The Contribution of Control Systems in LWR Safety

J. Alter, D. Okrent

School of Engineering and Applied Science, University of California, Los Angeles, California 90024, U.S.A.

The objective of this paper is to estimate the effects of non-safety-grade control systems in pressurized water reactors (PWRs) on the overall likelihood of accidents leading to severe core damage or core melt, as determined from operating experience. One hundred ninety operational events which involve failures of non-safety-grade control systems that have occurred at commercial PWR plants during 1969-1981 and which are considered to be precursors to potential severe core damage have been identified. These events are treated as initiating or concurrent events to be fit into appropriate event trees, which are then quantified using component failure rates and system unavailabilities taken from available PRA studies to estimate the frequency of severe core damage arising from non-safety-grade control system failures. An example is worked out in detail. Considerable uncertainty is introduced into the results by the choice of system and operator failure rates and the results reported herein are considered preliminary. No allowance is made in these estimates for plant changes made because of operational experience.

The frequency of severe core damage arising from non-safety-grade control system failure at plants for which a "complete" set of information is available is estimated to be 6×10^{-4} /reactor year for Babcock and Wilcox (B&W), and 2×10^{-4} /reactor year for Westinghouse (W)--Combustion Engineering (CE) reactor designs. Main feedwater (MFW) control system at B&W plants and auxiliary feedwater (AFW) control system (which has now becoming safety-grade) at W-CE plants are found to have been the major contributors to risk of core damage with frequencies of 5×10^{-4} /reactor year for B&W MFW control system and 2×10^{-4} /reactor year for W-CE AFW control system (these are lower bound values of core damage frequency in a sense because they are based on available incomplete information). The most severe events were the Rancho Seco loss of non-nuclear instrumentation (NNI) event which gave rise to conditional probability of severe core damage of 2×10^{-2} and the Zion Unit 2 AFWs failure to start which resulted in a conditional probability of 8×10^{-3} . Only four of the fifty-two top ranked events in the ORNL/SAI (precursor study) NUREG/CR-2497 [1] are control system failure related. Our results sometimes lie between those in reference 1 and those in the INPO critique [2] and sometimes are less than either. Further study is required to evaluate these differences, which arose primarily due to the difference in event tree logic and in equipment and operator action failure rates. It is noted that "feed and bleed" was included where physically possible. If condensate booster pumps were allowed for per INPO (2), the W-CE results would drop by a factor of ten.

1. Introduction

Operating experience such as that at Rancho Seco on March 20, 1978 [3] and at Crystal River Unit #3 on February 26, 1980 [4] has led to reexamination by the United States Nuclear Regulatory Commission (USNRC) of its prior regulatory approach, which emphasizes safety (protection) systems and the need for adequate separation of protection and control, and does not place any requirement on control system reliability. In the past NRC Staff reviews were performed with the goal of insuring that control system failures would not prevent initiation and operation of any safety system equipment required to trip the plant or maintain it in a safe shutdown condition following any "anticipated operational occurrence" or "accident". In general, systematic evaluations were not performed to determine whether control system actions could result in a transient such that core limits are exceeded or whether postulated accidents could cause control system failures which could lead to accident consequences more severe than usually analyzed.

The NRC effort is currently focused in considerable part on the efforts related to Unresolved Safety Issues A-47, "Safety Implications of Control Systems" and A-49, "Pressurized Thermal Shock" [5].

The paper attempts only to examine one aspect of the overall problem, namely an estimation of the contribution of control system failure to PWR risk, treating actual prior failures as initiating or concurrent events to be fit into appropriate event trees, which are then quantified. This study used a two pronged attack as follows:

- o an estimation of the frequency of severe core damage from control system induced or related events which are precursors to potentially serious accidents using licensee event reports (LERs) and data on forced outages.
- o an estimation of plant logs for several plants to obtain additional information about control system failures which would normally not be reported to the NRC.

2. Compilation of Data

A data base on control system failures was developed by a search of LER files for the period 1969 through 1981, supplemented with data derived from NUREG reports on Nuclear Power Plant operating experience such as plant outages, and other operating experience gleaned from a sampling of station records for several specific PWRs. Plant visits have generated reasonably detailed information concerning the plant operating history, and for such plants the data is considered to be "complete". For other plants, the information is partial, in that it is LER-based. We have accumulated 190 events that have occurred at PWR plants, in the period 1969 through 1981, of which only 60 are LERs.

3. Analysis

Failure Mode and Effect Analysis (FMEA)- An FMEA was performed for the control system equipment and channels involved in the particular incident, based on the Vendor's detailed FMEA as analyzed by B&W [6] and W [7]. The control system that actually existed in the plant under consideration was used. An effort was made to give credit for the actual mitigating systems for each plant. For example, FW runaway was analyzed according to the plant-specific FW isolation design.

Generation of plant event tree- The success criteria for function of mitigating systems were varied from plant-to-plant; certain functions do not exist at every plant. The effect of the accident precursor on the specific safety related system was considered when

failed or degraded states of the event tree functions were determined in order to identify dependencies.

Failure rates and system unavailabilities- The event trees were quantified using component failure rates and system unavailabilities taken from WASH-1400 [8], and other PRAs including those for Indian Point [9], Oconee [10], and Calvert Cliffs [11]. Table #1 outlines the failure rate values used in the study.

Quantification of the event tree- In those events involving the additional random failure of some other system, the unavailability of the latter system was updated, using Bayesian techniques. All events, except those that occur exclusively at low or zero power, were assumed to occur at full power; the plant was estimated to be in the vicinity of full power, 75% of the time. Steam generator (SG) overfill was treated with the assumption that the failure rate of flooded steamlines is 1×10^{-3} /demand as stated in the NRC staff analysis [12]. ATWS was considered to be a contributing effect to severe core damage in those initiating events which were recommended by the SAI technical support study for the "Utility Group on ATWS" [13]. ATWS event tree logic and system unavailabilities follow the recommendations of the NRC ATWS Task Force and Steering Group for resolution of ATWS issue vis-a-vis a proposed Commission Rule [14]. For B&W and CE plants we have assumed that 50 percent of the time the moderator temperature coefficient (MTC) is such that Service Level C (3200 psia reactor pressure vessel (RPV) pressure) will not be exceeded if turbine trip occurs and AFWS is initiated. For W plants we have assumed that 1 percent of the time, the MTC is such that Service Level C will be exceeded if turbine trip occurs and AFWS is available. Operator's action failure rates are taken from the Zion PRA [15] after having considered the comments by Sandia [16] on the Zion PRA. The frequency of severe core damage is estimated finally by summing overall initiating events of the same reactor type to assure that failures and effects of similar designs are combined together.

4. An Example of an Event Analysis

LER event #NSIC 171733; Zion Unit #2; Date 12-11-81, Power Level 90%.

Abstract: Two motor driven AFW (MDAFW) pumps fail to autostart, due to common cause design error, upon SG low-low level signal following a reactor trip. The two pumps were promptly manually started from the control room. Turbine driven AFW (TDAFW) pump was out of service at the time of the event.

Discussion: AFWS is called on in the following events:

- (1) Loss of MFW, frequency of occurrence 5.2/y
- (2) Reactor trip, frequency of occurrence 3.8/y
- (3) Turbine trip, frequency of occurrence 3.7/y
- (4) Loss of offsite power (LOOP), frequency of occurrence 0.041/y,
and other events of lesser contribution to severe core damage.

We assume that the AFWS is tested once a month, therefore the failure duration is $1/2 \times 720\text{h} = 360\text{h}$. The estimated initiating event probability of each of the four initiators is

- (1) Loss of MFW: $5.2/\text{y} \times 360\text{h} = 0.214$
- (2) Reactor trip: $3.8/\text{y} \times 360\text{h} = 0.156$
- (3) Turbine trip: $3.7/\text{y} \times 360\text{h} = 0.152$
- (4) LOOP: $0.041/\text{y} \times 360 = 1.68 \times 10^{-3}$

The presentation of the contribution of AFWS failure to severe core damage is via four event

trees namely, Loss of MFW; Reactor trip; Turbine trip & LOOP.

Updating the unavailability of the TDAFW train due to a random occurrence--its being out for maintenance is done by using Bayes techniques. Our calculations show that in this case only an 18 percent change exists from what is reported as an operating experience value in the Indian Point PRA. The operator can manually restart the electric pumps from the control room. We assume, following the Indian Point PRA, that 50% of the failures to start of a pump are recoverable within 30 minutes and the mean frequency of failure for the operator's not taking action from the control room within 30 minutes is 0.007. Our calculations yield a probability of MDAFW pump failure to manually restart of 0.5. Figure #1 shows the loss of MFW event tree. Reactor trip, turbine trip and LOOP event trees are quite similar to the loss of MFW event tree and are not shown here.

Quantification of the event- Each event tree is quantified taking into account only sequences which are related to the control system failure.

(1) Loss of MFW: $p(\text{severe core damage}) = 4.7 \times 10^{-5}$

(2) Reactor trip: $p(\text{severe core damage}) = 3.4 \times 10^{-5}$

(3) Turbine trip: $p(\text{severe core damage}) = 3.3 \times 10^{-5}$

(4) LOOP: $p(\text{severe core damage}) = 2.9 \times 10^{-7}$

The total conditional probability of severe core damage from this event is

$$p(\text{severe core damage}) = 4.7 \times 10^{-5} + 3.4 \times 10^{-5} + 3.3 \times 10^{-5} + 2.9 \times 10^{-7} = \underline{1.1 \times 10^{-4}}$$

5. Results

The results are presented in Tables II and III in the form of the frequency of severe core damage arising from non-safety-grade control system failures, and calculated separately for two PWR designs, namely B&W and W-CE plants. Table IV shows the conditional probability of severe core damage for the four top ranked events in each of the two reactor designs. Table V shows a comparison of the results of four events with those obtained in NUREG/CR-2497 and its INPO critique.

References

- [1] SAI/ORNL, "Precursors to Potential Severe Core Damage Accidents 1969-1979", NUREG/CR-2497 (June 1982).
- [2] INPO, "Review of NUREG/CR-2497", INPO 82-025 (September 1982).
- [3] Sacramento Municipal Utility District, Sacramento, CA, Letter, W/R-78-1 to USNRC director of regulatory operations; region V, (March 31, 1978).
- [4] Florida Power Co., LER #80-10.
- [5] USNRC, "Unresolved Safety Issues Summary", NUREG-0606 Vol. 4, No. 1 (February 19, 1982).
- [6] Babcock & Wilcox, "Integrated Control System Reliability Analysis", BAW-1564 (August, 1979).
- [7] Salem Generating Station, "Unit 2 Control System Failures Analysis", (June 7, 1982).
- [8] USNRC, "Reactor Safety Study", WASH-1400 NUREG-75/014, (October, 1975).
- [9] Consolidated Edison Co., "Indian Point Probabilistic Safety Study", (1982).
- [10] Sandia National Laboratory, "Reactor Safety Study Methodology Applications Program: Oconee #3 PWR Plant", NUREG/CR-1659 (May 1981).
- [11] Sandia National Laboratory, "Reactor Safety Study Methodology Applications Program: Calvert Cliffs #2 PWR Power Plant", NUREG/CR-1659 (May, 1982).

- [12] USNRC, "Preliminary Staff Analysis of SG Tube Rupture Risks", SECY-82-466 (November, 1982).
- [13] SAI, Inc. "Quantitative Evaluation of Industry Proposed Modifications Relative to Existing Plant ATWS Requirements-Technical Support for the Utility Group on ATWS"-SAI-011-82-SJ (December, 1981).
- [14] Boehmert, P., "Recommendations of the NRC ATWS Task Force and Steering Group", Memo to W. Kerr, Chairman ATWS Subcommittee, ACRS, (November 12, 1982).
- [15] Commonwealth Edison Co., "Zion Probabilistic Safety Study", (1981).
- [16] Sandia National Laboratory, "Review and Evaluation of the Zion Probabilistic Safety Study", Letter Report to the USNRC, (March 5, 1982).

TABLE I System Unavailabilities in PWR Plants

System	Indian Point PRA (W)	Calvert Cliffs PRA (CE)	Oconee PRA (B&W)
Reactor Trip	3.9×10^{-5}	2×10^{-5}	2.6×10^{-5}
Turbine Trip	2.8×10^{-6}	Same	Same
MSIV Trip	1.5×10^{-2}	Same	Same
AFWS	$1.5 \times 10^{-5*}$	$1.4 \times 10^{-4**}$	2.4×10^{-4}
Primary bleed and feed	4.5×10^{-3}	$6 \times 10^{-3***}$	1.5×10^{-2}
SR/demanded	-	-	0.25****
SR/VO	-	-	2×10^{-5}
SR/VR	Same	Same	5×10^{-2}
HPIS	1.3×10^{-4}	1.9×10^{-3}	1.4×10^{-3}
Recirculation cooling	4×10^{-3}	4.9×10^{-3}	4×10^{-3}

Notes: *Only for plants with 2 MD trains and one TD train.

**Calvert Cliffs AFWS unavailability is 3×10^{-3} (two TD pumps and is remote manually initiated). The reference for the value 1.4×10^{-4} is Palo Verde plant (NUREG-CR/2497).

***All CE plants currently licensed except for ANO-2 have two PORVs.

****Prior to TMI accident because of low PORV setpoints.

TABLE II - Frequency of Severe Core Damage (SCD)
by Reactor Design (For plants with a
"complete" set of information)

Reactor Design	No. of Events	Frequency of SCD
B&W	37	6×10^{-4} /RY
W - CE	47	2.4×10^{-4} /RY

TABLE III - Frequency of Severe Core Damage
by Control System Group

<u>Control System Group</u>	<u>B&W</u>	<u>W - CE</u>
Reactivity Control	$>2.8 \times 10^{-5}/\text{RY}$	$>9.1 \times 10^{-7}/\text{RY}$
Pressurizer Pressure Control	$>6 \times 10^{-6}/\text{RY}$	$>7 \times 10^{-8}/\text{RY}$
Pressurizer Level Control	No reported events	$>5.2 \times 10^{-7}/\text{RY}$
Feedwater Control	$>5.2 \times 10^{-4}/\text{RY}$	$>7.2 \times 10^{-6}/\text{RY}$
Auxiliary Feedwater Control	$>2 \times 10^{-5}/\text{RY}$	$>2.1 \times 10^{-4}/\text{RY}$
Turbine Control	$>5.7 \times 10^{-6}/\text{RY}$	$>5.7 \times 10^{-7}/\text{RY}$
Steam Dump Control	$>3.8 \times 10^{-5}/\text{RY}$	$>2.1 \times 10^{-5}/\text{RY}$

TABLE IV Top Ranked Events

	<u>Plant</u>	<u>Date</u>	<u>Event</u>	<u>Conditional Probability of SCD</u>
B&W	Rancho Seco	3-20-78	Loss of NNI	1.7×10^{-2}
	Rancho Seco	10-10-76	Loss of MFW	1.3×10^{-3}
	Oconee Unit 3	5-25-75	Failure of TPS	1×10^{-3}
	Oconee Unit 3	7-13-75	Failure of TPS	1×10^{-3}
W-CE	Zion Unit 2	9-14-81	AFWS failed to start	8.4×10^{-3}
	Sequoyah Unit 1	1-28-81	Steam dump valves failure	8.8×10^{-4}
	San Onofre Unit 1	9-3-81	Inverter failure	1.4×10^{-4}
	Zion Unit 2	12-11-81	AFWS failed to start	1.2×10^{-4}

TABLE V Comparison of Results with NUREG/CR-2497
and INPO Critique

<u>NSIC #</u>	<u>Plant</u>	<u>Date</u>	<u>Description</u>	<u>NUREG</u>	<u>INPO</u>	<u>This Paper</u>
138830	Rancho Seco	3-20-78	Failure of NNI	0.25	3.6×10^{-4}	1.7×10^{-2}
91676	Turkey Point 3	5-8-74	Failure of 3 TDAFWPs to start	2.5×10^{-2}	2.7×10^{-4}	1.6×10^{-4}
123150	Crystal River 3	3-3-74	Loss of ICS Power	1.3×10^{-3}	1×10^{-5}	2.5×10^{-4}
130788	Davis Besse	9-24-74	Stuck open PORV	1.3×10^{-3}	1×10^{-2}	1.1×10^{-5}