write a report on the research activities of this agency. And one question that has been raised if you think in terms of the future is how do we see an NRC Staff member operating ten years from now. And it seems to me a lot of this stuff might be relevant to that.

MEMBER POWERS: I should think.

CHAIR APOSTOLAKIS: Good. I'm glad you said that. Because, you understand, I mean we always look at things from the perspective of the agency.

MR. CANAVAN: Right.

CHAIR APOSTOLAKIS: So the last bullet there about review is really something that excites my interests.

MR. CANAVAN: I'm happy to excite your interest.

CHAIR APOSTOLAKIS: Happy to excite me? Thank you.

MR. CANAVAN: Excite your interest.

I did find it interesting when you said the reviewability is the biggest thing from the

Staff perspective. Because interestingly enough, the biggest thing from the licensee perspective is documentation. So that's why it's highlighted in this presentation.

CHAIR APOSTOLAKIS: Well, both. Both. Both. I'm sorry. Both. Both documentation and reviewability are very important to us.

MEMBER BLEY: You can't do one without the other.

CHAIR APOSTOLAKIS: Yes.

MR. CANAVAN: Well, our project status was we started many years ago with declarative modeling, perhaps about three to four now. But since then we were on, what I'd call a very low cost, low resource path where we were looking at interesting things doing some small amount of research, but not planning to finish until quite far out. We were looking at 2009/2010. But we recently received funding to accelerate the project in April of 2007, this year. And now we have a beta release by the end of the year of recovery and post processing. And with the recovery and post processing part that we just described. And a final release scheduled in the first half of 2008. So we continue to pursue that project and even accelerate it a bit.

MEMBER BLEY: Excuse me.

MR. CANAVAN: Sure.

MEMBER BLEY: Now this is, what you're telling us, this is for the upbringing CAFTA work? Is the same kind of work going on with other codes, are you aware?

MR. CANAVAN: The interesting thing about EPRI, CAFTA and R&R is that it's a relatively open platform. We actually have a book on how you can write your own software for R&R and CAFTA. It's called an API. Basically user programming.

We invite everybody to use that book and write the code. And we have a lot of utilities to avail themselves of that and others, vendors as well.

MEMBER BLEY: Okay. May I push this over to Mr. Epstein just a second?

MR. CANAVAN: Sure.

MEMBER BLEY: Does this idea of declarative programming tie into your quality checking and --

DR. EPSTEIN: Oh, yes. RiskSpectrum does it already for fault tree linking. And RISKMAN does it already for event tree linking. These are in place.

MEMBER BLEY: Okay. And that ties to the reviewability and all that?

DR. EPSTEIN: Absolutely. Yes.

MR. CANAVAN: I think in general the RiskSpectrum one is limited to notes. It has --

DR. EPSTEIN: No, no, no. They have everything from initiators to common cause. Most people in America don't know RiskSpectrum, but it is the largest selling risk software in the world. And it's extraordinarily good. As a matter of fact, even though I sell RISKMAN, I also sell RiskSpectrum all over Asia. I'm their agent. I wouldn't stand behind a competitor if it wasn't good.

CHAIR APOSTOLAKIS: Is that the Swedish thing, right?

DR. EPSTEIN: Yes. Yes. They're owned by ScandPower.

MR. CANAVAN: Moving on to advanced quantification techniques. And I've numbered the pages so you can sort of keep track of where I've started. I'm really glad I added a few of the graphs on the numeric slot late last night. Because I was debating on whether or not you wanted that level of detail.

And we're going to walk you through some of the current quantification approaches. The first one we're going to talk about is minimal cut upper bound, which is widely used. It does have simplifications. We talk about the rare event approximation being separate, but minimum cut upper bound is just one of the cases of rare event approximation. It doesn't subtract all the cross products, so therefore it's a case of rare event approximation. And it has a truncation limit. There are probably several others, I only gave these as examples. But success terms might be one, another example.

Then we're going to talk a little bit about direct probability calculation. It's new. It's going to be widely available in 2008. There are a few simplifications. And there is one downside that we did want to mention, and that is there are no cutsets this one.

And the last one is binary decision diagram. We're going to talk a little bit about this. It's successfully been used with small fault trees, and at least one case it's been used with a large fault tree. And it provides an exact solution without simplification. Large fault tree as a general rule remain intractable.

MEMBER BLEY: By direct probability calculation, you mean you just get a number? Core damage frequency?

MR. CANAVAN: Correct. You actually get several numbers.

MEMBER BLEY: Okay. So you'll tell us more?

MR. CANAVAN: I will.

CHAIR APOSTOLAKIS: Don't these include uncertainty propagation?

MR. CANAVAN: You can propagate uncertainty for several of the methods. I'm not sure you could --

CHAIR APOSTOLAKIS: Can you do it with BDDs?

MR. CANAVAN: Yes, but I think you -- with BDD would be a little time consuming.

DR. EPSTEIN: Yes. It's commercial.

CHAIR APOSTOLAKIS: I'd like to discuss that a little bit later at some point.

MR. CANAVAN: Again, this was another effort that we started about the same time, about four years ago. And we started looking at BDD solutions as being our first choice for the next generation of tools but realized that that might be several years off for solving all the fault trees that are out there. So while you might be able to solve one or two of the large fault trees in the next several years, which was our prediction, you probably wouldn't be able to solve some of the largest fault trees for quite some time. And we still think it's several years away before you can solve any of the broad range of fault trees using BDD. Because some of the trees get quite large. And the difference between, obviously, being solved it to one level and then another level that even includes just one more event might be the difference between being able to do it -- one event there's an exponential explosion of the results and one event might make all the difference being able to qualify it or not.

So we've looked at combinations of the approaches providing the best solution, at least in a stopgap way. So introducing these elements as over the next several years while we wait for the technology to improve to allow us to dequantify.

And the first one is the minimum cut upper bound most used now. And what we get out of the minimum cut upper bound right now is we get cutsets. We also get a value. We get several other things out of minimum cut upper bound, but for the combination approaches the important part would be the cutsets.

And then for DPC, what DPC provides are the direct probability calculation. It provides an exact solution value and it establishes the truncation for the minimum cut upper bound. So for example, if you know what the exact value is within some range, you can then use that range to establish when you want to stop making minimum cutsets.

CHAIR APOSTOLAKIS: Really? Isn't DPC-- how can it provide an exact solution value? I mean, I don't understand that.

MR. CANAVAN: Well, it could-- I'll explain it all on the next slide.

CHAIR APOSTOLAKIS: Okay.

MR. CANAVAN: Well, maybe not all.

CHAIR APOSTOLAKIS: Because if you can do that --

MR. CANAVAN: I'm sure you're going to end up with a lot of questions.

CHAIR APOSTOLAKIS: That's it. Right.

MR. CANAVAN: But it's a truth table that--

MEMBER BLEY: Don't know where it's coming from, so it's not it.

MR. CANAVAN: Right --

MEMBER STETKAR: It's a number.

MR. CANAVAN: It's a truth table approach.

CHAIR APOSTOLAKIS: Well the words "exact," exact is the --

MR. CANAVAN: Well, exactly --

CHAIR APOSTOLAKIS: Okay. You can tell us. You tell us.

MR. CANAVAN: Okay. Then the last part of the methodology of the combined approaches would be what we call MCBDD. It was discussed earlier in Steve's presentation as CBDD. And we started on this several years ago as well. I think it's almost two now where we were doing the BDD solution of cutsets. And in this case we provide the exact solution of the cutsets. We're subtracting cross products, BDD and BDDing the cutset.

The interesting thing becomes that the delta from the exact solution, the DPC exact solution and provide a knowledge of the numerical differences. And what we're really looking for in all of this, by the way, is not a better core damage frequency number. 6.41E to the minus six verses 6.40E to the minus six to any PRA practitioner is the same value. It is not different.

What we were looking for is to establish stable importance measures. Because as Steve Epstein pointed out in his last presentation was that the importance measures only become stable when the denominator really becomes stable. If the numerator is always participating, while there are rare situations where it doesn't participate fully, it would be odd for it not to participate at all. Well, if it did participate and the denominator is stable, the importance measure doesn't change much. And we've change that through a variety of studies. So in other words, the reason why the risk achievement worth is changing when you do for a component is no so much that the numerator is participating more, it's that the denominator, the core damage frequency is actually changing as a function of truncation. If you can stop that importance measures become relatively fixed and very difficult to change as a function of truncation.

And the beauty of this whole approach is that it can be performed for the large fault trees that are available today.

Here's the graphic that I was talking about, George. And I'll and explain it the best I can.

The first one, the brown line that's through the center there and relatively straight: I think it shows up as sort of a burnt red on the screen but it's brown on mine. That's the minimum cut upper bound approach as a function of truncation limit. So we took a model and we reduced its truncation limit by a decade and we plotted the resulting change in core damage frequency.

And while it looks very flat, it is indeed not completely flat; it is trending up. It's trending up very slowly. And if we look at the red line and the green line, the red line coming in from the upper left and the green line coming in from the bottom left, converging and to form sort of a cone, that's the results of a DPC. DPC is the truth table approach being quantified.

If you look at that, what happens is as we get the truncation out, the maximum and the minimum approach each other relatively quickly, and then asymptotically at the end. So if you look at 1E the minus 14 range, if you look very carefully and it's not very clear on this particular slide, but the minimum cut upper bound exits the maximum produced by the truth table approach. And in this case once you do that, once you exceed the maximum, you basically know that the core damage frequency is conservative.

Again, if you we continue to calculate this out, eventually those lines will converge and literally touch each other.

This is a real plant and we have real examples. There's a report out with actually four of these real examples plotted. It was published in December of 2006. And that report viewed these graphs for all four of those examples.

What this says is if you look at this, the minimum cut upper bound is conservative. We found the same shape every time; that the minimum cut upper bound was always conservative, that the percentage that it was conservative varied depending on some of the things that Steve mentioned earlier, which were what we would call elements of modeling style.

For example, if you put a lot of high values in your study, if you have a really lot of 1.0s that you used as flags and you have them in your model, you start flagging or tagging things with the 1.0, you find that that significantly impacts the answer. Because those 1.0s are actually mathematically manipulated within the model. So there are a few things that we learned out of this. Most of them we already knew and were actively discouraging, but there were a few examples where it still made a difference.

So this behavior was pretty typical. And what we found is we could generate that point every time. We could find out where the minimum cut upper bound crossed out of the maximum range as we converged.

The interesting thing to note is then the blue line. The blue line is the BDD of the cutsets. And it's not a full BDD of the cutsets. What we did here is we took the top 10,000 cutsets. We performed a BDD. We left the remaining cutsets, which were sometimes on the order of 3 million, 4 million, 5 million; we left them as minimum cut upper bound. And we simply added the total together.

The interesting thing to note is the blue line and the minimum almost meet. And the reason for that, what that is telling you is literally the model has converged. It's come to a point where the minimum isn't going up anymore from the truth table.

It's really the truth table at the top is coming down. And the minimum cutset continues to go up, but yet the BDD cutsets start to approach the true value.

So using the combination approach -- and by the way, the words on this were originally written for DPC to show when you get an accurate minimum cut upper bound solution. But what I did here was I provided the data so that you could look for yourself. And this is the data that the table was generated on. And this is, like I said, one of the four plants that we've done this for to confirm that the behavior was relatively similar for those four plants. And those four plants were taken from four different utilities, so we made sure we had a full range of the types of models we might see.

And if you look, the partitioned column is the MCBDD approach. And if you notice between 1E-13 and 1E-14 is not changing at all, at least in the significant figures that we have.

If you look at the columns for the exact minimum and a maximum, you'll find that they've gotten very close. In some of the other examples they are literally at the 6.41 and 6.40 are not made up numbers. They were actually numbers that we calculated here.

So we showed convergence and then we showed where the minimum cut upper bound start going out the top of that solution.

Yes.

MEMBER BLEY: I get lost in all the numbers. Can you back to the last slide?

MR. CANAVAN: Yes. Yes, this is much better.

MEMBER BLEY: There's a few questions I had.

MR. CANAVAN: Sure.

MEMBER BLEY: The first one you said the blue line is a BDD?

MR. CANAVAN: Yes.

MEMBER BLEY: But of the truncated cutsets?

MR. CANAVAN: Correct.

MEMBER BLEY: Of the truncated cutsets?

MR. CANAVAN: Correct.

MEMBER BLEY: Which is the stuff you told us --

MR. CANAVAN: Right.

MEMBER BLEY: -- it was squirrely for you guys.

MR. CANAVAN: Right.

MEMBER BLEY: The thing I'm a little --

MR. CANAVAN: Well, shows the --

MEMBER BLEY: Let me -- I think it's a lot different between your presentation and what we saw earlier.

MR. CANAVAN: Yes.

MEMBER BLEY: Especially if you take the min. cut and the BDD, they're essentially the same all the way across, everything's nice and stable. Everything's converging here. We're not seeing factors of two or ten like we saw in the examples that Steve presented. Can you two maybe say something about why these look so nice and why the others look so --

MR. CANAVAN: Sure. I will say that this is the nicest graph we got, so you are looking at the best one.

You will also find that the others have a much steeper -- so the brown line produced -- the other ones that we have is the burnt red line in the other cases is much steeper. And if we go back a decade or two, by the way, in the 1E-4 or 5 range, it is really steep.

So what this shows is that they got

stability very early. Not all the models show this behavior. Stability wasn't reached maybe until a little bit later in some of the models.

You see varying degrees of difference between the blue line and the red line in the other models, but certainly not the orders of magnitude that were discussed earlier in Steve's presentation and were real PRAs that would be out there being used, US PRAs. We would be able to describe where they came from, except that if you look at the chart, my guess would be when the eight cutsets didn't change or they were within ten percent, those were probably the top eight or close to the top eight in Steve's chart. And the ones that were changing significantly, like 300 percent, were probably very close to the truncation limit. Because we've seen that behavior. Because as the sequence gets really long, its cross products can become more important. So as the sequence gets bigger in terms of the amount of terms, not necessarily lower in frequency but more failures, then the cross products can become very important because there are more of them.

Literally as you get down towards the bottom of this, think about it like this: The cross products that you're subtracting in a 1E-12 sequence, it's 1E-12 and you're multiplying them altogether, then you're subtracting something that's A times B times C times D times E times F, and that's a really, really small number. And although there are really a lot of them, it's actually a way smaller number. So the mathematics that are going on here in the cross product substraction are that the value of the cutset, the value of the cross product is going down quicker than the total value.

MEMBER BLEY: Let me ask --

MR. CANAVAN: So low multiplication versus one more addition.

MEMBER BLEY: -- a little different way. You said you did like four others of these.

MR. CANAVAN: Yes.

MEMBER BLEY: Min. cut here by ten to the minus six truncation is pretty stable. I mean it's almost --

MR. CANAVAN: Yes.

MEMBER BLEY: Did the others come out that way or did you need to get down, like, to the ten to the minus ninth or tenth or even lower before they stabled?

MR. CANAVAN: I'd say anywhere between

1E-6 and to the 1E-9 was where stability was achieved for most of the models.

This is plotted in that order. I don't know if that report is publicly available.

MEMBER BLEY: I don't think we do.

MR. CANAVAN: But I'll be more than happy to provide any --maybe not the report, but any of the data if you were very interested in that.

I also could generate a presentation. We're restarting a lot of the research that we started here again. So we'll be doing some of that.

The interesting thing to note is that all of the analysis shows the same thing, which is if you take the top 10,000 or so cutsets and you do the BDD, and you compare it to any other value that you would get out of the model the same truncation, they showed the BDD -- that the model is very quickly convergent of that, the cross products of the remaining model, the stuff under for example 1E-10 ore 11 or 12 or 13 is rapidly becoming almost insignificant to the answer. And this all makes sense. This is all says that the original conclusions of rare event approximation are not bad. That the original conclusions of MCBDD -- minimum cut upper bound are not terrible, as Steve said.

They're actually quite good. Because at some point if you follow all the rules, they're actually quite excellent.

Where we find the differences is when people violated the rules of the rare event approximation. When they used higher numbers as a routine, not one or two, but they stuck in a whole bunch of 1.0s and kept them in as flag files, you have ones everywhere. Well, those aren't rare.

If you modeled initiating events, people have basic events in their fault trees of 365. Because they're trying to model initiating event. That is not a probability. That number can't be used.

Now the most recent quantification measures that do minimum cut upper bound, by the way, reduce everything below line before they do the calculations and then they go back in and they do the multiplication. The reason why they do is they're preserving the rare event approximation. They're making the math work better by making it rare and then subsequently multiplying it. While it remains another simplification, it is indeed a little bit better than allowing it to go through with the very high values.

MEMBER BLEY: Did you do any results like this on the RAW calculations? Is there anything you can share about that?

MR. CANAVAN: You know, that was the next step, and we just never got there.

MEMBER BLEY: You don't expect it to be very good, I imagine?

MR. CANAVAN: Once you get a stable denominator, we did some minimal calculations. What we found is that the denominator is what's changed the RAW, not the numerator. Because at this point at 1E-11 if something hasn't participated in the cutsets, it's not going to. And if it does, it's participating at 1E-12, 13, 14 sequences, and the core damage frequency 1E-5 or 6. So if it hasn't participated by the 12th, 1E-12, it really doesn't matter from that point on how many sequences that new component that never appeared in a core damage sequence suddenly starts appearing at minus 12 or 13. You have to ask yourself a bunch of questions:

(1) Is the sequence real? It came in at 1-13. You certainly didn't review it. It's cutset number 2,751,000 whatever. You never looked at it. So I would argue that at that point if it hasn't played a role, it's not going to, and

shouldn't.

I would also say that it's the denominator, a small change in the core damage frequency even 10 percent depending on how strongly the numerator has participated, in other words how big the top number is, all defines the risk -- and what we found is that the numerator changes more than -- the denominator changes more than the numerator.

So if you're calculating for a core spray pump, for example, if you drop it a decade, the core damage frequency a decade, what you find is that the amount of core spray participation in that next set of sequences is roughly equivalent to what it had played before in its other sequences, but the denominator has changed dramatically or significantly.

So when we get out to the flat parts -- I guess what all that comes down to is when you get out to the flat parts of this curve, the right side, the importance measures are not significantly changing because nothing --

CHAIR APOSTOLAKIS: Now, this graph does not have the full BDD solution?

MR. CANAVAN: Does not.

CHAIR APOSTOLAKIS: Does not.

MR. CANAVAN: That's correct.

CHAIR APOSTOLAKIS: Steve, you want to add anything to that?

DR. EPSTEIN: Yes. I'll start backwards.

The importance measures. Nicolov Duflot's work with a French referenced PRA showed the opposite, that at the high cutoffs there were problems and it's the numerator that got it --

MR. CANAVAN: The high cutoffs.

DR. EPSTEIN: The second thing is is that the BDD solution of the minimum cutsets was wrong. It's just not right.

CHAIR APOSTOLAKIS: Which one was it?

DR. EPSTEIN: Yes, that we talked about that the European guys did.

CHAIR APOSTOLAKIS: The one that's --

DR. EPSTEIN: Yes, it's the European group of developers was doing with it. We pretty showed mathematically that you don't know if it's too big, too small or what it is. You can't know.

And the third thing is is that I would say that if the DPC, as it's called, is based on truth tables, it should be examined very closely to the problem that we found that the Asian people had with their truth table solution. It's easy to make a mistake with this stuff.

MR. CANAVAN: This is the truth tables that have been around for 20 or 30 years. We actually--

DR. EPSTEIN: Yes, they were used. Kevin, they were used first for circuit reduction and circuit reduction doesn't care if there's redundancy. However, using the same thing to calculate probability is another question.

CHAIR APOSTOLAKIS: Is it one truth table or a series of truth --

MR. CANAVAN: It's a really big --

CHAIR APOSTOLAKIS: Yes, that was my next question. What are the dimensions of this truth table?

MR. CANAVAN: We've been trying to get both BDD and the truth table to work in conjunction. We were working on this for a long time. We now estimate the BDD solution, the true BDD solution for a full very large PRA to be in the area of 40 terabytes of solution. That's the equation. That's how big. If you save it to hard disk, that's the size the equation.

We based this on how we've been subsequently solving. I will tell you that we made an equation that was 500 gigabytes long. It took a week. And then we tried to solve it.

So the truth table is very similar. It's occupying -- since it's going through a process where it's destructive, in other words once it solves a branch it can eliminate it, it still ends up in the range of at least at its peak memory usage of something on the order of 100 gigabytes of information. So there is a lot of data there. It's a really big tree, that table.

MEMBER BLEY: This idea of verification that we talked about earlier --

MR. CANAVAN: Right.

MEMBER BLEY: -- we're pretty much stuck with experimental verification here, aren't we?

MR. CANAVAN: We are stuck with -- I mean, I think that's very interesting that that comes up. I will point out that everyone of these codes when operating on a large case, on a large fault tree, every single one of them including BDD and all of them, are all subject to the same issues and problems of coding and resolution. One of the biggest ways to do this comparison right now is to compare with another code, which may be written by the same set or group of people. By the same group of people, it's written by a guy who read the papers of all the other guys. So it becomes one of the things where, yes, we have a problem but it runs through BDD, it runs through DPC, it runs through minimum cut upper bound, it runs through -- and being a person who is extremely involved with the number of issues that come in when we update. For example, if we change an engine for somebody, which we've done several times or a version of an engine, the amount of people who run it, let's say several 100 might go off and run the new engine we put out, we might get 700 responses over a course of two years that say "When I ran this particular case or changed this little thing or did this little different thing, I got a ,00001 difference from this result to that result."

We go back and we find exactly why. But all of this is done by comparison. You'd be shocked at the amount of money that does go into comparing one engine to another engine and the subsequent results. And the number of test cases that are performed are very large.

And no offense to RiskSpectrum, but I do not believe that they are the broadest seller. But we can talk about that later.

CHAIR APOSTOLAKIS: Yes. I must say I'm a little confused now about the messages that you gentlemen are sending us.

MR. CANAVAN: I think -- I think --

CHAIR APOSTOLAKIS: I thought Steve was telling us that there are many cases where we really don't know. I think both of you agree that there are problems with the importance measures.

MR. CANAVAN: Right.

CHAIR APOSTOLAKIS: That we have not understood yet why we get different results. Is that the correct -- from Steve, at least, I get a message that if you have cutoff frequencies, you may have different rankings?

DR. EPSTEIN: That's right. We have found rocks --

CHAIR APOSTOLAKIS: And the BDD is the exact, right?

DR. EPSTEIN: Right.

CHAIR APOSTOLAKIS: Okay. That's your main message.

DR. EPSTEIN: Exactly. Yes. Yes. The BDD solution is the exact solution. And that there are many approximations, each of which have problems and that these have to be brought to light and compared into the --

CHAIR APOSTOLAKIS: Right. But also for the total for the core damage frequency, for example, you were not sure in some cases whether we're over estimating or under estimating or what was the exact value, is that correct?

DR. EPSTEIN: That they change depending on the order.

MR. CANAVAN: That's correct.

CHAIR APOSTOLAKIS: Now Ken comes here and says the approximate methods are good enough as long as you follow the conditions.

MR. CANAVAN: Yes. There are a lot of conditions --

CHAIR APOSTOLAKIS: I don't think you disagree with that, do you?

DR. EPSTEIN: No. I think that there is a couple of things. You have to make sure you're including success branches. And if your models have delete term, already you have negation in there. So to really do a full model, you're caught between the rock and the hard place of using things that can make things like minimum cut upper bound go wrong.

MR. CANAVAN: Right.

DR. EPSTEIN: Now also I think you have to be very careful about new methods and whether they're correct or not. I'm not saying that the code is correct. I'm not saying going over the computer program. But that the algorithm itself, algorithm proof of correctness is a branch of mathematics. We should use it period.

CHAIR APOSTOLAKIS: Yes.

DR. EPSTEIN: I have questions of everything I see, even my own staff.

MR. CANAVAN: I think we are in violent agreement on a few things. I guess that's what I wanted to say. I wanted to talk about where we agree.

In the models that we have looked at, we have not found all the issues that Steve brings out. We are aware of them on a sequence-by-sequence basis. If you pull out ATWAS and you start examining the ATWAS frequencies, for example, you will find out very quickly that it's very easy to get them to reorder, but they don't contribute to the total. So the fact that they reordered shouldn't be that disconcerting to the group. They're very small and very small things only require very small changes to reorder, right? That's what happens.

So in anything that doesn't contribute significantly to the result, it's very easy to get it to reorder. Small changes will make that happen. In the dominant contributors you won't find any of the stuff that we've just discovered, that we've just talked about, at least in the four models that we've checked. You might find that some things drop and some things increase, but it's not substantial.

If you calculate your importance measures at the right spots, you'll find that they're very stable as long as you when you build your model kept in mind a bunch of stuff: rare event approximation, the gated events and success terms. You made sure that you made some effort to them correctly.

In the end you can get very good results. The problem that we find is that there may be an occasion where someone violates the rare event approximation significantly. They stick ones in their models.

CHAIR APOSTOLAKIS: Yes, but that's a mistake. I mean, it's not a fault of the method.

MR. CANAVAN: Right.

CHAIR APOSTOLAKIS: It's a mistake.

MR. CANAVAN: Correct.

CHAIR APOSTOLAKIS: Let's talk a little bit about this importance measure ranking. I mean in risk-informed applications you really don't care whether the RAW of this component is 3.5 and the other component is three. We say all components or events that are upgraded on two are there. We have to do something about it.

MR. CANAVAN: It's one way to take 1.95.

CHAIR APOSTOLAKIS: So I'm wondering --

MR. CANAVAN: Or 1.9.

CHAIR APOSTOLAKIS: Now you might say what do you do about the ones that have exactly two or 1.9? Our Staff is smart enough to handle those. So I'm wondering whether that issue is really as important? I mean, from the mathematical point of view, it's probably interesting. But I really don't care whether I get ten or six. I know all of these will be above two and then if I'm doing special treatment requirement analyses --

DR. EPSTEIN: You're probably right.

CHAIR APOSTOLAKIS: -- I'll treat them the same way.

DR. EPSTEIN: You're right, but we have

to make sure that those are really the values.

MR. CANAVAN: We want to --

DR. EPSTEIN: Nicolov's work shows that it changes.

CHAIR APOSTOLAKIS: But it changes how? I mean can something --

DR. EPSTEIN: It depends on -- that's the point, we don't know. It depends on the model. That's exactly the point.

CHAIR APOSTOLAKIS: But it can it be with one model ten and with another model .2? I can't believe that.

DR. EPSTEIN: Well, you know --

CHAIR APOSTOLAKIS: Ken?

DR. EPSTEIN: I have seen --

CHAIR APOSTOLAKIS: Is it, Ken? Tell me.

DR. EPSTEIN: That's fine. That's fine.

DR. RAUZY: Yes. What Nicolov Dufolt has shown on the reference, the French reference PSA is really that you may have dramatic change in the absolute value -- both the absolute value of the -- and the ranking of the difference even. And the reason is very simple to understand.

At a given cutoff for a given truncation level you may have an event that just doesn't show up in the cutset. And if you go a bit below, you take a lower cutoff, then this even shows up.

And when you calculate the conditional probability, then really it will influence greatly the cutset you add by -- it really influence. And you may have cases in which you have a row of one until a given result, it gets 10,000.

CHAIR APOSTOLAKIS: Really?

DR. RAUZY: Yes. Yes, of course.

MR. CANAVAN: We're talking about a --

CHAIR APOSTOLAKIS: That sounds like an exaggeration to me --

MEMBER STETKAR: Let me ask a question. And this may get to part of this issue. Ken, you said you've run these comparisons on four U.S. existing PRAs, correct?

MR. CANAVAN: Yes.

MEMBER STETKAR: The comparisons that you've spoken about are for French --

DR. EPSTEIN: Japanese, Swiss.

MEMBER STETKAR: -- and Japanese and generally international.

DR. EPSTEIN: American. Also American.

MEMBER STETKAR: Let me say there are

substantial differences in these nuclear power plants and the level of detail in the PRA. I know that from my own experience. It would be interesting to see if EPRI did this type of comparison on an international PRA.

And the reason I bring this up is that in some sense this is relevant historically. In another sense, we're talking about new generation PRA software for evaluating new generations theoretically of nuclear power plants in the United States, which will probably have in some cases more complexity depending on the specific plant design. For example, the EPR is more complex than a typical existing U.S, nuclear plant. And will have many, many more passive features that have, depending on the data that one selects, exceedingly small number. The smaller the numbers and the larger the complexity the more important these issues become.

MR. CANAVAN: Especially the smaller number.

MEMBER STETKAR: Right. And when we're starting to talk about passive system components, we're starting to talk about digital for, if not software-based digital, at least solid state INC rather than clunk, clunk, clunk relays, the numbers start to become much smaller and the comparisons then start to become more important.

What I've seen on some of the comparisons I've looked at, I think where U.S. plants would tend to support Ken's conclusions and for European plants would tend to support some of the conclusions that Steve and Antoine have shown us. That's just pragmatic.

CHAIR APOSTOLAKIS: So if you take the European EPR to America, which guy do I follow?

MEMBER STETKAR: You have to be careful--

DR. EPSTEIN: I think the one thing is--

MEMBER STETKAR: All I'm saying is you have to be careful because I think that you're seeing numerical comparisons -- these are numerical comparisons from existing models and the models are different. And they're models of, in some cases, very different types of plants. So it's not a different model of a two train Westinghouse PWR. It's a model of a French standard plant or a rather advanced plant in Switzerland compared to a model of a two train Westinghouse or GE, or combustion or whatever plant.

DR. EPSTEIN: But our whole point was is

that if we're all working together without the parochialness of vendors, right? RelCon sells software, ABS sells software, EPRI sells software, everybody sells software. If we break these barriers down and work with Open PSA together in this spirit of real research and openness, we'll know these limits. We won't have to hide because we're worrying that somebody won't buy the software if they find out it only works for four models.

If we're all knocking our heads together, we can solve these.

CHAIR APOSTOLAKIS: Yes, I understand that. And I believe there are three or four different points are on table. And I don't think Ken is addressing this issue. Ken is addressing the issue of accuracy and different methods, and so on. You are also addressing that, Steve, but also you are making the proposal of this open meeting?

DR. EPSTEIN: Yes.

CHAIR APOSTOLAKIS: That's fine. We can discuss these later.

Ken?

MR. CANAVAN: I just want to try and get you back on schedule and make one more point about the risk achievement worth, then I'm just going to move on.

The point about the risk achievement worth, let's just for example let's say your core damage for simple matters is 1E-6. If your truncation is 1E-12, okay, and then a new participant comes in at below 1E-12, and let's say it's unavailability or unreliability is 1E-6. If it suddenly comes in, then it's risk achievement worth since your core damage was 1E-6 and it suddenly starts appearing in a sequence, it could have an impact. But at 1E-12 it really can't -- unless it's a very low unavailability, it cannot impact the core damage frequency at all.

So I would argue that with the U.S. current truncation limits it is not a function of the numerator at all for the risk achievement worth, which means they're stable if the core damage is stable.

So the key is -- and why MSPI would have us all lower seven decades below the CDF was to produce this result, which is if you look at the conventional minimum cut upper bound column you get the 6.6E-4 from 6.005E-4 down to 6.006E-4. And that makes importance measure stable, which is why MSPI made you go seven decades below the CDF. That was the whole point of that exercise.

Now, do I agree with that? Not entirely. While it makes it stable, it is also conservative. Because if we look at the minimum cut upper bound we know it over predicts as a general rule if you consider success terms appropriately.

With all that said, I'm going to move on. I'm going to talk about the pros and cons of the combined solution.

CHAIR APOSTOLAKIS: I think, though, it's important for you guys in your future work to bring into this the context in which these results are used.

MR. CANAVAN: Right.

CHAIR APOSTOLAKIS: When the industry and the Staff agreed that RAW values greater than two means something and RAW values less than two mean something else, they didn't do it capriciously. They thought about it. I mean, probably the uncertainties were taken into account and so on. So I think that's an important thing.

Now, you might want to come back and say well I can refine that with my new methods so you don't have to be overly conservative sometimes and so on. Because I have a better way of calculating

RAW, which now everybody agrees is a better way, or you know, or we might say this is a nice method, it gives more accurate results but I really don't care whether it's 3½ or 6.

MR. CANAVAN: Right.

CHAIR APOSTOLAKIS: Because as far as I'm concerned it's above two.

So the context, I think, is very important. Not just the mathematical which, as far as I'm concerned, is very interesting but remember at least here the real issue is how do these things effect the decisions that the agency makes

DR. EPSTEIN: As long as we're sure that--

CHAIR APOSTOLAKIS: I have no problem. Just take into account, that's what I'm saying.

DR. EPSTEIN: I agree completely.

CHAIR APOSTOLAKIS: Okay. Great.

Ken, bring us back to schedule.

MR. CANAVAN: I told you I'd get you back.

CHAIR APOSTOLAKIS: You're too slow, Ken. Too slow.

MR. CANAVAN: Pros and cons. Well, it was all a good discussions.

The pros and cons of combining the solution as we looked at it when we were generating these projects was that it was achievable. We knew we could do it all several years ago when we sat down and put pen to paper. It was challenging, but achievable. There was no significant simplifications. There were some significant disadvantages.

There were still some minor simplifications, and we still had some simplifications going on. It could require a full-- quantification at some points, which means the truth table evaluation takes some time. So if you need to walk back through that, it might save some time. It can range from anywhere from half an hour to several hours, maybe even a day for the really big models. And that takes some time. And so if you're looking at an application that a nuclear power plant is doing things, like identifications for George, if you're looking at online maintenance taking a day or two to analyze an emerging condition may not be okay.

But our project status was, again, we accelerated this in April and we've been a little bit slow. It's been difficult getting the people that we wanted to work on the project. So we got at it a little bit slow.

CHAIR APOSTOLAKIS: Can you tell us the people working on this?

MR. CANAVAN: Oh, sure. We use a combination. Our project team in general has been-- as a matter of fact, on some of this in the early days we did -- when this first came out we worked with Antoine Rauzy and Steve Epstein and they were our major considerations in the beginning of the project. And now we're using Dr. Woo Sik Jung of KAERI. He is the developer of FT Forte and the new engine FTRex.

CHAIR APOSTOLAKIS: Yes. He is the Korean Atomic Energy Research Institute.

MR. CANAVAN: That's correct. Yes, he's the Korean Atomic Energy.

And we work with Jeff Riley as well who is one of the principal programmers of the R&R workstations. He's been involved for about 25 years now.

We do expect a 2008 completion on the combined techniques, basically doing a series of anywhere from three to ten benchmarks through the whole process, running the whole thing, going start to finish. We will look at important specials. I will make it a point to do that.

CHAIR APOSTOLAKIS: But also I think you should consider what John Stetkar said earlier.

MR. CANAVAN: Absolutely. And we are very concerned about the future, which is why this was always looked at as a -- we feel BDD one day will be happening on everybody's computer. We think that's a few years away still and for some of the larger models maybe even a few more years than that.

So this is looked at by us as sort of a stopgap to get a more accurate result for the sake of importance measures stability. Not for the sake of getting a better 6.4 or 6.41.

Okay. The last couple of slides here. We're talking briefly about DocAssist. This is the need to control the documentation. It's gotten pretty complex. It's not directly tied to the model, and it's difficult to maintain an update. If you talk to utility members who may be here in the audience or own a PRA, they'll tell you that the documentation is very unyielding. It's one of the most resource intensive parts of them performing updates in PRA.

PRA DocAssist is the software tool

that's under development that basically allows us to tie the model and documentation a little closer together. It allows us to capture the information needed at the point of generation. So if you're in a fault tree and you want to capture why you're doing things the way you're doing it, you can do that.

It has a sorting capability which allows us, for example, you can sort the entire document by the ASME standard requirement to which it comports. So, for example, if you're doing an initiating event analysis and you take the time to say well each one of the supporting requirements you connect to a power graph in that document, later you can put the document together how you'd like to view it. But if you wanted to see how it comported with the ASME, you could then sort the document by ASME element.

The reason for this is there's an awful lot of peer reviews going on. And when we do a peer review it's very nice to be able to sort the documentation by the requirement for the reviewers.

There's also a bunch of other items. Navigation by user attributes so you can actually define your own attributes.

A reporting capability and configuration control.

I didn't go into a whole lot of detail. It's pretty neat in that PRA documents contain a lot of repetitive information. PRA DocAssist is trying to end that. So bottom line is if you're looking at the report, you open up DocAssist for looking at the database it's not a database that's in the report. It's the database that's in the model.

MEMBER BLEY: Ken, quick question related to one somebody asked you earlier.

MR. CANAVAN: Yes.

MEMBER BLEY: Does it come up with prompts to help make sure the user puts in information that reviewers might want or future users might need?

MR. CANAVAN: It actually has a template. So, yes. It's template approach driven. So it's actually putting out a template that says this is the recommended format of a system analyses. So when you use DocAssist you're cajoled.

Now can you modify the format? The answer is yes. Should you modify the format? No. You can.

This is another case where we've been under development for about the same amount of time.

You notice a common theme. The next generation of tools all started around three or four years ago. Each one of these elements was very carefully thought out in sort of a long term plan and how they interface with each other. And they're all in various stages of completion.

But, again, you'll notice another common theme that in 2008 the first half, we will have a version of DocAssist up to provide to all EPRI members. And we'll provide a limited support to get everybody going and then we're going to start a users group that people can join if they'd like, or they can use it on their own.

In any event, one of the very nice things about DocAssist is there is no repeated content. If you use something in several locations, you simply refer to that data and then it's used in those locations.

But what this does is it turns the PRA document into actually a database. And that database is assembled to produce reports or you can query it.

So it's a pretty powerful tool for controlling documents. It makes the resources associated with updating that information a lot quicker. For example, if you have 25 system notebooks, you'd have a boilerplate. That boilerplate is in there once and then it's referred to 25 times. So when you go to print out each notebook, you'll get that content immediately.

The same is true for the tables. If you print out a table of the database, if you do it on a system or you do on the data as a whole or you do it in the model, that's actually one piece of data. There's only one database and then everything refers to it.

The beauty is no more transposition errors, for example. No more repetition of writing numbers into a text. It basically refers back.

And we should be done in the first half of 2008.

I wanted to summarize a few things. I'm going to go through the slide, but this is our overall approach and the things that we have done to date. And the authors of the 2005 report that's listed are to my left and right.

And we're looking at a visual interphase. I found it very interesting looking at Steve's slides because there's a lot of good visual stuff there. We'll be talking to Steve about how we do that to both have the inputs of the PRA as well as the output be more useful. So we're looking at that.

One thing that hasn't been in our plan due to resources has been the visualization. And, again, we were initially a very long term, very low cost program, because we were limited in funding. This year EPRI took it upon itself to increase the funding in this particular initiative, and we welcomed that. And therefore, that's why you see a lot of things ending in 2008.

This is sort of a summary of the vision. You can see all the parts, sort of how we're looking at the future of the next generation of tools. This is a picture that was generated many years ago and this continues to be used.

Concluding, tomorrow we have a meeting, the first time that we're meeting, that EPRI is meeting with the Open PRA architecture folks. And we have an interest, mostly because as we spoke earlier, there are elements of model style that can impact the number, can impact the quantification of the resulting core damage. We're very interested in ensuring that everybody understands what they are for the current tools and any effort to eliminate them would be welcomed. So elements of an open architecture may lend itself to reducing or eliminating those occurrences where people use any values that may not be values --

CHAIR APOSTOLAKIS: Do you subscribe to this idea of Open PSA where nobody owns anything?

MR. CANAVAN: This is the presentation. Tomorrow we're going to give some more presentations and hear presentations. We're going to make some decisions as to our --

CHAIR APOSTOLAKIS: Because typically your products go to your members.

MR. CANAVAN: Correct.

CHAIR APOSTOLAKIS: And that's not what Steve is advocating.

DR. EPSTEIN: No.

CHAIR APOSTOLAKIS: No?

MR. CANAVAN: Steve is advocating an open architecture that would allow you --

CHAIR APOSTOLAKIS: Oh, just the fundamental --

MR. CANAVAN: That would allow you to transfer model-to-model. My concern about this--

CHAIR APOSTOLAKIS: But also he's advocating reviews, PRA previews and all that. I mean --

MR. CANAVAN: I think that would be in the interest of all. Peer reviews of software to figure out whether -- to first of all, I think, close some of these issues. But I think in many of the presentations somebody finds one situation where a risk importance measure changed. It was in a low truncation limit. They blow it all out of proportion and say, ah, all the risk importance measures are not accurate. Well, you find out that that person just reduced their truncation limit, they would have been fine.

Then you find out somebody else used a bunch of ones, so they're inaccurate. And you find out that if they didn't do that, their model would be very accurate, quite reasonably.

So you find out that individual instances get turned into globalizations which aren't true. So one of the reasons for open architecture is to allow us to have a common platform to reduce some of those misconceptions and cajole people into not doing the wrong thing.

We got to remember that we're all dealing with PRAs here, and the PRAs they're designed to have between zero and one in them, right? Probability, not numbers -- so we have an interest from that perspective.

I am concerned about one thing, and that is I heard recently that someone wanted to be able to convert to another platform because they were doing a peer review and they didn't understand the model in the current platform that they were looking at. And I thought that was a very poor reason to develop an open architecture to be able to go from one platform to the other. I don't understand how it was built there. Because guess what? If you don't understand how it's built there, what makes you think you're going to understand when it's converted, that's any better? You might actually be introducing errors that you now can't find because you're one step removed from the original model.

So I would argue that understanding is the key. Open architecture would allow us to be consistent, which would be positive.

And with that, I'll conclude.

CHAIR APOSTOLAKIS: You will be around until noon, right?

MR. CANAVAN: Sure.

CHAIR APOSTOLAKIS: Okay. Unless somebody has a burning question, I propose we recess. Okay.

Thank you very much, gentlemen.

We'll reconvene at 10:50.

(Whereupon, at 10:31 a.m. a recess until 10:54 a.m.)

CHAIR APOSTOLAKIS: We're back in session. The speaker is Dr. Antoine Rauzy, ARBoost Technologies, also University of Marseilles. And very prolific of papers on BDDs.

So, Antoine, can you finish by 11:30.

DR. RAUZY: Yes. Yes.

CHAIR APOSTOLAKIS: Okay.

DR. RAUZY: Well, I won't speak about BDDs right now, but about the work we did and we want to do on this international standard presentation format for PRA.

So here is another view of what I'm going to chat about, give some idea as to why we want to be able to understand it, give you a flavor of what the standard is and then go into more detail.

So where we are. Well, the discussion this morning showed that we have detailed models all over the world that have been developed for level 1 and 2 PSA. And we have good tools at hand; that's pretty clear. But models are now very big and so they are hard to master, to check for completeness to maintain and so on. And my feeling with respect to this morning's discussion is that this is the main issue.

Also, we know that models are tool dependent. It's almost impossible to take a developed with one software and to put it into another software. And calculation engines have some limits, which again doesn't mean that the result we get so far are completely wrong, not at all. Nor are they significantly wrong in some cases. The point is that in some cases we have wrong reasons and we don't exactly know when, and that's the problem.

So --

CHAIR APOSTOLAKIS: Is "wrong" too strong a word here, don't you think? Wrong is inaccurate. Perhaps would be a more --

DR. RAUZY: Yes, you're right. You're right. I agree with you. Yes.

CHAIR APOSTOLAKIS: Okay. We are on the record now you know, so --

DR. RAUZY: Okay.

CHAIR APOSTOLAKIS: You don't know who is going to be reading the transcripts.

DR. RAUZY: Where I'm about to go here's my dream for the future. Where we really want to go is to go toward the virtual nuclear power plant. That is --

CHAIR APOSTOLAKIS: Actually we want to build it. It will be virtual for 40 years.

I understand. I'm sorry. I couldn't resist that.

DR. RAUZY: Okay. But that's my idea of the future is that the future generation of -- maybe not the next one but the next, next one or something like will provide such a virtual nuclear power plant with a full 3D visualization, some realistic real time simulation with the equation of physics. And the third part of the triangle is full capabilities to make risk-informed decisions.

Okay. We are up here right now. It's maybe not that far, but we are here right now. And our idea is that the first step toward this goal is at least to have this international representation format for the PSA/PRA models.

So why do we need a standard? I would like to come back to that issue first.

The first point is to reduce tool dependency. Let me tell you a story about that. At the workshop Steve mentioned this morning there were there Steve with the main developer or in charge of the development of RISKMAN, there were Dr. Woo Sik Jung, who is charge of FTRex engine with the one we know developed the FTRex engine, there were Olivier Nusbaumer who is in charge of the development of calculation -- of RiskSpectrum and myself who is in charge of the development of Aralia, which is used in most of Japanese PSA as a calculation. And we all went to dinner at the restaurant in the same car.

Assume that we got in a car crash. No, it's not a joke. The situation would have been that all of the engine of all of the PSA in the world would have been for at least two years completely unmaintained.

So the story of reducing the tool dependency is really an issue. If for some reason Dr. Woo Sik for instance, quit KAERI, who going to maintain? He's the developer and was the knowledge of the code.

And so reducing the tool dependency is really an issue.

Well, the second point that's been discussed at length this morning is to have a better confidence in approximation we are doing when calculating. Again, well this has been discussed and the best way probably to do that is to be able to cross check calculations, that is to apply different engines on the same model.

Indeed, if we have an open standard, then it opens the markets to new ideas, to new developments where now the situation is that we cannot do that. If someone in some good university has a good idea to develop a new calculation engine, it's almost impossible for him to get noticed and check whether his engine is really good or not. And, indeed we want to have an open architecture and we'll go back to that to be able to design new model browser, new safety monitor and et cetera, et cetera.

And also an important issue and Ken pointed out very well this morning is to be able to review and document existing model. By giving them more structure, it help to do so.

Another point, we worked in the Open PSA group on the different PSA coming from Japan, Europe and the U.S. And we found that the modeling methodologies are completely different. That is the way the models are designed are completely different according to the place where they have been developed. And maybe to have an international standard like this would help to at least clarify or unify the modeling methodologies. Well, that's what you pointed, Ken, this morning saying that to be sure that the calculation engine gives good result, we have to base on rules. And maybe to add such an international presentation would help to clarify which rules e have to apply to make good models.

And, indeed, the other issue like to be able to call external tools for final PSA or system PSA, for instance, to extend the fault tree/event tree formalities, then to get -- I don't know -- some mark of description or some human reliability issue or something like that.

So is our vision of the open PSA architecture. But the idea is really to have this standard representation format in the middle and to be able to plug many tools on this common format. So calculation engine existing or new calculation engine, databases of basic event values, safety monitors and so on. So this is really the main idea of this project, of this initiative towards this open architecture.

What are the requirements for this

standard presentation format? Well, clearly it should be possible -- our idea is that it should be possible to cast any existing model into the standard. That is, the standard should be a superset of what is existing in the different tools. And so we designed the standard with that idea in mind, with that guidelines.

The second point that the role of each element of the standard, each element of the model should be clearly identified and should have an unambiguous semantics in such a way that it is for someone who want to develop a new tool, it should just from the standard it should be able to develop a new tool and get the same result or a similar result as an existing tool.

And the last point, but Ken discussed that this morning as well, is that it should be easy to embed the standard into the existent tool. Should not be too much an effort to do that. And for that reason we choose to use XML as the representation format, as say the basis, which as the tool to be supporting an open format, used on the World Wide Web.

Okay. So let me give you an idea of what the standard looks like. And we get that.

What we did, actually, is that we consider models deals with the main tool available in the market, which means the list I wrote here. And we considered both U.S., Japanese and European PSA. And we tried to make a taxonomy of all the elements of these models. That is to understand what are the elements of these models. And to give them a precise semantic. And once we achieved this goal, we give an operational semantics for each element and we designed an XML representation.

So that's the way we proceed. And we ended up with a five layers architecture for the models. So at the very bottom there is what we call the stochastic layer, which is populated with all the construct we need to define, to describe probability distribution of the basic elements. And probability distribution that are needed to perform sensitivity, things like that.

Then there is the fault tree layer. The fault tree layer is what you expect. That is the description of the fault trees with gates, basic events, house events and so on.

And then the third layer is what I call the extra-logical layer, which is populated with common cause failures, delete terms excluding events we discussed this morning, exchange event and things like that.

Then there is the fourth layer, and then there is the report layer.

And this way of thinking really structured more help and helped to understand each element and how they work together.

So to give you a picture of what we obtained, it's something like that. And the report layer is not here because the report layer is concerned with the results of calculation. It is just for the models. And you can see here the four layers. At the very bottom the stochastic layer, then the fault tree layer, the extra-logical layer and the event tree layer. And all objects that lay in these different layers and their relationships.

So this is how the standard works. Yes. And we are now able to cast any of the motivates we looked at into this framework and to give a precise syntactic to each element.

So let me give you more idea of the different layers.

So the fault tree layer, which is here. So the fault tree layer is populated with fault trees, gates, basically you're going to see like that.

So for instance, here is the XML representation for this very small fault tree. Well, the idea is that you define the fault tree, you define the gates inside this fault tree, which is the top event. You give the type of the gate and so on.

So this a computer representation. XML is not well suited for human reading, but it's very well suited for computer interaction. Almost all of the file exchange are now done with such XML representation.

So that's the idea. And the good point of these representation is that it is very structured. So it's possible exactly as Ken mentioned this morning, to give attributes to each element and to be able to browse the model according to these attributes or the structure. It's possible to group things together and everything like that.

So gates are just designed like this. And the standard includes a full branch of logical connectives and or -- in many of the models. And -- well, that's it.

Similarly, we can define basic events so we have a very clear definition of what is basic event with a name and a probability distribution. Here is a negative exponential probability distribution with a parameter.

CHAIR APOSTOLAKIS: Maybe I'm missing something here. But isn't that already being done? Why not?

DR. EPSTEIN: Well, why haven't lots of good ideas happened before they happen?

CHAIR APOSTOLAKIS: No. But I mean if I go to Saphire --

DR. EPSTEIN: It has no proprietary --

CHAIR APOSTOLAKIS: Now wait a minute. What if asking to define the gates --

DR. EPSTEIN: Sure.

CHAIR APOSTOLAKIS: Define, that includes give them a name. So what's the difference?

DR. EPSTEIN: Because it in Saphire. It's not open to other software.

CHAIR APOSTOLAKIS: Ah, so that's it.

MEMBER BLEY: If you want to take that Saphire model and --

CHAIR APOSTOLAKIS: I see.

DR. EPSTEIN: Sure, we've got a CAFTA model, but you can't move it without all these machinations back and forth. So what we've tried to do is abstract.

CHAIR APOSTOLAKIS: So it's not only then logic that's new, it's the format?

DR. RAUZY: It's the format. Yes, right. Right.

And more this way of defining things make it possible to extend the format in an easy way. And you'll see that's the main advantage of the--

CHAIR APOSTOLAKIS: And if you give me a fault tree with this format, then if I want to use RiskSpectrum or Saphire, I can go from this to them easier?

DR. EPSTEIN: Absolutely.

DR. RAUZY: Absolutely.

CHAIR APOSTOLAKIS: How about the other way?

DR. EPSTEIN: Yes.

CHAIR APOSTOLAKIS: The other way? Can I go from Saphire to this?

DR. EPSTEIN: Yes. We started to do this because we had to move models --

CHAIR APOSTOLAKIS: So this is a common language?

DR. EPSTEIN: Exactly.

CHAIR APOSTOLAKIS: All right.

MEMBER BLEY: So this is where it takes it, but you need a translator for each of those or something?

DR. RAUZY: Absolutely.

DR. EPSTEIN: But they are all public domain. This is wonderful. You don't have to write the software. You can pull them off the net.

DR. RAUZY: That's wonderful.

CHAIR APOSTOLAKIS: You mean this?

MEMBER BLEY: The translator.

DR. EPSTEIN: You can translate these back and forth. You give it a template and a file and you can get for free software that puts them together and then you just do what you want. That's why we started this, because we didn't have to write the software.

DR. RAUZY: But I would like to point out, sir, that it's not -- what is easy to do is to take, for instance, the CAFTA model to translate it into the standard and to translate it back to the CAFTA format. But I won't say that it's easy to take a CAFTA model to translate it into the standard and then to go to RiskSpectrum, for instance. This is a big work. Because indeed the way the models are designed are really different.

CHAIR APOSTOLAKIS: Yes, but if I have this--

DR. RAUZY: If you have this, you can do it anywhere.

CHAIR APOSTOLAKIS: Yes.

DR. EPSTEIN: Right. Right.

MEMBER SHACK: But CAFTA has to give you the translator to take its model to this?

DR. EPSTEIN: CAFTA has an open API, which means that I can write the translator myself. I don't need a CAFTA person.

DR. RAUZY: No. Basically we need them -- almost --

MEMBER BLEY: The goal is for the Open PSA group to write all these translators?

DR. EPSTEIN: Sure. Yes. One of the things is we will write many tools for everybody.

CHAIR APOSTOLAKIS: I see. That's good.

DR. EPSTEIN: Yes.

DR. RAUZY: So the stochastic layer, which is the lower part here --

CHAIR APOSTOLAKIS: Ken, you don't seem to object to any of this?

MR. CANAVAN: No, no. The API is open

for all. It's actually quite easy to get CAFTA to go to -- to use the API to get it to translate to this. The problem it starts to become is, I don't know if we've gotten it to you yet, but you said it exactly right. You're generating a language. Well, languages are really complicated. Beyond the simple mechanisms of grammar , there's sort of --

MEMBER BLEY: The semantics?

MR. CANAVAN: -- semantics, there's idioms and expressions. And, you know, those are going to be the things that are actually hard to convert from one methodology to another. And idioms and expressions become individual exceptions to the grammar -- grammatical rule, right? If I easy as pie, that is -- we all understand that, but in Russia easy as pie does not translate to anything that makes any sense. I know this because I was in Russia saying easy as pie and getting funny looks.

So that's where you're going to get into trouble because there are models built with those types of exceptions in them where you actually -- the analyst has essentially created a situation that won't translate well.

MEMBER BLEY: What is API?

DR. EPSTEIN: Application Programming

Interface.

CHAIR APOSTOLAKIS: That was very simple.

DR. EPSTEIN: It's very simple.

CHAIR APOSTOLAKIS: As API, it sounded-- okay. Go on.

DR. RAUZY: Okay. So I just give reviewed the different layers. So I give you a flavor of what is the stochastic layer. Basically it define all stochastic expression and parameters needed to define probabilistic.

CHAIR APOSTOLAKIS: Probabilistic, by the way, not stochastic.

DR. EPSTEIN: Okay. We'll change it.

CHAIR APOSTOLAKIS: Stochastic is -- I wouldn't call for example state of knowledge distribution as representing stochastic uncertainty, no. But here you will put --

MEMBER POWERS: You're misunderstanding the state of my mind then.

CHAIR APOSTOLAKIS: I mean it's just a friendly suggestion. You don't have to follow it.

MEMBER STETKAR: This is more, though. This also is what type of model you assign to a particular basis event.

DR. RAUZY: Absolutely.

MEMBER STETKAR: So it's more than just data variables. It's also am I going to use a repetitive testing model or an untested model, or a time dependent --

CHAIR APOSTOLAKIS: What do you mean? What do you mean?

MEMBER STETKAR: Want to use the minus lambda T for an unavailability or am I going to use a different type of model for the failure that I assigned to a particular basic event. So it's not just --

CHAIR APOSTOLAKIS: Probabilistic is broader.

DR. EPSTEIN: We only used stochastic because it made our wives think we were doing something important. That's all.

CHAIR APOSTOLAKIS: Probabilistic is not important?

DR. EPSTEIN: To wives? No.

DR. RAUZY: Okay. So we defined the stochastic layer, we add to the stochastic layer many constructs we need to define all of that, like -- different built-ins that make it possible to define a time dependent distribution and all things.

So --

CHAIR APOSTOLAKIS: Strictly speaking you're not really -- you shouldn't be assigning probabilistic values or quantities to individual events because various strategies like periodic tests and so on tend to couple these things.

DR. RAUZY: Absolutely, that --

CHAIR APOSTOLAKIS: And you can do that here?

DR. RAUZY: Yes, sure. Because at the stochastic layer we define what we call parameter which as stochastic or probabilistic variable, stochastic variable. And we can use, for instance, the same rates for two different pumps. So it's possible that the stochastic layer is a whole universe in some sense. You can really define stochastic equations with variables and everything.

DR. EPSTEIN: So if you calculate to the po;int estimate, it uses the mean value. If you calculate with the Monte Carlo method, it actually performs a Monte Carlo simulation. Those are the ideas we're trying to capture.

DR. RAUZY: And we have also built-ins to define time-dependent components and things like that.

And moreover, the idea of adding external like this, it's if you need a particular function, we can add it quite easily to the standard.

DR. EPSTEIN: And there's also a way to add a user defined function.

CHAIR APOSTOLAKIS: You can assign probabilistic expressions to a couple of different events?

DR. RAUZY: Sure.

CHAIR APOSTOLAKIS: Okay. Sure. But in the common cause failure probability would be at this level, correct?

DR. RAUZY: No, it will be at the --

CHAIR APOSTOLAKIS: At the higher level.

DR. RAUZY: At the higher level.

CHAIR APOSTOLAKIS: So this is not a complete stochastic representation?

DR. RAUZY: No, no, no. But the idea really is to have here a kind of language to define all that we need for the different kind of studies we have to perform.

MEMBER SHACK: But going back to Ken's point, when you said "idiom," what you meant is in the models that exist and existing, people have cobbled them up to do things they don't have explicit model for. So everything they have an explicit model for is not going to be a problem here. It's when the guy has cobbled things together in some way?

DR. EPSTEIN: It's like if you have a recovery rule, in CAFTA they are computed in one way, in RiskSpectrum it's another way. I think that those are the idioms really here.

MR. CANAVAN: Yes. To be real simple we're talking about nouns and verbs here as we walk through each section. But I keep an example fault tree that I've kept for 15 years that I can give to anybody that I think you will find almost intractable to understand.

You want to know something really funny? It's right.

Now there's a really much easier way to do it, and it's actually quite elegant how it was the done. The easier way is brute force and longer. The way it was done is quite elegant, but when you look at it it looks wrong.

There are two completely different things that I find would be very difficult to translate because the analyst cobbled it together or they had a certain impression in mind and went about it in a certain way, given the tools that they had to produce a result. That's going to result in this place as being an exception to the rule. And what I'm thinking is as you go through building these little blocks and trying to be able to call everything a certain size Lego, that there might be a few special Legos that look a little different that may not --

DR. EPSTEIN: No, no, no. We will do that as a test. That's a great test.

MR. CANAVAN: And I will provide you the test.

DR. EPSTEIN: Great.

DR. RAUZY: Really, I don't think so. Because this is really a descriptive way of --

MR. CANAVAN: It is.

DR. EPSTEIN: We'll see. We'll see. The more people we have involved, the better things will be.

MEMBER SHACK: Well that's an extensible language, so presumably --

DR. EPSTEIN: That's right.

MEMBER SHACK: -- if you have an exception, you can extend it.

DR. EPSTEIN: Exactly.

DR. RAUZY: The only point is that an extension is acceptable if its semantics is clearly defined.

MR. CANAVAN: Yes, correct.

DR. RAUZY: And it's clear that, for instance, some tools may not be able to deal with some particular construction. Okay. But at least we know where these construct are and we know their semantics, and that's all.

So I don't like to go into detail, but we have many built-ins like this to define an exponential or many other -- it's very complete right now.

And same for random-deviate. So we include well normal, uniform, low normal --

CHAIR APOSTOLAKIS: When you say "we include," you mean this exists already?

DR. RAUZY: Yes. Yes.

DR. EPSTEIN: We're on version two.

MEMBER SHACK: Now you have eight APIs for CAFTA. How many of these other programs do you have the APIs for?

DR. EPSTEIN: APIs don't exist for other programs.

DR. RAUZY: That's more or less all of the other programs are saving that data onto file so we can pass the file and --

MEMBER SHACK: Okay. But I mean they pare-able files?

DR. EPSTEIN: Right. And all the vendors are really on board here. All of them.

DR. RAUZY: So, well that's the stochastic layer. And we even include histograms like this to describe by hand probability distribution.

And also, to be able to take the result of a calculation which gives you a histogram and to put it back into the calculation engine. Histograms are used at the stochastic layer to define probability distribution of basically and then also as a result of calculations. And because we use the same formula, so it's easy to them back and forth.

So the extra-logical layer is really populated with all the extra-logical construct like CCF, delete terms, recovery rules that are used in PSA.

And why we put that at that level is that because basically this construct will change, as Ken say this morning, will change the fault tree.

I mean, they are applied into a fault tree and it change the fault tree.

So for instance, well delete terms, which is exclusive you mentioned this morning. There are many use to model impossible physical configuration like two train amendments at the same time. And there are different ways of interpreting such group of exclusion difference. For instance, we can use to post-process cutset, we can use as a global constraint or to perform local substitution in fault trees. And all these possibilities can be described within the standard and the tool can choose the most convenient for it, the most convenient semantics for it.

MEMBER SHACK: Finish your --

DR. RAUZY: And we have very simple XML definition of exclusion rule which is very easy to understand.

MEMBER SHACK: I'm assuming this is the layer where you would insert things like operational alignments and things like that that I want to run my model with train A running and I have three or four different maintenance alignments? Or is that something that's hard wired into the fault tree.

DR. RAUZY: No. We think that this

should be at the even tree layer, when at some sense you -- we have construct to define mission profiles. And you say you want to --

MEMBER SHACK: Okay. Continue with the event tree then, and see if I understand it there.

DR. RAUZY: Okay. So those layers, the three first layers are conceptually -- contain conceptually very different object, but there is nothing really new on that. It's just giving a format to existing stuff.

The real things are at the event tree layer. So that upper part of the diagram.

So we have to accelerate --

DR. EPSTEIN: No, no, no. Keep going.

CHAIR APOSTOLAKIS: IF you could speed it up a little bit.

DR. RAUZY: Yes, yes.

If you look at textbook at the event tree formalism is rather easy to understand. You just have functional event and then you follow the sequence; well, you know all of that. This appear simple. But if you look at what is done by the tools, actually it's not at all that simple for many reasons.

The first one is that while working

along the sequence you give flavor to the fault tree by setting out events, changing current events, things like that. The way you are house events depends on the branch you are working on. And the same fault tree for the sack of compactness may contain several initiating events. Some success branching in some tools are just interpreted as bypass actually. And there you may have multi-state branches and so on and so forth.

So really the point is that what are event tree, those that are actually used in practice is -- they really should be seen as a graphical programming language. And this is the man idea of this layer of the standard representation format. That is that we have the graphical view to describe the paths, the sequences and we have the sets of instruction to modify the fault tree we are considering while working along the sequences. And this has a formal semantics.

So we have a way to define event trees like this and a full set of instructions, but I won't go into detail to speed the process. The idea really is that we can do all that the tools are doing because we have this vision of event trees as graphical programming languages.

DR. EPSTEIN: This captures the flags in CAFTA. It captures the exchange events in RiskSpectrum. And it captures the split fraction rules in RISKMAN. So as far as we can tell from talking with all the people involved, this semantics and syntax will capture situations.

DR. RAUZY: Yes. To one more point --

MEMBER SHACK: I don't see where it captures the question that I asked, but we'll see if there's more time later. So keep going.

DR. EPSTEIN: Well, the idea --

MEMBER SHACK: Just finish the presentation. There's time for questions.

DR. EPSTEIN: Okay.

MEMBER SHACK: If there's time, we can come back to it.

CHAIR APOSTOLAKIS: Anytime you want, John.

DR. RAUZY: Okay. And the report layer just contains what is needed to describe the results of calculations and -- well, in different ways. So, for instance, we have a description for which calculation has been used with limits, which preprocessing techniques and so on and so forth. And some feedback about the results.

And also we start off with represent cutsets and to represent the result of the different probabilistic measures.

Okay. So that was to give you an idea of what the stand is. I would like to conclude my talk with some work for the future, that is the future phase back to 2008.

So we have the first version of the standard already on the website. And the version 2 will be available by the end of October and should be rather complete.

And in 2008 we defined a number of work packages we want to do, which includes some extension and evaluation of the standard expression prototyping and some organizational issue like giving a formal status to our group.

The work packages includes the scene you have here. The main ones are to validate what's the existing standard and to make extensive experiments by casting different types of modeling to the standard and see what happens in this level And also we want to study rules of modeling. We want to organize workshop to animate the community on these topics and to go on with the website, which will be a common forum for everybody.

And for prototyping, the idea is really to make this translator back and forth to the different PSA groups and calculation engine. And well that's the way it works.

Okay. That's what we want to do next year.

CHAIR APOSTOLAKIS: Thank you.

John, you wanted to ask now?

MEMBER STETKAR: Yes.

CHAIR APOSTOLAKIS: Okay.

MEMBER STETKAR: Well, I wasn't sure how long it would take.

Two actual questions. One I'll go back to this question regarding what I call system operational alignments. So think of testing maintenance normally running standby equipment. You know, think of it in a context of something like a service water system where I have some number of pumps normally running, some in standby, some can be out of service for maintenance, et cetera, et cetera.

I'm not aware of any modeling software that easily allows the user to specify those conditions. I can certainly wire them into a fault tree. This is running and this is not running, and this is not running. But if I have each train running, let's say, one third of a time in a three train system, I must consistently align my plant so that when service water train A is running, component cooling water train A is running and the equipment that's cooled by all of that stuff is running. It's not in a standby.

Now, why is this important? It may not be very important to calculate an average core damage frequency. It is very important when I'm looking at certain risk informed applications of testing and maintenance and how I operate the plant. It becomes very, very important if I look at shutdown risk.

This is not an event tree split fraction boundary condition walk the sequence type issue. Because the event trees typically do not show difference maintenance alignments in the event trees. Not in it he way people normally think of event trees.

So my question is how has this formalism thought about that part of the problem, because that is a difficult pat of the problem and it's an area of -- it is one area where I have seen huge differences depending on the particular software that people use in terms of how does an analyst, a poor analyst solve that problem?

So I'm not sure -- I've read and I've seen what you've presented here. And I haven't seen how the construct addresses that issue.

DR. RAUZY: Well, my answer will be in several steps.

The first one is that there is no silver bullets, that's for sure. Those are complex problems, and it's not easy to solve and I cannot do that and solve the problem for sure.

What we have here is really the vision that to get the model you're going to calculate, that is the fault tree you're going to calculate, you work through an event tree by setting different parameters. And this working mechanism provide you at the end the formula you are calculating of. And you are constructing the standard to describe the way you want to go through the sequences.

So if you are able by this construct on the top of the event tree in some sense to describe the specific plant operation you want to analyze, then the working mechanism will prove you a fault tree that describes this specific situation.

Now, this is a very technical answer,

and indeed I don't say the PSA analyst can do that easily. Then there is another job, which is to make it easy for the PSA analyst to do that, and this is the role of graphical user interface. Indeed, the standard representation cannot do that by itself. But that's the idea -- well, that's one of the idea Ken suggested this morning as well. That we need some high level graphical representation to be able to generate these things.

MR. CANAVAN: May I take a quick shot at addressing your problem?

MEMBER STETKAR: Sure.

MR. CANAVAN: This is the quintessential problem. This is the one where it doesn't translate directly between several methods. So you can't, even if you've done a right one, it will not directly convert to another. For example, if you modeled maintenance within a split fraction of RISKMAN, then it's modeled within the split fraction which is different than modeling in the link fault tree, which is among all the systems, right? Because the link fault tree, the maintenance terms will appear among all the systems. So that's one of the problems.

It's hard to write a language when you

don't have two things that actually agree. So you're going to have to make them agree. In other words, there'll be a cutset that you can't produce from the RISKMAN model that appears in the link fault tree model, which is maintenance of high pressure injection, maintenance of low pressure injection. Same cutset. But you wouldn't see that as an individual term in event tree unless it's a top event.

So there's one thing. It's different. You're going to have to make it talk.

The other part of the problem is that you brought up is it's really a hard problem. We're currently encouraging people to model their trees by changing the data to do what you're saying making it one-third, one-third, one-third and then just letting it solve itself. Because --

MEMBER STETKAR: That's a way.

MR. CANAVAN: Yes. Because if you don't do that, what you have to do is put in one-third, one-third, one-third as an event and then turn to of them off and one of them on. And what that starts to happen, is you have two big numbers in the fault tree again, and you don't want to do that. So sort of --

MEMBER STETKAR: Well, I recognize that. The only thing I was asking is when you're talking about a standard and framework and a language that you say is infinitely flexible or very flexible, let's say, and you talk about these different layers where the different layers have different interactions with the model itself, it's clear you've thought pretty carefully about several of the problems that many people have solved already. The development, common cause failures, the expansion of the logic and whichever type model you want to use for quantifying common cause failures, the ability to switch on and off house events, the ability to delete terms, things like that. It's not clear that you've thought or whether there is a simple construct or a reasonably standard construct that will help in some of these other areas. Because --

DR. EPSTEIN: John, if you can use a fault tree to represent it, it can be represented in the format. Now if that's the best way to represent it, fine. If you're doing it as a split fraction, it can also be represented. It's another question about whether new things, how we would do it. They don't exist right now in the tools, so they don't exist in the standards.

DR. RAUZY: But the standard is extension of enough --

DR. EPSTEIN: IF they exist in the tools, then we we'll make it exist in the standard..

DR. RAUZY: Now we plan to have several working groups and such issues can arise into the working group and we can try to provide new construct if necessary to the standard to do that.

MEMBER STETKAR: Let me ask you one other thing. And that has to do with the report layer. I actually read through the paper that was sent.

One thing that the report layer, and I understand all of what's here, do you envision, and this again is only for my own benefit, very useful in terms of reviewability of a risk assessment. And if you want to consider that as part of the function of a report. I may ask a question as a reviewer: Show me all of the contributors to core damage from reactor coolant pump seal LOCA. Okay.

Now, depending on how my results are developed I may have thousands and thousands of cutsets that are in the format of a battery fails and a pump failed to start and, you know, I don't know a valve failed to open.

When you solved the model if you had infinite knowledge, you would be able to look at that and say, oh well, it's clear. That's a reactor coolant seal LOCA, you know, cutset.

Do you envision as part of this reporting capability the ability for a user or reviewer to develop those types of logical questions? In other words, group all of the cutsets together that contribute to a specific set of sequences in an event tree?

DR. RAUZY: I didn't show because I --

MEMBER STETKAR: Because that was in your presentation or anything that I read in the paper either.

DR. RAUZY: No, no, no. It's not in there. But in the standard a version to it. The standard it's possible to define as many attributes as you want and to attach them to the different elements.

MEMBER STETKAR: Okay.

DR. RAUZY: And so you can have compacted version of the cutset, for instance, that say I want the cutset note by -- dated even, but by attributes.

MEMBER STETKAR: Okay.

DR. RAUZY: And so this is what I call the cutset browser. That means to use this notion of attributes to -- in some sense to collapse different cutsets to have an abstract vision of the cutset. This is the way they used, for instance, in the airplane manufacturing. They are using extensively that. So this feature would exist. And we put them into the standard --

MEMBER STETKAR: I just wanted to make sure you had thought of that. Because everything I had read it was kind of sort of the different ways of cutting sort of the standard things that you could see easily.

DR. EPSTEIN: Well, that's really going to be the job of each user interface. Like Risk, like RiskSpectrum, they're the ones that have to have the information to make the report that you're talking about. This is just a way to capture the information. We call it a report layer. Maybe a better name is the meta layer or the solution layer.

It gives the information from the calculation. If a calculation machine can put these attributes in, it will be captured. If it can't, they won't be there. All we're trying to do is make this part for all the viewers and applications to come in. That's all we're trying to do.

MEMBER STETKAR: Okay.

CHAIR APOSTOLAKIS: Dennis?

MEMBER BLEY: Yes, I've got a couple of related questions to go through the set.

I know a lot about how hard it is to look at a real physical system, including the people who work on it and build a fault tree. I don't know anything about how you go from that real physical system to BDD. Everything I read talks about processing the BDDs and the accuracy of that. I'm a little interested in how hard it is to actually develop the BDD and verify it. And related to that we're looking a lot at code correctness and algorithm correctness, which for more cases on a practical basis is a big deal but for some nasty cases it can be extreme. I would agree with that.

Is Open PSA looking at all that fault tree or BDD correctness and, you know, 30 years ago when we first started, 40 years ago with the fault trees the only way we knew to compare them with the simple systems we were looking at was to have two different people build fault trees, look at them in cutsets, which ought to be the same. With these massive models you're talking about you don't -- it real tough.

DR. EPSTEIN: Well, you're right. We don't build a BDD. All you do is build a fault tree. The BDD's constructed from the fault tree automatically by the code. By all of the codes. No one builds a BDD.

We take your good old fault tree you just built and we create a BDD out of it.

CHAIR APOSTOLAKIS: At this point I want to interject something. There is a question from a member, former member. You are the expert on BDDs. Can you give us in two sentences what is a BDD?

DR. RAUZY: It's a compact encoding of the truth table of the functions.

CHAIR APOSTOLAKIS: The truth table?

DR. EPSTEIN: That's all it is.

DR. RAUZY: It's a compact encoding of the truth table. That's all it is.

CHAIR APOSTOLAKIS: So you have input zero ones and you get a output zero one?

DR. RAUZY: Absolutely.

DR. EPSTEIN: It's just a fault -- it's just a truth table, that's all it is.

CHAIR APOSTOLAKIS: Okay. So Tom is happy and go back to Dennis.

Is your question answered?

MEMBER BLEY: No. The other side of the question is is Open PSA looking at correctness of the fault trees themselves or how to approach that, especially in these large ones?

DR. EPSTEIN: No. But if there's people that want to join and work with us who that's their area of expertise, good. It just isn't ours.

We have HRA groups now, a working group because there's HRA people that got involved. Not because of us.

MEMBER BLEY: Does anybody have an idea of where the greatest variability and results could be coming from as opposed to building the tree and the code themselves can?

MR. CANAVAN: No, I actually wanted to chime in on the last question because I would have answered it differently, because I would have answered yes. Because you're tackling a part of the correctness. Because if you plan to make it standard and generic transportable, if that's the goal of the standard, then you will lay down some rules that you can't violate.

Example, rare event approximation you might actually start putting in. You don't really want to use a number that's greater and you might actually physically the standard it could disallow the use of certain numbers and force you into a different route for handling it when it was inappropriate.

So in some cases I might argue that there's a fine line where you're start crossing into well should we let a modeler do something that's incorrect? Because you're writing standard. You're allowing the grammar in syntax. You're connecting a basic event --

DR. EPSTEIN: But that's -- what you're saying is not syntax. It's not syntax

MR. CANAVAN: -- it's another step.

DR. EPSTEIN: It's not syntax or semantics. What you're saying is right, but we're not the people to criticize the way models are built. We can point out where you'll have problems solving your models because of choices. But, however, we don't see that as our job or we haven't seen that as what we're pursuing.

MR. CANAVAN: You might get into some of it. I think there's no arguing that somewhere along the line there will be a correct usage of the language and an incorrect uses of the language and, you know, proper English or proper fault tree encoding will dictate some of the things.

For example, when you get into the special cases of putting in numbers like 365 into a fault tree. You may allow any value to be put in a certain field, but you may not. And as pat of that you get into the -- I mean, the whole purpose of a standard is to guide behavior, right, or codify existing practice. So you're sort of weighing in on what that practice is. So I might have answered the question and say well we're not the police but certainly in some cases we may end up correcting or adjusting some behaviors that happened in the past that we know are not valid.

DR. RAUZY: Let me add something about that. Right now to check the correctness of models people are using, and PSA analysts are using cutsets. Right? Cutsets are not only used to perform probabilistic calculation, but also to check up, yes, this is a potential scenario of failure of core damage or whatsoever.

What we think is that beyond the cutsets something that would be very interesting, and we're going to work on that, is to view what part of the model is actually used once you have computed cutset.

Let me explain it. For instance, under the US PSA it was Duke? So we looked at -- it's clear that only five percent of the basic even show up in the cutset. So the cutset give information that it's really interesting to take this model and to use the cutset to prove the model and to keep into the model only the relevant parts, that is the part that has been actually calculated. And this, you start with a model with almost three times in basic event and you end up with a model that has something like 100 or 200 basic events, which is much more human readable, much more human understandable. And this is the kind of thing we want to do with this Open PSA initiative is to provide that kind of tools.

DR. EPSTEIN: Yes. Already we've done that. We've taken huge, huge trees, we've pruned them down to what's actually calculated, then moved back into the tool they came from so you can look at the fault tree you really solved.

Some people --

MEMBER BLEY: Really interesting, yes.

DR. EPSTEIN: It's really interesting. And then to say well why did I leave out? What is it?

MEMBER BLEY: Why doesn't it matter?

DR. EPSTEIN: Why doesn't it matter? It's the questions that it raises that are more important than the numbers.

CHAIR APOSTOLAKIS: You are --

MEMBER BLEY: I'm sorry. I have one more if you get a chance.

CHAIR APOSTOLAKIS: Oh, okay. Go ahead.

MEMBER BLEY: Well, the other one, and we were close with John's question, in your report layer are you giving any thought to things that non-PRA specialists, presentations -- you talked about visualization -- presentations of the results and ways to use this that non-PRA experts might find easier to understand?

DR. EPSTEIN: Yes. We're trying to get a working group that is in the visualization of results. And there's a guy that just the McCarthur Award from Karolinska Institute who has developed a lot of his technique from the World Health Organization. And he wants to work with us on this. So we'll get that work --

MEMBER BLEY: It might be nice if he had some operators that can do that.

DR. EPSTEIN: Yes, it's really interesting. And we'll be getting this together at the meeting in Vienna in December.

I think that Mark Reinhardt who sits on the Board of Open PSA, he's from IAEA and hosting the meeting. And he's really interested in data visualization and sharing of industry data.

MR. REINHARDT: Maybe I would just comment on that.

I'm Mark Reinhardt from the International Atomic Energy Agency. And when we heard of the Open PSA we did become very interested. And maybe just to show why, I'm sure many of you know the perspective we have. If you look today there's 32 member states that have nuclear power plants. Our 20/20 planning approximation is that 15 additional states have already declared an intent to go to nuclear power. Twenty more are interested. So that gives us about 440 nuclear power plants worldwide, assuming even if 80 shutdown, there's 20 additional plants being built. And many of these countries are not what you would call the sophisticated infrastructure countries. So they're going to need some simplification, some standardization.

So what we're looking for is a way to do that. And to support this effort, among other things, we're developing or have a developed a center. It's called CASAT. It's the Center for Advanced Safety Assessment Tools. And we're looking for ways to assimilate, coordinate and disseminate data assumptions, information that goes into the PSA so that the various member states can use that.

And an illustration I like to use is looking at the U.S. a few years back going into the Civil War, there were 20 standard railroad gauges n the United States. Twenty standards. So there was no standard. A train on one track would encounter another track, and to offload freight, passenger, reload to another train. So we ask is that efficient? Is that effective? Is it safe? Well, no it's really not.

The Congress mandated that the U.S. have a standard gauge. And during the Civil War they relaid 3,000 miles of track and countless miles afterward.

And you might ask yourself was that expensive, was that effort? Sure it was. But if you ask the railroad industry today was it worth it, I think they'll say that it was.

And so what we're trying to do is look down the road. Internationally nuclear energy technology use is more closely coupled. So what can we do today to make things better in the future. And we think this is a piece of that.

CHAIR APOSTOLAKIS: I can't hear you.

Okay. Okay. Are there any other questions from the members, because there's one last thing I want to do.

Your second slide, Steve, was a list of questions.

DR. EPSTEIN: Right. Want me to put them up?

CHAIR APOSTOLAKIS: Maybe we can them up and see if we can give concise answers.

So the first question is what the issue? Can we summarize what is the issue here in a sentence or two? What is the issue?

DR. EPSTEIN: What is the issue?

CHAIR APOSTOLAKIS: Yes.

DR. EPSTEIN: From my viewpoint?

CHAIR APOSTOLAKIS: Well, if you can give me somebody else's.

DR. EPSTEIN: All right. I could give you many things --

CHAIR APOSTOLAKIS: Well, I mean you guys are the --

DR. EPSTEIN: The issue is how do we go forward with new software and mathematical methods in nuclear PSA. And why is it an issue? Because we think we have found some rocks in the garden. The work of the -- flow, the thing we found in the Japanese plant. This isn't to say it's all bad. We have found rocks in the garden.

CHAIR APOSTOLAKIS: Now, Ken, you agree with those?

MR. CANAVAN: I have a different what and I have a different why.

My what would be well what's the issue? We spend a lot of resources on this, PRA.

CHAIR APOSTOLAKIS: Yes.

MR. CANAVAN: And we peer review each other. And we have to divide ourselves by BWR or by PWR and by method, and by approach and even then it's difficult to understand what one analyst did versus what another analyst did.

And lastly, sometimes analysts do it wrong.

So the whole idea here in my opinion would be if you were to develop an architecture where analysts were a little bit constrained, not crazy, but a little bit. And that architecture constrained them to what's right. You could literally possibly start to merge and come closer when you have a standard. So going through peer reviewing one to another becomes easier.

So my explanation is: What is the issue? Well, the issue is moving ahead with resources and being able to understand all the platforms and to peer review them, verify them and have reasonable trust in their accuracy.

Why is it an issue? I don't disagree with the rocks in the garden. I think some people put them in there on purpose. They're not just not good gardeners. They had an issue and they didn't fully check. I mean if you're going to use risk importance measures and you have a truncation limit, one would assume that you take your model and run it until you get something stable before you report to the regulator. At least that's what I did in 1995. And in 1990 -- I think it was '93, actually, I published a paper in one of the PSA forums which is the Effective Truncation on Risk Achievement Worth Calculations. And that totally delineated the fact that you need to run various truncations until you get an established reasonably stable point measure.

So why is it an issue? Well, it's an issue because we have some rocks in the garden, some people threw them in, but again really to me the why aren't really that far. It's resources.

CHAIR APOSTOLAKIS: Okay. Third question.

DR. EPSTEIN: Would changing the PSA calculation methods effects NRC's decision making processes?

CHAIR APOSTOLAKIS: Well, significantly to justify.

DR. EPSTEIN: Well, until we have the exact answer for some large scale industrial strength PRAs I can't answer that, because I don't know what the difference is.

CHAIR APOSTOLAKIS: And risk issue.

MEMBER BLEY: How likely are these funny cases?

CHAIR APOSTOLAKIS: Yes.

DR. EPSTEIN: Yes. I just don't know. But I think that if we have the exact answers, that we'll know. We can say, look, we accept answers. We can it the fast way.

CHAIR APOSTOLAKIS: Ken, I assume you

agree with Steve. I mean, please, speak up Antoine, if you disagree or you want to clarify something?

DR. RAUZY: No, no. Just to correct a bit what you say. Ken, about this importance factors done at EDF by Nicolov Duflot. HE went up to a cutoff of 10 to the minus 20, and it still -- and the number of cutset he has to deal with was several hundred millions. So it's not an issue of going bit with -- you know decrease a bit the cutoff. Because here it takes weeks of calculations. So it's -- well --

CHAIR APOSTOLAKIS: So the way I understand it is there are some disturbing messages from these studies, and we would like to understand what is going on. Okay.

DR. EPSTEIN: I want to see the why.

DR. RAUZY: But just I want to add something is that I don't in the beginning, since I was the one who introduced BDDs in this field, I really wanted to make the BDD methods very successful and to be able to calculate everything with BDD. But after years of working in that domain, first of all, I think that it's not that easy to convert everything into a BDD. And second, and mainly I think the main problem stands in the model. Not in the calculation necessarily. The main model is to understand, to master, to maintain, to document, to structure the models. And for me that's the main issue and that's the main issue of the Open PSA initiative.

CHAIR APOSTOLAKIS: Okay. Good. Good.

MR. CANAVAN: Well, that was an excellent segue, because I think in this particular case we start getting confused about the initiative and BDD. BDD is a quantification method. There's a bunch of them. BDD is not attractable for all the models. Can't use it for everything. Can use it for some things.

So I don't see it having a lot to do with BDD here. If you develop a PSA method that allows you to go from method to method to method, I think that how it stands upon its own and it's its own benefit. BDD is something that we all should strive for, not because we want to eliminate simplifications, just because we're tired of describing them and explaining them. If we didn't have them, it would be better. It's simple. We're struck with them for now, so being able to move from model to model to model satisfies an objective, something we do right now, which is when we quantify the models we check it for sanity and then we compare to what we think would have gotten using other methods. And that's what we do. We peer review against ourselves. So we swap our new quantification engine, and the first thing we do is is say -- well, we say the old modification engine produced this, what's the difference.

And we go through a million cutsets when we switch from FTRex to a FTForte to FTRex. And we find the two that are different and find out why. And go to the code and find out that one code truncates slightly earlier than the other, and there's four cutsets missing out of a million.

So we are pretty confident that that result is at least stable and probably reasonably accurate if they use the method appropriate.

So in the end I think the answer to that is I think that if we had consistent treatment of all the models, we would more than cost justify the resource the allocation.

I do think that there's a lot more work than you might have been portrayed at this particular meeting in getting there. I think that there's a lot of exceptions. And if we start imagining by exception the workload gets big. Does it outweigh moving ahead? I'm still thinking about that personally. I think in the long term, paying the fee that we pay now by putting in resources constantly to review desperate things; that's a lot of resources that add up over a long period of time to answer the question that yes, it's worth looking at doing something that's more consistent, more accurate and more reviewable.

CHAIR APOSTOLAKIS: So if you were to advise the Commission what to do tomorrow, what you would advise them to do?

MR. CANAVAN: Well, I'd have to ask them to wait until Wednesday so I went to tomorrow's meeting and heard how far we're going, what the approaches we're taking. But I think it is worth pursuing commonalities.

One of the things I've noticed in all the advance research that even without this initiative going on is all the methods are quickly coming closer together. Anybody noticed declarative modeling and linked fault tree space is awfully similar to rules in RISKMAN. And that's because many years ago I worked in RISKMAN space and wrote rules. So when I moved to link fault tree space, I said you know what this is missing? This is missing rules. So declarative modeling was born as a way to add a depth to the model that reflected something, a positive of another method.

Now there are probably some issues with that method as well where we could sort of bed back. And I think as these exchange efforts go on you can see methods moving towards a central point. And that's good. Because we have 64 different PRAs and having been a PRA reviewer on about 10 of them, they're too different. We need to move together. And any effort that gets us closer together, including this one, is a good thing.

That's how I would weigh in.

CHAIR APOSTOLAKIS: Comments? What would you tell the Commission to do?

DR. EPSTEIN: I would say to support this notion of building a standard representational format. And to do a test case very quickly to see if it's workable in the things the Commission is interested in, such as review of models that are made in different software by people who know how to review the models.

It seems to me if we could make a good success of that, it would seem to me to be something that we should then say let's move forward. That's what I would say.

CHAIR APOSTOLAKIS: Antoine, do you have any final comments?

DR. RAUZY: I agree with both.

CHAIR APOSTOLAKIS: Do the members have any comments or views that they would like to air? This is the time.

MEMBER MAYNARD: I don't want to extend it on out. I believe that the more we can do to move toward standardization I think helps not only the analyst and everybody else. I try to look at it from a regulator standpoint. You know, what's important to the regulator. And with all the different models, different methodologies, different things out there it really becomes quite difficult, I think, for the regulator to be able to evaluate and know what to believe and what not to believe. So I'm all in favor of moving towards standardization.

I'm not sure how fast we're going to be able to get there and be effective, but I do think that it's important to start moving down a path in that direction.

I also want to make sure that we -- I think we have to be careful that we don't try to make PRA so accurate that we start believing the actual numbers. I think the trends and the tools, I think are very important. But you know maybe in a million years of operating the same plant with no changes, we would know which method might be the most accurate. But, you know, I don't know.

I think the trends and relative importance -- I think just putting the models together is one of the most important parts of getting value out of a PRA.

But at any rate, bottom line I think moving towards standardization would be good from a regulatory process.

MR. GUARRO: George, just a comment. That having worked in related areas with models that are not binary can be used to support a PRA binary model, I would just kind of want you to think about how a standard would somehow house input that may come from these supportive models.

DR. EPSTEIN: It does already. It handles both RISKMAN and RiskSpectrum are multi-state trees, so it goes far beyond the binary part of it. It's already part of it.

MR. GUARRO: Because it might otherwise might --

DR. EPSTEIN: No, no. Your tool can move right into it.

MR. GUARRO: No, no. I don't like to --

DR. EPSTEIN: That's right. But I understand. Yes. There's no problem. No problem.

CHAIR APOSTOLAKIS: John?

MEMBER STETKAR: Otto, I wholeheartedly agree with you. I think risk assessment 99 percent of the worth of it or more is just building the model. However, in practice and unfortunately as we go forward here, people tend to rely more and more and more and more on those numbers.

And in terms of where do we go from here, both in methods development and what helps the staff, what helps the agency, again I'll bring up the fact that I believe, and we've already seen some evidence of this that the new generation of plants, however you want to define that, the vendors, the licensees are paying much, much more attention and putting much, much weight on those numbers from the risk assessment as we go into more complicated designs and as we go into more passive features and things like, as I mentioned before, digital I&C stuff that people tend to assign very, very high reliabilities resulting in very low numbers, I think that the tools that we use then must acknowledge the fact that we can't cut as many corners as we used to because well, you know the core damage frequency is X and there are only 500 cutsets that contribute to X, and we can be confident that that's 95 percent or a better percent of X.

I think that what we'll see in the future is not that simple. So anything that extends our ability to more consistently evaluate and understand those -- not just evaluate, not just quantify the precision in a very small number. But really understand the contributors to that very small number in a consistent manner would help a lot. And help at the regulatory review level also.

CHAIR APOSTOLAKIS: Okay.

MEMBER BLEY: I would move to add something a little bit.

Standardization on the surface sounds really good to me. I think we need to be careful, and John hit on some of the points, as we go to new designs. These are open ended models or open ended questions that require a lot of thought and understanding. The standardization can't mean doing thing by rote. You have to keep the thinking in. And as we go to some of these more passive designs, you have to think a lot harder about how you could break down supposed redundancies by dependent effects. And I don't think that's ready quite for standardization yet.

CHAIR APOSTOLAKIS: Any other comments or views? Okay.

MEMBER POWERS: Well, I'll just reiterate a lot of what has been said today has been intensely interesting to me because I think that it's important that we not allow within the agency methods to stagnate. And I think that's happened because of the press of business, likely. And the press of business that's coming up is liable to let it continue to happen. And we need people out there thinking about new methods and whatnot.

I'm not a real fan of standardization in this area because I think it's a little premature to do it. I think the regulator's approach is going to have to be to do things independently, to a large extent, for some time yet.

I do come back to concern about importance measures. But I think they are the real key to the regulatory use of PRA Much more so than even defining dominant sequences or certainly much more important than bottom line risk numbers. And I continue to think that our important measures are primitive, not consistent with our understanding. They tend to amount to looking at one event at a time kinds of things when we know that they are things that are multiple events and stuff like that.

And I think that one of the directions I would hope thinking about PRA goes is improved importance measures.

CHAIR APOSTOLAKIS: But this is a little outside of what they're going to do.

MEMBER POWERS: It is outside of what they're trying to do.

CHAIR APOSTOLAKIS: Yes.

MEMBER POWERS: And that's why I bring it up. Because there's another dimension here that needs to get our attention.

CHAIR APOSTOLAKIS: Okay. Anything else?

Well, gentlemen, thank you very much. It's clear from the comments of the members of this Committee it has been very interesting. And thank you for coming here.

And all the success tomorrow.

And this meeting is adjourned.

(Whereupon, at 12:13 p.m. the meeting was adjourned.)

CERTIFICATE

This is to certify that the attached proceedings before the United States Nuclear Regulatory Commission in the matter of:

Name of Proceeding: Advisory Committee on Reactor Safeguards

Docket Number: n/a

Location: Rockville, MD

were held as herein appears, and that this is the original transcript thereof for the file of the United States Nuclear Regulatory Commission taken by me and, thereafter reduced to typewriting by me or under the direction of the court reporting company, and that the transcript is a true and accurate record of the foregoing proceedings.

Charles Morrison

Charles Morrison
Official Reporter
Neal R. Gross & Co., Inc.

Software and Standards: Words from History, Bits from the Future

Steve Epstein
Open PSA
ABS Consulting
sepstein@absconsulting.com
SKYPE woodyep

The Purpose of This Meeting

- What is the issue?
- Why is it an issue?
- Would changing the PSA calculation methods affect the NRC's decision-making processes significantly to justify the resources required to effect such a change?
- How is your approach different from that of traditional methods? Minimum mathematical arguments, please. Be descriptive.
- Can you give clear examples demonstrating that current results are inadequate to a degree that would affect decisions?

21 years ago, risk software boldly stepped out to go where no risk software had gone before …

… to the PC.

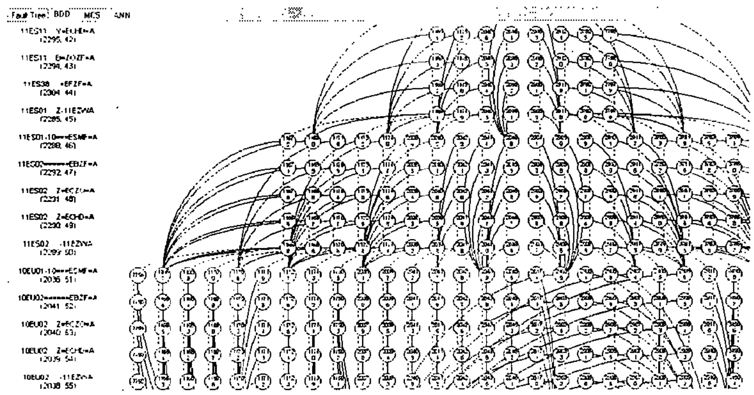
CAFTA, RISKMAN, Saphire, SETS, FTAP, and NUPRA in a group photo, circa 1986 and over those 21 years, our abilities in and demands of PRA analysis have grown …

- Safety Monitors;
- Model size;
- On Line Maintenance;
- Risk Informed Applications
- Seismic, fire, BOP, and flood analyses;

… we have made strides in computer software as well…

Alternative Data Structures
Directed Acyclic Graph (DAG) and BDD

- BDD complexity is not related to the number of prime implicants of the encoded formula
- This small BDD (37620 nodes) encodes a total of 10^9 cutsets

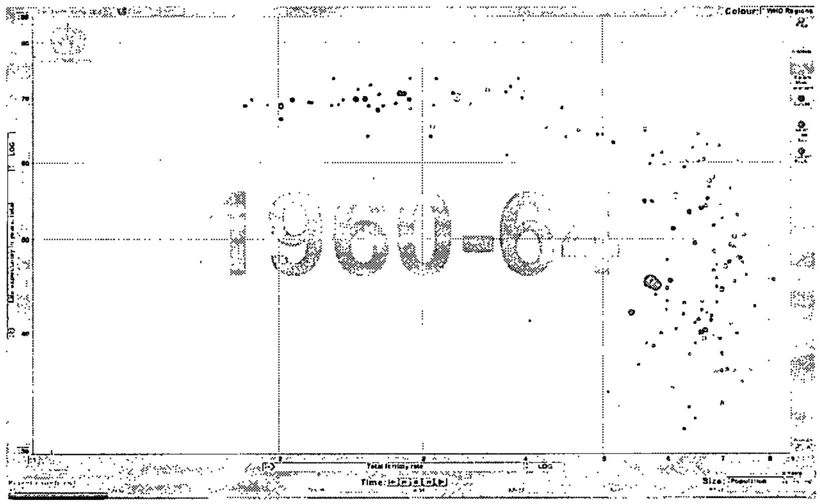


Coding Breakthroughs

In a recent PhD thesis concerning nuclear PSA* large FT models could be solved analytically for >3000 basic events, with no truncation.

* Analytical Solutions of Linked Fault Tree Models using Binary Decision Diagrams with Emphasis on Nuclear Probabilistic Risk Assessment
---------- Dr. Olivier Nusbaumer, 2007

New Ways of Visualizing Data



Because of these successes, we have heard in the streets and marketplaces the rumblings and rumors of creating …

PRA SOFTWARE
The Next Generation

We, however, a small group of computer scientists working in risk assessment, became focused on some other issues …

- Quality assurance by comparison; ☑
- Peer review of algorithms; ☑
- Portability of the models between different software;
- Clarity of the models;
- Correct uncertainty and importance calculations; ☑
- Assurance of model completeness as quantified; ☑
- Model access by new PRA software;
- Formal verification of calculation methods; ☑
- A universal format for industry data.

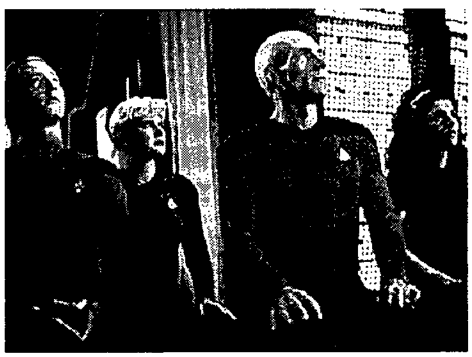
What is really needed, before we develop new methods, software, and user interfaces, is to take a look at what we have now and to realize …

There is no free lunch.

Model Size And Problem Complexity

What's in a name?
That which we call a truth table
By any other name would taste as bad;
- William Shakespeare

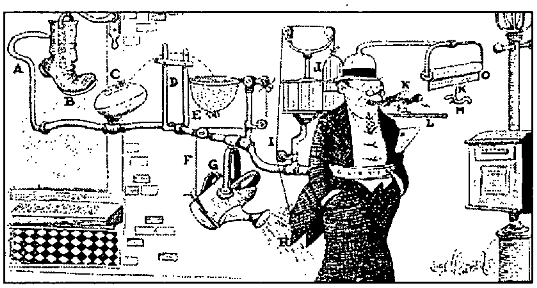
So before beginning the "Next Generation" PRA Software (no matter how nice the vision ...)



Looking at The Vision of the Next Generation PRA Software

... and to avoid the dreaded ...

Second System Effect



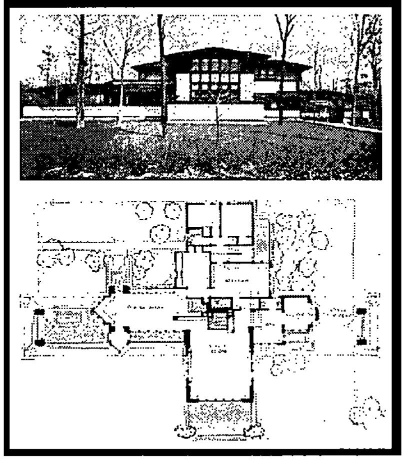
Rube Goldberg gets caught in a revolving door and becomes dizzy enough to dope out an idea to keep you from forgetting to mail your wife's letter.

As you walk past cobbler shop, hook (A) strikes suspended boot (B), causing it to kick football (C) through goal posts (D). Football drops into basket (E) and string (F) tilts sprinkling can (G) causing water to soak coat tails (H). As coat shrinks, cord (I) opens door (J) of cage, allowing bird (K) to walk out on perch (L) and grab worm (M) which is attached to string (N). This pulls down window shade (O) on which is written, "YOU SAP, MAIL THAT LETTER." A simple way

...we must create a PSA Software ...

ARCHITECTURE

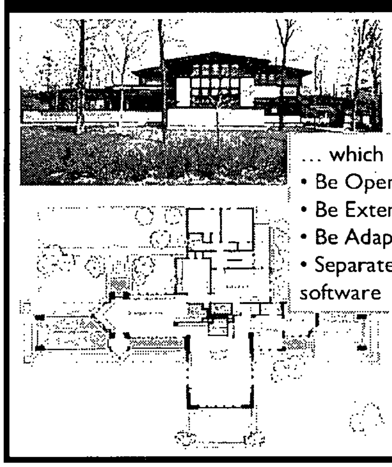
Ward W. Willits House, 1901, Highland Park, Illinois



...we must create a PSA Software ...

ARCHITECTURE

Ward W. Willits House, 1901, Highland Park, Illinois

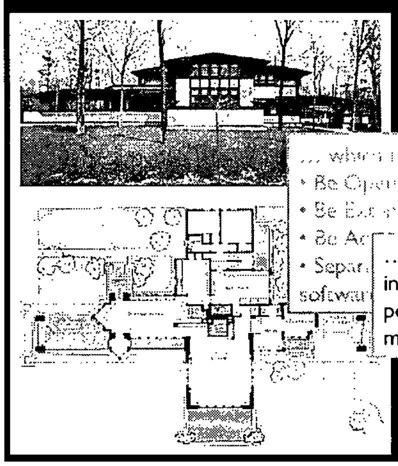


... which must:
- Be Open
- Be Extensible
- Be Adaptable
- Separate data and software

...we must create a PSA Software ...

ARCHITECTURE

Ward W. Willits House, 1901, Highland Park, Illinois



... to allow the greatest inter-connectivity and portability between data, models and software.

... and in this way, we can make headway against the hobgoblins of complexity.

- Model Size
  - Elements of Modeling Style
  - Declarative Modeling
- Problem Complexity
  - Modeler based heuristics
  - Structured Modeling

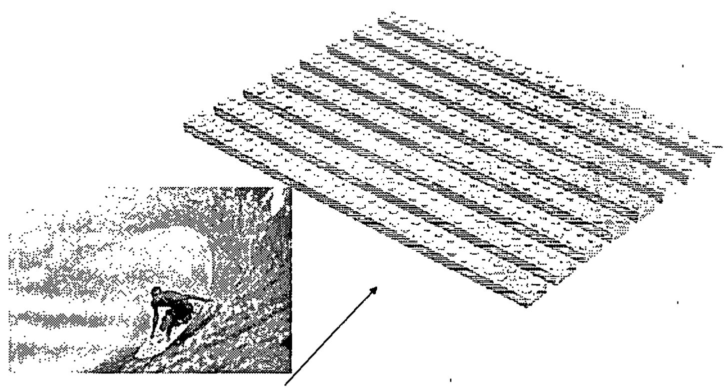
Our Proposed PSA Software Architecture

- The foundation is a standard for representing a PSA model, therefore facilitating independence between model representations and software;
- Each risk application would generate a model in this standard from it's own internal representation;
- Viewers and calculation engines would interface with models via the standard representation.

… but enough words, let's look at this like engineers ...

The LEGO Model of the PRA Architecture

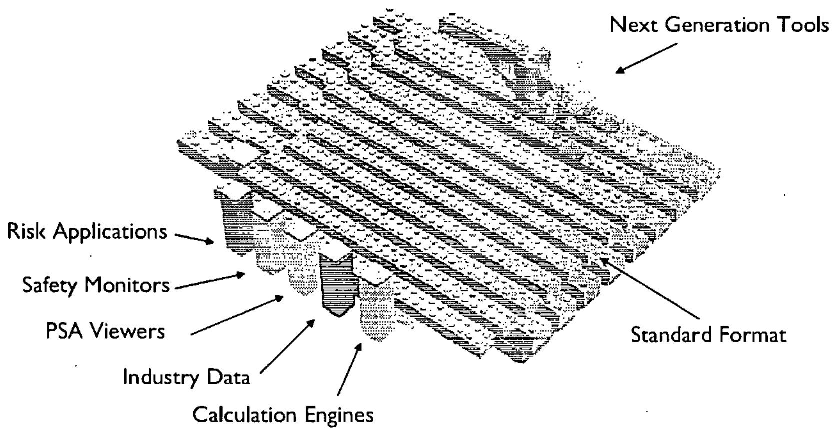
… first the foundation …



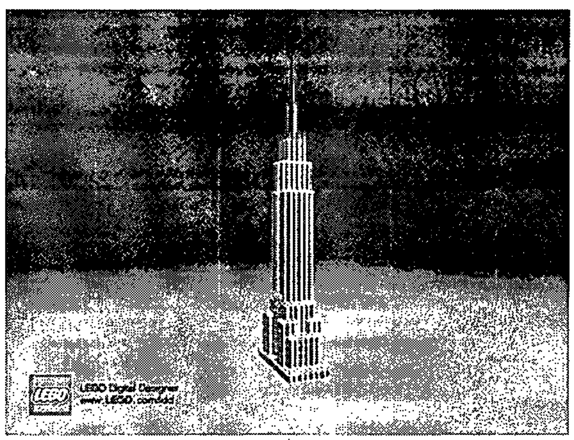
Standard Representation Format (SuRF)

catch the wave of the future

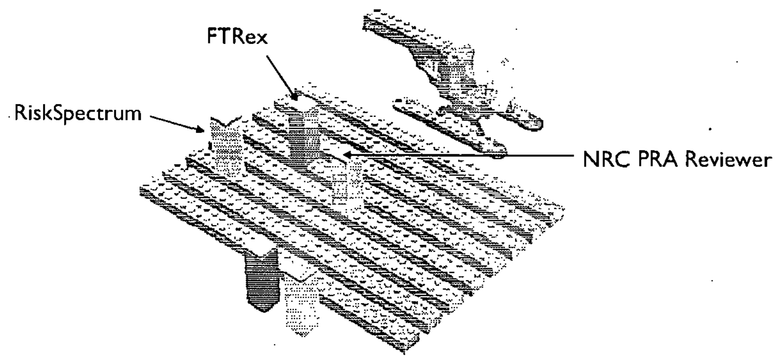
… now assemble the risk applications and data …



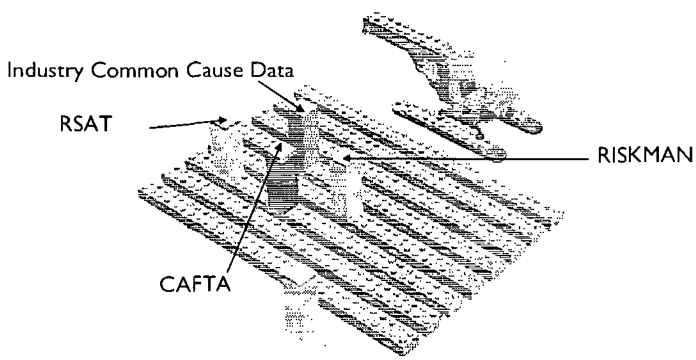
… and then build upon the foundation …



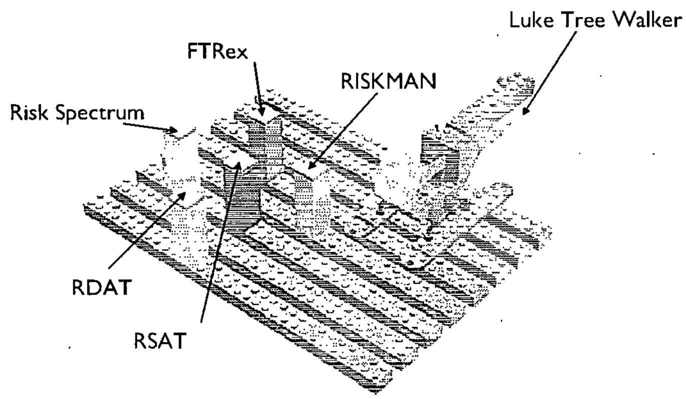
… for example …



… or this …



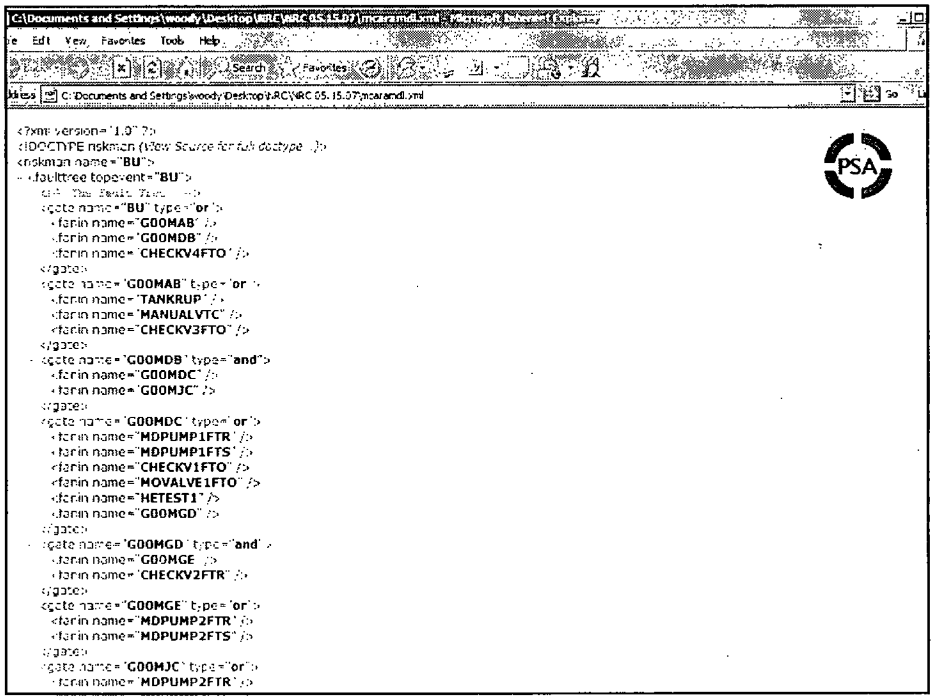
… or even this …



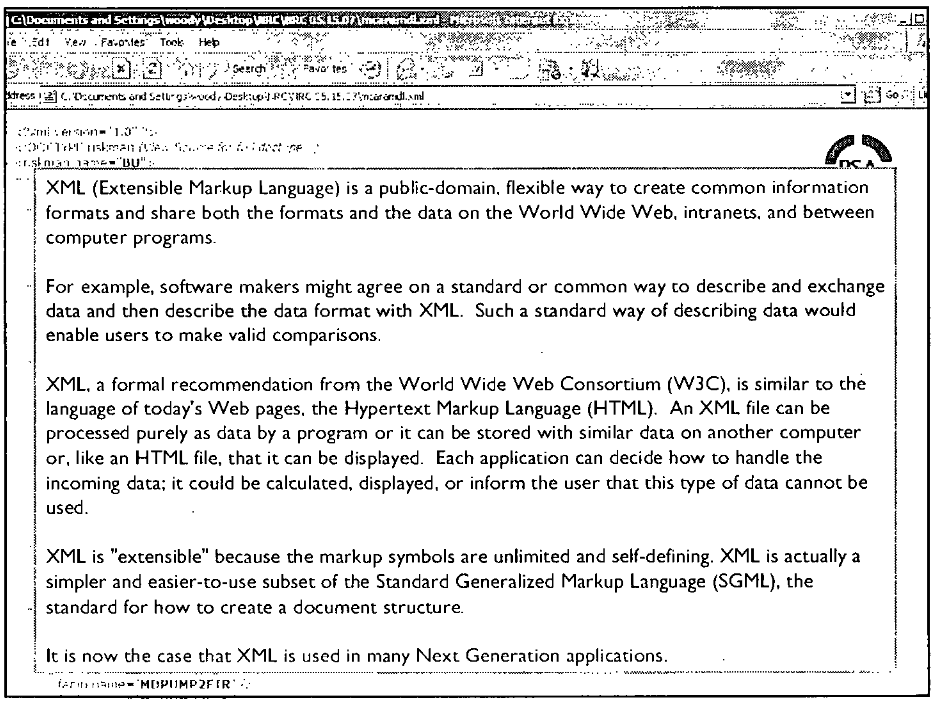
… all interconnected through the foundation: a Standard Representation Format.

This is not just imagination.

We have actually used a prototype format like this in research and production.




```
<?xml version="1.0" ?>
<!DOCTYPE riskman (View Source for full doctype...)>
<riskman name="BU">
- <faulttree topevent="BU">
    <!-- The Fault Tree -->
    <gate name="BU" type="or">
      <fanin name="G00MAB" />
      <fanin name="G00MDB" />
      <fanin name="CHECKV4FTO" />
    </gate>
    <gate name="G00MAB" type="or">
      <fanin name="TANKRUP" />
      <fanin name="MANUALVTC" />
      <fanin name="CHECKV3FTO" />
    </gate>
  - <gate name="G00MDB" type="and">
      <fanin name="G00MDC" />
      <fanin name="G00MJC" />
    </gate>
    <gate name="G00MDC" type="or">
      <fanin name="MDPUMP1FTR" />
      <fanin name="MDPUMP1FTS" />
      <fanin name="CHECKV1FTO" />
      <fanin name="MOVALVE1FTO" />
      <fanin name="HETEST1" />
      <fanin name="G00MGD" />
    </gate>
  - <gate name="G00MGD" type="and">
      <fanin name="G00MGE" />
      <fanin name="CHECKV2FTR" />
    </gate>
    <gate name="G00MGE" type="or">
      <fanin name="MDPUMP2FTR" />
      <fanin name="MDPUMP2FTS" />
    </gate>
    <gate name="G00MJC" type="or">
      <fanin name="MDPUMP2FTR" />
```

XML (Extensible Markup Language) is a public-domain, flexible way to create common information formats and share both the formats and the data on the World Wide Web, intranets, and between computer programs.

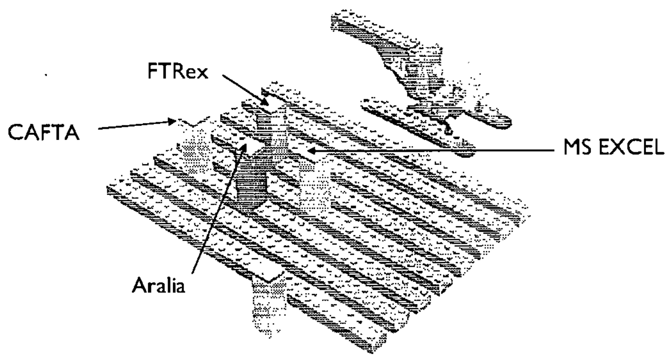
For example, software makers might agree on a standard or common way to describe and exchange data and then describe the data format with XML. Such a standard way of describing data would enable users to make valid comparisons.

XML, a formal recommendation from the World Wide Web Consortium (W3C), is similar to the language of today's Web pages, the Hypertext Markup Language (HTML). An XML file can be processed purely as data by a program or it can be stored with similar data on another computer or, like an HTML file, that it can be displayed. Each application can decide how to handle the incoming data; it could be calculated, displayed, or inform the user that this type of data cannot be used.

XML is "extensible" because the markup symbols are unlimited and self-defining. XML is actually a simpler and easier-to-use subset of the Standard Generalized Markup Language (SGML), the standard for how to create a document structure.

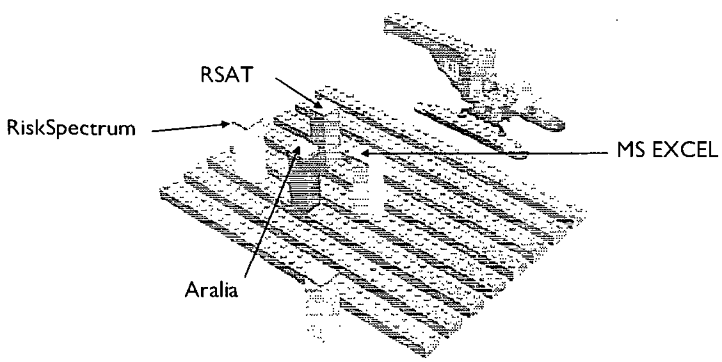
It is now the case that XML is used in many Next Generation applications.

Example #1



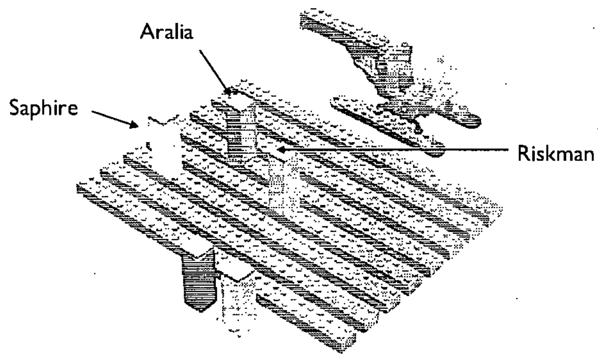
Three different FTL models from three different US organizations.

Example #2



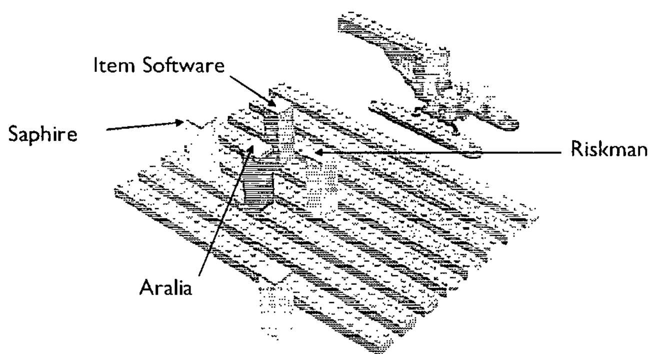
A Japanese core damage model solved exactly with BDD.

Example #3



An investigation of a SPAR model.

Example #4



A sanity check on the MER PRA done by NASA.

So what have we been doing to bring these benefits into existence?

- Quality assurance of calculations;
- Peer review of algorithms;
- Portability of the models between different software;
- Clarity of the models;
- Correct uncertainty and importance calculations;
- Assurance of model completeness as quantified;
- Model access by specialized PRA software;
- Consistent knowledge of numerical approximations' error bounds;
- A universal format for industry data.

---

arboost   Kernkraftwerk Gösgen   ABS Consulting

Workshop Announcement

Next Generation PSA Software, Declarative Modeling, and Model Representation Standards

[illegible]

Kernkraftwerk Gösgen-Däniken, Switzerland

Call for Participation: [illegible]

- Quantification Methods;
- User Interfaces;
- Declarative Modeling;
- Standard Model Representations;
- PSA Visualization;
- PSA Software Architectures;
- New Algorithms;
- Modeling Styles and their Effects on Clarity and Quantification;
- PSA Software Verification, Benchmarks, and Quality Assurance

How to Participate: [illegible]

Organizers: [illegible]

Steve Epstein	[illegible]
Antoine Rauzy	[illegible]
Dan Wakefield	[illegible]

We created the Open PSA Initiative

EdF
AREVA
KAERI
PSI
RelconScandpower
IAEA
Gesellschaft für Anlagen-und Reaktorsicherheit
AXPO/NOK
KKL
ABS Tokyo
ABS Irvine
ARBoost Technologies
Empresarios Agrupados
KKG
Swiss Federal Institute of Technology (ETH)
BKW FMB
UTT
RISA
Instituto de Investigacion Tecnologica.Universidad Comillas Madrid

We wrote a Statement of Purpose and created a web site to share ideas.

"We hope to provide an open and transparent public forum to disseminate information, independently review new ideas, and spread the word. We want to emphasize an openness which will lead to methods and software with higher quality, lead to better understanding of PSA models, encourage peer review, and allow the transportability of models and methods." --- from www.open-psa.org

Open Initiative for Next Generation PSA Software

arboost EDF ABS Consulting

Technical Working Group Meeting #1
Standard Representation Format for PSA Models

July 19th, 2007
Electricité de France
département Management du Risque Industriel, Paris

Call for Participation: In response to the "next steps forward" charge given by the Open Initiative, the first working group meeting for the Standard Representation Format for PSA Models will begin discussions. Dr. Antoine Rauzy will be the session chairman. Participation is open to anyone in the international PSA community.

How to Participate: Please fill out the attached form and eMail to Antoine Rauzy at [illegible] as soon as possible. Please put the word "Working Group" in the subject line. We will make every effort to make room for anyone who wants to participate. This is an open technical forum for the exchange of ideas.

Meeting Location: The workshop will be held at Electricité de France, at the département Management du Risque Industriel, which is located in Clamart, a southern suburb of Paris, about 25 minutes from Porte d'Orleans, the terminus of Metro line #4. For location information: [illegible]. If you do not know Paris well, there will be a meeting place at Montparnasse at the cafe of the restaurant Le Dome (Metro Vavin) at 08h30 and at Porte d'Orléans at 09h15.

Open Initiative for Next Generation PSA

arboost EPRI ABS Consulting

Workshop Announcement
Next Generation PSA Software and Model Representation Standards

October 3rd, 2007
EPRI, Washington D.C., USA

Call for Participation: [illegible] PSA [illegible]

- Quantification Methods and Algorithms
- User Interfaces and results presentation
- Declarative Modeling
- Standard Model Representations
- Data and Results Visualization
- PSA Software Architecture
- [illegible]
- Modeling Styles and their Effects on Clarity and Quantification
- Uncertainty and Importance
- PSA Software Verification, Benchmarks and Quality Assurance

How to Participate: Registration must be done on the EPRI website [illegible]. As well, please fill out the attached Intention to Participate form and eMail to Steve Epstein [illegible] as soon as possible. [illegible]

Organizers: This workshop is organized by ABS Consulting, ARBoost Technologies, and EPRI, the Electric Power Research Institute. [illegible]

Steve Epstein	[illegible]
Antoine Rauzy	[illegible]
Ken Canavan	[illegible]

A Standard PSA Model Representation Format
Scope and Needs Statement for ASME

Scope: We propose that an independent international standard format be created to represent computerized PSA models and industry data in digital form. We propose that an ASME subgroup be created to (1) create a prototype Standard Model Representation Format (SMRF), (2) present examples in the prototype format, and (3) deliver a report as to the efficacy of the prototype in addressing the "Needs" statement, below.

Needs: Over the last 5 years, new calculation techniques, such as BDD, have been extensively studied in nuclear PSA, and research efforts made in the direction of "next generation" PSA software and "declarative modeling", which try to present a more informative view of the actual systems, components, and interactions which the model represents.

The concern of these studies has been to end the use of approximations, numerical approximations for which we do not know the error factors, and modeling approximations which leave out perhaps critical elements of the actual plant.

From all these investigations, some alarming issues related to large nuclear PSA models have been raised, which we feel need to be addressed before we put new calculation engines or next generation user interfaces into place. We believe that to address these issues enumerated below, a SMRF for PSA models, a representation which is independent of all PSA software, must be in place. Each software would retain their own internal representation for a model, but each software would also be able to share models and industry data by means of the SMRF

1. **Quality assurance of calculations:** at the moment, a model built with one software, such as CAFTA, cannot be simply quantified with another software, such as SAPHIRE or RiskSpectrum, and visa versa; there are too many software dependent features used by modelers to make inter-calculation comparisons a one-step process. A standard representation will allow models to be quantified by several calculation engines, therefore quality assuring results in a strong way.

2. **Over reliance on numerical approximations and truncation:** while this cannot be solved directly by a standard representation, as new calculation engines are completed, a standard representation will allow new engines to be snapped into new (or existing) user interfaces without changing the model or user interface software.

3. **Portability of the models between different software:** at the moment, models are essentially non-portable between calculation engines, as pointed out above. We would like to emphasize here that a standard representation would allow complete, whole models to be shared right now between software; the onus will be on each software to correctly interpret the model representation. We have

ASME Proposal

Create an Open Standards Working Group

- make a preliminary design for a PRA software architecture;
- create a structured modeling grammar;
- choose a model representation format;
- use the grammar and representation to define a standard model format;
- show examples with large existing PRAs.

What we can do NOW

An Example Test Case of the Idea

- APL uses RiskSpectrum;
- Most other models are made with CAFTA;
- NRC would like to review easily both model types with Saphire;
- create a prototype representation format;
- create model closures using the format;
- attempt to exchange models using the format.

How Can You Help?

Support the Open PSA Initiative

- Standard Model Format guardians;
- independent from any one company;
- quantification research and verification;
- measure degree of standardization;
    - software
    - models
- provide a pool of professionals for
    - software testing;
    - benchmarking;
    - algorithm peer review;
- solicit membership;
- manpower support from industry;
- internships for universities.

Quality Assurance by Comparison: Is the MCS Result a Good Result?

The Model

- A full PSA for the Loss of Offsite Power of a Japanese nuclear power plant
- 181 sequences (171 lead to a Core Damage)
- Up to 1128 gates and 1745 basic events per sequence
- More details in (Epstein & Rauzy 04)

→We Compared the BDD Solution to the MCS Solution

MCS (with truncation) vs. BDD (with success branches)

MCS Solution < BDD Solution	number of sequences
less than 10%	8
between 10% and 50%	19
between 50% and 100%	9
between 100% and 310%	15
total	53/181

MCS Solution > BDD Solution	number of sequences
less than 10%	15
between 10% and 100%	9
100% up to a factor 10	44
a factor 10 up to 96.83	60
total	128/181

What You See Is Not What You Get

The Model

- A full PSA for the Loss of Offsite Power of an American nuclear power plant (Epstein & Rauzy 05)
- 136 sequences (95 lead to a Core Damage)
- Core Damage modeled as one Fault tree
- Up to 1551 gates and 2439 basic events per sequence
- 52 Common Cause Groups
- 34 Initiating Events
- Fault Tree was 133 Levels Deep
- Modeled using Fault Tree Linking

What We Did

- Chose the largest Core Damage sequence
- Pruned the tree to only include this sequence
- Calculated all initiators simultaneously
- Obtained the cutsets generated by the FTL engine
- Generated the cutsets with ARALIA (ZBDD) down to different levels until we had the same cutsets as the FTL engine

What We Found

- 462 Cutsets (the same cutsets as with the FTL engine)
- Depth of the solution was only to level 4 (!!!!!!!)
- 95% of the modeled gates were not used
- 96% of the modeled basic events were not used
- We then quantified the fault tree to level 4 and created a BDD, ignoring success branches

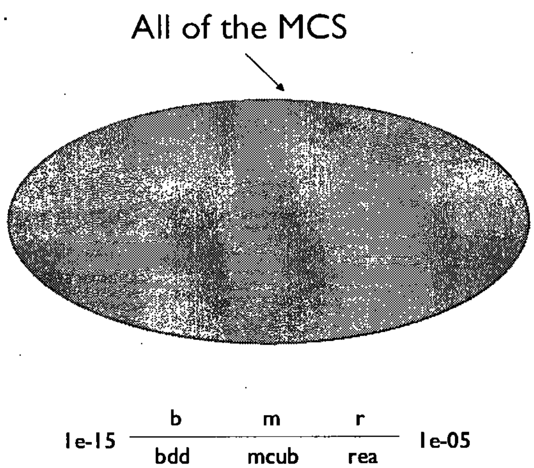
Moreover ...

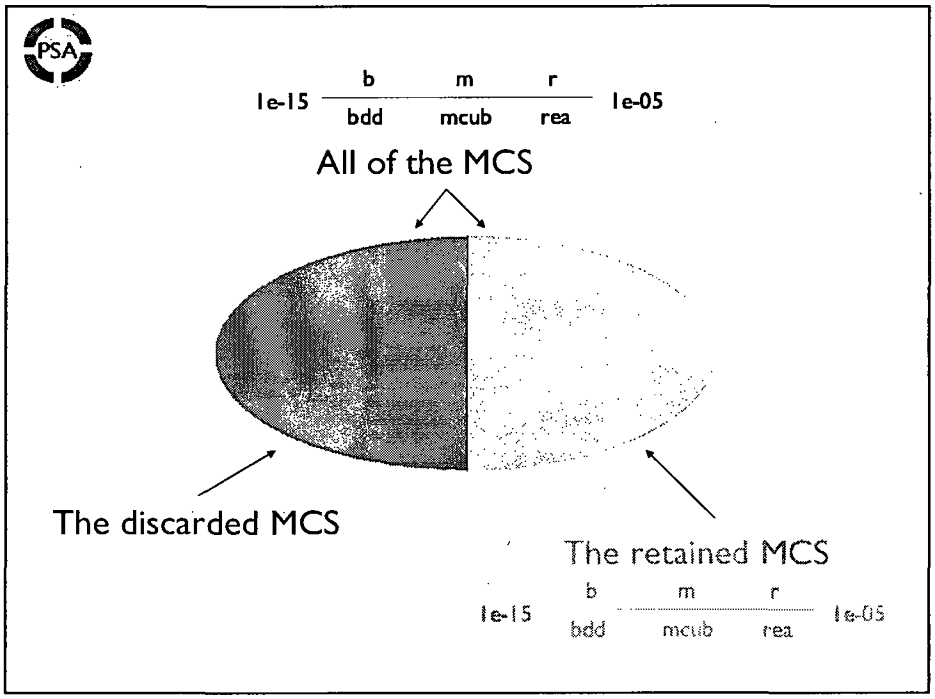
- MCS-REA quantified frequency was 7.88e-6 for this sequence
- BDD quantified frequency was 4.40e-6 for this sequence
- This is a difference of 1.76 times
- This is a large difference considering we excluded success branches
- We calculated the truncation upper bound: 5.06e-6
- Truncation upper bound is larger than the BDD solution

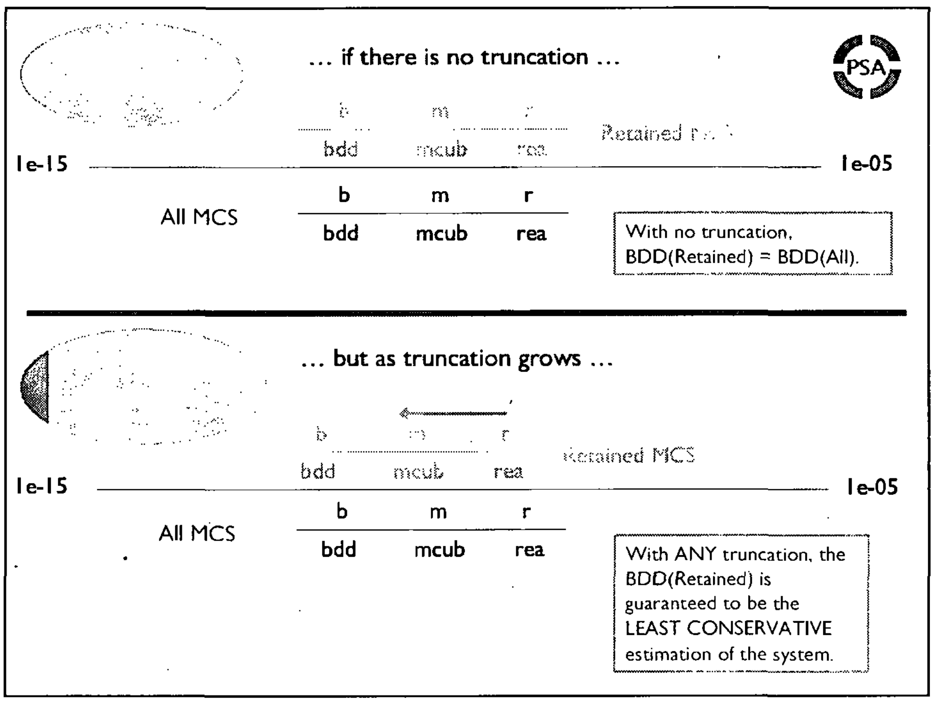
The fault is not in the tree, my dear Horatio,
But in our models themselves.
- William Shakespeare

The MCS to BDD Algorithm

1. Generate the MCS with truncation;
2. create a BDD from the MCS;
3. calculate the exact value of the cutsets from the BDD.




PSA
b m r
1e-15 bdd mcub rea 1e-05
All of the MCS
The discarded MCS
The retained MCS
b m r
1e-15 bdd mcub rea 1e-05


... if there is no truncation ...
PSA
bdd mcub rea
1e-15 1e-05
All MCS
b m r
bdd mcub rea
With no truncation, BDD(Retained) = BDD(All).
... but as truncation grows ...
b m r
bdd mcub rea
Retained MCS
1e-15 1e-05
All MCS
b m r
bdd mcub rea
With ANY truncation, the BDD(Retained) is guaranteed to be the LEAST CONSERVATIVE estimation of the system.

… and grows …

b m r

bdd mcub rea

Retained MCS

1e-15 1e-05

All MCS

b m r

bdd mcub rea

Here, MCUB is the best CONSERVATIVE value, but cannot be used in non-coherent systems nor systems with events with high probability, like initiating events.

b

bdd m

1e-15 1e-05

With any large system we do not know the exact value, therefore we do not know which of these cases truly apply.

All MCS

bdd mcub rea

… then the Rare Event Approximation of the retained MCS may be the best CONSERVATIVE approximation to the exact value of all of the MCS, and sometimes is an UNDER ESTIMATION of the exact values of the system if truncation is severe.

… for example the SWS system of Seabrook …

There are 101,639 MCS which are retained.

Rare Event Approximation: 2.2767e-09

… but the true value of the system …

Binary Decision Diagram: 2.8499e-08

The REA is an UNDER ESTIMATION of the exact value

… and in a simple example to further illustrate the point …

A Small Backup Cooling System

Rare Event Approximation: 5.6465e-04

Min Cut Upper Bound: 5.6458e-04

BDD of the MCS: 5.6410e-04

… but the true value of the system …

5.6882e-04

The REA of the MCS is the best approximation to the exact value of the system.

Know What Problem You Are Trying to Solve

We are not interested in the exact value of the RETAINED MCS.

We are interested in the exact value of the system, and the best approximation of that value.

Importance Measures and Chaos (Duflot, 2006)

Let's Take a Look at RAW

$$\boxed{RAW = P(S|e)/P(S)}$$

All importance measures are built on conditional probabilities.
They are calculated from the minimal cutsets generated for S.
With any sufficiently large and interesting system, the cutsets are truncated.

But generating MCS with truncation and then calculating the importance measures can have problems:

a * P   1e-3 * 1e-9 = 1e-12
-- truncation limit 1e-13
b * Q   1e-6 * 1e-8 = 1e-14

If there is no recalculation of the MCS:

p(S|a) = p(P) = 1e-09   RAW(S,a) = 1e-3
p(S|b) = p(a*P) = 1e-12   RAW(S,b) = 1

But generating MCS with truncation and then calculating the importance measures can have problems:

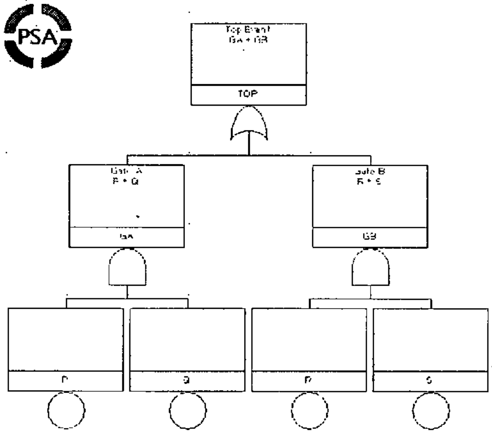
a * P   1e-3 * 1e-9 = 1e-12
-- truncation limit 1e-13
b * Q   1e-6 * 1e-8 = 1e-14

However, if there is regeneration of the MCS:

p(S|a) = p(P) = 1e-09   RAW(S,a) = 1e-3
p(S|b) = p(a*P + Q) = 1.1e-08   RAW(S,b) ≈ 1e-4

Moreover, while a given truncation limit may be good for calculating an end state, like CDF, the order and value of importance measures may be chaotic at this same truncation value. Dr. Duflot demonstrated these effects on the French reference PSA.

The Destructive Truth Table Method with Truncation



			Pmin
p	q	TRUE	P(p) * P(q)
p	not q	FALSE	P(p) * (1- P(q))
not p	q	FALSE	(1-P(p)) * P(q)
not p	not q	FALSE	(1-P(p)) * (1- P(q))
GA		TRUE	P(p) * P(q)
		FALSE	P(p) * (1- P(q)) + (1-P(p)) * P(q) + (1-P(p)) * (1- P(q))
r	s	TRUE	P(r) * P(s)
r	not s	FALSE	P(r) * (1- P(s))
not r	s	FALSE	(1-P(r)) * P(s)
not r	not s	FALSE	(1-P(r)) * (1- P(s))
GB		TRUE	P(r) * P(s)
		FALSE	P(r) * (1- P(s)) + (1-P(r)) * P(s) + (1-P(r)) * (1- P(s))
GA	GB	TRUE	P(p) * P(q) + P(r) * P(s)
GA	not GB	TRUE	P(p) * P(q) + (1-(P(r) * P(s)))
not GA	GB	TRUE	(1-(P(p) * P(q))) + P(r) * P(s)
not GA	not GB	FALSE	(1-(P(p) * P(q))) + (1-(P(r) * P(s)))
TOP		TRUE	(P(p) * P(q) + P(r) * P(s)) + (P(p) * P(q) + (1-(P(r) * P(s))) + (1-(P(p) * P(q))) + P(r) * P(s)
		FALSE	(1-(P(p) * P(q))) + (1-(P(r) * P(s)))

The Method

1. Start at the bottom of the tree with an empty truth table;
2. At each gate, add its inputs to the truth table;
3. If a line in the truth table is lower than the truncation limit, add it to Delta and eliminate from the table;
4. Solve the probability for the gate;
5. Collapse the truth table by substituting the gate name for its inputs;
6. Continue up the tree.

The Claim

Ptop <= Pexact <= Ptop+Delta

Example #1 sent to us ...

Truth Table Method for Solving T = x + y

T = x + y	Pr a		0.01
x = a (b + d)	Pr b		0.01
y = d	Pr d		0.01
Find	d	0.01	TRUE
	/d	0.99	FALSE
Collapse for y	y	0.01	TRUE
	/y	0.99	FALSE
Expand for (b + d)	y	0.01	TRUE
	/y	0.99	FALSE
	bd	0.0001	TRUE
	b/d	0.0099	TRUE
	/bd	0.0099	TRUE
	/b/d	0.9801	FALSE
Collapse for (b+d)	y	0.01	TRUE
	/y	[illegible]	FALSE
	(b + d)	[illegible]	TRUE
	/(b + d)	0.9801	FALSE
Rename (b+d) to Z	Z	0.0199	TRUE
	/Z	0.9801	FALSE
Expand for a/Z	y	0.01	TRUE
	/y	0.99	FALSE
	Z	0.0199	TRUE
	/Z	0.9801	FALSE
	a	0.01	TRUE
	/a	0.99	FALSE
	aZ	0.000199	FALSE
	a/Z	0.009801	TRUE
	/aZ	0.019701	FALSE
	/a/Z	0.970299	FALSE
Collapse for x	y	0.01	TRUE
	/y	0.99	FALSE
	x	[illegible]	TRUE
	/x	0.990149	FALSE
Expand for x y	y	0.01	TRUE
	/y	0.99	FALSE
	x	[illegible]	TRUE
	/x	[illegible]	FALSE
	xy	0.00009801	TRUE
	x/y	0.00970299	TRUE
	/xy	0.00990129	TRUE
	/x/y	[illegible]	FALSE
Collapse for T	T	0.01970029	TRUE
	/T	[illegible]	FALSE

The true value for T as calculated by Aralia is: 1.9301e 02.

In this example, if 0 <= Delta <= 1e-4, then Pexact lies outside the upper bound: Ptop = (Ptop+Delta) <= Pexact

... example #2 sent to us ...

Truth Table Method for Solving T = x + y

T = x + y	Pr a		[illegible]
x = a (b + d)	Pr b		[illegible]
y = d	Pr d		[illegible]
Find	d	[illegible]	TRUE
	/d	[illegible]	FALSE
Collapse for y	y	[illegible]	TRUE
	/y	[illegible]	FALSE
Expand for (b + d)	y	[illegible]	TRUE
	/y	[illegible]	FALSE
	bd	[illegible]	TRUE
	b/d	[illegible]	TRUE
	/bd	[illegible]	TRUE
	/b/d	[illegible]	FALSE
Collapse for (b+d)	y	[illegible]	TRUE
	/y	[illegible]	FALSE
	(b + d)	[illegible]	TRUE
	/(b + d)	[illegible]	FALSE
Rename (b+d) to Z	Z	[illegible]	TRUE
	/Z	[illegible]	FALSE
Expand for a/Z	y	[illegible]	TRUE
	/y	[illegible]	FALSE
	Z	[illegible]	TRUE
	/Z	[illegible]	FALSE
	a	[illegible]	TRUE
	/a	[illegible]	FALSE
	aZ	[illegible]	FALSE
	a/Z	[illegible]	TRUE
	/aZ	[illegible]	FALSE
	/a/Z	[illegible]	FALSE
Collapse for x	y	[illegible]	TRUE
	/y	[illegible]	FALSE
	x	[illegible]	TRUE
	/x	[illegible]	FALSE
Expand for x y	y	[illegible]	TRUE
	/y	[illegible]	FALSE
	x	[illegible]	TRUE
	/x	[illegible]	FALSE
	xy	[illegible]	TRUE
	x/y	[illegible]	TRUE
	/xy	[illegible]	TRUE
	/x/y	[illegible]	FALSE
Collapse for T	T	[illegible]	TRUE
	/T	[illegible]	FALSE

The true value for T as calculated by Aralia is: 9.9000e-01

In this example, with any Delta, Pexact lies below Ptop by 9e-2: Pexact < Ptop <= (Ptop+Delta)

So why does this happen?

Consider the two simple cases:

1) F+F where p(F)=0.1: With the method you get (even without a Delta)
   p(F+F) = p(F)+p(F)-p(F).p(F) = 0.19 which is an overestimation

2) F.F where p(F)=0.1: with the method you get p(F.F) = p(F).p(F) = 0.01 which is an underestimation.

You could argue that one can detect this repeated F case. But it is easy to hide it by taking two formulae F and F' that are structurally close, but not the same, and very far apart in the tree.

This developer has not followed the "Gate Collapse Rule" to be sure that all such cases are eliminated.

So why does this happen?

Consider the two simple cases:

1) F+F where p(F)=0.1: With the method you get (even without a Delta)
   p(F+F) = p(F)+p(F)-p(F).p(F) = 0.19 which is an overestimation

Gate Collapse Rule

A gate *g* can be collapsed iff:

1. All other gates which share at least one of its inputs are in the truth table;
2. Gate *g* has all inputs resolved in expanded form;
3. All gates which share inputs fulfill the above two conditions.

We don't present this example to criticize the algorithm, but, rather, to show that an attempt must be made to PROVE the algorithm's correctness and limits.

We have had techniques for over 40 years to demonstrate algorithm and program correctness.

- Floyd (1967, *Assigning Meanings to Programs*)
- Hoare (1969, *An Axiomatic Basis for Computer Programs*)
- Scott & Strachey (1972, *Denotational Semantics*)

Algorithm development is a branch of mathematics.

We must concern ourselves with **accuracy** of calculations and the **proof** of such before concerning ourselves with speed. Remember, **good cooking takes the time it takes.**

ELECTRIC POWER RESEARCH INSTITUTE

Next Generation Tools – Project Status

Ken Canavan
Risk and Safety Program Manager
October 2007

Issues with Current Tools ...

- Fault Tree / Event Tree Approach to PRA Modeling
  - Developed in 1970's gave shape to our risk modeling efforts
  - Models have increased in scope and complexity
  - Technology has improved
- The quantified PRA is a simplified estimate of risk
  - Simplifications to reduce calculation time (e.g., truncation and rare event approximation)
  - Risk metrics can change as a result of simplifications
- PRA Basis Documentation and Analysis
  - Need to "control" PRA model, documentation, and applications
  - Demonstrate the PRA reflects "as-built" & "as-operated" plant

The Solutions …

- **Next Generation of Risk Analysis Tools consisting of new and improved**
  - **logic modeling**,
  - **quantification** techniques, and
  - **documentation** techniques

- Common elements of the Next Generation of Tools
  - "Evolutionary" as opposed to "revolutionary"
  - Easy to develop, maintain, verify and reviewed
  - Visual Interface and Connectivity – necessary but not yet evaluated

Next Generation of PRA Tools

Improved Modeling	➔	**Declarative Modeling**
Improved Quantification	➔	**Quantification Techniques** – Binary Decision Diagram (BDD) – Minimal Cutset BDD – Direct Probability Calculation™
Improved Documentation	➔	PRA Documentation Assistant (**PRA DocAssist**™)

Declarative Modeling (1 of 3)

- Allows attributes to be assigned to fault tree elements
  - Attributes include:
    - Probability, frequency or conditional values
    - Settings under various conditions (True or False)
  - Elements include:
    - Basic Events
    - Gates
    - Initiating Events

Declarative Modeling (2 of 3)

- Declarative Modeling Capabilities
  - Simplify Recovery and Post Processing
    - Treat dependent human actions in the fault tree
    - Specify mutually exclusive events within fault tree
    - Handle phase mission times (e.g., LOOP recovery)
  - Simplify Logic Model
    - Alignments and frequency without using additional events
    - Initiating event impacts without repetitive houses/events
  - Documentation and Reviewability
    - Notes to clarify logic development
    - Fault tree viewed by attributes, such as initiator specific trees or with and without dependent human actions or recovery

Declarative Modeling (3 of 3)

- Project Status
  - Accelerated in April 2007
  - Beta release by end of year (Recovery and Post-Processing)
  - Final release first half of 2008

Advanced Quantification Techniques (1 of 5)

- Current Quantification Approaches
  - Minimal Cutset Upper Bound (MCUB)
    - Widely used
    - Has simplifications (e.g., rare event approximation and truncation)
  - Direct Probability Calculation (DPC™)
    - New (widely available in 2008)
    - Few simplifications
    - No cutsets
  - Binary Decision Diagram (BDD)
    - Successfully with small fault trees
    - Provides exact solution without simplification
    - Large fault trees remain intractable

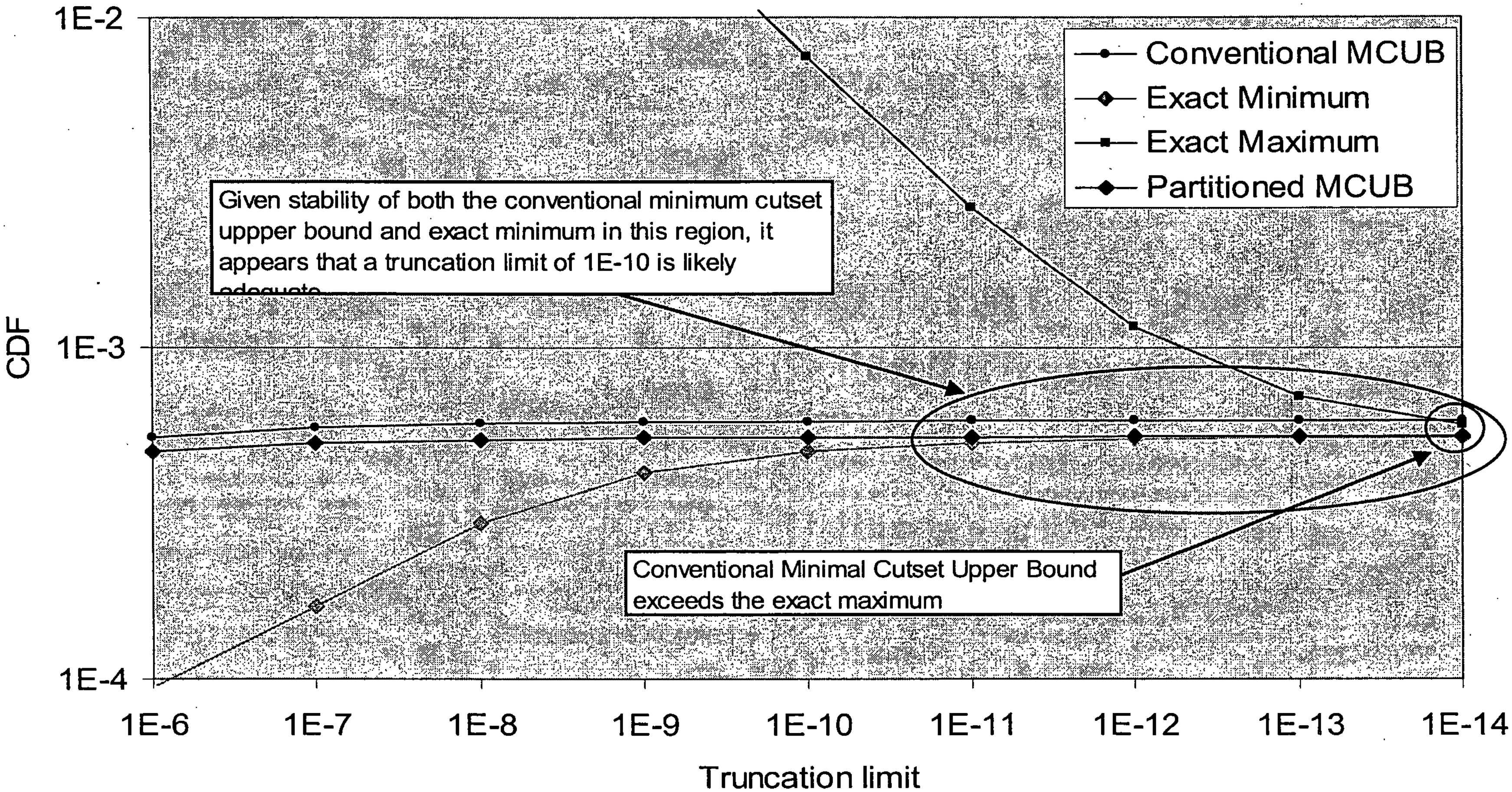
Advanced Quantification Techniques (2 of 5)

- Combination of approaches will provide best solution
  - MCUB
    - Provides cutsets
  - DPC™
    - Provides exact solution value
    - Establishes truncation limit for MCUB quantification
  - MCBDD (BDD of solution of the cutsets)
    - Provides exact solution of cutsets
    - Delta from exact DPC solution provide knowledge of numerical differences
    - Establishes stable importance measures
    - Can be performed for large fault trees

EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Advanced Quantification Techniques (3 of 5) – DPC Comparison

Adjusted Truncation Comparison Results



Advanced Quantification Techniques (4 of 5) – DPC Comparison

- Comparison Data

Truncation	Conventional MCUB	Exact Minimum	Exact Maximum	Partitioned
1E-5	3.679E-04	3.010E-05	8.73E-01	3.43E-04
1E-6	5.335E-04	9.430E-05	4.21E-01	4.83E-04
1E-7	5.749E-04	1.660E-04	1.85E-01	5.17E-04
1E-8	5.890E-04	2.960E-04	6.93E-02	5.28E-04
1E-9	5.956E-04	4.180E-04	2.34E-02	5.34E-04
1E-10	5.988E-04	4.870E-04	7.61E-03	5.37E-04
1E-11	6.000E-04	5.170E-04	2.65E-03	5.38E-04
1E-12	6.004E-04	5.290E-04	1.16E-03	5.38E-04
1E-13	6.005E-04	5.340E-04	7.12E-04	5.39E-04
1E-14	6.006E-04	5.350E-04	5.84E-04	5.39E-04

Advanced Quantification Techniques (5 of 5)

- Pros and Cons of Combined Solution
  - Advantages:
    - Achievable
    - No significant simplification
  - Disadvantages:
    - Still some minor simplifications
    - Full model re-quantifications with substantial model changes will require calculation time
- Project Status
  - Accelerated in April
  - Project progress slow
  - Expect 2008 Completion

PRA DocAssist™ (1 of 2)

- Need to control PRA documentation, provide basis for assumptions and model development
  - Documentation complex
  - Not directly tied to model
  - Difficult to maintain and update
- PRA DocAssist™ is a software tool under development that more closely ties PRA documentation with the model. Capabilities include:
  - Capture of information
  - Sorting capability (e.g., ASME Standard requirements)
  - Navigation capability by user attributes
  - Reporting capability
  - Configuration and Version Control

PRA DocAssist™ (2 of 2)

- Project Status
  - Development funding obtained
  - Release 1.0 will not be developed
  - Release 2.0 – all the bells and a few whistles
    - will be provided in first half of 2008
    - to all EPRI members
    - limited support for installation and getting started
  - Users Group Begins in 2008

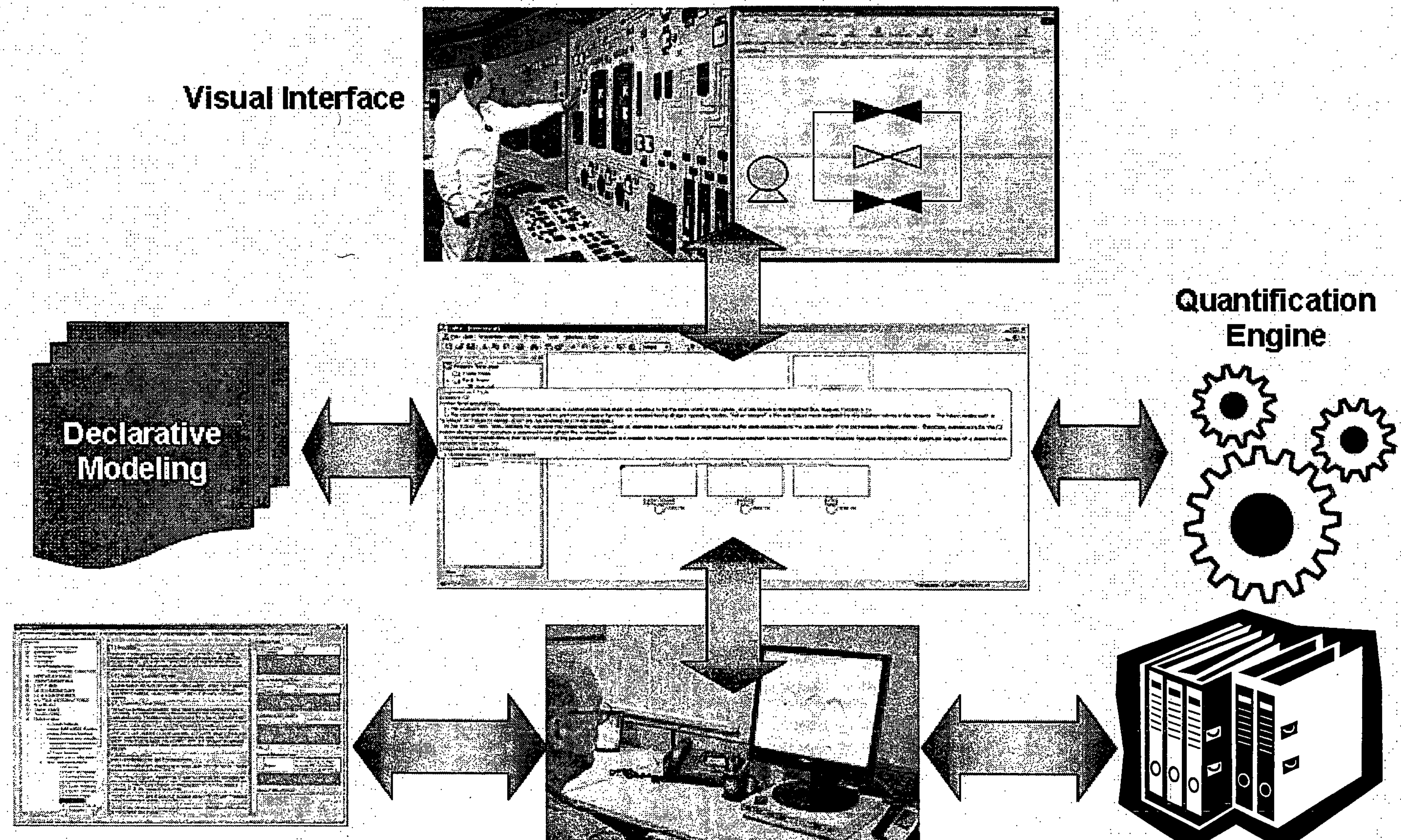
Overall Approach to Next Generation Tools

- To date …
  - Long term (low cost) program
  - Modular in nature – addressing each issue
- Recently … (April 07)
  - Accelerated to produce significant results in 2008
- Previous / Current Activities
  - 2004: Declarative Modeling Proof-of-Principles
  - 2005: BDD Quantification Proof-of-Principles
  - 2006: Declarative Modeling Add-in to CAFTA (2007)
  - 2007: DPC Solution Research (Woo Sik Jung – 2006)
  - 2008: PRA DocAssist™ Software – Beta Version

Visual Interface

- Currently the visual interface for the PRA are the event trees and fault trees
  - Other interfaces may be beneficial in some cases
  - Process flow diagrams maybe more intuitive
- Investigating various methods for interactive event tree and fault tree development from process diagrams
- KB3 a software tool with this type of capability in under investigation as a possible interface
- Limited evaluation done in 2006

The vision ...



PRA DocAssist™ Database

The Open-PSA Initiative

Standard Representation Format for Probabilistic Safety Analyses

Towards a New Generation of Models and Tools

The Open-PSA Initiative

Credits

Author: Antoine B. Rauzy
Version: 1.1a
Date: September the 5th 2007

The Open-PSA Initiative

Content

- Open-PSA Initiative
- Rationale for the Standard
- Anatomy of the Standard
- Fault Tree Layer
- Stochastic Layer
- Extra-Logical Layer
- Event Tree Layer
- Report Layer

The Open-PSA Initiative

Where Are We?

- Detailed models have been developed for level 1 and level 2 PSA
- Good tools have been developed to design and assess models

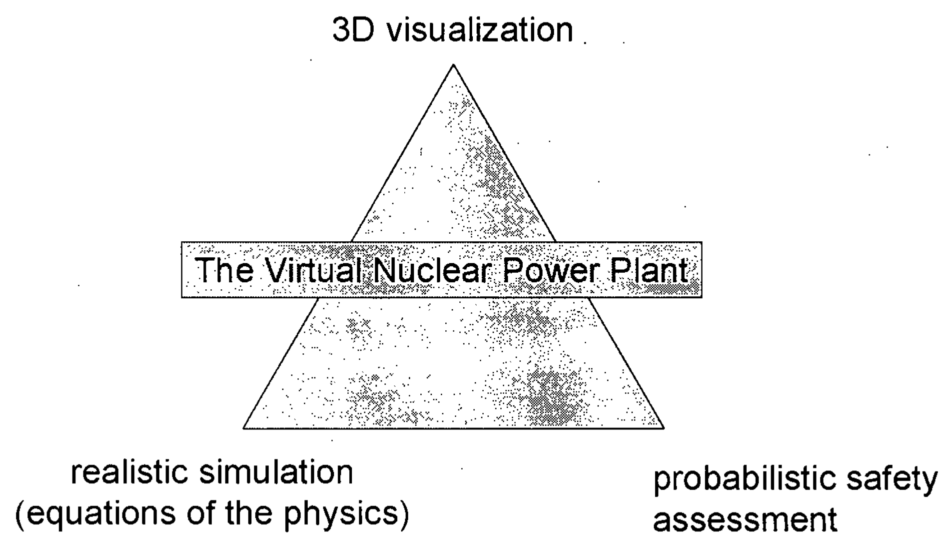
... but

- Models are hard to master, to check for completeness, to maintain...
- Models are tool-dependent
- Calculation engines have flaws

The Open-PSA Initiative

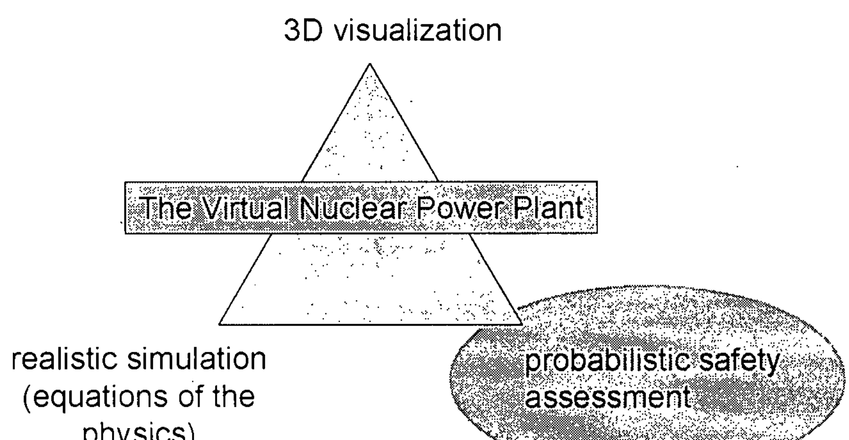
Where We Want to Go?

The future ...



The Open-PSA Initiative

A First Step...



An International Standard Representation Format
for PSA Models

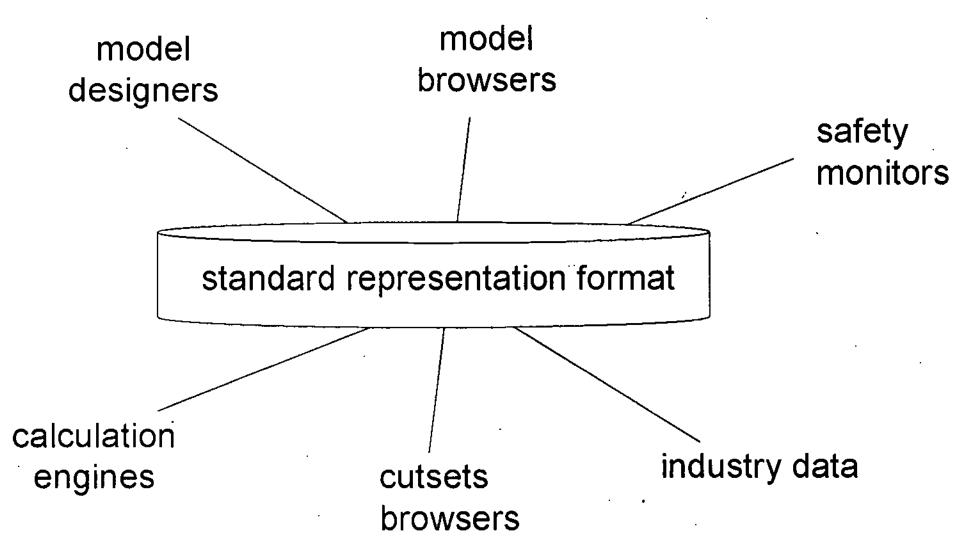
The Open-PSA Initiative

Why Do We Need a Standard?

- Reduce tool dependency
- Have a better confidence in approximations (quality insurance)
- Cross check calculations
- Develop new calculation engines
- Design new model browsers and safety monitors
- Review and document (existing) models
- Clarify (unify?) modeling methodologies
- Call external tools (Level 2 PSA)
- Extend fault trees/events trees formalism
- …

The Open-PSA Initiative

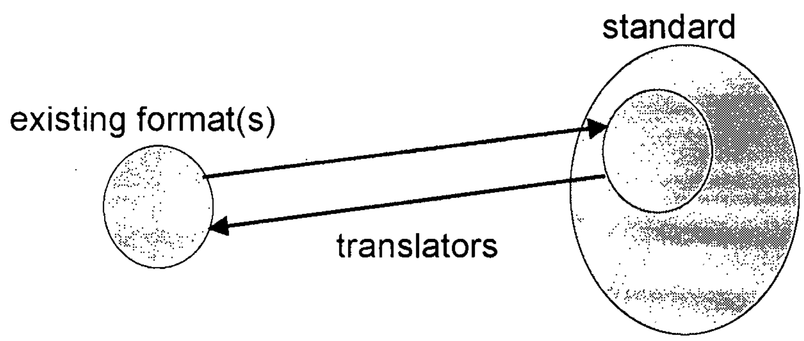
The Open-PSA Architecture



Requirements

The Open-PSA Initiative

- It should be possible to cast any existing model



- The role of each element should be clearly identified and have an unambiguous semantics
- The standard should be easy to embed in existing tools and easy to extend

… XML format

The Open-PSA Initiative

Anatomy of the Standard

The Open-PSA Initiative

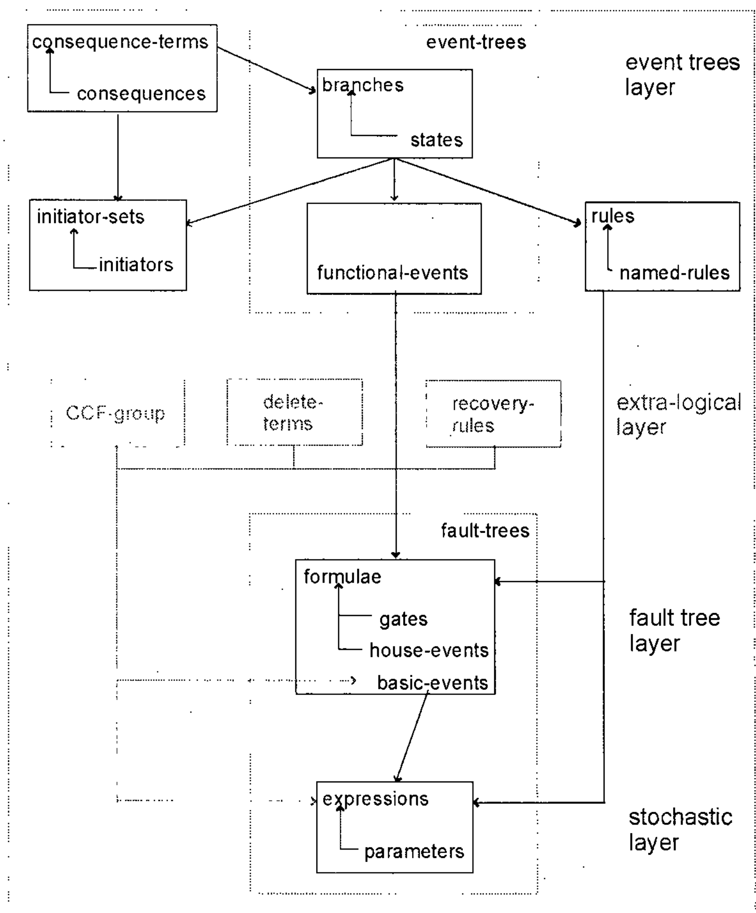
Methodology

- We considered models built with the main tools available on the market
  - Cafta, Saphire, RiskSpectrum, Riskman, Fault Tree free...
  - US, Japanese and European PSA
- We made of taxonomy of all syntactic categories we found in these models
  - Gates, basic events, house events, sequences...
- We gave to each category a formal operational semantics
- We designed a XML representation of categories

The Open-PSA Initiative

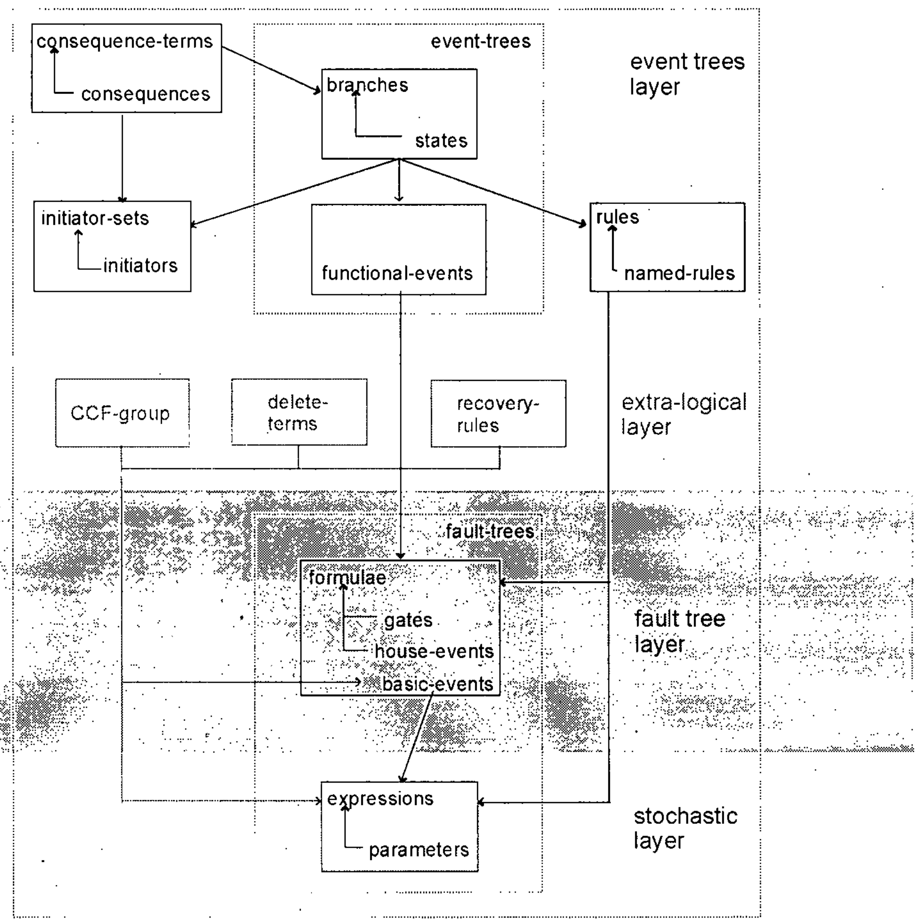
Five Layers Architecture

- Report Layer
  - Results of calculation...
- Event Tree Layer
  - Event trees, initiators, sequences, consequences
- Extra-Logical Layer
  - CCF-groups, delete terms, exchange events...
- Fault Tree Layer
  - Fault Trees, gates, basic events, house events
- Stochastic Layer
  - Probability distributions, parameters



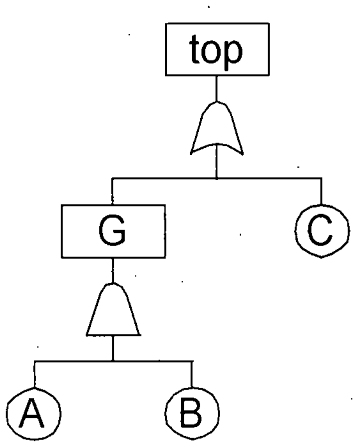
Fault Tree Layer

The Open-PSA Initiative



The Open-PSA Initiative

Declarations of Fault Trees




```
<define-fault-tree name="FT1" >
   <define-gate name="top" >
      <or>
         <gate name="G" />
         <basic-event name="C" />
      </or>
   </define-gate>
   <define-gate name="G" >
      <and>
         <basic-event name="A" />
         <basic-event name="B" />
      </and>
   </define-gate>
</define-fault-tree>
```

The Open-PSA Initiative

Declarations of Gates

```xml
<define-gate name="valve-failed-closed">
    <or>
        <basic-event name="valve-hardware-failure" />
        <gate name="valve-human-failure" />
        <basic-event name="valve-test-failure" />
    </or>
</define-gate>
```

the standard provides a complete set of logical connectives

The Open-PSA Initiative

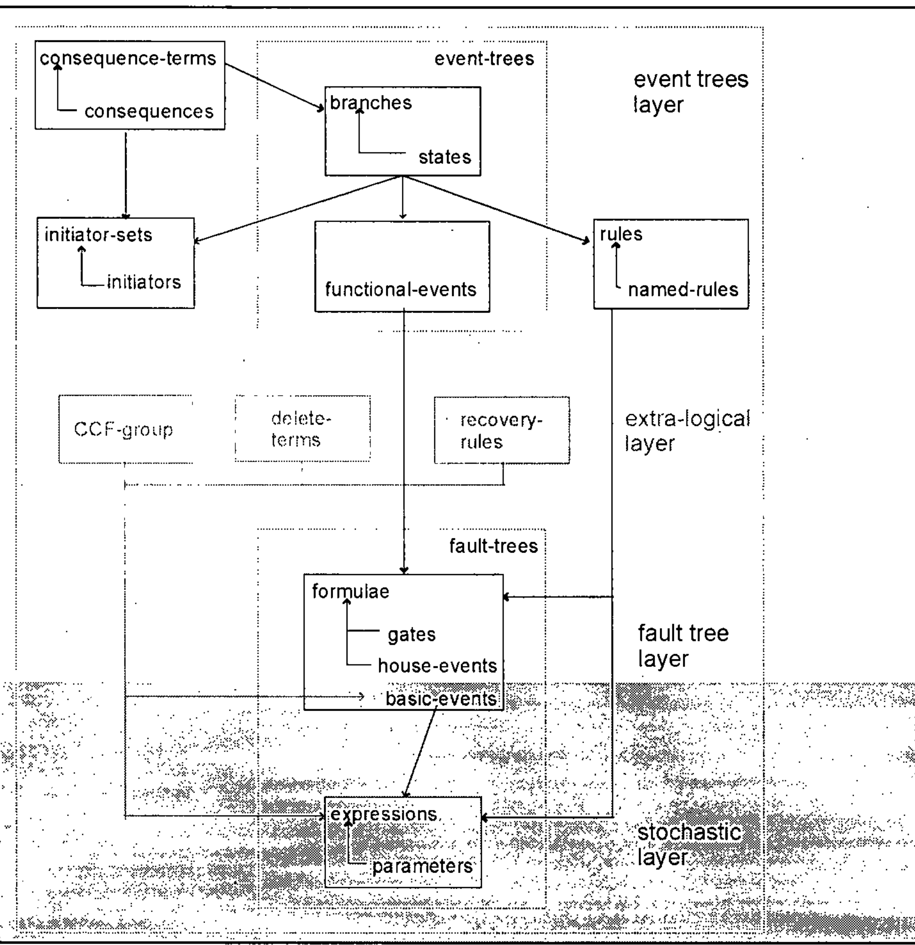
Declarations of Basic Events

```xml
<define-basic-event name="valve-hardware-failure" >
    <exponential>
        <parameter name="failure-rate-valves" />
        <mission-time />
    </exponential>
</define-basic-event>
```

The Open-PSA Initiative

Stochastic Layer

The Open-PSA Initiative



The Open-PSA Initiative

Stochastic Layer (Content)

1. Stochastic expression and parameters
   role and definition
2. Operations
   Arithmetic operations, logical operations, conditional operations
3. Built-ins
   usual time-dependent distributions
4. Random Deviates
   uniform, normal, lognormal deviates, histograms

The Open-PSA Initiative

Role of Stochastic Expressions

1. Associate (possibly time-dependent) probabilities with basic events. E.g.

```
<define-basic-event name="BE">
  <exponential>                          negative exponential distribution
     <parameter name="lambda" />         failure rate
     <mission-time />                    mission time
  </exponential>
</define-basic-event>
```

2. Define distributions for these probabilities (and more generally for parameters). E.g.

```
<define-basic-event name="BE2">
  <uniform-deviate>                      uniform random deviate
     <float value="1.0e-4" />            lower bound
     <float value="2.0e-4" />            upper bound
  </uniform-deviate>
</define-basic-event>
```

Built-ins

The Open-PSA Initiative

Set of predefined function to describe time-dependent distributions. E.g.

```
• <exponential>
        <parameter name="failure-rate-pump" />
        <mission-time />
  </exponential>
• <Weibull>
        <parameter name="shape1" />
        <parameter name="scale1" />
        <sub>
            <mission-time />
            <parameter name="locality1" />
        </sub>
  </Weibull>
• ...
```

Random-Deviates

The Open-PSA Initiative

To perform sensitivity analyses. E.g.

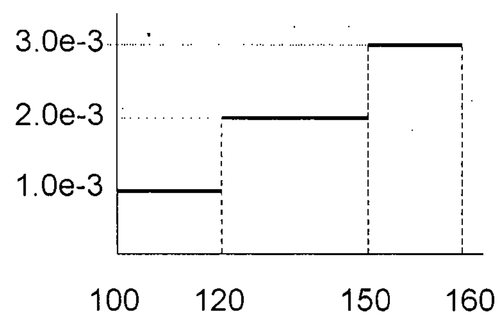
```
• <uniform>
        <float value="1.0e-3" />          lower-bound
        <float value="2.0e-3" />          upper-bound
  </uniform>

• <lognormal>
        <float value="1.23e-4" />         mean
        <int value="3" />                 error-factor
        <float value="0.90" />            confidence
  </lognormal>

• ...
```

The Open-PSA Initiative

Histograms

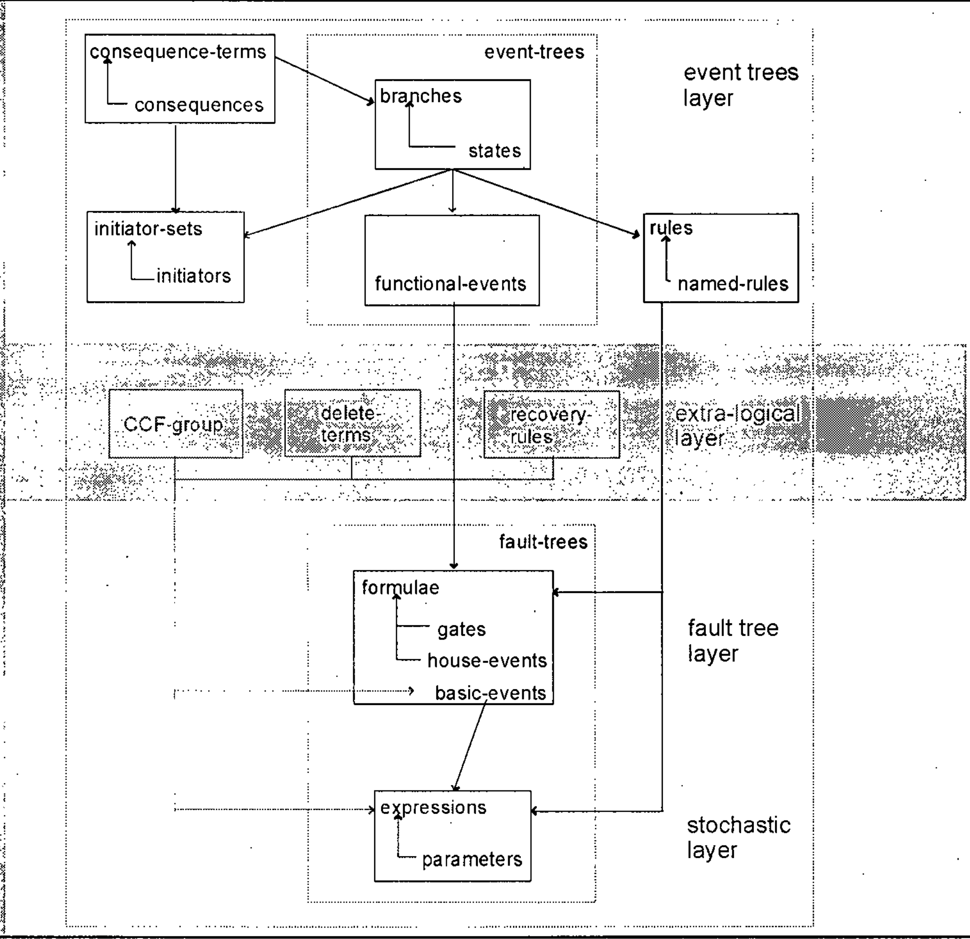



```
<histogram lower-bound="100" >
   <bin upper-bound="120" >
      <float value="1.0e-3 />
   </bin>
   <bin upper-bound="150" >
      <float value="2.0e-3 />
   </bin>
   <bin upper-bound="160">
      <float value="3.0e-3 />
   </bin>
</histogram>
```

The Open-PSA Initiative

Extra-Logical Layer

The Open-PSA Initiative



The Open-PSA Initiative

Extra-Logical Layer (Content)

1. Common Cause Failures
   - models, declarations
2. Exclusive events (delete terms)
   - model, declaration
3. Recovery rules
   - model, declaration

The Open-PSA Initiative

Delete Terms

Delete terms are groups of exclusive (basic) events.

- Used to model physically impossible configurations such as simultaneous maintenance

Three possible interpretations/uses of the exclusive group g={e1,e2}

1. Post-processing of cutsets
   - (e1 and e2 and ...) deleted
2. Global constraint
   - NewTopEvent = TopEvent and [not (e1 and e2)]
3. Local subsitution
   - e1 $\rightarrow$ ge1 = (e1 and not e2)
   - e2 $\rightarrow$ ge2 = (e2 and not e1)

The Open-PSA Initiative

Delete Terms (continued)

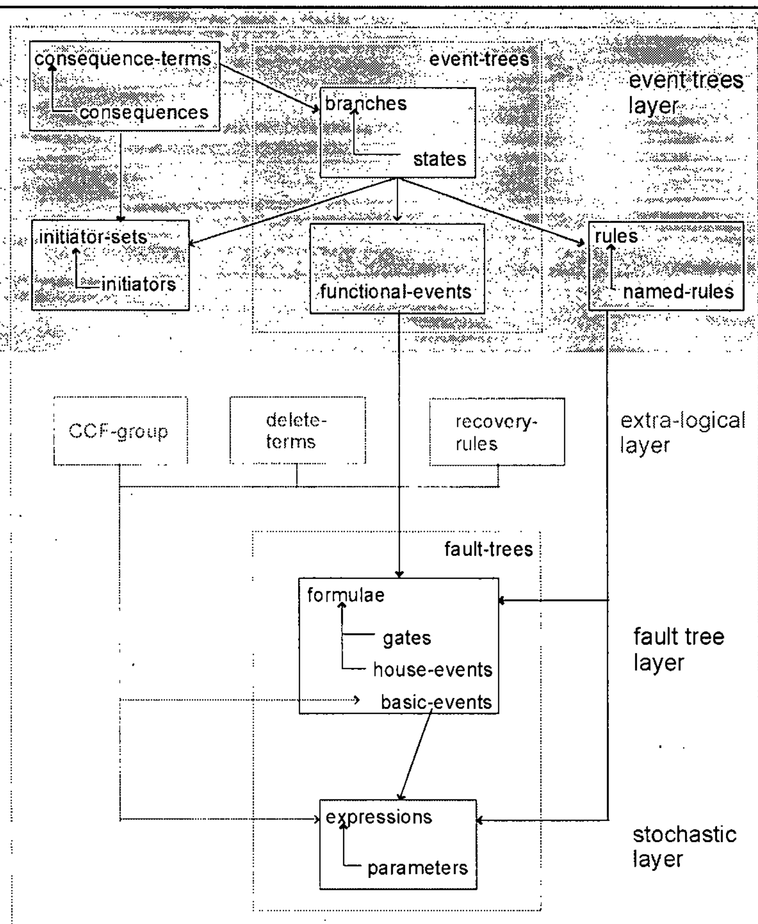
XML representation

```
<define-exclusive-group name="g1" >
    <basic-event name="e1" />
    <basic-event name="e2" />
    <basic-event name="e3" />
</define-exclusive-group>
```

The Open-PSA Initiative

Event Tree Layer

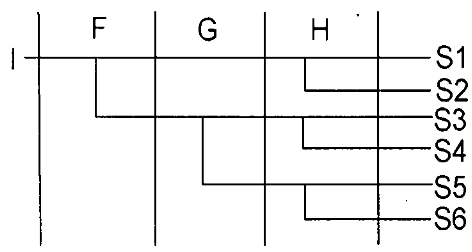
The Open-PSA Initiative



The Open-PSA Initiative

Preliminaries (1)

Graphical presentation of Event Trees



Interpretation

S1 = I and not F and not H
S2 = I and not F and H
S3 = I and F and not G and not H
S4 = I and F and not G and H
S5 = I and F and G and not F
S6 = I and F and G and H

A priori simple but …

The Open-PSA Initiative

Preliminaries (2)

- Fault trees may be given flavors (by setting house events)
- These flavors may depend on the current branch
- There may have several initiating events
- Some success branches may be interpreted as a bypass
- There may have multi-states branches
- Branches may be defined as references to other branches
- …

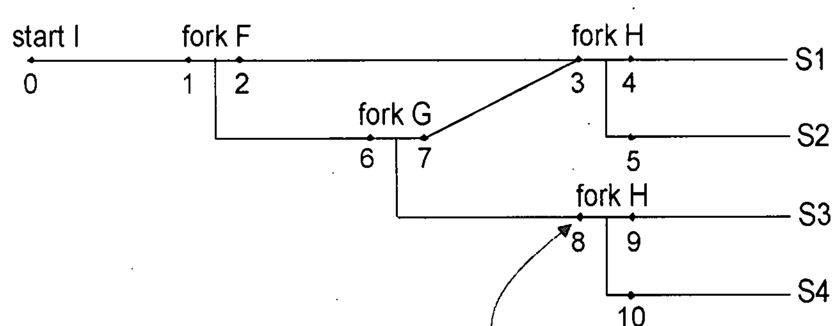
Preliminaries (2)

- Fault trees may be given flavors (by setting house events)
- These flavors may depend on the current branch
- There may have several initiating events
- Some success branches may be interpreted as a bypass
- There may have multi-states branches
- Branches may be defined as references to other branches
- …

Event Trees should be seen as a graphical programming language!

- The graphical view described the structure of the tree, i.e. the different sequences
- Instructions are provided to give flavors to fault trees
- The interpretation of sequences (Boolean formula) is built while walking along the branches

Structure of Event Trees (1)



Walk:

- 0, 1, 2, 3, 4 (S1)
- 0, 1, 2, 3, 5 (S2)
- 0, 1, 6, 7, 3, 4 (S1)
- …

at each point some instructions can be executed in order to set values of house events and parameters and/or to collect functional event

The Open-PSA Initiative

Structure of Event Trees (2)

```
<define-event-tree name="ET1" >
  <define-functional-event name="F">          declarations of functional events
    <fault-tree name="FTF" gate="top" />
  </define-functional-event>
  ...
  <define-consequence name="S1" />            declarations of consequences
  ...
  <path>                                      definition of the structure
    <fork functional-event="F" >
      <path>
        <collect functional-event="F" polarity="success" />
        <fork functional-event="H" >
          ...
        </fork>                               instruction
      </path>
      ...
    </fork>
  </path>
</define-event-tree>
```

The Open-PSA Initiative

Instructions (1)

Instructions to set parameters/house event values

```
– <set house-event="H1" >
    <constant value="false" />
  </set-parameter>
– <set parameter="lambda" />
    <float value="0.001" />
  </set-parameter>
```

Instructions to collect functional events

```
– <collect functional-event="F" polarity="failure" />
```

Conditional instructions

```
– <if>
    <collected functional-event="F" />
    <set house-event="H2"> <constant value="true" /> </set>
  </fi>
```

The Open-PSA Initiative

Instructions (2)

Blocks

- <block>
  instruction+
  </block>

Rules (named blocks of instructions)

- <define-rule name="R1" >
    <set house-event="H1"> <constant value="false" /> </set>
    <set house-event="H2"> <constant value="true" /> </set>
    <set house-event="H3"> <constant value="true" /> </set>
    ...
  </define-rule>

The Open-PSA Initiative

Report Layer

Report Layer (content)

The Open-PSA Initiative

1. Description of Calculations
   – model, tool, algorithm, mission-time, cutoff...
2. Description of Results
   – minimal cutsets
   – probabilistic measures

Description of Calculations

The Open-PSA Initiative

- Software
  – version, contact organization (editor, vendor)
- Calculation algorithm
  – name
  – limits (number of basic events, cutsets...)
  – preprocessing techniques
  – cutoffs
  – handling of success branches, use of delete terms
  – external routines
  – calculation time
  – ...
- Feedback
  – success, failure

The standard provides examples rather than a strict syntax for these items

The Open-PSA Initiative

Descriptions of Results

```
<sum-of-products name="MCS1" basic-events="3" products="2" >
  <product order="2">
    <basic-event name="A" />
    <basic-event name="B" />
  </product>
  <product order="2">
    <not>
      <basic-event name="A" />
    </not>
    <basic-event name="C" />
  </product>
</sum-of-products>
```

The Open-PSA Initiative

Descriptions of Results

```
<measure name="RAW" system="TopEvent" component="BE33" >
  <mean value="0.00149807" />
  <standard-deviation value="0.000385405" />
  <error-factor percentage="90" value="1.00056" />
  <histogram lower-bound="0" >
    <bin upper-bound="0.25"> <float value="0.00112081"> </bin>
    <bin upper-bound="0.50"> <float value="0.00136203"> </bin>
    <bin upper-bound="0.75"> <float value="0.0016188">  </bin>
    <bin upper-bound="1.00"> <float value="0.00186128"> </bin>
  </histogram>
</measure>
```

The Open-PSA Initiative

Future Work (2008)

Where Are We?

- Version 1 of the standard available on the website
- Version 2 (major revision) available end of october 2007

2008

- Extension/validation of the standard
- Experiments
- Prototyping
- Give a formal status to the Open-PSA initiative

WorkPackages (2008)

The Open-PSA Initiative

- Validate the kernel
- Include HRA
- Include BE Data
- Cast at least one large ET small FT model into the standard
- Cast at least one small ET large FT model into the standard
- Study in more details the notions of boundary conditions, mission profile, time dependencies...
- Study rules of generic modelling
- Technical coordination
- Organizational coordination
- Workshop organization
- Website

The Open-PSA Initiative

Prototyping