Relay Chatter and its Effects on Nuclear Plant Safety

Howard E. Lambert  
FTA Associates, Oakland, CA USA

Robert J. Budnitz  
Future Resources Associates, Inc., Berkeley, CA USA

INTRODUCTION

This paper describes a limited scope probabilistic risk assessment (PRA) that was conducted for the U.S. Nuclear Regulatory Commission, (Budnitz, Lambert and Hill, 1987). The PRA addressed the effect of a strong-motion earthquake on the control and instrumentation systems at a nuclear power plant. Accident sequences were generated that incorporated seismically induced failure modes of relays, pressure switches, circuit breakers, motor operated valves, instrumentation, control systems and electrical systems. Specifically, the effects of chattering of relay contacts and pressure switch contacts during a major earthquake were studied. Special emphasis was placed on identifying circuits that could seal-in due to the effect of relay contacts chatter. In this paper, we emphasize qualitative insights that were obtained from the PRA. Chattering of protective relay contacts is a potentially important failure mode. Protective relays sense fault conditions such as overcurrent, undervoltage, reverse current and overvoltage. The relays work by sensing some parameter on an electrical bus, and actuating other relays such as lockout relays if the parameter does not agree with a standard or expected value. The PRA was conducted for two plants: the Zion Nuclear Power Plant (Zion-1), and the LaSalle County Station Nuclear Power Plant (LaSalle-2). Both of these plants are owned and operated by Commonwealth Edison (Chicago). The Zion-1 is a four-loop Westinghouse PWR with a large, dry containment. LaSalle-2 is a General Electric BWR-5 with a Mark II containment. Each of these plants has a twin unit.

SCOPE OF THE ANALYSIS

This study focuses on the loss of offsite power (LOSP) accident sequence that is expected to occur following a strong-motion earthquake due to the low median fragility value of ceramic insulators in the electrical grid. Fragility is a random variable and is characterized by a probability distribution that describes the probability of component failure as a function of a critical response parameter such as (1) local response in g's or (2) bending moment. In the following discussion, we will briefly describe how AC power is restored using the auxiliary power system (the diesel generators). For the moment, we will assume that following LOSP no other failures occur such as pipe break of the primary coolant boundary. We will assume that the plant is at full power before LOSP. When LOSP occurs, undervoltage is sensed on critical engineered safety feature (ESF) buses. Circuit breakers to loads that are normally operating will trip. Diesel generators, which serve as the auxiliary source of AC power, will start. When each diesel generator is at proper speed and voltage, its diesel generator circuit breaker should close (approximately 10 seconds to 15 seconds following LOSP) and supply 4.16 kv power to the ESF buses. In the case of Zion-1,
circuit breakers to important loads will close sequentially in time by the use of a load sequencer. These loads, which are important for shutting down the plant safely, include component cooling water pumps, service water pumps, and auxiliary feedwater pumps. It is expected that the circuit breakers at Zion will operate during the period of strong motion, which we assume will last for at least 20 seconds. In the case of LaSalle-2, circuit breakers to ESF loads are not expected to operate during strong motion. This is because ESF loads necessary for primary coolant makeup do not start until primary coolant level is boiled off to a specific set point (called "level 2"), after which two key systems are started: the reactor core isolation cooling system (RCIC) and the high pressure core spray system (HPCS). Given that no makeup systems are operating, boiloff to level 2 is expected to occur at LaSalle-2 by about 10 minutes after LOSP. Both Zion-1 and LaSalle-2 have three ESF electrical divisions. One electrical division for each plant has a swing diesel shared by the twin unit (Zion-2 or LaSalle-1). In addition, each plant has a steam-driven pump that is used either for primary coolant makeup or for heat removal. At Zion, this is the auxiliary feedwater pump and at LaSalle, it is the RCIC pump. Neither of these pumps has a dependency on AC power in the short term, except that the auxiliary feedwater pump at Zion-1 depends upon service water for cooling. The Zion service water pumps are supplied by 4.16 kv power. Failure modes of these systems are important because, for the accident sequences considered in this analysis, their operation or failure determines whether or not the sequences are safely terminated. It is important to note that the computational procedure and data bases developed by the Seismic Safety Margins Research Program, SSMRP, (Bohn et al, 1983) were used to quantify the accident sequences described below.

ASSUMPTIONS MADE IN GENERATING THE ACCIDENT SEQUENCES

Simplified fault trees have been used to generate various accident sequences that describe how a core-damage accident can occur. The following assumptions have been made for both plants in generating these sequences:

- we assume that loss of offsite power (LOSP) occurs with a certain probability due to earthquake-caused failure of the electrical grid's ceramic insulators, because their seismic capacity is generally much lower than that of any other components and structures; we use an SSMRP-derived fragility function for LOSP which is convoluted with a response function;

- LOSP is the only earthquake-induced initiating event that we consider in this analysis; we assume that LOSP occurs whenever the ceramic insulators are damaged by the earthquake;

- we assume that the reactor protection system will shut down the fission chain reaction and keep it down after the earthquake;

- we assume that offsite power is not recovered—therefore, the main feedwater system is not recovered and is unavailable for coolant makeup and/or heat removal;

- we pessimistically assume that there is no operator action, and in particular that operators do not reset circuit breakers and relays; thus no credit is taken for operator actions in the analysis;

- we assume that DC power is always available after the earthquake;

- we assume that the SSMRP "hazard curves" used in this analysis are correct;
We consider only failure modes due to chatter of relay and pressure switch contacts.

It is important to note that we assume that there is no other transient event besides LOSP when the strong-motion earthquake occurs. For example, random pipe breaks, valve mechanical failures, and structural failures are not considered. Furthermore, as mentioned above, we assume that LOSP does not occur with 100% probability; a seismic fragility function has been assigned for LOSP. Past seismic PRAs have assumed that the operator can always recover from failure modes induced by chattering of relay and pressure switch contacts. We discuss operator recovery at the end of this paper. As described in the body of the paper, relay chatter can cause switch gear failure and subsequently cause a station blackout (i.e., loss of all AC power) following loss of offsite power. An important observation is that chatter sometimes occurs at a much lower acceleration level than do structural failures such as building collapse or bending of pipes, which implies that the chatter mode can sometimes have a higher probability of occurrence for a given earthquake size.

LOSS OF OFFSITE POWER FOLLOWING AN EARTHQUAKE

This study focuses on the loss of offsite power (LOSP) accident sequence that is expected to occur following a strong-motion earthquake due to the low median capacity of ceramic insulators (i.e., approximately 0.3 g). Numerous circuit breakers important to plant safety will operate while strong motion is occurring. In the following discussion, we will briefly describe how auxiliary AC power is restored. When LOSP occurs, undervoltage (UV) is sensed on critical ESF buses. Circuit breakers to loads that are normally operating should trip. Diesel generators, which serve as an auxiliary source of AC power, should start. When the diesel generator gets to its proper speed and voltage, the diesel generator circuit breaker should close (approximately 10 seconds following LOSP) and supply 4.16 kv power to the ESF bus.

FAILURE MODE ANALYSIS

Given an earthquake, two types of relay contact chatter are possible. Contacts that are normally open can chatter close. In addition, contacts that are normally closed can chatter open. The authors have observed for armature-type relays that it is much easier for normally closed relays to open than it is for normally open relays to close. This observation can be made by simply shaking the relay, and is reflected in test data. In the failure mode analysis described below, we assume that chatter can occur long enough to cause a change in electrical continuity which in turn will cause a relay to change state or a solenoid to energize.

Circuit Breaker to ESF Loads (Zion-1)

There are numerous contacts to protective relays in control circuits to circuit breakers that can chatter and cause tripping of breakers to ESF loads. In addition, these breakers will not close if they do not receive a close signal due to load sequencer timer failures. The load sequencers will not work if 480 volt power is not available. This can be caused by tripping of the feed breaker from the 4.16 kv bus to the 480 V bus, due to relay chatter.

Circuit Breaker to the Diesel Generator (Zion-1 and LaSalle-2)

The control circuit for the breaker has numerous protective contacts that can cause the DG breaker to trip if these contacts chatter closed.
RCIC Failure (LaSalle02)

RCIC can successfully operate for a LOCA in the steam line with size less than about 0.01 square-foot. Two or more SRVs opening creates an inventory loss greater than the equivalent of 0.01 square feet, which is a break that RCIC's capacity cannot replace. There are 18 SRVs and each has its own pressure switch. When these pressure switch contacts close, the "C" solenoid is energized which causes the SRV to operate. These pressure switch contacts can chatter close, which would cause inadvertent inventory loss greater than RCIC's capacity to make up. The failure logic is that 2 contacts out of 18 must chatter. In addition, RCIC could fail if the steam supply to the RCIC turbine is unavailable. This can occur if an isolation signal is generated which in turn causes closure of an AC-powered motor operated valve. Chattering of a seal-in relay can cause such an isolation signal. It is important to note that the seal-in must occur before loss of AC power if the valve is to close.

Failure of the Steam Driven Auxiliary Feedwater Pump (Zion-1)

The auxiliary feedwater pump requires cooling by the service water system. There are six service water pumps and at least two are required for safe shutdown heat loads. Since two are required, the service water system will fail to remove heat if at least five service water pumps fail.

LaSALLE-2 REACTOR ACCIDENT SEQUENCES

The reactor accident sequence considered is failure to make up within 80 minutes. 80 minutes corresponds to the time fuel damage is expected to occur if no coolant makeup is available following LOSP.

The sequence consists of the following events:

- RCIC fails due to any one of two causes:
  1. inadvertent SRV actuation (two or more SRVs open due to chatter of pressure switch contacts, so that RCIC is inadequate),
  2. steam supply to RCIC turbine fails because the outboard isolation valve closes due to chattering of a seal-in relay.

- High pressure makeup system (HPCS) and low pressure makeup systems fail due to station blackout, i.e., loss of all AC power on all three electrical divisions as described below:
  1. there is no electrical power on the division 1 bus since the diesel swings to unit 1 (assumed to occur with probability 0.5),
  2. there is no AC power on division 2 and 3 because the DG breakers fail to close or trip after closure because lockout relays inadvertently energize due to relay chatter.

There were 408 min cut sets of order 5 generated and 60,000 min cut sets of order 6. Min cut sets of order 5 (order 6) contained the following basic events: (1) loss of offsite power, (2) diesel on division 1 swings to unit 1 and, (3) three sets (four sets) of relay/pressure switch contacts chatter close.

ZION-1 CORE MELT SEQUENCES

Two core melt sequences were identified and considered for Zion-1: (1) small LOCA through the reactor coolant pump seals, caused by failure of the component cooling water system (CCWS) and the high pressure injection makeup systems, i.e., safety injection system and charging system and, (2) secondary
system heat removal fails because the auxiliary feedwater system fails and primary system heat removal fails because feed and bleed fails.

**Small LOCA Sequence (Zion-1)**

In the small LOCA sequence, failure of the CCWS will cause the reactor coolant pump seals to heat up and subsequently leak. In addition, failure of the CCWS will fail the high pressure injection pumps due to pump overheating. Hence failure of the CCWS is a single event leading to core melt (given the other assumptions above). The CCWS consists of five pumps, three of which are assigned to unit 1 and two to unit 2. According to the Sandia review (Berry, et al, 1984), two out of five pumps must operate for successful heat removal, implying a failure logic of four out of five pumps. Each CCWS pump can fail for any one of three reasons: (1) the supply breaker can trip if the trip coil is inadvertently energized due to chattering of any 1 of 4 contacts, (2) the supply breaker can fail to close if the load sequencer is not energized, which could happen if there is no power on the 480 V bus due to the chattering of any 1 of 4 contacts and, (3) the power on the 4.16 kv bus which supplies the pump can fail, if the DG breaker has tripped open or if theswing diesel has swung to the other unit. It is important to note that when the swing diesel aligns to one bus, the other bus is unavailable. This implies that one CCWS pump is unavailable. (The same is true of the service water pumps of which there are six, one attached to each 4.16 kv bus of both units 1 and 2.) The small LOCA sequence has generated approximately 28,000 min cut sets of order 5 and 17,000 min cut sets of order 6 that contain the following basic events: (1) loss of offsite power, (2) diesel swings to unit 1 or unit 2 and, (3) three or four sets of relay contacts chatter. There is uncertainty as to when core damage is expected to occur by this small LOCA sequence, since the leakage rate through the coolant pump seals is unknown. Sandia's report (Berry, et al, 1984) quotes a reference from the Seabrook nuclear power plant analysis that quotes a time of ten hours.

**All Secondary and Primary Heat Removal Fails**

Another accident sequence is failure to remove heat because the secondary heat removal system, the auxiliary feedwater system, has failed and the primary heat removal system, feed and bleed has failed. Failure of the service water system can cause this sequence to occur. Failure of the service water system leads to overheating of the diesel generators and subsequently loss of all AC power. In addition, the steam driven auxiliary feedwater pump would fail due to overheating of the pump. The sequence takes approximately 1 to 1.5 hours for core damage. Assuming that two service water pumps are needed for a safe shutdown at both units, approximately 152,000 min cut sets of order 6 are generated and contain the following basic events: (1) loss of offsite power, (2) diesel swings to unit 1 (or unit 2) and, (3) four sets of relays chatter close.

**OPERATOR ACTION (ZION-1)**

For ESF loads, the operator from the control room can reclose these breakers, if they fail to close by simply closing the control switch in the control room. Closing the control switch by manual control causes the Y relay (i.e., anti pumping relay) to drop out, permitting reclosure of the circuit breaker. The only exceptions are the two DG breakers to the dedicated diesels (not the swing diesel). Breaker closure requires manual operator action at the motor control center in the event of trip after closure. In this case, the Y relay seals-in. Commonwealth Edison has made changes to the control circuits so that the seal-in can be dropped out by operation of the control switches from the control room.
OPERATOR ACTION (LaSALLE-2)

In the event that lockout relays seal-in, the operator can drop the seal-in by operation of reset switches in the control room. Reclosure of the DG circuit breaker is then possible from the control room. The operators can do nothing about inadvertent operation of the safety relief valves.

ACKNOWLEDGEMENTS

This project has been supported by the U.S. Nuclear Regulatory Commission's Office of Nuclear Regulatory Research, as part of the Small Business Innovation Research Program. The authors wish to thank the following organizations for their technical guidance: Lawrence Livermore National Laboratory, Sandia National Laboratories, Commonwealth Edision and Sargent & Lundy.

References

