AEOD/E92-02
Supplement 1

INSIGHTS FROM COMMON-MODE FAILURE EVENTS

FEBRUARY 1993

By: S. Israel

Office for Analysis and
Evaluation of Operational Data
U.S. Nuclear Regulatory Commission

SUMMARY

An engineering evaluation report on insights from common-mode failure events (AEOD/E92-02) was issued in June 1992. Additional common-cause failure events identified in 1990 LERs were added to the study. The summary tables were reorganized to clarify the potential impact of generic corrective actions applicable to the observed events. The corrective actions were also reformulated to make them easier to comprehend. The results are still dominated by errors that occur at the design, fabrication, and installation stage which are undetected for extended periods of time.

INTRODUCTION

Engineering Evaluation report titled "Insights from Common-Mode Failure Events," AEOD/E92-02, June 1992, was based on 44 licensee event reports (LERs), mostly from 1990. An additional 18 LERs were identified during a review of 1990 licensee reporting patterns. Common-mode failures were considered synonymous with common-cause failures for the purposes of the study. As noted in AEOD/E92-02, recoverable situations, self-revealing situations, and miscalibration events were not analyzed as part of this study. Questions arose concerning the robustness of the results because of the deletion of the miscalibration events. This issue is addressed below.

Some confusion about the potential corrective actions became evident after the original study was published. The intent of the study was to identify dominant corrective actions that would preclude or reduce the likelihood of common-cause failures in safety systems at operating plants if the actions were applied to all important safety components or systems. The potential corrective actions considered in the study require some sort of active inte action such as performing a test or replacing equipment, as opposed to a more passive activity, such as design reviews, which normally are performed at the initial phases of a plant's development.

Some of the corrective actions were retitled to clarify what was intended. It should be noted that no judgement was made regarding the effectiveness or practicality of applying any of these corrective actions to all important safety components at a plant. Comments raised concern about the effectiveness or practicality of implementing some of these potential corrective actions in a universal fashion at all operating plants.

DISCUSSION

An additional 18 events having common-cause failures were identified in the 1990 LERs. These are summarized in Appendix 1. The 44 events identified in AEOD/E92-02 and the additional 18 are displayed in Tables I and II, which show situations related to design, fabrication, installation errors and maintenance errors. The event number in the tables corresponds to those presented in the appendices of AEOD/E92-02 and this supplement. The events in Table I include component and system deficiencies related to internally initiated events such as transients and loss-of-coolant accidents (LOCAs) and equipment

deficiencies related to externally initiated events such as fires, floods, and seismic events. The events in Table II include deficiencies in preventive maintenance as well as errors in corrective maintenance.

Each of the events in Tables I and II was reviewed to identify potential corrective actions that could have eliminated or reduced the possibility of the common-cause failure noted in the LER. An "X" indicates a potential corrective action for that event in the judgement of the author. A single event can have more than one potential corrective action; no judgement was made about which action was preferable or that one action might preclude the necessity of another action. The various corrective actions are the same as those considered in AEOD/E92-02, except the labels have been changed to improve understanding. These actions are defined below:

COMPREHENSIVE TESTS refers to an integrated systems test program that envelopes all operating conditions.

STAGGERED TESTS refers to uniformly staggering surveillance tests on redundant trains. The test interval on a given train would not be changed, but the test schedule for redundant trains would be uniformly offset.

POST TEST refers to appropriate post maintenance testing.

DIVERSE EQUIPMENT refers to using equipment from a different manufacturer in redundant trains.

ADDITIONAL MARGIN refers to replacement with equipment having a larger design margin.

MORE TESTS refers to more frequent tests. For this study, it was only flagged for those situations with chronic degradation.

SPLIT TRAIN refers to having adequate train separation.

SEPARATE MAINTENANCE refers to using different personnel perform maintenance on different trains.

The largest group of events (roughly two-thirds) is associated with errors at the design, fabrication, and installation phase of plant development. This group combines environmental qualification and train separation events from Table I in AEOD/E92-02 and design, installation events from Table III in AEOD/E92-02. These events, shown in Table I, are particularly significant because they generally exist for long periods of time before they are detected. The fractional representation of these events may be skewed by the event selection process discussed in AEOD/E92-02.

The dominant potential corrective action indicated in Table I is component substitution with equipment having a larger design margin (ADD MARGN). Comprehensive system tests (COMPR TEST) and substitution of equipment having a different manufacturer (DIVRS

EQUIP) had smaller potential impacts. The effectiveness or practicality of any of these three corrective actions depends on judgement during implementation and therefore is speculative. This concern was also reflected by Advisory Committee on Reactor Safeguards comments. Questions were also raised about the potential downside risks associated with implementing any one of these corrective actions in a universal fashion.

It should be noted that comprehensive system tests were supposed to be performed during the preoperational and startup phases of the plant. Evidently these initial tests were not sufficiently comprehensive in all cases based on these results. Adequate train separation (SPLIT TRAIN) is another important corrective action that should have been implemented at the design phase of the plant.

The maintenance related events are presented in Table II. The dominant corrective action for these events is staggered surveillance testing (STAGR TEST). This action does not eliminate the source of the potential common-cause failure, it just reduces the potential exposure to a time dependent common-cause failure arising from the deficient maintenance action. More frequent tests (MORE TESTS) also reduce the exposure to the deficiencies. It should be noted that the exposure to the maintenance deficiencies or errors is generally less than a refueling cycle.

Taking all the events together, using equipment with larger design margins had the highest potential impact, about 56 percent of the situations examined in this study. Performing comprehensive systems tests, insuring adequate train separation, and the use of diverse equipment each had a potential impact on about 27 percent of the cases. The use of staggered surveillance testing impacted 20 percent of the events. The use of staggered testing varies widely among the U.S. plants. Some equipment such as relief valves (RVs) are tested on a staggered basis at all plants. Some plants use staggered testing for all surveillance tests while most of the plants appear to use some form of sequential train testing. Staggered surveillance testing is widely used at foreign nuclear plants.

These results are consistent with those presented in AEOD/E92-02. However, in AEOD/E92-02 it was noted that train maintenance by separate personnel may be an important consideration for precluding some of the maintenance related situations. On closer examination, it was observed that 60 percent of the situations amenable to train maintenance by separate personnel would be captured by post maintenance tests that are already required. Consequently, train maintenance by separate personnel does not appear to be a dominant potential corrective action based on this new evaluation of the data.

Questions were raised about the deletion of miscalibration events from the database. Thirty five miscalibration events were identified in the original 500 LERs (from 1990) related to common-cause failures. Fifteen of these LERs involved miscalibration of RVs, because of set point drift or otherwise. These deviations were small and did not significantly degrade the pressure relief function. Ten of the events involved miscalibration of reactor trip settings. Based on a previous study on trip settings, AEOD/T92-05, the trip functions are generally diverse so that any serious miscalibration of one function would be nullified by some other diverse trip function. The other 10 events involved pressure instrumentation and relay settings. The deviations were generally small. The miscalibration events were skewed

toward maintenance related deficiencies. Based on the perceived small impact of these events, available diversity and redundancy, and their distribution between maintenance and design errors, that their deletion has a minimal impact on the overall results of this study.

Table 1 Corrective Actions for Design, Fabrication, and Installation Related Events

EVENT	COMPR TEST	STAGR TEST	POST TEST	DIVRS EQUIP	ADD MARGN	MORE TESTS	SPLIT TRAIN	SEPAR MAINT
10	X	.	.	.	X	.	.	.
12	X	.	.	.	X	.	.	.
15	X	.	.	X	X	.	.	.
17	X	.	.	X	X	.	.	.
22	X	.	.	.	.	.	X	.
25	X	.	.	.	.	.	.	.
28	X	.	.	X	X	.	.	.
29	.	.	.	.	X	.	.	.
30	X	.	.	X	X	.	.	.
34	X	.	.	X	X	.	.	.
35	.	.	.	.	.	.	X	.
37	X	.	.	X	X	.	.	.
40	X	.	.	.	X	.	.	.
60	X	.	.	.	X	.	.	.
46	.	.	.	.	.	.	X	.
51	.	.	.	.	.	.	.	.
54	.	.	.	.	X	.	.	.
55	.	.	.	X	.	.	.	.
56	X	.	.	.	X	.	X	.
3	.	.	.	X	X	.	.	.
4	.	.	.	X	X	.	.	.
9	.	.	.	X	.	.	.	.
27	.	X	.	X	X	.	.	.
5	.	.	.	.	X	.	X	.
53	.	.	.	.	X	.	.	.
48	.	.	.	.	X	.	X	.
6	X	.	.	.	.	.	X	.
7	.	.	.	.	.	.	X	.
11	.	.	.	.	.	.	X	.
14	.	.	.	.	.	.	X	.
8	.	.	.	.	X	.	.	.
13	.	.	.	.	X	.	X	.
41	.	.	.	.	X	.	.	.
61	.	.	.	.	X	.	.	.
62	.	.	.	.	X	.	.	.
50	.	.	.	.	X	.	.	.
52	.	.	.	.	X	.	.	.
58	X	.	.	.	.	.	X	.
59	X	.	.	.	.	.	X	.
23	.	.	.	X	X	.	.	.

Table II **Corrective Actions for Maintenance Related Events**

EVENT	COMPR TEST	STAGR TEST	POST TEST	DIVRS EQUIP	ADD MARGN	MORE TESTS	SPLIT TRAIN	SEPAR MAINT
1	.	X	.	.	X	X	.	.
2	.	X	.	.	X	X	.	.
16	.	X	.	.	X	X	.	.
24	.	.	.	.	.	X	X	.
33	.	X	.	X	X	.	.	.
38	X	.	.	.	.	X	.	.
39	.	X	.	.	X	X	.	.
45	.	X	.	.	X	X	.	.
57	.	X	.	X	.	.	.	.
18	.	.	.	X	.	.	.	.
19	.	.	.	.	.	.	.	.
20	.	.	X	.	.	.	.	X
21	.	.	.	.	.	.	.	.
26	.	X	.	X	.	.	.	X
31	.	X	X	.	.	.	.	X
32	.	X	.	X	.	.	.	X
36	.	X	.	X	.	.	.	.
42	.	.	.	.	.	.	X	.
43	.	X	.	.	.	.	.	.
44	.	.	X	.	.	.	X	X
47	.	.	.	.	X	.	X	.
49	.	.	.	.	X	.	.	.

Appendix 1

Additional Summaries of 1990 LERs

45. **Haddan Neck LER 213/90-23** Low service water flow was observed in two of four containment cooling fans during surveillance. This degradation was caused by excessive debris.

46. **Oyster Creek LER 219/90-17** A common duct in the SBGT was found sufficiently degraded to impair the operability of both trains of SBGT.

47. **Millstone LER 245/90-10** Doors were open for 16 hours that created a flow path between the turbine deck and the switchgear area. This would expose switchgear to a potential harsh environment.

48. **Millstone LER 245/90-09** An evaluation concluded that rupture of a house heating steam line could adversely impact unprotected class 1E equipment.

49. **Turkey Point LER 250/90-14** PORV block valves inoperable because of inadequate thrust settings.

50. **Monticello LER 263/90-19** Discovered that emergency procedure for external flooding did not include protective measures for diesel generator fuel oil transfer house.

51. **Calvert Cliffs LER 317/90-12** Determined that procedure for LOCA would not ensure post-LOCA core flush in time to prevent boron precipitation.

52. **Millstone LER 336/90-17** During an evaluation of seismic class 1 hangers, corrosion was noted on a service water hanger. An error was found in the original seismic calculations for this hanger. The net result was that the hanger would have failed during a design basis earthquake and would have adversely impacted both service water headers.

53. **Millstone LER 336/90-05** Discovered that a high energy line break in the auxiliary steam system could adversely impact safety related equipment.

54. **North Anna LER 338/90-08** A design error was discovered where the service water system pressure exceeded the design values for the anchored piping supports on the supply and return lines for the recirculation spray heat exchangers.

55. **Summer LER 395/90-09** It was discovered that the chilled water expansion tank instrumentation was unable to detect a loss of inventory under certain conditions. Loss of this system would adversely impact safety injection pumps and component cooling pumps.

56. **Grand Gulf LER 416/90-03** The licensee discovered a system interaction that could result in loss of both core spray systems for long term post-LOCA core cooling.

57. **Braidwood LER 457/90-04** Resistors in the governor unit of two different diesels failed within weeks of each other because of thermal degradation.

58. **Wolf Creek LER 482/90-02** It was determined that Halon release in either ESF switchgear room would trip both class 1E electrical equipment air conditioning units.

59. **Callaway LER 483/90-03** Both trains of class 1E air conditioning units could have been disabled by the fire protection system. Same as Wolf Creek above.

60. **Point Beach LER 266/90-11** Low net positive suction head to containment spray pumps in the recirculation mode occurred. Caused by procedural deficiency.

61. **Point Beach LER 266/90-03** Supports in fuel oil pump house can not meet loading conditions from operating-basis earthquake.

62. **Trojan LER 344/90-14** Wall forming control room ventilation boundary would fail during a seismic event.

Discussion

The Office for Analysis and Evaluation of Operational Data published the enclosed reports, "Insights from Common-Mode Failure Events," AEOD/E92-02, and Supplement 1. The staff reviewed 62 selected LERs that contained actual or potential common-cause failures. Most of these LERs occurred in 1990 and were limited to those situations judged not recoverable (in the event of a coincident accident) or not self-revealing during normal plant operation.

The intent of this work was to identify dominant corrective actions that would preclude or reduce the likelihood of common-cause failures at operating nuclear power plants. Each of the events was reviewed against a set of corrective actions. No unique corrective action can minimize all the potential causes of common-cause failures. Taking all the events together, using equipment with larger design margins had the highest potential impact, about 56 percent of the situations examined in this study. Performing comprehensive systems tests, insuring adequate train separation, and the use of diverse equipment each had a potential impact on about 27 percent of the cases. The use of staggered surveillance testing impacted 20 percent of the events. The effectiveness or practicality of applying any of these corrective actions to all important safety components or systems at operating plants was not explored.

It was noted that about two-thirds of the events were related to design, fabrication, and installation errors which go undetected for long periods of time. The dominant corrective action for these situations was using equipment with larger design margins. The remaining one-third of the events was associated with maintenance deficiencies, either preventive or corrective. The dominant corrective action for these maintenance related events was staggered surveillance testing.

Sixteen of the events reviewed were identified as precursors by the accident sequence precursor program and thus exemplify the importance of this issue. Furthermore, common-cause failure has been cited as a major uncertainty in probabilistic risk assessments of nuclear power plants.

No written response to this notice is required. If you have any questions regarding this matter, please contact the Regional Administrator of the appropriate NRC Regional Office.

Technical Contact: S. Israel, AEOD
(301) 492-4437