CT-2079
PDR 3/25/94

WILLIAM KERR

2009 Hall Ave.
Ann Arbor, MI 48104

Tel. 313-662-8701
Fax 313-763-4540
william_kerr@um.cc.umich.edu

18 May, 1993

MAY 25 1993

Dear Sam:

You may know that Stu Long, at Hal Lewis's direction, made arrangements for me to attend a meeting of the Nuclear Utilities Software Management Group (NUSMG) held in Palm Beach Gardens, FL April 28-30, 1993. The meeting was billed as a Workshop on Digital Systems Reliability and Nuclear Safety. A NUSMG representative who had attended one of the meetings of the ACRS subcommittee on software reliability had asked that ACRS send someone to the meeting. None of the ACRS members were available. I agreed to attend.

I have previously sent to Stu Long a copy of some notes that I used as the basis for a presentation that I made to members of the group. Since I gather that Stu Long has by now left the ACRS, I am sending my comments on the meeting to you, with the expectation that you will make proper disposal of them.

Following are my comments on the meeting:

NUSMG has been in existence for only a short time, and, not surprisingly, it is still groping for a purpose and a mission. It appears that the founding group felt that some mechanism for exchanging information on software management and quality control, and on NRC licensing related to software would helpful to nuclear utilities, and this is a principal function of the group so far. Throughout the meeting there were discussions of what NRC had and would be likely to require or approve.

The papers presented at the meeting were not related to any particular theme or aimed at any identified problem. My impression is that they looked for people who would be willing to make a presentation, and put the finger on them to do so.

One of the early papers was presented by a representative of Canberra. He described the design and testing of a set of software developed to implement a system for assembling and analyzing measurements made by the health physics staff of a utility, and for making calculations and assessments required in connection with the new version of 10CFR20. The method they used for developing the software was a classic example of how not to do it. They had seven separate groups working on each of several parts of the software, with little or no central direction. They developed a set of tests

which they believed demonstrated the validity of the completed system. I asked what their goals were, and how they knew when they had been achieved. The answer was that they continued the testing until the customer was satisfied with the result!

Richard Cobb of Software Engineering Technology gave a presentation on the "cleanroom" approach to software development. I was not impressed. His paper was presented with a lot of enthusiasm, and with the implication, if not a direct statement, that if the approach that his organization developed is used, error-free software will result. (I can't believe he really thinks this method will always produce error free software, but this is what he seems to be saying!) When asked to give examples of software developed by his organization he gave a couple, and to illustrate that when first tested it proved to be error free, he stated that when first tested it ran. Now as anyone with even limited experience knows, the fact that a program runs, even if it gives a correct result for a limited set of exercises, is no guarantee that it is error free. Yet no one in the audience called him on his example. This may be a measure of the sophistication of his audience. Or maybe they were just being polite.

One of the presentations was made by an engineer from Commonwealth Edison, who described their problems in obtaining approval of the NRC staff for the installation of the Westinghouse Eagle 21 system in Zion 1 and Zion 2 to replace the original system. The replacement was motivated to a considerable extent by their inability to obtain replacement parts for the original system, but also by their judgment that the new system was more reliable than the original.

Initially they had not anticipated any problems because several plants, Sequoyah, Watts Bar, and Turkey Point had already received approval. However they were in for a big surprise! They first discussed the question informally with the NRC, proposing that the change be treated under 50.59, i.e. that it did not constitute an unreviewed safety question. NRC was unwilling to accept this, so they applied for a license amendment.

I won't go into all the gory details, but they estimate that it cost them an additional $300K to do all of the studies that were required before they finally received approval. And the young man making the presentation said that the results of the studies did not lead to any change in what they had originally proposed to do. He felt that part of the problem was caused by the staff's use of consultants in the review. One of the consultants was from Oak Ridge where he has been involved in electromagnetic interference research. Commonwealth had done what they considered a thorough measurement for emi in connection with the performance of the initial system. What they measured was far below the tolerance of the Eagle 21 system. In spite of this, NRC insisted on another survey!

One might argue that, aside from a waste of limited resources, this incident did not produce any negative impact on safety. However the Commonwealth engineer told us that as a result of this experience they have decided to cancel plans they had developed for replacing a relay-based emergency diesel control system (using about 50 electromechanical relays) with a solid-state-based system which they are convinced would be more reliable. They have ordered another relay based system. On the basis of their experience in getting approval for the Eagle 21 system, they felt they could not afford the expense and uncertainty of the review process! This appears to be an example of an overzealous review process producing a negative impact on safety. I believe Mr. Selin has asked for examples.

During a presentation on security system software, Al Weinstein, of Securacom, pointed to inconsistencies region to region, saying that some regional staffs would accept systems and equipment that were not accepted by others.

Incidental Comments:

One of the participants commented that one utility had discovered a virus in its software. He was not at liberty to identify the utility.

A representative of the Callaway plant commented during one of the discussion sessions that he was convinced that Callaway was removed from the Good Plant list because they disagreed with the NRC staff.

On the basis of my observations during the meeting I suggested to the group that they give more attention to how they should go about getting the software performance that they consider to be required for safe and reliable plant operation, rather than giving principal emphasis to what the NRC wants or will require.

Sincerely,

William Kerr