



ENCLOSURE 1

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

JAN 21 1980

Generic Task A-17

MEMORANDUM FOR: John Angelo

FROM: S. H. Hanauer, Director
Unresolved Safety Issues Program

SUBJECT: COMMENTS ON DRAFT FINAL REPORT - SYSTEMS INTERACTION
PHASE I

Reference: Draft Final Report dated September 21, 1979

My principal review was concentrated on Chapters 1 and 7 and on the so-called Executive Summary (what contribution does the word "executive" provide; why not just "summary?").

Overall I think this is a very good piece of work. It has made a substantially larger contribution to our understanding of Systems Interaction than I expected last June when I first began to pay detailed attention to this work. However, I believe that improvements can and should be made to this report.

Perhaps my most important comment relates to the imprecise wording used, particularly with regard to safety and risk. Consider for example, "to assure that systems interaction which are important to public safety have been identified" (page 1-2); "significance to unacceptable core damage and thus importance to public safety" (page 1-13); "areas of greatest importance" (page 7-1). These statements are true in a dictionary sense and can be explained to be true as we understand and use these terms; however, they are unsatisfactorily vague. The authors of the report never do come out and say what "important to safety" means or how it's measured. This is a general theme that runs through the report. It may be that one good paragraph in the right place would fix it or that the tone of these various phrases, and the large number of similar ones I haven't identified, should be changed in some respect.

My other general problem with this report relates to the general conclusions which seem rather over-blown compared to the specific things that were done and the specific results that were obtained. An example is "a wide range of potential systems interactions" (page 7-1).

8002250 372

JAN 21 1980

Here are some detailed comments:

1. Page iv, line 6 - Independent of what? The meaning and the significance are both unclear. The same statement is made on page 1-1, line 10.
2. Page iv, lines 20-22 - This premise is correctly stated, but nowhere is its validity or lack of same or limitations discussed. This would seem to be an important point, well worth discussing by the authors of this report. What limitations does this introduce into the results of the study? Do the authors think they are important? Is further study justified? and so on.
3. Page v, line 1 - "Functions" should be "equipment". I believe that it is the equipment to which the fault trees actually pertain and which are actually modeled even though the results are in many cases given in terms of functions in the top line. The rest of it is pretty much equipment oriented.
4. Page v, lines 7-10 - This sentence is somehow garbled. It is failures of energy sources etc. which are being discussed.
5. Page v, line 13 - "a wide range" is not quite as wide as here implied since it is limited both by the "commonality" premise and by the various limitations which were put on to make the study scope manageable. Thus the quoted result does not follow from the actual work performed.
6. Page v, line 16 - "greatest importance" needs some definition.
7. Page v, lines 25 and 26 - This is a very important point and needs expanding. In fact the work is not restricted to systems identified as "safety related" and therefore the results form an important contribution to the current study of the safety significance of "non-safety related" equipment. This seems not to be touched on adequately anywhere in the main part of the report and deserves a paragraph or even a section.
8. Page vi, line 2 - "The potential for an interaction was found to be reasonably high", sounds like a measure or at least a judgement regarding the probability of occurrence of the sequence or the combination. Here again is an important concept which seems nowhere to be developed in the body of the report. I don't think probability evaluations were actually performed and yet here is an implication that some judgements along this line were actually taken. Thus, the summary statement is beyond the scope of the work actually performed and not only misleads the reader but has important implications not fulfilled.

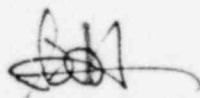
JAN 21 1980

9. Page vi, line 7 - "The absence of explicit assurances" - does this mean the absence of inclusion explicitly in the Standard Review Plan or something else? I couldn't tell.
10. Page 1-2, line 8 and 10 - "To assure that systems interactions which are important to public safety have been identified and their significance evaluated" - this is much too strong. No such assurance is provided or can be by a study of this type, which is more of a pilot study with definite scope and limitations as discussed elsewhere in this report. The trouble is that as written, the text implies that all systems interactions important to public safety (whatever that means; see previous comment) are turned up by this method which we know is not true. "Significance" is also not defined, nor is its method of evaluation given. Note that the last two or three lines on this page show how much more limited the actual study was, compared to this fulsome declaration.
11. Page 1-3, line 3 - "Estimated relative likelihood of the interaction". This is the second of two cryptic references to probability which are never followed up. See my previous comment.
12. Page 1-3, lines 5-8 - The meaning of this sentence ("the purpose...achieved.") is not at all clear to me. What are "the same goals"? My understanding was that the purpose of the SRP assessment was kind of an audit of the SRP to see whether, and to what extent, it includes systems interactions as determined by a bounded study considering certain defined kinds of systems interaction. I can't find this thought in any of these discussions.
13. Page 1-8, last paragraph - An important omission, namely, interactions that come about through the process itself, are not at all treated here. This is the place to address my previous comment about studying commonalities as a subset of systems interactions. Somehow this seems not to be carried over to the discussion that starts on page 1-8, which is where I think it belongs.
14. Page 1-9, first two sentences - Why apologize in this way? What do the authors intend by this disclaimer?
15. Page 1-9, line 15 - Why is this restricted to components? I would think that interactions between subsystems or redundant trains is the objective here and that if one puts on blinders and restricts himself to a view component by component some important system interactions or commonalities will be missed.
16. Page 1-9, lines 23-25 - These are not the only causes or even the only ultimate causes. Other examples are load disturbances (an external event which is not a high energy occurrence); high energy events within the plant and thus not external; the effect of one failure (from one of the causes enumerated, perhaps) upon other components or subsystems either by being close spatially or by being related through the process; and control system reactions to single failures which lead to additional functional unavailabilities. There are others, I'm sure. It is the exclusiveness of this sentence that I am objecting too.

17. Page 1-10, lines 2 and 3 - Not everybody agrees that all hardware failures are governed by the laws of probability. Is this important to the discussion? If so, the basis for it should be given.
18. Page 1-10, table - The inclusion of design errors in "construction" is confusing. It deserves its own line.
19. Page 1-10, line 10 and 11 - By no means everybody agrees that human errors of all types are "probabilistic". Again, if this is important to the development of the work, the basis for this statement should be given.
20. Page 1-11 - On line 3 it is stated that human errors may be a cause and a connection, but the table that follows in the middle of the page doesn't include human error as a connection. Why this disconnect?
21. Page 1-11 - table - "Inherent" is a poor term. "Common manufacturer" is an inadequate representation of the class of errors which includes the mistake made by a single designer or installer or maintainer who produces common mode failures which are a form of system interaction.
22. Page 1-13, line 7 - "Important to public safety". See previous comment.
23. Page 1-13, "Actuation" - Does this include control signals and control logic?
24. Page 1-13, line 17 and 18 - "Significance to una core damage
and thus importance to public safety". See my p omment.
25. Page 1-14, Step 1 - Is this a failure modes and effects analysis or something different?
26. Page 1-15, Step 11 - This is incomprehensible to me. Is it really only changing names? Who cares? Why is it significant? If it's something more than changing names, then the whole point is lost in the present description.
27. Page 1-17 - This table is really quite obscure. Does "methodology applicable" mean "outside the scope of the program of work being described in this report but we think this methodology would apply?" If so what is the basis? It needs to be discussed somewhere. Shouldn't there be a third column or discussion of things for which this methodology is not applicable in the general realm of systems interaction? This reader would like to have such a discussion. An obvious example is sabotage.

JAN 21 1980

28. Page 7-1 - As discussed previously the "principal result" is given a far wider scope than is justified by the actual work performed and reported in this report.
29. Page 7-1, line 12 - I don't know what "reasonably" means in this context. Does the author mean the methodology in its present form can address this particular subset? I think that's right and I think it's a useful thing to say, if that's what is meant.
30. Page 7-1, line 21 - What does "traditional" mean? In fact, what does the whole sentence mean? It somehow seems like an important point, but I don't get it.
31. Page 7-1, line 23 - "Greatest importance" - see previous comment.
32. Page 7-2 - The conclusion given single-spaced does not in any obvious way follow from the work which is described in this report. I think it's true. I also think the authors who wish to draw such a conclusion from this work have an obligation to show the reader how this conclusion follows from the work which they have reported.
33. Page 7-3 - Again, this conclusion, which I believe to be true and about which I have already commented on the general subject, is again not well related and based on the work which is actually reported here.
34. Page 7-3, line 13 and 14 - "The potential for an interaction is bound to be reasonably high". See my previous comment. Does this mean probability? If so, how is it measured?



S. H. Hanauer, Director
Unresolved Safety Issues Program