



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

MAR 02 1981

Part 4-40

(84)

NOTE TO: [REDACTED]  
Instrumentation & Control Systems Branch  
Division of Systems Integration

FROM: J.T. Beard  
Operating Reactors Assessment Branch  
Division of Licensing

SUBJECT: CANDIDATE CRITERIA FOR CONTROL SYSTEMS

Per your request, I am providing my comments on your memo of February 12, 1981 on this subject. First, let me say that work in this area is long overdue; I'm glad to see effort is finally going toward this area. Second, your candidate criteria appear to be perceptive and well thought out. I hope that the type of peer review you have initiated will serve to finalize your candidates into an effective set of NRC criteria.

1. Re: Candidate Criterion #1

I believe this criterion should be expanded from the classical "non-interference" requirement to include also what could be called a "not-frequent challenge" requirement. We have all worked hard over the years to assure that the protection system is highly reliable and has a low failure rate. We must, however, not forget that the failure rate is not zero. Even if a failure rate for a system is very low, a large number of challenges (demands) will cause failures. Further, these failures can occur

PDR XA  
8103250472

either early or late in a set of challenges. Therefore, failures of control systems should not cause frequent challenges of the safety systems.

2. Re: Candidate Criterion #3

I am not aware of any technical basis for limiting the number of control systems failures to a "single credible failure." As a design criterion, the protection systems assume a single failure within the protection system. The validity of this assumption is supported by high quality equipment, electrical independence requirements, physical separation requirements, periodic testing requirements, etc., etc. However, these requirements are directly applicable only to the protection systems and are not applied generally to control systems. In the absence of such supporting requirements, I find no technical basis for "single failures" in control systems. Single failures grow into multiple failures.

For this situation I suggest a set of criteria. First, the control system should include sufficient independent performance limiting or mitigating features that no "single failure" within the control system will necessitate action by the protection system. (An illustration example would be to provide an automatic rod insertion if neutron power should exceed 103%.) Second, the control system

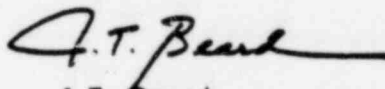
C.E. Rossi

- 3 -

MAR 02 1981

should include sufficient features that upon postulated gross (i.e., multiple) failure of the control system the resultant plant conditions shall not exceed the capabilities of the safety system.

Obviously, we could (and probably should) discuss these concepts at length. Maybe this note could serve as the basis of such discussions not only between the two of us, but between you and others.



J.T. Beard  
Operating Reactors Assessment Branch  
Division of Licensing

cc: ICSB Members  
A. Szukiewicz  
K. Wichman  
J.T. Beard



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

February 12, 1981

*copies for Part 4-41*  
*H. Fitz*  
*W. Rossi*  
*Capone*  
*Check*  
*Ross*

Ivan W. Smith, Esq., Chairman,  
Administrative Judge  
Atomic Safety and Licensing Board  
U.S. Nuclear Regulatory Commission  
Washington, D.C. 20555

Dr. Walter H. Jordan, Administrative  
Judge  
881 W. Outer Drive  
Oak Ridge, Tennessee 37830

*return to CR*

Dr. Linda W. Little, Administrative  
Judge  
5000 Hermitage Drive  
Raleigh, North Carolina 27612

In the Matter of  
METROPOLITAN EDISON COMPANY, ET AL.  
(Three Mile Island, Unit 1)  
Docket No. 50-289

Dear Board Members:

At the hearing session of January 27, 1981 (Tr. 11,027-11,030) the Board indicated that it did not understand a statement relative to the direct applicability of his views to TMI-1 that was made by Demetrios L. Basdekas in his memorandum to James R. Tourtellotte dated October 10, 1980, entitled, "Safety Implications of Control Systems and Plant Dynamics, and their Relevance to the TMI-1 ASLB Hearing." At my request Mr. Basdekas has prepared a written explanation of how he believes his views presented in documents previously provided to the Board have direct application to TMI-1. That explanation is set forth in a memorandum to James R. Tourtellotte dated February 9, 1981, entitled, "Safety Implications of Control Systems and Plant Dynamics, and their Relevance to the TMI-1 Restart ASLB Hearing." Copies of that memorandum and its attachment are enclosed.

Sincerely,

James M. Cutchin, IV  
Counsel for NRC Staff

Enclosure: As stated

cc w/enclosure:  
see next page

*202170263*

Licensing Board

-2-

George F. Trowbridge, Esq.  
Karin W. Carter, Esq.  
Honorable Mark Cohen  
Mr. Steven C. Sholly  
Mr. Thomas Gerusky  
Mr. Marvin I. Lewis  
J. G. Herbein  
Ms. Jane Lee  
Walter W. Cohen  
Thomas J. Germin  
Allen R. Carter  
Robert Q. Pollard  
Chauncey Kepford  
Ms. Frieda Berryhill  
Gail P. Bradford  
William S. Jordan, III, Esq.  
John Levin, Esq.  
Jordan D. Cunningham, Esq.  
Louise Bradford  
Ms. Ellyn R. Weiss  
Ms. Marjorie M. Aamodt  
Atomic Safety and Licensing Board Panel  
Atomic Safety and Licensing Appeal Board Panel  
Secretary



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

FEB 9 1981

MEMORANDUM FOR: James R. Tourtellotte, Esq.  
Assistant Chief Hearing Counsel, ELD

FROM: Demetrios L. Basdekas  
Reactor Safety Engineer, RSR, RES

SUBJECT: SAFETY IMPLICATIONS OF CONTROL SYSTEMS AND PLANT DYNAMICS,  
AND THEIR RELEVANCE TO THE TMI-1 RESTART ASLB HEARING

This is in response to Mr. Cutchin's request of February 3, 1981 to provide a written explanation of how my views, presented in documents provided to the Board, have direct application to TMI-1.

I have read pages 11,027-11,030 of the hearing transcript and I believe that the Board desires an explanation specifically focused on my statement that "Even though [the issue of the effects on safety of the control systems] has been treated as a generic issue, it applies directly to the TMI-1...." I believe that the center of the Board's question is the word directly. The following explanatory remarks are intended to answer the Board's question on this point.

The fact that a Failure Modes and Effects Analysis (FMEA) has been performed for the Integrated Control System (ICS) by Babcock & Wilcox does not mean that it has been an effective one in identifying important weaknesses in the TMI-1 (a sister plant of TMI-2) control systems. The recommendations I make in my memorandum to Dr. Ahearne of September 4, 1979 (Reference No. 1 in my memo to you of October 10, 1980) with respect to follow-up effort to complete the FMEA with the objective of accounting plant-unique features, applies directly to the TMI-1, in that the B&W performed FMEA was never extended, as it should have been, to include the TMI-1 plant design features of its control systems and plant dynamics, which are unique to it. An example of lack of such effectiveness is on page 4-32 of B&W-1564 (copy attached). In Item 1-30 it is stated that no effect is expected for the case of steam-generator-level loss of control. This statement is not correct. The implications of this and related failures in the main feedwater control system are discussed in documents No. 12 and 16 on the list of documents I supplied to Mr. Cutchin of your office on October 30, 1980. Control system and other "non-safety" system failures on the secondary side may result in a rapid overcooling of the primary system subjecting the reactor vessel to a pressurized thermal shock that would threaten its very structural integrity. During our meeting in your office with NRR representatives sometime in early September 1980, I mentioned,

9762170266

FEB 9 1981

as an example, that my understanding was that TMI-1 was one of two plants in the country that did not have a "safety grade" main feedwater pump trip function on reactor/turbine trip.

Furthermore, I believe that testimony which had been prepared by the staff on this generic issue for the TMI-1 Restart Hearing needed to be challenged. I am addressing this point in the fourth paragraph of my memorandum to you dated October 10, 1980. My use of the word directly was intended to point the direct applicability of my concerns on the subject issue to the TMI-1 in terms of this generic concern, in view of its specific similarities to TMI-2, and the specific points I have discussed earlier.

I hope that this discussion is responsive to the Board's question, and I request that you make a copy of this memorandum available to the Board.

*Demetrios L. Basdekas*

Demetrios L. Basdekas  
Reactor Safety Engineer  
Plant Instrumentation, Control &  
Power Systems Branch, RSR, RES

Enclosure: As stated

cc: W. S. Farmer  
L. H. Sullivan



Table 4-3. (Cont'd)

SHEET & ITEM NO.	INPUT	FAILURE MODE	EFFECTS ON NSS	REACTOR TRIP	REMARKS
1-26 (continued)		0%	No effect if MFWBV is open. If MFWBV is closed, the Loop A S.U. valve goes 80% open, causing the switch from S.U. to Main for feedwater flow indication. Subsequently, the S.U. valve on Loop A will cycle between 50% and 80% open until level reaches the high level limit (FW 17.6).	Possible RC pressure trip	The M/A stations can be used to control level after a trip if necessary.
1-27	Startup Feedwater Flow (Loop B)		Same as Loop A.		
1-28	Temp. Compensated RC Flow, Loop A	100%	This failure could cause an undesired reratioing of feedwater flow and very likely a reactor trip on RC pressure. Control after reactor trip is not changed.	Probable on high RC pressure.	
		0%	Feedwater flow will reratio, with SG-A going on the low level limit, and the SG-B feed flow limited only by BTU limits. For initial load of 100%, there is a net reduction in feedwater flow, and the reactor trips on high pressure. Control after reactor trip is not changed.	Probable on high RC pressure	
1-29	Temp. Compensated RC Flow, Loop B		Same as for Loop A.		
1-30	SG-A, Operate Level	252." (High)	Loop A feed flow is reduced until SG-A reaches the low level limit. The net loss of feedwater flow causes heatup of the primary and reactor trip on high pressure. Control after reactor trip is not changed.	Yes	
		0."	No effect, except that SG-A loses the protection of having a high level limit.	Not expected.	