



BROOKHAVEN NATIONAL LABORATORY  
ASSOCIATED UNIVERSITIES, INC.

Upton, Long Island, New York 11973

(516) 282-2363  
FIS 666-2363

Department of Nuclear Energy  
Building 130

March 21, 1990

Dick Robinson  
Probabilistic Risk Analysis Branch  
Division of Systems Research  
Mail Stop NLS-345  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555

Re: Senior Consultant Group Activities on "Low Power and Shutdown  
Accident Frequencies" Project

Dear Dick:

It was a pleasure to join you and the other members of the Senior Consultant Group in Albuquerque for the briefing by BNL and Sandia. Enclosed are my comments on the briefings. I will also review the material supplied to us at the meeting, and if I have any additional comments, I will let you know. Unless I see something unexpected in the new material, the attachment to this letter fulfills my action item from that meeting.

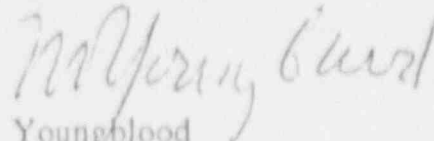
One concern which was mentioned at the meeting, but not adequately resolved, is the level of cooperation which we can expect from Surry. I gather that the choice of Surry was driven in part by the need to compare with 1150, and perhaps a wish to avoid doing another shutdown study of Zion. These factors are certainly legitimate considerations. However, prospects for cooperation from the plant must also weigh heavily. This point seems especially important to me, because the kind of hazard assessment which I am recommending in the attachment would

9202260124 910726

PDR FOIA  
REDDA91-267 PDR

ideally involve the *active* participation (at the level of perhaps a staff week) of an operations type. This kind of cooperation involves more than transmittal of information. It seems to me that at this early stage, BNL has relatively little to lose from changing plants (certainly less than it will have later). This would not be the first project to spin its wheels for lack of sufficient information, but in an area as unexplored and as potentially significant as this one, the consequences of a lack of cooperation will be particularly regrettable. If a high level of cooperation is not obtained soon, then consideration should be given to analyzing a different plant.

Sincerely yours,



R. Youngblood  
Facilities Risk Analysis Group

Enc.

cc: R. A. Bari (Enc.)  
W. Y. Kato (Enc.)  
W. T. Pratt (Enc.)

## Comments Following Presentations by BNL and SNL on Low Power and Shutdown Accident Frequencies

R. Youngblood  
Member, Senior Consulting Group

The Senior Consulting Group is called upon to express its priorities and recommendations as early in the process as possible. The following comments are offered in that spirit. My recommendations are based on my belief that both teams (BNL and SNL) are highly qualified in systems analysis and human factors modelling, and can be expected to do a good job of quantifying scenarios *once they are identified*. It seems to me that in this project, identifying the scenarios is the trick, and it is more of a trick at shutdown than it is at full-power operation. This argues for project priorities which are different from those which were set in 1150, for example.

Numerous comments were made by other members of the SCG. I agree with nearly all of them. One which seems to me to be particularly important is that it would be useful for both teams to pick one or two areas ("modes" or perhaps even subsets of modes) and carry the analysis all the way through for the selected areas, rather than trying to do all areas at once in parallel. This has the programmatic merit of producing results at an early stage of the project, and the technical merit of helping to set priorities in the rest of the work. In calling for particular intermediate results, some of the recommendations made below would have similar effects, although they have been offered for different reasons.

### Identification of Initiating Events

In the area of initiating event identification, both labs are making heavy use of the historical record. It is appropriate to do this, but it seems to me that one or two important steps have been skipped by both labs. First of all, the notion of "initiating event" is itself hazy (at least, no one at the meeting could explain it except by example), and needs to be defined. At the meeting, I argued that initiating events at power operation are extremely well defined, i.e., it is formally possible to decide whether any given event is an "initiator." At power operation, there is an envelope in physical state-space inside which operation is allowed to continue, and outside which a plant trip is warranted; any excursion outside this envelope is an initiator. No comparable definition for non-power modes was articulated at the meeting; rather, the attitude seemed to be that you

know an initiator when you see one. Actually, after a few days' reflection, this definition doesn't look as bad to me as it did in Albuquerque; the events that people are seizing on as "initiators" have the property that somebody had to do something in response. In my terminology, the response is required *because* the event constitutes an excursion outside of some envelope, which I still argue needs to be carefully defined.

We can recognize initiators in the historical record, because somebody needed to do something in response to them; but the historical approach will only alert us to initiators which have occurred, and in fact only to initiators which (a) have occurred, (b) were either serious in themselves or became serious as a result of an inadequate first response, (c) were written up, and (d) were read about by the team. Initiators which don't strongly resemble events that we read about won't be identified except by a systematic (algorithmic) approach to identification of initiators. At the meeting, I gave Donnie Whitehead some references to methods of hazard identification which are used in the chemical process industry. These may be overkill for the needs of this project, but right now it's too early to tell.

#### Recommendations:

Develop a formal, explicit, physical definition of initiating event in each alignment of each mode.

Specify (and then apply) a formal, algorithmic approach to development of a list of initiating events at each alignment of each mode. Note that the chemical process hazard technique mentioned above is applied in process variable space, and if this is done carefully enough, there is some chance of picking up events in which flashing occurs in an elevated section of piping (to use one of Warren Lyons' examples).

### Event Sequence Diagrams

Event Sequence Diagrams (ESDs) have become increasingly popular as a modeling step. In a way, they're just flowcharts, but it is very useful to apply them systematically at an early stage of scenario development. PLG began using them some years ago (I don't know who first used them systematically). Part of their value lies in communication with plant personnel, which many of us feel is an important element of this project. Since operator response to very diverse situations is a major element of this project, ESDs would appear to be especially valuable here. In fact, an ESD on which key operator actions are highlighted in scenario-specific

contexts should be a prerequisite to expenditure of effort in human factors analysis.

Recommendation:

Develop Event Sequence Diagrams on which key operator actions are highlighted.

### Allocation of Resources

Risk (according to Kaplan and Garrick) is best thought of as a set of triplets: scenarios, likelihoods of the scenarios, and consequences of the scenarios. The effort in this project is concerned primarily with the first two elements (it is understood that core damage events are the general consequence type of interest). The scope of this project includes a great deal of relatively unexplored territory, and there is anecdotal evidence that minor variations in system alignments in various modes can have considerable impact on initiating events and on response to initiating events. It seems to me that it is more important to do a thorough job of scenario development than an elaborate job of quantification. Without some sort of quantification, there is no way to set priorities within the project, but a screening process can suffice. Even if comparison with 1150 is the goal, it will not be well served by a careful quantification of an incomplete scenario set. It would be preferable to come out with a somewhat uncertain quantification of a scenario set that we felt good about.

Both labs appear to be geared up to invest substantial resources in quantification. Both labs are searching data bases. Both labs are spending time thinking about which PC package to use. Both teams have lined up human factors specialists well in advance of having identified the scenarios, the "errors," and the associated procedural/physical/etc. information which human factors people require as input. It is too early to be certain that any of this activity is unnecessary; some of it is necessary. But it should not be allowed to consume more than its fair share of resources. It is clear that human response will be important to the evolution of the scenarios, but significant expenditure of project resources in human factors analysis *per se* (as opposed to *identification* of key actions) can be justified only after the scenarios are well developed and the priorities are clear.

#### Recommendation:

Complete and document the initiating event exercise and the Event Sequence Diagram exercise before investing too substantially in data crunching or human factors analysis.

### Truncation and Completeness

One of the stated project goals is to compare the risk from low power and shutdown with the risk from full-power operation. This poses a significant challenge. The 1150 analyses resulted in fairly small core damage frequencies, so that in order to argue that the risk from shutdown is *relatively* small, it is necessary to consider initiating events down to extremely low frequencies. In fact, the natural truncation level of this problem may turn out to be so low that it is necessary to consider coincident initiators. (Example given at meeting: loss of service water followed by a random loss of offsite power within a few hours. The frequency of this conjunction could be of order  $10^{-8}$  per year, and this might not be negligible on the scale of events being analyzed.) Of course, it may turn out that risk from shutdown is relatively large, saving us a lot of trouble.

#### Recommendation:

During the process of screening initiating events, care should be taken that initiators are not discarded unless they are clearly incapable of affecting the risk profile. Since it is the stated intention to consider offsite consequences eventually, this logically implies an extremely low frequency cutoff for initiators which can occur with an open containment. To put it another way, the cutoff must be a very small fraction of the frequency of large releases from accidents initiated at full power.

If an extremely low cdf begins to emerge, coincident initiators need to be considered.

The screening of the initiator set should be documented. This need not be elaborate, but there should be a table establishing the disposition of initiators (either that they were explicitly analyzed, subsumed by another, or considered incredible).