



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

DEC 19 1979

MEMORANDUM FOR: Darrell G. Eisenhut, Acting Director,
Division of Operating Reactors

THRU: Gus Lainas, Acting Assistant Director,
Systems Engineering, Division of Operating Reactors *J.L.*

FROM: Paul S. Check, Chief, Reactor Safety Branch,
Division of Operating Reactors

SUBJECT: STATUS REPORT - HIGH ENERGY LINE BREAK WITH CONSEQUENTIAL
CONTROL SYSTEM FAILURE

1.0 INTRODUCTION AND SUMMARY

On September 17, 1979, all licensees of light water reactors were requested to determine if an unreviewed safety question related to the interaction of safety grade and non-safety grade equipment existed at their respective nuclear plants. On the basis of scenarios involving interactions such as those identified by Westinghouse and submitted to NRC by Public Service Electric and Gas Co. (Reportable Occurrence 79-58/1P) we were concerned that consequential control system failures following a high energy line break (HELB) might cause the consequences of the HELB to be more severe than previously expected.

All licensees responded to our request within the requisite 20 days. We have screened these submittals. On the basis of our review to date, we find no specific identified safety problems; that is, we find no event sequence that clearly leads to an unacceptable consequence. However, both general and specific concerns remain.

Our general concern relates to the variability in breadth and depth of the initial systems reviews, the lack of a consistent methodology of review, and the failure to characterize the relative risks among the interactions considered. We believe these broad concerns will be dealt with by the systematic assault on this and closely related topics proposed by Recommendation 9 of NUREG 0585. Industry is currently forming a group to develop a plan for resolving the issues raised in Recommendation 9. We emphatically recommend NRC participation in this activity.

The industry group augmented by NRC representatives would form an NRC-Industry Steering Group on Systems Interaction. Such a group could provide the forum and mechanism for exploring and implementing new and presumably more efficient ways of handling this unresolved safety issue. In addition to its overall responsibility for ultimately responding to Recommendation 9, a near-term objection of this group could be identification of high risk events for consideration by TAP A-17 and IREP. The NRC-Industry Steering Group could readily be employed to accomplish

Contact: B. Morris, RS/DOR, 28173
Bea Rosenberg, RS/DOR, Vydec Disc 21

8005280473

DEC 19 1979

Tasks II.C.1 Items B-9 and C-9 outlined in Denton's Draft Action Plan to the Commissioners (December 11, 1979).

Our specific concern relates to new scenarios generated by some licensees during their reviews and described in detail in their reports. Although each new scenario was resolved by the licensee who developed it, we cannot tell whether other, similar plants considered these scenarios. We recommend that the scenarios described in Appendix A be addressed by the appropriate LWR licensees within the next 60 days. Interim criteria for these reviews are also stated in Appendix A.

2.0 EVALUATION OF RESPONSES

Each licensee employed a matrix to identify potential interactions. Control systems and functions are listed on one axis and type of HELB along the other. Sample matrices are included in Appendix B. Identified potential interactions were then examined by the vendors and licensees. The extent or completeness of the matrices and the thoroughness of the examinations of potential interactions show considerable variation with vendor and licensee.

A general appraisal by NSSS vendor, based on our initial screening, is presented below.

2.1 WESTINGHOUSE PLANTS

Westinghouse identified 15 potential interactions out of an array of seven control systems with seven accidents. Four of the 15 potential interactions were considered limiting by Westinghouse. Generic analyses were provided to the licensees, who in turn submitted the analyses to the Commission. Most licensees modified this submittal with plant-specific considerations such as physical separation, environmental qualification of equipment, operating mode, and operator training. Licensees have relied on the fact that for several scenarios the operator would have in excess of one-half hour to take corrective action.

It remains to be shown conclusively that (1) the operator has sufficient reliable indication and training to cope with all 15 potential interactions, (2) that the enumerated set is complete.

Licensees have proposed to perform additional work in conjunction with forthcoming Lessons Learned requirements contained in the final report (NUREG 0585).

2.2 BABCOCK & WILCOX

All B&W supplied NSSS owners have relied on a generic B&W analysis (see Appendix B). Each B&W reactor owner related its plant-specific equipment features (e.g., location and/or qualification of existing equipment) to the characteristics of certain plant functions (e.g., the reactor or turbine trip may occur before non-safety-grade systems can deteriorate as a result of the HELB considered). Some interactions when compared to the FSAR analysis are either unchanged or changed in the conservative direction. The rest were rejected on the basis of low probability. In this regard, licensees referenced a probabilistic analysis by the Nuclear Safety Analysis Center (NSAC), sent under cover of an AIF letter, Ward to Denton, dated October 19, 1979.

FWLB inside containment and its potentially adverse effect on PORV (i.e., spurious openings, or failure to close after opening) was not analyzed in the FSARs. Post TMI-2 analysis and operator guidelines have been developed for LOFW concurrent with an open PORV. B&W plant licensees referenced this analysis. MFW control/EFW initiation and control interaction with a small LOCA or MFWLB inside containment (steam generator level transmitters) has been addressed in the B&W plant licensees responses to Information Notice 79-22.

All B&W plant licensees have proposed a long-term assessment of environmental effects on NSGS to include

- (a) Defining instrumentation and control functions required for safe shutdown;
- (b) Identifying applicable equipment errors and responses in an adverse environment;
- (c) Preparing a safety assessment and recommending corrective actions, if required.

B&W licensees plan to couple this proposed assessment with the Abnormal Transient Operating Guidelines (ATOG) currently under preparation, and will focus on additional operator training to recognize and respond to an adverse HELB/NSGS interaction.

Certain scenarios generated during the B&W plant reviews had not been included among the original scenarios identified by Westinghouse. These have been included in Appendix A. They should be addressed by all PWR licensees in their follow-up reviews.

2.3 COMBUSTION ENGINEERING

All CE reactor owners have also relied on a generic CE analysis that identified potential adverse HELB/NSGS interactions (see Appendix B). Each plant considered the plant specific characteristics: location and/or qualification of equipment, modes of operation of certain systems.

Some potential interactions were either inconsequential or act in a conservative direction relative to the FSAR analysis. The rest were rejected on the basis of low probability (NSAC letter, op. cit.). Some plant owners plan to alert the operator to the potential interaction scenarios stressing the necessity of prompt action and will instruct the operators to search for diverse indication signals.

2.4 GENERAL ELECTRIC

Most BWR licensees responded using a format developed by a BWR Users Group with GE advice. As many as 70 plant systems were considered in conjunction with a variety of postulated HELBs. The matrix developed (Appendix B) contains entries classifying the effect of the particular HELB on the particular system. In all these cases, the licensee concluded that HELB consequences would not be more severe than previously reported in safety analyses. The reasons for these conclusions included claims that the equipment is qualified to perform adequately in the HELB environment, that the consequences would not be worse even if the equipment malfunctions in the most adverse way possible, or that the equipment would not experience an adverse environment. No further details were given to justify these conclusions and detailed scenario descriptions were not provided.

A few BWR licensees not following the BWR Users Group format identified and described specific scenarios in detail. In each case, the licensee determined, on the basis of environmentally qualified control equipment or operator action or accident analysis, that the consequences of the scenarios would meet licensing criteria. The specific scenarios are described in Appendix A.

Two BWR licensees (LaCrosse, Humboldt) responded formally but failed to address the main issues raised in the letter of September 17, 1979. In both cases, the licensees have stated their intention to perform an appropriate review and submit a report.

The reports following the BWR Users Group format are in general more extensive in terms of systems and types of HELBs considered than reports from PWRs. However, the BWR reports do not include details to support the conclusions reached as did the PWR reports.

3.0 RELATED NRC ACTIVITIES

Two major generic NRC activities, Systems Interactions (TAP A-17) and the Integrated Reliability Evaluation Program (IREP), have the potential for developing methodologies to resolve the concern regarding consequential control system failures due to HELBs. The same methodologies would also be applicable to resolution of other concerns related to control systems. Recommendation 9 of NUREG 0585 summarizes these concerns and calls for the nuclear industry to resolve them as follows:

*The owner of operating plants and all plants under construction should be required to evaluate the interaction of non-safety and safety-grade systems during normal operation, transients, and design basis accidents to assure that any interaction will not result in exceeding the acceptance criteria for any design basis event. The review should be systematic and include all non-safety components, equipment, systems, and structures under all conditions of normal operation, anticipated operational occurrences, and design basis accidents initiated both within the plant (such as pipe breaks) and from outside the plant (such as earthquakes, other natural phenomena, and offsite hazards). The interactions and effects should consider various failure modes including spurious operation, failure to operate upon demand, and any unusual or erratic operation that might result from exposure to the abnormal process or environmental conditions accompanying the event under study. As a necessary part of this evaluation, proper qualification of safety systems, including mechanical components, should be verified.

*The number of simultaneous failures of non-safety equipment considered should reasonably reflect the expected number of non-safety systems simultaneously exposed during the event under study to conditions for which they were not designed or qualified.

*Equipment identified as the potential cause of violation of the acceptance criteria for any design basis event should be appropriately modified to eliminate or significantly reduce the probability of the adverse interaction. Alternatively, the affected safety systems or structures should be modified to cope with the interaction. The results of the evaluations should be used to review and modify as appropriate, the plant operating and emergency

procedures and operator training. The Task Force recommends that these studies be completed within a year, at which time licensees should submit proposed schedules for making the modifications identified in the evaluations. Completion of this study would not be a condition of licensing new plants in the interim of one year if the basis for continued licensing in face of the present unresolved safety issue on systems interaction is judged by the staff to continue to be valid."

The development of the scope and the schedules for TAP A-17 and IREP should be guided by Recommendation 9; i.e., to the extent possible the objectives and schedule of Recommendation 9 should be made the objectives and schedule of these tasks. This conclusion is consistent with our interpretation of Tasks II.C.1 of Denton's Draft Action Plan of December 11, 1979. However, given the complexity of application of these powerful methodologies, it is unlikely that completion could be achieved within several years. Nevertheless, these programs can provide a check on the resolutions developed through the efforts of the Industry-NRC Steering Group described below.

4.0 INDUSTRY ACTIVITIES

On November 8, 1979, a group of utility, AIF and NSSS vendor representatives met with NRC staff members in Bethesda to consider how a joint industry-NRC steering committee could assist in resolving the concerns expressed in Recommendation 9, including the HELB consequential Control System Failure concern.

The industry representatives are now organizing their effort. We recommend that NRC steering committee representatives be named as soon as possible.

Current NRC activities related to Recommendation 9, i.e., TAP A-17 and IREP, are unlikely to provide resolutions within several years. We believe the Industry-NRC Steering Group should have as its principal objective the identification and resolution of the highest risk systems interactions concerns within one or two years.

Denton's Draft Action Plan, in describing Task II.C.1 provides the following direction.

for NRC---

"Reliability engineering techniques can complement quality assurance and provide a disciplined approach to multidisciplinary systems engineering in the design of nuclear plants, the development of startup test procedures, the development

of operating, maintenance, and emergency procedures, and in operations. Specifications will be developed for acceptable reliability assurance programs to be implemented by operating license holders, construction permit holders, and future construction permit applicants. The role of applicant-supplied probabilistic safety or reliability analysis in future safety analysis reports will be defined in this program. Reliability assurance program requirements will be promulgated by a new Regulatory Guide."

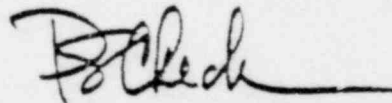
for Licensees---

"Applicants and operating license holders will be required to develop reliability assurance programs for NRC approval and implementation."

These tasks can readily be pursued by the Industry-NRC Steering Group.

5.0 SPECIFIC RECOMMENDATIONS

- (a) Each operating reactor licensee should address the specific scenarios and criteria expressed in Appendix A and report their findings within 60 days.
- (b) An Industry-NRC Steering Group should be formed with the objective of identifying and resolving the highest risk Recommendation 9 and Task II.C.1. concerns within two years. The key near-term action here is naming 3 NRR BC/ADs and a task manager to serve on this Committee.



Paul S. Check, Chief
Reactor Safety Branch
Division of Operating Reactors

cc: R. Mattson
D. Ross
R. Tedesco
S. Hanauer
G. Lainas
Y. Moore
Y. Panciera
F. Coffman
S. Weiss

J. Rosenthal
S. Diab
R. Satterfield
E. Butcher
J. Angelo
F. Rowsome
M. Aycock
D. Tondi
B. Morris ✓

APPENDIX A

SPECIFIC SCENARIOS AND INTERIM CRITERIA TO BE CONSIDERED IN FOLLOW UP REVIEWS OF HELBs WITH CONSEQUENTIAL CONTROL SYSTEM FAILURE

General Criteria - Licensees should reconsider their original review and the additional scenarios described below. The following criteria should be applied.

1. Equipment Qualification - Equipment needed to achieve emergency reactor shutdown, containment isolation, reactor core cooling, containment and reactor heat removal and prevention of significant release of radioactive material to the environment is to be designated "Class IE" or safety-grade and must be environmentally qualified. If such equipment is discovered not to be environmentally qualified during these reviews, the NRC should be informed according to appropriate reporting requirements.

If non-safety-grade equipment exposed to a HELB environment could interfere with operation of safety equipment intended to mitigate the HELB, the non-safety equipment must be moved to a protected area, be de-energized, or its environmental qualification documentation must be available for NRC audit.

2. Operator Actions - In any case that operator actions are required to remedy a situation of concern resulting from a control system failure subsequent to a HELB, the revised emergency procedures relevant to the concern should be available for NRC audit. Furthermore, if a HELB could cause non-safety-grade instrumentation to malfunction and confuse the operator, the emergency procedures should include appropriate warnings.
3. De-energization of Controls - In any case that power or control circuits for non-safety-grade equipment have been de-energized to prevent interference with safety functions, consideration must also be given to the possibility that an adverse HELB environment could cause electrical shorts to ground or to power sources or mechanical failures of control equipment which could result in re-energizing the control or power circuits.
4. Simultaneous Failures of Multiple Non-Safety Components or Systems

In any case that a given HELB location can result in simultaneous failure of more than one Non-Safety-Component or System all the potential failures

must be considered. For example, if a PORV fails due to a HELB, the related block valve will probably be subjected to the same environment and might also fail and the block valve may not be relied on to mitigate the situation. Credit cannot be taken for block valve action in such a situation unless the valve can be shown to be environmentally qualified.

Scenarios To Be Considered

We cannot determine from the initial reports whether the following scenarios have been considered by all licensees. The scenarios should be reviewed. If they have been considered, the licensee should inform the NRC project manager; if not, the results of the review and actions taken should be reported within 60 days.

1. Inadvertent Removal of ECCS Recirculation Water (PWRs) - Systems for draining or pumping leakage from the containment or reactor building could be inadvertently actuated in a LOCA environment and reduce the ECCS recirculation water inventory in the active sump.
2. Failure to Isolate Broken Steam Generator Loop (PWRs) - The inappropriate opening of a main steam isolation valve bypass valve because of the steam environment would preclude complete steam generator isolation.
3. Inability To Maintain Fuel Pool Cooling (BWRs) - Fuel pool cooling may be lost due to a LOCA environment and the situation cannot be remedied because of high radiation in secondary containment.
4. Moisture in Compressed Air System - (All plants) The compressed air system air dryer controls could malfunction while the compressors continue to operate. Moist compressed air could cause malfunction of the Containment Atmosphere Dilution System control valves (backup control air for these valves would not be operable until loss of control air pressure). Other systems may also be affected.
5. Overflow of Liquid Radwaste System (BWR) - A HELB resulting in failure of the condensate filter/demineralizer controls could result in simultaneous transfer of liquid to the liquid radwaste systems from the break and from the filter/demineralizers. This could overflow the radwaste system resulting in more severe radiological consequences than anticipated from an HELB. This is of particular interest for multiple units sharing common liquid radwaste systems.

6. Isolation of Recirculation Loops (Non-Jet Pump BWRs) - HELB induced closure of recirculation pump valves could isolate the recirculation loops. Accident analyses have assumed these valves to remain open.
7. Opening of Reactor Vessel Head Vent Valves (BWRs) - Many BWRs considered the possibility that the RPV Head Vent Valves could fail open during a LOCA. A generic analysis was done for these plants showing a negligible increase in PCT. The remaining BWRs should confirm that this analysis is applicable to their designs.

APPENDIX B

FORMAT USED BY VENDOR USER GROUPS TO RESPOND TO
HELB CONSEQUENTIAL CONTROL FAILURE CONCERNS

Control System Accident	Reactor Control	Pressure Control	Level Control	Feedwater Control	Steam Generator Pressure Control	Steam Dump System	Turbine Control
Small Steamline Rupture	X	X			X		
Large Steamline Rupture		X			X		
Small Feedline Rupture	X	X		X	X		
Large Feedline Rupture	X	X			X		
Small LOCA	X	X		X			
Large LOCA							
Rod Ejection							

TABLE 1

PROTECTION SYSTEM-CONTROL SYSTEM POTENTIAL ENVIRONMENTAL INTERACTION

X - Potential Interaction Identified that could Degrade Accident Analysis

- No such Interaction Mechanism Identified

WESTINGHOUSE

IMPACT OF CONTROL SYSTEM EFFECTS ON SAFETY ANALYSIS

	Licensing Basis		Accidents		Large LOCA	Small LOCA
	SLB Inside Containment	SLB Outside Containment	FWLB Inside Containment	FWLB Outside Containment		
I. Reactor Power Control and Shutdown						
Control Rod Drive Control System	(2)	(2)	(2)	(2)	(2)	(2)
Reactor Pressure Control						
Power Operated Relief Valve	(1)		(1)			(3)
Pressurizer Heaters						
Pressurizer Spray						
Steam System Isolation and Pressure Control						
Turbine Trip/Turbine Stop Valves		(2)		(2)		
Turbine Bypass/Atm Relief Valves	(1)	(3)	(1)	(3)	(3)	(3)
IV. Feedwater System Isolation and Control						
Main Feedwater Control	(4)	(4)	(4)	(4)	(3)	(4)
Main Feedwater Isolation Valves		(1)		(1)		
Auxiliary Feedwater Isolation Valves		(4)		(4)		
Auxiliary Feedwater Initiation		(1)		(1)		
Auxiliary Feedwater Level Control	(4)	(4)	(4)	(4)	(3)	(4)

- 1) Equipment Can be Shown to Perform Intended Function
 2) Required Period of Operability Is Short
 3) Equipment Performance Is Conservative In Adverse Environment
 4) Potential Inconsistency With Safety Analysis Inputs and Responses
 Note: All Open Entries are Either a Dash (-) or a Y on Table II

BARBOUR & WILCOX

MATRIX OF EVENTS/CONTROL FUNCTIONS
FOR FURTHER CONSIDERATION AND ACTION

Pipe Break Control Function	SLB	FWLB	CEA Ejection	SBLOCA	LBLOCA
Pressurizer Level		X			
Pressurizer Pressure					
Pilot Operated Relief Valves	X	X			
CEA Position	X	X	X	X	
Feedwater Flow	X	X			
Boron Concentration					
Turbine Control	X				
Steam Bypass	X				
Steam Dump Upstream of MSIV	X	X			
Steam Dump Downstream of MSIV	X				
Steam Gen. Blowdown					
Condenser					
Reactor Coolant Flow					

COOPER NUCLEAR STATION
ENVIRONMENTAL INTERACTION TABLE

SYSTEMS	LOCATION	MAIN STEAM			FEEDWATER			LOCA		RUCB REACTOR BUILDING	RCIC REACTOR BUILDING	HPCI REACTOR BUILDING
		INSIDE SMALL	INSIDE LARGE	REACTOR BLDG.	TURBINE BLDG.	INSIDE REACTOR BLDG.	TURBINE BLDG.	SMALL	LARGE			
Suppression Pool:												
Temperature Monitoring	RB/Toruo	2	2	2	4	2	2	2	2	4	4	4
Level Monitoring	RB/Toruo	4	4	2	4	2	4	4	4	4	2	2
Circulating Water System (Non-Safety)	InTake/TB	4	4	4	2	4	4	4	4	4	4	4
HVAC System	All	2	2	2	2	2	2	2	2	2	2	2
Non IE Battery System	CU	4	4	4	4	4	4	4	4	4	4	4
A. C. Auxiliary Electric	RB/TB	4	4	4	4	4	4	4	4	4	4	4
Condensate Transfer and STORAGE	TE	4	4	4	2	4	4	4	4	4	4	4
Main Turbine & Controls	TB	4	4	4	2	4	4	4	4	4	4	4
Main Condenser & Control	TB	4	4	4	2	4	4	4	4	4	4	4
Instrument (Control)												
ALL SYSTEMS: Compressor Piping and Controls	TB/RB/DW	2	2	2	2	2	2	2	2	2	2	2
Fire Protection System	RB/TB	4	4	2	4	2	4	4	4	2	2	2
CRB Hydraulic System (Non-Safety)	RB	4	4	2	4	2	4	4	4	4	4	4
RV Head Vent	DW	2	2	4	4	4	4	2	2	4	4	4
Standby Liquid Control	DW/RB	3	3	4	4	4	4	3	3	4	4	4

32

COOPER NUCLEAR STATION
ENVIRONMENTAL INTERACTION TABLE

SYSTEMS	LOCATION	DATH STEAM			FEEDWATER			LOCA		RUCU REACTOR BUILDING	RCIC REACTOR BUILDING	HPCI REACTOR BUILDING
		INSIDE SMALL	INSIDE LARGE	REACTOR BLDG.	TURBINE BLDG.	INSIDE BLDG.	REACTOR BLDG.	TURBINE BLDG.	SMALL			
Turbine Pressure Control:												
By Pass Valves	TB	4	4	4	2	4	4	4	4	4	4	4
Pressure Sensors	TB	4	4	4	2	4	4	4	4	4	4	4
Control System	CR	4	4	4	4	4	4	4	4	4	4	4
Neutron Monitoring System:												
LPRM's & Cables	DW/RB	2	2	2	4	4	2	4	2	2	4	4
APRM's & Cables	DW/RB	2	2	2	4	4	2	4	2	2	4	4
RPIS/Rod Block Mon.	DW/RB	2	2	2	4	4	2	4	2	2	4	4
TIP	DW/RB	2	2	2	4	4	2	4	2	2	4	4
Reactor Protection System:												
Turbine Scrub	TB	4	4	4	2	4	4	4	4	4	4	4
HC Set	CB	4	4	4	4	4	4	4	4	4	4	4
Reactor Manual Control System	RB/CR	4	4	4	4	4	4	4	4	4	4	4
SHV System (Non ADS)	DW	3	3	3	4	4	3	4	3	4	4	4
RBCCM System	RB	4	4	2	4	4	2	4	4	2	4	4
RUCU	DW/RB	3	3	2	4	4	2	4	3	2	2	2

34

COOPER NUCLEAR STATION
ENVIRONMENTAL INTERACTION TABLE

SYSTEMS	LOCATION	HAIR STEAM			FEEDWATER			LOCA		RUCU REACTOR BUILDING	RCIC REACTOR BUILDING	HPCI REACTOR BUILDING
		INSIDE SMALL	INSIDE LARGE	REACTOR BLDG.	TURBINE BLDG.	INSIDE REACTOR BLDG.	FEEDWATER TURBINE BLDG.	SMALL	LARGE			
Recirculation System:												
Pumps	DW	2	2	4	4	2	4	4	2	4	4	4
Valves & Oper.	DW	3	3	4	4	3	4	4	3	4	4	4
HG Set	RB	4	4	4	4	4	4	4	4	4	4	4
HCC	RB	4	4	4	4	4	4	4	4	4	4	4
Flow Control Sys.	CR/RB	4	4	4	4	4	4	4	4	4	4	4
Control Inst. Trans.	RB	4	4	4	4	4	2	4	4	4	4	4
Feedwater Delivery System:												
Flow Elements	TB	4	4	2	2	4	4	4	4	4	4	4
Level	DW/RB	2	2	4	4	2	4	4	2	4	4	4
Pumps	TB	4	4	4	2	4	4	4	4	4	4	4
Valves & Oper.	TB	4	4	4	2	4	4	4	4	4	4	4
Flow Control Sys.	CR	4	4	4	4	4	4	4	4	4	4	4
Feedwater Heating	TB	4	4	2	2	4	4	4	4	4	4	4
Instrument AIs	TB	4	4	4	2	4	4	4	4	4	4	4
Control Inst. Trans.	RB/TB	4	4	2	2	4	2	4	4	4	4	4

3A



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

OCT 22 1979

MEMORANDUM FOR: Commissioner John F. Ahearne
THRU: Lee V. Gossick, Executive Director for Operations (Signed) Lee V. Gossick
FROM: Harold R. Denton, Director, Office of Nuclear Reactor Regulation
SUBJECT: SAFETY IMPLICATIONS OF CONTROL SYSTEMS AND PLANT DYNAMICS

Introduction and Summary

By memorandum to you dated September 4, 1979, Mr. Demetrios Basdekas identified a number of concerns related to control system design and plant dynamics. This memorandum addresses those concerns and discusses related work that NRR has either planned or is underway.

Mr. Basdekas maintains that, because design criteria are inadequate and there is no detailed staff review of plant control systems, it cannot be concluded that the staff safety reviews are adequate to ensure that plant designs are acceptable. In addition, he contends that control system malfunctions should be considered as initiators of anticipated operational occurrences* or postulated accidents. Further, these malfunctions, together with the effects of other normally functioning control systems, should be considered during and subsequent to AOOs or accidents. In assessing the impacts of these malfunctions on the consequences of both transients and accidents, Mr. Basdekas believes that the analytic modeling must accurately describe the various dynamic processes. Without such an assessment, he concludes that there may be sequences of events not now considered in the safety analyses for which inadequate mitigating features have been provided. He cites TMI-2 as an example.

Mr. Basdekas makes a number of recommendations for addressing the concerns he has raised. These include:

1. Failure Mode and Effects Analyses (FMEA) of control systems for each plant;
2. Establishment of design criteria for control systems;
3. Establishment of requirements for control system design and installation;
4. Revision of the Standard Review Plan (SRP) to include the detailed review of control systems;
5. Training and/or hiring of suitably trained staff to perform the control system reviews; and,
6. Derating of operating plants until a preliminary review of control systems has been completed for each plant.

*Anticipated operational occurrences (AOOs) are those events which are expected to occur at least once during the life of the plant.

Rec'd OIL ENO
Date 10/12/79
Time 11:23 A.M.

In the discussion which follows, we describe the review process presently used to judge the adequacy, from a safety standpoint, of plant protection systems, our treatment of control systems in that process and efforts that are planned or underway to provide added assurance that this process is adequate or identify changes necessary to satisfy Commission safety requirements. As this discussion indicates, we share some of the same concerns that Mr. Basdekas raises and we believe that the work we have initiated addressed those concerns. We agree with the need to investigate control system failures and design inadequacies. However, we do not assign the same importance to the review of plant dynamic and control system performance, including stability, as does Mr. Basdekas. We do plan to investigate the possibility of simulating the dynamics of control systems in a representative B&W plant but we do not believe there is sufficient justification for an immediate detailed review of control system dynamics at all operating plants.

Finally, while we agree with the need to investigate the effects of control system failures and design inadequacies, we do not believe there is sufficient evidence to suggest that conclusions drawn from safety analyses are not valid. Therefore, we do not believe there is adequate justification for the recommendation to reduce power at operating plants pending a preliminary review of control systems.

Discussion

As Mr. Basdekas notes in his memorandum, the staff has not reviewed control systems in detail. The staff requires that all applicants for an operating license demonstrate by analysis that the plant is designed to mitigate the effects of a defined set of anticipated operational occurrences and postulated accidents. In assessing the effects of anticipated events, it is assumed that the events can be initiated by single control system malfunctions. These malfunctions are non-mechanistic in that no cause for the malfunction is identified nor are other associated malfunctions considered. For example, the loss of all main feedwater is considered an anticipated event, but, in analyzing this event, it has not been necessary to identify, for example, that a power supply failure caused the loss of feedwater and the coincident malfunction of other equipment powered by that same supply. The staff followed this approach, reasoning that the event would not be substantially changed because of the specific component which was assumed to have failed. This simplified the staff review since it would not be required to identify all single failures which could cause the event regardless of the probability of its failure. Further, the analysis assumed that all control systems respond as designed (unless the equipment malfunction is associated with a particular control system). All plant neutronic and thermohydraulic parameters are assumed to be at their worst-case values at the time the event is initiated.

Similarly, in analyzing postulated accidents, plant control systems are assumed to respond normally except that no credit is taken for such a response that would be of benefit in mitigating the effects of the accident. It has been assumed that the consequences of design basis accidents (e.g., LOCA, steamline break) would not

be significantly affected by control system malfunctions because of the rapid change in plant parameters during such accidents.

We believe that the review approach followed by the staff has been an effective use of resources for evaluating the adequacy of plant designs. The analytical demonstration that the plant safety systems can successfully mitigate the effects of the defined set of anticipated operational occurrences and postulated accidents, provided the staff with adequate basis to conclude that the designs of these protection systems were adequate and that the consequences of these design basis accidents would not be significantly affected by malfunctions in plant control systems.

The staff has recognized that there are drawbacks in the approach discussed above in that the events considered in the analysis do not bound all events which can be postulated. For example, recently in a letter from Westinghouse Electric Corporation to one of their operating plant customers (Attachment 1), a number of control systems could potentially malfunction if impacted by adverse environments due to a high energy line break inside or outside containment. Westinghouse indicated that the effects of such failures could lead to high energy line break consequences more severe than those presented in the safety analysis reports. The staff responded by issuing a letter to all operating light water reactors (Attachment 2) requesting that each licensee review their plant design in light of this concern and respond within (20) days with regard to whether operation of their plant should be modified, suspended, or revoked. It is expected that evaluations will be performed to evaluate the consequences of these and other potential control system failures which can be postulated to ensure that while this safety concern may exist, the overall conclusions regarding the adequacy of plant protection features and operator actions necessary to mitigate these events are adequate to meet all safety criteria necessary to permit continued plant operation.

The staff has raised questions regarding the acceptability of multiple challenges to the reactor protection system due to problems related to control system actions at several B&W plants (Attachment 3). The Crystal River events mentioned by Mr. Basdekas are discussed in Attachment 3. The events were either initiated by equipment malfunction or operator induced. While none of these events led to significant consequences, the frequency with which these events have occurred has highlighted the need to give greater regulatory attention to the control systems involved.

In a very related way the "Lessons Learned Task Force Status Report and Short-Term Recommendations, NUREG-0578" required in Section 2.1.9 that analysis of design and off-normal transients and accidents scenarios be performed including operator actions not previously analyzed. This position requires that, in addition to the normal single failure assumption, consequential failures shall also be considered. The staff also required that operator errors that could cause the complete loss of safety function shall also be considered. Thus it is expected that through these efforts a variety of event trees will be investigated for their probability

of occurrence as well as possible consequences. In response to this requirement of B&W Owner's Group (TMI Effects Subcommittee) has discussed with the staff a program they intend to follow to be responsive to this requirement. Briefly, the program has the following objectives:

- Investigate a wide range of reactor plant transients, including failures not normally considered in Safety Analysis Reports.
- Provide appropriate information to the plant operators to enable them to deal effectively with abnormal transients.
- Promote a better understanding of system fundamentals and abnormal transient operation.

The B&W owners have stated that the engineering support to accomplish these objectives are estimated at 30,000 man-hours, independent of the efforts that will be provided at each licensee plant. The staff is currently reviewing the program to better understand how responsive this program is to the requirement stated in NUREG-0578 and the time necessary to implement the program.

Recognizing the importance of control systems and the role those systems can play in both the initiation and mitigation of off-normal events, the staff has a number of other initiatives either in the planning stage or presently underway to enhance our knowledge of these systems. These initiatives are aimed at improving our understanding of possible control system failure mechanisms and their frequency of occurrence, and establishing the effects of these failures.

- As a followup to the TMI-2 events, the Commission issued orders to the B&W operating plants. As part of these orders, B&W was required to submit to the NRC staff a failure modes and effects analysis of the Integrated Control System. This analysis has been completed and the results are included in a B&W report entitled "Integrated Control System Reliability Analysis," BAW-1564, August 1979.

The report includes a number of recommendations by B&W regarding improvements in the performance of the ICS and related systems. The staff is presently reviewing this report with the assistance of Oak Ridge National Laboratory. Recommendations regarding possible system improvements will be developed and future work will be defined. As part of this effort, ORNL is investigating the possibility of producing a computer simulation of a representative B&W plant which would include plant control systems. Such a simulation, if it proves feasible, would allow us to evaluate a variety of different kinds of control system failures including the effects of plant dynamics.

- The staff has for some time recognized the need for criteria for equipment and systems important to safe plant operation but which need not be designed in compliance with safety system requirements. In 1977,

the Office of Standards Development was requested to begin the development of such criteria but no work was done because of unavailability of manpower in both OSD and NRR. We have recently held discussions with OSD regarding the need to begin the development of these criteria and they agree with the need to proceed. Further work is being delayed until the Lessons Learned Task Force decides on the scope of equipment to be covered by the criteria.

Prior to the TMI-2 event, the staff had begun to investigate the interaction of the various plant systems. This activity, defined in Task Action Plan TAP-A17 "Systems Interaction in Nuclear Power Plants," involves the application of fault tree methodology as a means of systematically reviewing plant systems for susceptibility to systems interactions. Particular emphasis is being placed on the presumed redundancy and independence of safety systems. As Mr. Basdekas notes in his memorandum, this analysis does not treat the dynamic aspects of control-protection system interactions. We believe that this detailed analysis of control system malfunctions is unnecessary at this time.

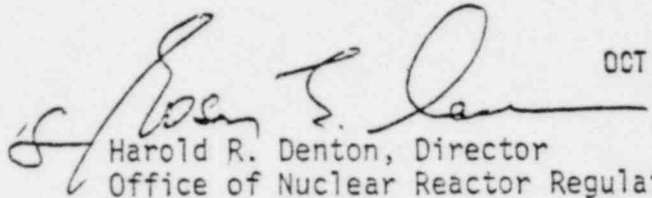
Westinghouse also has a study underway that is closely related to A-17. As a part of our review of the Westinghouse Integrated Protection System (IPS), we requested that an analysis be made of possible interactions between the IPS and the plant control systems and/or the engineered safety features (see NUREG-0493). The objective of this analysis is to assess the degree to which these interconnected systems are susceptible to common mode failure. The methodology which is currently being developed by Westinghouse for this purpose makes use of fault tree analysis. The Westinghouse study will not only give us additional insight into the interaction of complex control and protection systems, but it should also provide us with additional guidance on methodology for assessing the impact of control system failures for other plant designs.

Finally, we are planning to devote more manpower to the analysis of operating experience. Events have occurred in the past which have received insufficient review effort. Such events can indicate the existence of control system problems and possible problems associated with operator errors. This knowledge should be fed back into the review process. It will also be useful input to a technical assistance effort to be initiated shortly on control room design improvements.

We believe each of these initiatives will add to our understanding of the importance of control system malfunctions and operator action and help us confirm the adequacy of our current review process. Our approach emphasizes only those concerns that we believe deserve immediate attention, thereby ensuring that limited staff resources are used wisely. We have not concluded that these concerns are of sufficient

significance to warrant either the plant-by-plant control system analysis or the temporary reduction in power that Mr. Basdekas suggests would be prudent.

I hope this memo has been responsive to the concern highlighted by Mr. Basdekas. If you have any questions, I will be glad to discuss them with you at your convenience.



OCT 15 1979

Harold R. Denton, Director
Office of Nuclear Reactor Regulation

Enclosures:
As stated

cc: Chairman Hendrie
Commissioner Gilinsky ✓
Commissioner Bradford
Commissioner Kennedy
OGC
OPE
SECY

NINETY-SIXTH CONGRESS

MORRIS K. UDALL, ARIZ., CHAIRMAN

PHILLIP BURTON, CALIF.
ROBERT W. KASTENMEIER, WIS.
ABRAHAM KAZEN, JR., TEX.
JONATHAN B. BINGHAM, N.Y.
JOHN F. SEIBERLING, OHIO
HAROLD RUNNELS, N. MEX.
ANTONIO BORJA WON PAT, GUAM
BOB ECKHARDT, TEX.
JIM SANTINI, NEV.
JAMES WEAVER, OREG.
BOB CARR, MICH.
GEORGE MILLER, CALIF.
JAMES J. FLORIO, N.J.
DAWSON MATHIS, GA.
PHILIP R. SHARP, IND.
EDWARD J. MARKEY, MASS.
PETER H. KOSTMAYER, PA.
SALVADOR CORRADA, P.R.
AUSTIN J. MURPHY, PA.
NICK JOE RAHALL II, W. VA.
BRUCE F. VENTO, MINN.
JERRY HUCKABY, LA.
LAMAR GUDGER, N.C.
JAMES J. HOWARD, N.J.
JERRY M. PATTERSON, CALIF.
RAY KOGOVSEK, COLO.
PAT WILLIAMS, MONT.

DON H. CLAUSEN, CALIF.
MANUEL LIJAH, JR., N. MEX.
KEITH G. SEBELIUS, KANS.
DON YOUNG, ALASKA
STEVEN D. BYMMS, IDAHO
JAMES P. (JIM) JOHNSON, COLO.
ROBERT J. LAGOMARSINO, CALIF.
DAN MARRIOTT, UTAH
RON MARLENEE, MONT.
MICKEY EDWARDS, OKLA.
RICHARD B. CHENEY, WYO.
CHARLES PASHYAN, JR., CALIF.
ROBERT WHITTAKER, KANS.
DOUGLAS K. BEREUTER, NEBR.
MELVIN H. EVANS, V.I.

COMMITTEE ON INTERIOR AND INSULAR AFFAIRS
U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, D.C. 20515

February 7, 1980

CHARLES CONKLIN
STAFF DIRECTOR
ROBERT A. REVELES
ASSOCIATE STAFF DIRECTOR
LEE MC ELVAIN
GENERAL COUNSEL
STANLEY SCOVILLE
SPECIAL COUNSEL
FOR LEGISLATION
GARY G. ELLSWORTH
MINORITY COUNSEL

The Honorable John Ahearne
Chairman, Nuclear Regulatory Commission
Washington, D.C. 20555

Dear Mr. Chairman:

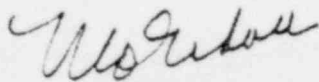
It has recently been brought to my attention that certain kinds of nuclear reactor control system failures could lead to accident sequences that have not been anticipated in the NRC's regulatory requirements. I would appreciate your providing the Subcommittee the following:

- An outline of the Commission's program for determining the extent to which control system failures that have not been anticipated could aggravate accident sequences currently considered in the NRC's regulatory requirements.
- A listing of significant corrective measures which have been or will be required as a result of control system malfunction or failure analyses conducted to date.
- Brief descriptions of the analyses upon which decisions concerning the foregoing corrective measures have been based.

I would also appreciate the Commission's position with regard to staff recommendations as to the need for power derating while this matter is under review.

Thank you for looking into this matter.

Sincerely,



MORRIS K. UDALL
Chairman