NOTICE
PORTIONS OF THIS REPORT ARE UNCLASSIFIED

It has been reproduced from the best available copy to permit the broadest possible availability.

BNL-NUREG--34146

DE84 006477

CONF-830901--23

CONTROL ROD TRIP FAILURES; SALEM 1,
THE CAUSE, RESPONSE, AND POTENTIAL FIXES

Robert E. Hall, John L. Boccio, and William J. Luckas

Department of Nuclear Energy
Brookhaven National Laboratory
Upton, New York 11973

I. OBJECTIVE

The objective of this paper is to present a systems and reliability analysis of recent nuclear reactor control rod failure-to-trip (or scram) events that have been experienced in the U.S. commercial nuclear industry. This analysis will introduce the operational factors of hardware, procedures, and the human into the analysis of transients without scram.

II. SCOPE

A discussion of the two 1983 Salem 1, Pressurized Water Reactor (PWR), failures to trip are presented. The principal details of these two control rod trip malfunctions are investigated and used to calculate the Reactor Protection System unavailability. As a comparison, a brief discussion of the 1980 Browns Ferry 3, a Boiling Water Reactor (BWR), scram failure is presented.

III. SYSTEMS DEFINITION OF CONTROL ROD TRIP FAILURE

There are several examples of control rod trip failures which have occurred in commercial operating light water reactors in the U.S. The 1980 event at the Browns Ferry Unit 3, BWR, is one example. In this case, the common Scram Discharge Volume (SDV) which includes the header and instrument volume tank, see Figure 1, was insufficient to remove all the water from above the Control Rod Drive pistons and their individual hydraulic units. Thus, when each of the control rod's solenoid operated scram inlet

This work was performed under the auspices of the U.S. Nuclear Regulatory Commission.

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

Figure 1. BWR Control Rod Drive Hydraulic System Scram Diagram

and exhaust valves opened, as required by the reactor protection system, 76 of the 185 rods did not insert fully. After draining the SDV, all the rods were fully inserted by the operator manually. This event represents a case where the control logic and active devices functioned correctly but the hydraulic system initially failed to fulfill its mission. In this case, as will be seen again for the Salem events, the operating team's quick reaction terminated the transient events without necessarily diagnosing the cause.

In contrast, the two 1983 events at the Salem Unit 1, PWR, represent reactor trip breaker (RTB) failures. The details of these events are contained in Section IV. When signaled to open by the Solid State Protection System (SSPS), the two in-series trip breakers RTB "A" and RTB "B" did not open (see Figure 2). Thus, the control rods were not released and did not enter the reactor core. When the input from the SSPS did not open the RTBs, the operator's manual trip caused the breakers to open and all rods successfully dropped into the core. Although these events were initiated by an active demand failure of the breakers to respond to the control logic, again we see the operating team's pre-diagnosis reaction terminated the transient. This quick, "something not right" response warrants further investigation since we can gain insights into the actual team response when time does not allow investigative thinking or procedure reference.

Before discussing the details of optimizing the time dependent availability of the Salem type of Reactor Protection System (Section V), a review of the internal reactor trip breaker logic as related to the Westinghouse DB-50 breaker application is in order. As shown in Figure 2, the SSPS's redundant trains (A&B) receive plant status signals and when required, de-energize the undervoltage trip coil (UV) in each of the two reactor trip breakers (RTB). This, under normal conditions, will open RTB A and B which in turn de-energizes the control rod drive mechanism and release the control rods. In the two Salem events, both UVs failed and therefore the redundant RTBs failed closed. Referring to Figure 2, it is indicated that a reactor trip requires either one of the two to function.

Once the failure was noted and the operator manually actuated the trip system, the UV trip coils were again de-energized. In addition, this manual trip signal energizes the Shunt Trip devices (ST). The two STs, one in each RTB, being positive action type of mechanisms, helped to assist the RTBs to open. This action was successful and the reactor trip was attained. It should be noted that in some reactor designs the automatic signal triggers both the UV and ST in each RTB. This design difference in the control logic was investigated and is discussed in reference 1.

Figure 2. Trip breaker logic as utilized in the Salem event¹

IV. THE 1983 SALEM CONTROL ROD TRIP FAILURE EVENTS^{2,3}

February 22: At 20% of full power, with the main generator synchronized to the grid and feedwater control in automatic, the operator attempted to transfer a 4 kV electrical power supply (startup to normal).

- Electrical power was lost to one reactor coolant pump, control power to turbine driven main feed pump (TDMFP), feedwater flow indication, and normal control room lighting (40 seconds on emergency lighting).
- TDMFP tripped (due to loss of control power).
- Steam generator (SG) water level decreased (to low low SG level reactor trip signal).
- Auxiliary feedwater pumps started (on above trip signal).
- Reactor manually tripped 3.6 seconds after trip signal (due to degraded plant conditions).
- Reactor trip confirmed.

February 25: Increasing from 10 to 14% of full power with generator synchronized to the grid and feedwater control in manual, the operator had trouble maintaining SG water level.

- SG water level decreased (to low low SG level reactor trip signal).
- Auxiliary feedwater pumps started (on above trip signal).
- Operator noted low low SG level reactor trip signal "first out" annunciator (assumed trip and announced same).
- Another operator (in the control room for requalification training) noted no reactor trip based on no rod position indicator and no rod bottom lights.
- The senior shift supervisor noted no turbine trip on assumed reactor trip and SG level below trip point.
- Operator manually tripped reactor 25 seconds after trip signal.

A brief analysis of the differences between the above two events from an operational perspective is in order. In the earlier event, many disruptions and distractions, as a result of the loss of the 4 kV bus, competed for the attention of the operators

to the extent that the failure for automatic trip was not confirmed until after the second event.

By contrast, the second event had far fewer disruptions and distractions in the control room. Other than the normal problems of keeping all four steam generator water levels in the operating ranges and a few annunciator alarms, the startup was quite routine. In fact, the operator anticipated the reactor trip by announcing it upon receiving the "first out" annunciator which indicates the first alarm received. Time was available to assess other indicators to assure that the reactor had not in fact tripped. Therefore, the short reaction time needed by the operating crew to perform manual initiation of a reactor trip is a strong indication of the need for operators to be trained to respond to the need for manual reactor trip. We should, however, be cautious not to draw too many conclusions about this extremely short reaction time. The operators were in an interactive mode with the plant controls and were primed to respond. The quick response and the lack of need for diagnosis most probably rests heavily on this fact. This area of non-diagnosis decisions require further research to make full use of the data.

V. IMPACT OF TEST AND MAINTENANCE ON SYSTEM CHALLENGES

The primary function of a standby safety system (in this case the RPS) is to mitigate the ensuing consequence of preconceived accidents. As such, these systems, designed to transit from an idle state to an active state upon demand, can be in the idle phase for long periods of time. In most respects, the operational status (or availability) of standby systems cannot be either fully monitored or fully assessed while in the idle phase. Establishing a quantitative basis, therefore, for judging appropriate plant operational policy, largely in the form of periodic inspection policies, is the prime impetus in the evolution of a family of codes with the surname FRANTIC.^{4,5}

Basically, FRANTIC, an acronym for Formal Reliability Analysis including Normal Testing, Inspection, and Checking, evaluates the time dependent along with the time-average unavailability for any general system model, whose failure can be described by a coherent fault tree. Components which comprise the elements of this fault tree are classified in FRANTIC as non-repairable, monitored, and periodically-tested components. For the latter, time-dependent aspects such as the effects of test downtimes, test overrides, detection inefficiencies, and test-caused failures can be modeled and subsequently analyzed. Burn-in and wear-out effects can also be modeled using time-dependent hazard rates, along with various component renewal options, e.g., GOOD AS NEW, GOOD AS OLD, etc.

Common cause and human errors associated with operational procedures are included as well, usually by ascribing an appropriate constant failure probability for the contributors.

The unavailability then of the RPS as a function of time t , $Q(t)$, is a function of the unavailabilities of its components $x_i(t)$, $i=1, \dots, N$. Conceptually $Q(t)=f[x_1(t), \dots, x_N(t)]$, where the nature of the function f is dictated by the logic of the interconnections and other dependencies of the components that form the system. Basically, the major four data elements needed for quantification of the RPS fault tree are: Solid State Protection Systems failure probabilities, probabilities of main and bypass trip breakers (RTA, RTB, BYA, BYB) to open, probability of open breaker to fail closed, and human error associated with leaving bypass breakers (BYA, BYB) closed.

The SSPS logic train (A,B) failures to initiate on automatic trip when required was ascribed a failure frequency $2.7E-06/\text{hr}$ which essentially follows the procedure used in WASH-1400⁶. For trip breaker failures, $4.0E-03$ failures/demand (F) with 625.7 hours between demands (T_e) was calculated. This is based on LER data which indicate 26 failures were observed in 2 breakers; each had 14 demands per year for the presumed time period of 220 reactor years. Partitioning the observed failure rate into failures per demand (q_D) and failure per hour (λ), where $F=q_D + (1-q_D)[1-\exp(-\lambda T_e)] \sim q_D + \lambda T_e$, were based upon LER review see reference 7, pg. 3-22 which indicate that approximately 90% of the failures seemed to be related to time-dependent causes such as dirt, lack of lubrication, and out of adjustment. Based on this survey, values of $\lambda T_e=90\%$ of and $q_D=10\%$ of F were chosen as the base case.

The bypass breaker, which, if failed close defeats the safety function of its respective train, was assigned a failure rate of $1.0E-06/\text{hr}$. This is a WASH-1400 value and was used in the FRANTIC sensitivity analysis with no parametric variation. It may seem somewhat high since the bypass can be "racked out" of the circuit when not in use thus reducing this risk, this value. Notwithstanding, to see the effect of "racking out," a run was made setting the probability of an internal short to zero. Also, leaving the bypass switched on after the surveillance period was considered as a possible human error. Since this event is annunciated in the control room, it was permitted to remain for only 8 hours (thus assuming that it would be detected no later than the next shift).

The only other human error considered allows for the possibility of leaving the SSPS in a degraded condition at the end of the test and maintenance (perhaps a misposition of one of the IC boards). This particular aspect was modeled through FRANTIC's

"test inefficiency" data input. Certainly other human errors could have been studied, and parametrically assessed, such as leaving other trips and safeguards in an inhibited state after test of the SSPS but they were not considered at the time.

For other common cause failures, consideration was only given to its impact on the breakers. The bistables (which were not modeled) were the only component which seemed subject to simultaneous failure of like components with identical functional requirements. Common cause and human error effects are included through the so-called β -factor. Thus a β -factor of 0.01 is given for human error associated with leaving in the bypass breaker for 8 hours and for leaving the SSPS in a degraded state after testing. Three times this β -value was considered as the base case for common cause breaker failure.

With these failure modes ascribed to the requisite elements of the fault tree, sensitivity studies on system unavailability were performed. This included the effects of test duration times, maintenance times, and surveillance procedures. A staggered test and maintenance routine was assumed with each train tested bi-monthly, and alternate train tested midway between these tests.

VI. SYSTEM UNAVAILABILITY - SELECT CASES

Although a total of 36 FRANTIC runs were made with test frequency as the basic independent variable, the following only highlights 2 out of the 12 parametric variations that were performed. The basic purpose for these sensitivity studies is to determine if an optimum test frequency for RPS breaker could be established. At the outset, it must be stated that for the cases considered no well-defined optimum could be defined for which system unavailability achieves a minimum.

Figure 4 compares the effects of three test duration times. Understandably, for a given test frequency, the system unavailability increases with test duration. A minimum on test frequency (between 22 and 30 days) is indicated. (Other parametric tests yield results which cluster around a minimum of 8 days, but it is likely that other factors, not modeled, would come into play in affecting system unavailability had 8 days been established for a test frequency.)

The composite plots in Figure 5 show a comparison of "observed" breaker failure rate, F , and the breaker demand failure rate, q_D . Specifying these two variables tacitly specifies the components hazard rate, λ , since $\lambda \sim (F - q_D)/T_e$. The top-most curves showing the highest unavailability represent the current breaker under discussion. When $q_D = 0.1F$, 90% of the observed failure rate is assumed to occur during the standby time.

Figure 4. Comparison of Test Duration

Figure 5. Comparison of Breaker Demand Failure and Failure Rate

More frequent testing results in lower system unavailability but no minimum is indicated. Had demand failure rates been ascribed a larger portion of those which had been observed (as indicative of the case when $q_D = 0.5F$ instead of $q_D = 0.1F$), a minimum test frequency of about 25 days is shown; but, frequent testing isn't as dominant as previously and the unavailability starts higher and increases less rapidly with longer test intervals. The same can be said for the middle two curves; the last curve is shown only to reflect the effect of a hypothetical breaker with a very low failure rate.

The top curve (solid line) represents an optimistic estimate (human error = 0) of the unavailability of the current Westinghouse RTS. Had the Westinghouse DB-50 breaker been modified with the addition of a start coil to activate simultaneously with the under voltage trip, one would expect an increase in the reliability of the modified breaker to trip upon demand. Whether a four-fold reduction in observed failure rate would occur due to this modification is speculative. Notwithstanding, the middle solid line is indicative of the reduction in system unavailability and apparently is representative of the Combustion Engineering version of the GE AK-2 breaker. This curve is about a factor of 3 lower and the unavailability doubles for every 50-day increase in test interval.

VII. CONCLUSIONS

Although the failure to trip or scram represents a single class of initiators, the actual events of each transient are quite operationally unique and require individual human response. The operational team's reaction to the challenge can be successful, in very short response times, and without complete diagnosis of the event's root cause. This underscores the need for a better basic understanding of the team response patterns in such cases, to allow designs, procedures, and training to take advantage of it.

In addition, as one analyzes the recent failure at the Salem 1 reactor, it becomes obvious that the optimization of test and maintenance practices are essential and the use of time dependent reliability analyses lend themselves nicely to such calculations.

VIII. REFERENCES

1. Examination of Breaker Testing Frequency for the Westinghouse RTS - NRC Internal Document.
2. The Salem Case: A Failure of Nuclear Logic, News and Comments, Science, Vol. 220.

3. Salem Breaker Incident, P. 540, Nuclear Safety, Volume 24, No. 4, July-August, 1983.
4. W. Vesely, F. Goldberg, R. Powers, J. Dickey, J. Smith, and R. Hall, FRANTIC II - A Computer Code for Time Dependent Unavailability Analysis, NUREG/CR-1924, April 1981.
5. T. Ginzburg, J. Dickey, and R. Hall, Sensitivity Study Using the FRANTIC Code for the Unavailability of a System to the Failure Characteristics of the Components and the Operating Conditions, NUREG/CR-2542, February 1982.
6. U.S. Nuclear Regulatory Commission, Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400, (NUREG-75-014), Washington, D.C., 1975.
7. U.S. Nuclear Regulatory Commission, Generic Implications of ATWS Events at the Salem Nuclear Power Plant, NUREG-1000, April 1983.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.