A.11 LER No. 412/93-012

Event Description: Failure of Both Emergency Diesel Generator Load Sequencers

Date of Event: November 4-6, 1993

Plant: Beaver Valley 2

A.11.1 Summary

On November 4, 1993, the automatic loading capability of the 2-1 emergency diesel generator (EDG) on a safety injection (SI) signal failed during a test. Two days later, on November 6, 1993, the automatic loading capability of the 2-2 EDG on an SI signal also failed during a test. This failure would only occur when an SI signal was present coincident with a loss of the normal power supply to the engineered safety features (ESF) bus. The failure mechanism had existed since November 1990. Operator actions would have been necessary to allow manual loading of equipment on the ESF buses. The conditional core damage probability estimated for this event is 2.1×10^{-6}. The relative significance of this event compared to other postulated events at Beaver Valley 2 is shown in Fig. A.11.1.

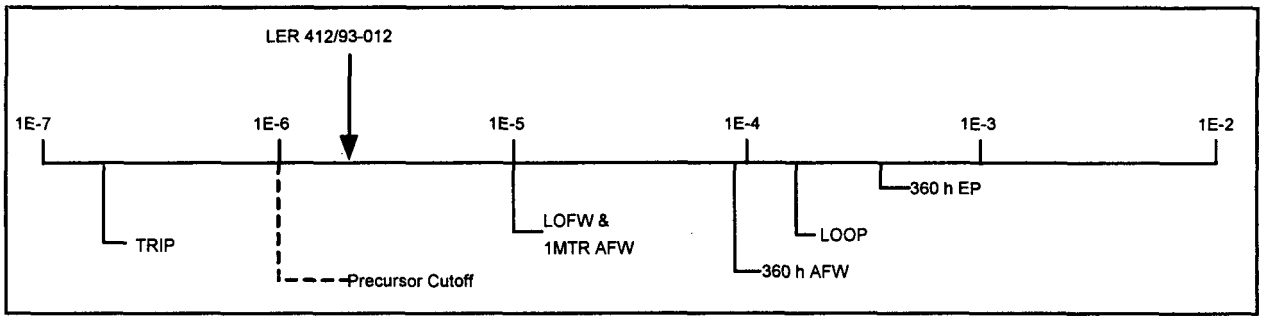

Fig. A.11.1 Relative event significance of LER 412/93-012 compared with other potential events at Beaver Valley 2

A.11.2 Event Description

On November 4, 1993, with the Beaver Valley 2 plant in cold shutdown, a test of the automatic loading capability of the 2-1 EDG on an SI signal was conducted. The test is performed during each refueling outage and verifies that the EDG circuitry will automatically load the safety-related loads on the ESF buses at the required time following the EDG start. During the test, the EDG started and reenergized the associated ESF bus, but the safety-related equipment did not automatically sequence onto the bus as expected. Approximately 2 min into the test, the SI signal was reset, and the loads began to automatically sequence on the bus. An investigation following the test indicated that two relays in the solid-state protection system had the potential to cause the observed failures. The two relays were replaced, and the test was successfully rerun the following day.

On November 6, 1993, the automatic loading capability of the 2-2 EDG on SI also failed during a test. Diagnostic test equipment installed on the load sequencer identified the SI reset relay as the cause of the failure. This relay resets the sequencer if an SI signal occurs during a loss-of-bus-voltage event. Voltage

spikes caused by the opening of this relay resulted in the relay reclosing. This caused the loading sequencer to "lock-up."

This failure would only occur when an SI signal was present coincident with a loss of the normal power supply to the ESF bus. The automatic loading would have functioned properly for a postulated accident without the loss of normal power or if the SI signal was actuated after the normal supply to the ESF bus was restored. The failure mechanism had existed since a modification of the sequencer relays in November 1990 (36 months). Operator actions would have been necessary to allow manual loading of equipment on the ESF buses. These actions include locally resetting the motor-control centers to restore service water (SW) to the EDGs, the high-head SI (HHSI) pump coolers, and to operate essential emergency-core-cooling system (ECCS) valves.

A.11.3 Additional Event-Related Information

Two sequencers automatically place vital safety-related equipment onto the ESF buses. The SI sequencer will operate whenever an SI signal is generated, regardless of the source of power to the ESF buses. This sequencer loads essentially all of the ESF equipment onto the ESF buses. The blackout sequencer will operate whenever the EDGs are required to supply power to the ESF buses and an SI signal is not present. Most ESF equipment is loaded by this sequencer. This includes the HHSI pumps but does not include the low-head SI (LHSI) pumps. The load sequencers are used to distribute the loads placed on the EDG in six discrete steps over a 1-min period. This prevents an overload of the EDG by spreading out the high starting currents of the motors over time. If a blackout signal and an SI signal are generated simultaneously, the SI sequence will be implemented. If an SI signal occurs after the blackout sequencer has gone to completion, the equipment loaded by the blackout sequencer remains connected to the bus. The additional equipment started by the SI sequencer would be loaded onto the bus.

During the first refueling outage in 1989, problems were encountered with obtaining the necessary set-point repeatability with the existing electromechanical timer/relays used in the sequencer circuitry. During the second refueling outage in 1990, the electromechanical relays were replaced with microprocessor-based timer/relays to improve set-point repeatability. The timers were also modified to be continuously energized to improve performance. During the third refueling outage, tests revealed that three of the eight timer/relays in each train had failed. The failures were due to overheating caused by the continuous energization. The timer/relay configuration was changed to be energized only when actuated. These previous failures were unrelated to the cause of the failures in 1993. Following the 1993 failures, diodes were installed to suppress the voltage spikes across the relays. The results of tests following the modification showed no failures after 80 cycles.

A.11.4 Modeling Assumptions

Four situations were considered: (1) a postulated loss-of-offsite power (LOOP) where SI is initiated for feed-and-bleed, (2) a postulated LOOP with an SI occurring as a result of equipment failures or operator actions, (3) a LOOP-induced loss-of-coolant accident (LOCA), and (4) a postulated LOCA that induces a LOOP as a result of the effects of the plant trip on the electrical grid.

A.11.4.1 Feed-and-Bleed following a postulated LOOP

Following the postulated LOOP, feed-and-bleed would be required after the postulated failure of main and auxiliary feedwater (AFW). The requirement for feed-and-bleed would have to occur before offsite power was recovered. Recovery of offsite power would eliminate the lock-up problem. During the initial LOOP response, the blackout sequencers would operate (because they were not affected by the relay problems)

and would start the EDGs and load most ESF equipment, including the HHSI/charging pumps. When feed-and-bleed is initiated, the operators would manually actuate SI to enable the automatic switchover to containment sump recirculation. The sequencers would lock-up at this point. However, the need for the LHSI pumps and the switchover to containment sump recirculation would not occur for an extended period. In addition, procedures would require the reduction of the SI flow rate [to one pump and one power-operated relief valve (PORV)] to reduce the rate that the refueling water storage tank is depleted and extend the time to recirculation. To recover from this failure, the operator would have to reset the sequencer locally and manually start the LHSI pumps from the control room. Given the likelihood of a LOOP coincident with a failure of all AFW (motor- and turbine-driven pumps) and the extended period of time the operator has to recover from the sequencer failure, this scenario did not contribute significantly to the conditional core damage probability.

A.11.4.2 SI signal generated following a postulated LOOP

In the second situation, following the postulated LOOP, a postulated SI signal would be generated due to equipment failures or operator actions. For example, a stuck open steam generator (SG) safety valve would actuate SI due to the large cooldown and depressurization of the primary system. An operator overfeeding a SG could have a similar effect. Voltage perturbations during electrical system transients and realignments could cause spurious actuations of the SI relays.

A search of LOOP events from 1987 through 1993 revealed that of the 55 LOOPs that occurred during that time period, 9 involved the actuation of SI (four at pressurized-water reactors, five at boiling-water reactors). These SI signals were generated as the result of operator actions and equipment failures similar to those described in the examples above. In the most severe of these cases, HHSI was required initially. However, long-term use of SI that would require switchover to recirculation was not necessary in any of these events.

During the initial LOOP response, the blackout sequencers would operate (because they were not affected by the relay problems) and would start the EDGs and load most ESF equipment, including the HHSI/charging pumps. Because the switchover to the recirculation mode would not be required, no additional operator actions would be needed in this situation. Therefore the sequencer lock-up problem is not a concern in this situation. For plants where the HHSI pumps are not started by the blackout sequencer, this situation could contribute significantly to the conditional core damage probability.

A.11.4.3 LOOP-induced LOCA

In this case, the plant response to the postulated LOOP results in a postulated LOCA event. This scenario was considered highly unlikely except for the potential for a stuck-open pressurizer PORV/safety relief valve (SRV) following the LOOP. This situation is similar to that of the bleed-and-feed scenario in that the HHSI pumps are started by the blackout sequencer before the initiation of the SI sequencer. However, in this case, long-term SI operation would be required. Operator actions would be needed to start the LHSI pumps because the SI sequencer would lock-up before starting these pumps. Given the low probability for this event and the low operator failure rate (due to the extended period for LHSI recovery), this situation did not significantly contribute to the overall conditional core damage probability for this event.

A.11.4.4 LOCA with transient-induced LOOP

In this case, a postulated LOCA is the initiating event. When the plant trips in response to the LOCA, the transient results in the LOOP to the station. If offsite power is available, loads are fast-transferred to the alternate offsite power source, and the SI sequencer would operate properly. If offsite power is not available,

then the EDGs will start. The normal feeder breaker to the ESF buses trips open, and load shedding occurs. The sequencer would then start and lock-up. It is assumed that one-half hour is available to establish make-up to the reactor coolant system (RCS) before core damage will occur. This event tree (Fig. A.11.2) is based on the accident sequence precursor (ASP) LOCA tree for PWR class A plants (see NUREG/CR-4674, Vol. 17, Appendix A, Section A.3-1 and Fig. A.6). Values used in the quantification of the event tree are provided in Table A.11.1.

A.11.4.5 LOCA initiation frequency

The condition existed since the 1990 refueling outage (~ 36 months). ASP analyses have typically modeled long-term unavailabilities for a 1-year period. ASP initiating event frequencies are based on operation for 70% of a year (an approximation of the percentage of the year that a typical plant spent at power). Therefore, the initiating event frequency is multiplied by 6132 h (365 d × 24 h/d × 0.7).

A.11.4.6 LOOP and short-term offsite power recovery

It is assumed that the probability of a LOOP induced by a LOCA is 1.0×10^{-3} (*Reactor Safety Study*, WASH-1400, NUREG-75/014, p. II-90). A search of the Sequence Coding and Search System for transient-induced LOOPs from 1984 to present revealed five transient-induced LOOPs out of 3985 trips. This yields a rate of 1.25×10^{-3} per trip. This provides a degree of substantiation for the WASH-1400 value. It was assumed that offsite power recovery is possible only in the first one-half hour. If the EDGs fail and a LOCA is in progress, offsite power must be restored within a half-hour to repower the HHSI pumps. The nonrecovery value of 0.48 is that associated with a grid-related LOOP (from ORNL/NRC/LTR-98-11, *Revised LOOP Recovery and PWR Seal LOCA Models*, August 1989), because the initiating cause of the LOOP was assumed to be grid disturbance caused by the plant trip. Note that if no LOOP occurs, the event is simply a small-break LOCA, and the sequencers will operate properly. Therefore, this branch does not contribute to the conditional core damage probability.

A.11.4.7 Emergency power

If the EDGs fail to start, it is assumed that insufficient time is available to recover the EDGs and to manually load the buses. Therefore, the nonrecovery value of the EDGs for this case is set to 1.0, and the failure of the EDGs to start leads directly to core damage (sequence 24).

A.11.4.8 Loading of the ESF equipment on the ESF buses

The operator actions necessary to load required equipment onto the ESF bus are treated as a single top event. It would be obvious to the operators that manual actions were required to load equipment on the ESF buses because none of the ESF equipment loads would be picked up by the EDGs. With both an SI and blackout signal present, the SI signal would dominate, and equipment would not be loaded by the blackout sequencers. In addition, the fact that nothing loaded onto the EDGs would probably lead the operators to suspect a sequencer failure. It is assumed that the operators would have procedural guidance to direct their actions. Equipment recovery would have to be prioritized to prevent equipment damage. SW would have to be restored to the running EDGs to cool them, and HHSI pumps would be needed to provide make-up to the RCS. Local actions would be required to reset the MCCs to restore SW to the EDGs, the HHSI pump coolers, and to operate essential ECCS valves. Because this process requires many coordinated actions and

local operator actions, an operator failure rate of 0.34 was assumed (ASP Recovery Class R3, see NUREG/CR-4674, Vol. 17, Appendix A, Sect. A.1).

Failure to successfully load equipment onto the ESF bus leads to a core damage state (sequences 11 and 23). Although the turbine-driven AFW pump will operate to remove decay heat, no RCS make-up is provided. Therefore, core damage will occur. If loads are successfully loaded, then the remainder of the tree (sequences 1-10 and 13-23) is the same as the typical LOCA tree (see NUREG/CR-4674, Vol. 17, Appendix A, Sect. A.3-1 and Fig. A.6, Sequences 71-77 and 80-82) and uses standard ASP values.

A.11.5 Analysis Results

The estimate of the conditional core damage probability for this event is 2.1×10^{-6}. There are two dominant core damage sequences, shown in Table A.11.1. Sequence 11 involves a postulated LOCA, a transient-induced LOOP that is recovered in the first half-hour, and failure to load the ESF buses. The other dominant sequence (sequence 23) involves a postulated LOCA, transient-induced LOOP that is not recovered in the first half-hour, initial emergency power success, and failure to load the ESF buses.

The conditional core damage probability is directly affected by the transient-induced LOOP probability and the assumed operator failure rate for the loading of the ESF buses. If the operator failure rate for loading of the ESF buses is changed from 0.34 to 0.12 (ASP recovery class R3), the conditional core damage probability for the event is reduced by a factor of 2.8 to 7.4×10^{-7}.

Additional information concerning this event is included in Augmented Inspection Team report 50-412/93-81.

Table A.11.1. Values used in the quantification of the event tree

Top Event	Description	Value
LOCA	LOCA initiator Initiating frequency = 2.4×10^{-6}, nonrecovery = 0.43 Duration of unavailability = 6132 h	6.3×10^{-3}
LOOP	Transient-induced LOOP Frequency = 1×10^{-3}/demand	1.0×10^{-3}
LOOP	LOOP recovery (short-term)-recovery in the first half-hour for transient-induced LOOP From ORNL/NRC/LTR-98-11*Revised LOOP Recovery and PWR Seal LOCA Models*, August 1989 Nonrecovery in the first half-hour = 0.48	4.8×10^{-1}
RT/LOOP	Reactor trip given a LOOP Failure probability = 0	0
EP	Emergency power system (LOCA and transient-induced LOOP) Failure probability (1 of 2) = Train1 × Train2 × nonrecovery Train 1 = 0.05, Train 2 = 0.057, nonrecovery = 1.0	2.9×10^{-3}
ESF LOADING	Loading of the ESF buses Operator failure probability = 0.34	3.4×10^{-1}

Top Event	Description	Value
AFW	Auxiliary feedwater system Failure probability (1 of 3 + serial failure) = [(Train1 × Train2 × Train3) + Serial] × nonrecovery Train 1 = 0.02, Train 2 = 0.1, Train 3 = 0.05, Serial = 0.00028 Nonrecovery = 0.26	9.9×10^{-5}
MFW	Main feedwater system Failure probability (1 of 1) = Train1 × nonrecovery Train 1 = 0.2, nonrecovery = 0.34	6.8×10^{-2}
HPI for feed-and-bleed	High-pressure injection initiated for feed-and-bleed Failure probability p(HPI) + operator failure p(HPI) = 2.5×10^{-4} Operator failure = 0.01	1.0×10^{-2}
HPR	High-pressure recirculation Failure probability (1 of 2 + operator action) = (Train1 × Train2 × nonrecovery) + operator action Train 1 = 0.01, Train 2 = 0.015, nonrecovery = 1.0 Operator failure = 0.001	1.1×10^{-3}
PORV OPEN	PORV open for feed and bleed Failure probability (1 of 1) = (Train1 × nonrecovery) + operator failure Train 1 = 0.01, nonrecovery = 1.0, Operator failure = 0.0004	1.0×10^{-2}
CSR	Containment sump recirculation Failure probability (2 of 4) = [4(Train 1 × Train 2 × Train 3) - 3(Train 1 × Train 2 × Train 3 × Train 4)] × nonrecovery Train 1 = 0.01, Train 2 = 0.03, Train 3 = 0.1, Train 4 = 0.3 Nonrecovery = 1.0	9.3×10^{-5}

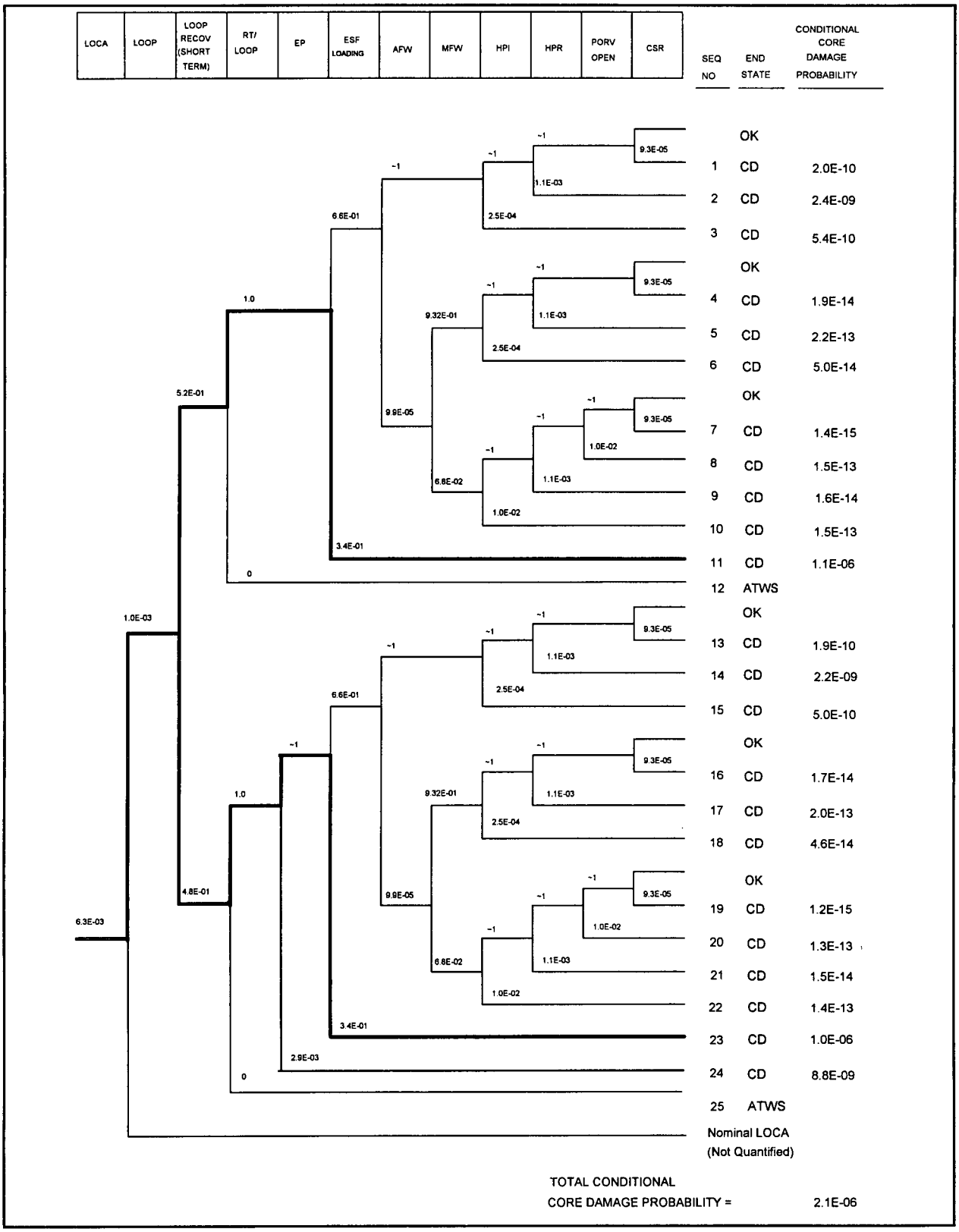

Fig. A.11.2 Dominant core damage sequence for LER 412/93-012