



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

DEC 15 1980

MEMORANDUM FOR: Robert B. Minogue, Director
Office of Nuclear Regulatory Research

THRU: Robert M. Bernero, Director
Division of Systems & Reliability Research
Office of Nuclear Regulatory Research

FROM: Frank H. Rowsome, Deputy Director
Division of Systems & Reliability Research
Office of Nuclear Regulatory Research

SUBJECT: ATWS CALCULATIONS

On November 10, 1980 Chairman Ahearne requested that the Division of Systems & Reliability Research, SARR, RES, review and comment upon the ATWS calculations presented to the Commission by J. Lellouche of EPRI and W. Minners of NRR. We committed to do so by December 12. A summary of our findings follows:

- o The EPRI ATWS calculations are highly misleading in one important respect. It is not legitimate to calculate system unavailability by comparing the number of component, channel, or subsystem tests in an interval with the number of system failures or the system failure rate in the interval. The Lellouche model implicitly assumes that each and every surveillance test wipes the slate clean of undetected and unrepaired failures throughout the whole RPS system. Subsystem tests do not verify the operability of whole systems. For example, a test of one channel of a reactor protection system logic cannot detect failures in other channels or in the mechanical-hydraulic portions of the system. It would be legitimate to compare the whole-system test rate with the whole-system failure rate to obtain system unavailability. Even the smaller number of tests credited by NRR are not fully comprehensive. Some failure modes could be missed by some of the tests credited by the staff.

There is a narrow sense in which the Lellouche calculations are legitimate. System failure modes entailing the simultaneous failure of all channels of the RPS logic could be effectively detected by each of the logic subsystem tests, provided that the detection of a failure immediately triggers not only the repair of

8103180 248

the fault but also tests (and repairs if necessary) of the other channels. Thus, the Lellouche calculation might be correct for the subset of the many contributors to system unavailability which--like the Kahl failure of nearly all the logic relays--strikes all logic channels almost simultaneously. There are, however, many other system failure modes for which this is not true. It is also not clear that a detected RPS logic fault triggers the immediate testing of the other channels or logic modules. The Lellouche calculation of RPS unavailability does not properly consider, for example, Browns Ferry-like failure modes (blocked scram discharge volume) to which conventional surveillance testing is blind. Thus, his system unavailability estimates are incomplete, over-optimistic, and misleading.

- o The EPRI statistical analysis of the "rectification" of the Kahl failure mode appears to be correctly done; it is a legitimate use of statistical methods. The NRR staff analysis of "rectification" also appears to be correct. The two positions can be reconciled as follows. We can reject the hypothesis that Kahl-like failures are as likely today as their early appearance in BWR operating experience suggests. We cannot distinguish two alternate hypotheses with statistical arguments alone: (1) Kahl-like failures are really less probable since the event than they were before, or (2) it was a statistical fluke that Kahl happened as early as it did, but its likelihood is unchanged.

There is a compelling case to dismiss the Kahl event from statistical analyses of actual ATWS experience. The Kahl fault was detected and corrected in surveillance testing; it did not result in a genuine RPS failure on demand. Thus, it is legitimate to count Kahl as a precursor but not as a real ATWS occurrence.

Two different and equally legitimate estimates of the probability of ATWS precursors can be obtained by (1) counting the Kahl failure and the successes preceding it as well as after it, and (2) counting only experience since the Kahl event. It would be illegitimate to dismiss the Kahl failure but to credit the prior successes, as Lellouche correctly acknowledges.

- o The EPRI arguments are legitimate in pointing out that Kahl-like failures can be effectively screened out by the test program and in noting that a large fraction of genuine failures to scram are likely to occur under circumstances in which no core damage would result. A comprehensive, realistic statistical analysis of the risk posed by ATWS events should credit both types of opportunity to nip failures in the bud, either through repair-in-kind or through better-than-before fixes of the kind we hope to see emerging from the Browns Ferry experience.

- o Statistical analyses of very rare events in complex systems are very sensitive to the assumptions implicit in the statistical model. Levels of confidence and other such statistical measures of uncertainty ignore uncertainties originating in completeness or modeling approximations, and should not be treated as comprehensive. Little faith should be accorded to estimates of the ATWS probability and its statistical uncertainty unaccompanied by an analysis of these other sources of uncertainty. Both the EPRI and NRR analyses are flawed by this omission. It is well within the state-of-the-art to assemble an array of statistical analyses of ATWS likelihood employing models of different implicit assumptions and to compare the statistical inferences with engineering judgments of plausibility of the assumptions. In so doing one can obtain a more illuminating and trustworthy picture of ATWS risks than either the staff or the industry has done to date.
- o The argument by J. Lellouche that the provision of additional pressurizer safety valves in PWRs would increase the risk is spurious. Safety valves may stick open--once lifted--but they are extremely unlikely to fail open at pressures well below their setpoint. Thus the likelihood of LOCA will not be significantly increased by the addition of high-quality safety valves set at pressures well above that of existing safety or relief valves. Also, Lellouche used a failure rate applicable to power operated relief valves rather than for safety valves.

SARR/RES is pursuing the ATWS issue in three ways. A fault-tree-based system reliability analysis is being prepared of the Browns Ferry Reactor Protection System (RPS) to assist NRR in determining the adequacy of the proposed corrective actions. The five ongoing Interim Reliability Evaluation Program studies include system reliability analyses of the subject plants' RPS. The ongoing program in failure rate data analysis continues to assemble and refine component failure rates, operator, and maintenance error rates that are useful in synthetic system reliability analyses, including RPS systems.

Overview of ATWS Risks

Our experience with WASH-1400, several subsequent risk assessments, reliability engineering studies, and our understanding of the ATWS dialogue lead us to a perspective on ATWS summarized below.

- The NRR approach to ATWS probabilities is generally conservative (noteworthy exception: RPS failure modes that cannot be detected in surveillance tests, e.g., scram discharge volume blockage). The NRR approach also fails to take differences in the severity of ATWS consequences into account.

- The EPRI (Lellouche) approach is unduly optimistic.
- The expected frequency of ATWS events predicted by WASH-1400 and other examples of probabilistic risk assessment, including that of Biblis B by the Germans, fall in the middle ground between the NRR and EPRI estimates.
- The offsite consequences of an ATWS-induced core melt are expected to be more severe in small pressure-suppression containments than in large dry containments.
- ATWS-initiated core melt sequences appear to be the dominant or one of the dominant contributors to risk for BWRs. ATWS is also among the more likely causes of core damage or core melt for BWRs.
- ATWS-initiated core melt sequences have not been found among the predicted risk-dominant sequences for PWRs in those risk assessments done to date. Something like ten percent or less of core damage occurrences are predicted to be caused by ATWS in most PWRs studied.
- Our reading of the literature on ATWS phenomenology suggests that the principal issue for ATWS in PWRs lies in the potential for high reactor coolant system pressures occurring early in ATWS transients. The high pressure may challenge the integrity of the pressure boundary or pose hazards for interconnected systems, e.g., high pressure makeup and boration systems, which would be needed to cope with ATWS after the pressure subsides.

Although no PWR risk assessment has found ATWS to be a dominant contributor to risk, both likelihood and pressure spike severity suggest that the ATWS problem for PWRs is most severe in CE plants, less in B&W plants, and still less in Westinghouse 3 and 4 loop reactors. We have not examined any Westinghouse 2 loop plants.

- We find it disturbing that neither NRR nor the licensees have catalogued the failure modes of their reactor protection systems. No one systematically determines which design errors or failure modes are effectively detected in startup or surveillance testing and which can be detected only in genuine scram attempts. No one passes upon the acceptability of the lacunae in the test program.

The Browns Ferry incident is not the only case in which experience has revealed an RPS failure mode to which surveillance testing is blind. For example, during the startup testing of Crystal River Unit 3, Florida Power Corporation discovered a short in the RPS logic which would disable a channel in a genuine scram but which would not show up in surveillance tests of the affected channel. We suspect that there are other test loopholes.

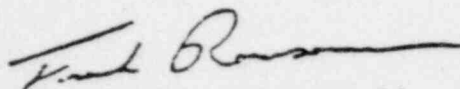
One regulatory strategy is to mandate improved prevention and also ATWS-tolerant designs, i.e., to mandate improved mitigation as well. This NRR proposal has the advantage that no extensive case reviews are required of the staff. If it is done well it should suffice. However, it has the disadvantage of not being very discriminating. It may mandate expensive backfits that are unnecessary or not safety-effective. It's non-mechanistic approach may leave design flaws, installation flaws, or some of the test-blind failure modes unaffected. The staff does not have a good record in the selection of design bases that are intended to envelope broad classes of unanalyzed accident scenarios.

An alternative regulatory strategy that we believe deserves consideration is to mandate a reliability assurance program for the RPS along the lines of aerospace reliability engineering programs. The agency would be prescriptive about the analytic methods, thoroughness, schedule and problem resolution criteria and procedures. The agency would not be prescriptive about backfits, at least not at the outset.

System reliability studies of nuclear safety systems frequently expose design errors, installation errors, undue susceptibility to maintenance error or to failures, etc. These discoveries are subject to the completeness problem, but in general such qualitative findings are far more trustworthy than probabilistic risk assessments. The reliability assurance program could be tied to qualitative or administrative guides to acceptability; it need not be primarily quantitative. For example, qualitative characteristics of discovered failure modes could be used to determine who has the responsibility for passing upon acceptability. It could be given teeth by expanding the reportage and responsibility provisions of 10 CFR 50.54 to embrace the lacunae of the reliability assurance program.

This regulatory strategy has several advantages. It makes a reality out of the policy that the industry has the prime responsibility for safety. Those, far closer than the staff could ever be to the design and operation of the RPS, must take responsibility for its adequacy. Second, if it can be done well, it could be far more effective in rooting out safety flaws than the NRR proposal. Third, it should be very much more cost-effective.

The reliability assurance option has the disadvantages that neither the staff nor the industry has much experience with aerospace reliability engineering practices and it places a burden of review and quality verification upon the staff. Despite these very real disadvantages, we think the advantages predominate.



Frank H. Rowsome, Deputy Director
Division of Systems & Reliability
Research
Office of Nuclear Regulatory Research

DRAFT ENVIRONMENTAL IMPACT ASSESSMENT FOR PROPOSED ATWS
RULEMAKING

• ELEMENTS OF ASSESSMENT

BACKGROUND

- PROPOSED RULE REQUIREMENTS

IMPACT CONSIDERED

- RADIOLOGICAL
- ECONOMIC

• BASIS OF ASSESSMENT

SECY 80-409

NUREG-0460

BOUNDING CONSIDERATIONS FOR OCCUPATIONAL EXPOSURE

SH 081515

RADIOLOGICAL IMPACT CONSIDERATIONS

* OCCUPATIONAL EXPOSURE

- BASIS: - BOUNDING ASSESSMENT
ASSUMED TO BE INSTALLATION OF RELIEF VALVES ON PRIMARY
SYSTEM - ACTUAL PLANT USED
- GROSS EXTRAPOLATION TO OTHER MODIFICATIONS

- RESULTS: - < 10 MAN-REM/PLANT FOR VALVE INSTALLATION
< 100 MAN-REM/PLANT TOTAL

- TOTAL IMPACT: - 0.15 PREMATURE CANCER DEATHS
0.375 CASES FOR GENETIC EFFECTS OVER NEXT 5 GENERATIONS
- NO EARLY FATALITIES OR HEALTH EFFECTS

- REMARKS: - APPROXIMATELY 300 WORKERS INVOLVED
- CANCER DEATHS DUE TO NATURAL CAUSES \approx 1 IN 5 \approx 60 WORKERS
- 10% OF LIVEBORN OFFSPRING HAVE SERIOUS GENETIC DISORDERS

RADIOLOGICAL IMPACT CONSIDERATIONS

- POPULATION EXPOSURE

- TWO TYPES OF IMPACTS
 - NORMAL OPERATION
 - ATWS EVENT

- RESULTS

- NORMAL OPERATION
 - IMPROVE RELIABILITY OF SCRAM
 - ESSENTIALLY NO IMPACT ON POPULATION EXPOSURE
- ATWS EVENTS
 - OVERALL ENVIRONMENTAL RISK FOR ATWS EVENTS
COMPARABLE TO OVERALL RISK FROM NORMAL OPERATION
 - ESSENTIALLY NO IMPACT ON POPULATION EXPOSURE

ECONOMIC IMPACT CONSIDERATIONS

- REPLACEMENT POWER
 - STAFF ESTIMATES 4 TO 6 WEEKS PLANT SHUTDOWN FOR ATWS MODIFICATIONS
 - REFUELING OUTAGES (1978 AVERAGE)
 - BWR'S 5.8 WEEKS
 - PWR'S 7.8 WEEKS
 - TOTAL OUTAGES (1978 AVERAGE)
 - BWR'S 12.9 WEEKS
 - PWR'S 13.0 WEEKS

- ECONOMIC IMPACTS (NO REPLACEMENT POWER COSTS)
 - STAFF ESTIMATES DIRECT COST \cong INDIRECT COSTS
 - LARGEST IMPACT ESTIMATED \ll 3% OF CAPITAL COST OF NUCLEAR PLANT (AT \sim $\$1 \times 10^9$ /1000 MWE PLANT)

TOTAL ESTIMATED COST OF
ATWS MODIFICATIONS

(DIRECT & INDIRECT, NO REPLACEMENT POWER COSTS)

	PLANT TYPE	NO. OF PLANTS	COST (\$) x 10 ⁶ PER PLANT*	TOTAL \$ x 10 ⁶
PRE '69	GE(BWR)	6	7	42
	CE	0	6	0
	B&W	0	6	0
	W	3	4	12
'69-84	GE(BWR)	31	22	682
	CE	15	6	90
	B&W	13	6	78
	W	47	4	188
POST '84	GE(BWR)	15	14	210
	CE	8	5	40
	B&W	1	5	40
	W	11	4	44
	TOTAL	150		1,426

*1980 DOLLARS