CAROLINA POWER & LIGHT COMPANY

HUMAN RELIABILITY ANALYSIS
OF THE H.B. ROBINSON DEDICATED SHUTDOWN SYSTEM

SUPPLEMENT TO THE REPORT
"DB-50 BREAKER INTERRUPT ACCIDENT SEQUENCE ANALYSIS
FOR THE
HBR UNIT 2 ELECTRICAL DISTRIBUTION SYSTEM"

NOVEMBER 1987

Prepared By: J.C. Moxley - NSR/CNS

Reviewed By: R.E. Oliver - NSR/CNS

Approved By: J.G. Hammond - NSR/CNS

Reviewed By: M.D. Macon, Electrical Unit/NELD

8801120427 880106
PDR ADOCK 05000261
P PDR

TABLE OF CONTENTS

Human Reliability Analysis (HRA)

H.B. Robinson Dedicated Shutdown System

1.0 INTRODUCTION

The following evaluation summarizes the HRA conducted to quantify the likelihood of operators to use the standby Dedicated Shutdown System (DSS) to mitigate the consequences of the most risk significant event identified and analyzed in the DB-50 Breaker PRA (Reference 1). The corresponding final estimate of HRA failure probability resulting from a rigorous analysis confirms the validity of the preliminary estimate used in the Reference 1 analysis.

The effectiveness of the (DSS) to mitigate the potentially risk significant events analyzed in the DB-50 breaker analysis depends on two major factors: the design of the system and its ties to equipment necessary for safe shutdown; and the reliability of operators to decide when to use the system and to establish its operational mode. This report addresses the issue of human reliability through an analysis of the DSS that was based on a system walk-down and procedures review (Reference 2).

2.0 THE DEDICATED SHUTDOWN SYSTEM

The H.B. Robinson plant, in response to the Appendix R rule, installed an additional, separate, and redundant power supply and appropriate equipment to power safe plant shutdown equipment following a fire.

2.1 The System Design

The DSS includes a diverse set of equipment:

1. A DS 480V bus
2. A DS diesel generator (DSDG)
3. DS instrumentation
4. DC power supply

The following equipment were modified to allow energization through the DS 480V bus.

5. Charging pump A
6. Component cooling water (CCW) pump A
7. Service water (SW) pump D
8. SW discharge valve V6-12D
9. The steam driven auxiliary feedwater pump (SDAFWP) valves V1-8A and V2-14A
10. The steam generator power operated relief valves (PORV's)
11. Motor control center (MCC-5)

The DS bus is independent of the emergency 480V busses, E1 and E2, and its cables are separated from these busses by fire walls. The normal offsite ac power sources tie into the DS bus.

This equipment is located in or near the Reactor Auxiliary Building (RAB) and the Turbine Building, except for the SW pump and its discharge valve V6-12D which are located at the service water and circulating water intake structure. Restricted access is by computerized badge key cards or security keys. The equipment can be manually controlled outside the control room from three general areas of the plant: the Turbine Building, the 4160V equipment room, and the Reactor Auxiliary Building (RAB). Critical equipment is provided with emergency lighting.

2.2 Past DSS Operational Philosophy

Operationally, the DSS is used only in the event that offsite power and both emergency diesel generators are unavailable. In the event of a major fire in one or more critical areas of the plant, power to vital and safety equipment may be sporadic or lost and the Emergency Operating Procedures (EOP's) are not relied on to mitigate and terminate the incident. Under the most severe conditions that can be postulated, the operators would be directed to isolate all normal power sources from equipment to prevent spurious operation. The DSS is designed to be used in such cases.

2.3 Determinants of the DSS human reliability

The DSS is a manually aligned and actuated system that requires the success of several operator actions. The critical human reliability assessment factors of the DSS are:

1. The decision criteria for actuating DSS.
2. The use of procedures to identify 50-100 specific components.
3. The physical workload and demand on available time in accomplishing the procedural steps.
4. The ambient lighting around the equipment during a fire-induced loss of ac power.
5. The access to DSS equipment located in several rooms in the RAB and the Turbine Building.
6. The ability for three or more operators to coordinate and communicate their actions.

A review and walk-down of the DS procedures revised May/June, 1987 were performed to quantify their adequacy in providing operator decision criteria and guidance for responding to the accident sequence analyzed in the Reference 1 PRA. Operators have been trained on the latest DSP's and retraining will be conducted as appropriate in accordance with retraining selection methodology.

3.0 THE PROCEDURE CONTEXT

A good procedure must provide a balance between three objectives:

1. To provide plant operators with an efficient mnemonic aid in carrying out complex or infrequently experienced activities.

2. To provide training material related to a specific plant upset condition, for plant, NRC, or other audiences.

3. To formally document a preferred, optimal solution to a specific plant upset condition.

Procedures provide guidance that must accommodate a nearly infinite set of possible details in any one upset condition. Operators must still fundamentally use their best judgment in off-normal situations, based on training, experience, and their knowledge of the plant. Uncertainties remain in trying to find the best strategy during an actual event. Currently, EOP's at the Robinson plant and at other LWR's are developed to be "symptom-based", i.e., actions are based on easily observable parameters that can be provided by the instrumentation in the control room, or other nearby facilities. Diagnosis, in large part, has been reduced to the recognition and matching of symptom sets. Decision making is supported by so-called rules that take the form of:

IF symptom set is observed

THEN perform the associated action set.

The DSP's, to the degree possible, provide the operators with a rule(s) for going to the DSS as the sole recovery option. The symptom set is necessarily more abstract, i.e., less easily correlated to particular, direct indication. For example, DSP-002, revised 6/7/87, calls for a symptom set as follows:

"IF the fire prevents access to E1 and E2,

THEN OPEN Switch 2F, ..."

The procedure writers meant by the second phrase that the fire damage to the cables might induce sporadic equipment actuation or equipment inoperability and the EOP's could not be implemented due to multiple equipment failures. The control indications for such a severe situation would also be numerous, including equipment status alarms and system function alarms in numerous locations. A fire, as a result, would not necessarily produce a unique or specifiable pattern of indications but would none-the-less be readily recognizable (at least, the fact that the proximal cause of the indications would be recognizable as a major loss of control and/or motive power). DSP-001, Revised 6/1/87, contains specific symptom sets as entry conditions to the subsequent procedures and are directly applicable to the Reference 1 scenario if a fire is present. If a fire is not present, symptoms indicating a loss of both emergency busses would be similar and would be expected to lead to entry to the DSP's.

4.0 THE RISK CONTEXT

The potential risk significant scenario determined in Reference 1 represents a coincident loss of both E1 and E2 emergency busses. In the context of potential fires, this scenario seems to be the most credible. This type of sequence begins with a three phase bolted fault that is strong enough to fault one of the busses and, by explosion or fire, the other bus is assumed to sustain damage because of its proximity. This common-cause failure, among other effects, faults the two normal charging pumps B and C, and normal component cooling water, that together provide seal cooling and injection to the reactor coolant pumps (RCP's). A non-operating RCP's seals can be expected to survive without either injection or cooling for at least 30 minutes (a very conservative estimate based on WCAP 10541 Rev. 2). Offsite power is still available to other equipment on the non-emergency 480V bus and is available to the DS bus. The operators must align a series of equipment and, in particular, start charging pump A using either offsite power or the DS diesel generator to power the DS bus.

The human failure probability is the sum of two distinct potential human failure modes - a failure in the decision process associated with the DSP and a failure in the decision implementation. Table 1 lists values for each of these two failure mode probabilities. The DSP's represent an overall probability of 0.03 (1b+2) if no fire is present or 0.012 (1a+2) if fire is present.

Table 1. Probabilities of Human Failure Versus DSP Characteristics

Characteristic	
Decision mode	
Symptom-based entry conditions	
Fire Present	(1a) 0.002
Fire not present	(1b) 0.02
Implementation mode	
Back-and-forth activities	(2) 0.01

Explanatory notes:

Decision mode component;

(1a) Symptom-based procedures present and no conflict exists between using DSDG rather than available offsite power.
(1b) Symptom-based procedures present (except no fire) and conflict exists.

Implementation mode component;

(2) Based on the number and complexity of tasks (number of room transferrals).

5.0 CONCLUSIONS

The final, smaller human failure probability has a corresponding impact on the TfOmDh sequence analyzed in Reference 1. The TfOmDh sequence probability of 2E-06 was based on the availability and initial reliance on offsite power but with no clearly defined rule-based DSS procedure entry criteria (HRA probability of .04). With the HRA failure probability reduced to .03 (no credit taken for the explicit procedure entry conditions as if a fire were present), the final calculated sequence probability is reduced to 1.4E-6, (3.0E-3)(1.5E-2)(.03), lower than both the criteria used of less than 5E-6 and the preliminary probability of 2E-6 reported in Reference 1.

Reference 1. "DB-50 BREAKER ACCIDENT SEQUENCE ANALYSIS FOR THE HBR UNIT 2 ELECTRICAL DISTRIBUTION SYSTEM", MAY, 1987. R.C. Anoba, Carolina Power & Light Co.

Reference 2. "HUMAN RELIABILITY ANALYSIS FOR THE H.B. ROBINSON DEDICATED SHUTDOWN SYSTEM". May 18, 1987. Ed M. Dougherty, SAIC.

APPENDIX: DETAILS FOR THE QUANTIFICATION OF HUMAN FAILURE PROBABILITIES

There are two human failure modes that are potential contributors to the human reliability of the DSS. The first involves the decision/diagnosis aspect of actuating the system, the resulting failure of which is termed a mistake. The second involves the actual implementation of the system's actuation, failure of which is termed a slip.

The potential for mistakes arises from several sources, the dominant of which are:

1. Uncertainty about the actual conditions when compared to the experience of the operators or the anticipation of procedure writers.
2. Conflicting goals or competing options in the decision making.
3. The number of events with which the operators have to deal.
4. The time available to make the decision.
5. The remoteness of other crew members in trying to synchronize activities.

The potential for slips arises from several sources, the dominant of which are:

1. The number of actions necessary to carry out a procedure; i.e., the amount of physical burden and burden on the recall and memory capacities.
2. The presence of other crew members to assist in activities and provide redundancy.
3. The proximity of the equipment, its controls and instrumentation.
4. The ease with which specific equipment or its instruments and controls can be located among other adjacent equipment, e.g., the adequacy of labeling.

The model for mistakes is a family of four time reliability correlations (TRC's). These correlations apply to diagnosis and decision making whether or not there are strong rules and, in either case, when conflict or burden are dominant. Each TRC can be adjusted to reflect other human factors and influences on the success of the activity by a success likelihood index (SLI) between 0 and 1. Table A-1 shows the values for mistakes assuming 15 minutes is available to make the decision. This estimate arises from an estimate of 30 minutes to a seal LOCA (now considered to be extremely conservative in WCAP-10541 Rev. 2) minus 15 minutes to affect the DSP's related to the seal LOCA.

Table 1 is obtained from first assuming the least optimal DSP, i.e., little definition in the entry symptom set and the conflict of turning off available offsite ac power, as originally specified in DSP-001. This value is found from the non-rule-based with conflict column in Table A-1. Adding well-defined symptoms uses the rule-based curve. Removing the conflict uses the rule-based TRC without conflict. A SLI of 0.7 was assumed. A sensitivity analysis showed these values to vary by no more than a factor of 5 if the worst assumptions are made.

Table A-1. Probabilities of Mistakes with 15 Min. Available

	Rule-Based		Non Rule-Based	
SLI	without conflict	with conflict	without conflict	with conflict
0.3	0.010	0.07	0.09	0.2
0.5	0.006	0.05	0.04	0.1
0.7	0.002	0.02	0.02	0.1

The quantification of slips takes a simplified version of the Technique for Human Error Rate Prediction (THERP) developed at Sandia National Laboratories. The number of activities in reinstating seal cooling is taken as an estimate of the intrinsic task workload; this includes about 20 valve manipulations in several rooms. A generic THERP failure of probability of 0.001 is multiplied by these 20 manipulations to get a basic probability of 0.02. No credit is given for redundancy, since these actions may be taken by only one person. This number is assumed to represent any likely improvement on the basic workload of the procedure; but a reduction of a factor of 2 is credited since the DSP's, Rev. 1 contain significantly reduced "back-and-forth" activities among alternative rooms. The results are the values in the implementation mode section in Table 1.