DRAFT 8/19/82

Conf-820802--23-Draft

RELIABILITY OF THE EMERGENCY AC-POWER SYSTEM AT NUCLEAR POWER PLANTS

CONF-820802--23 DRAFT

DE82 022336

R. E. Battle

Oak Ridge National Laboratory
Oak Ridge, Tennessee 37830, USA

D. J. Campbell

JBF Associates, Inc.
Knoxville, Tennessee 37919, USA

P. W. Baranowsky

Nuclear Regulatory Commission
Rockville, Maryland 20852, USA

ABSTRACT

The reliability of the emergency ac-power systems typical of several nuclear power plants was estimated, the costs of several possible improvements was estimated. Fault trees were constructed based on a detailed design review of the emergency ac-power systems of 18 nuclear plants. The failure probabilities used in the fault trees were calculated from extensive historical data collected from Licensee Event Reports (LERs) and from operating experience information obtained from nuclear plant licensees. It was found that there are not one or two improvements that can be made at all plants to significantly increase the industry-average emergency ac-power-system reliability, but the improvements are varied and plant-specific. Estimates of the improvements in reliability and the associated cost are estimated using plant-specific designs and failure probabilities.

*Research sponsored by the Office of Regulatory Research, U.S. Nuclear Regulatory Commission, under Interagency Agreement No. 40-544-75 with the U.S. Department of Energy under contract No. W-7405-eng-26 with Union Carbide Corporation.

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.

INTRODUCTION

NRC identified station blackout, the loss of all ac power at a nuclear plant, as a generic safety issue because of the frequency of ac power systems failures and because of the reactor core damage and radioactivity release that could result. The purpose of this study is to estimate the reliabilities of representative onsite power systems and to estimate the costs of improvements for the NRC's use to resolve this generic safety issue.

The generic safety issue of station blackout was divided into three separate tasks: offsite power system reliability,[1] onsite power system reliability,[2] and accident sequence after a station blackout.[3] This paper summarizes the results of the onsite power system reliability analysis.

SCOPE

The scope of the onsite ac power system analysis was to (1) select a number of plants that are representative of ac power system designs used in the nuclear industry, (2) gather detailed historical data, and (3) perform a reliability analysis.

Five generic diesel generator configurations and eighteen representative plants were selected for detailed design review. These 18 plants were selected to be representative not only of diesel configuration, but also diesel age, vendor, and size, reactor vendor, and plant architect-engineer.

The data were collected for 1976 through 1980 from Licensee Event Reports (LERs) and responses to station blackout, NUREG/CR-0660, and NUREG-0737 questionnaires. Each event was categorized by failure type. Detailed historical data were used to calculate probabilities of failure-to-start, failure-to-run, common-cause failure (CCF), scheduled maintenance unavailability and system repair. A review of diesel generator subsystem failures was performed to determine failure modes and the percentage of failures caused by each subsystem.

The onsite ac power systems of the eighteen plants and five generic configurations were modeled by fault trees. A fault tree for a 1-of-2 success-logic configuration is shown in Fig. 1, and a simple block diagram of the same system is shown in Fig. 2. The fault tree analyses were quantified SUPERPOCUS computer code.[4] An expected number of station blackouts per year was calculated from the onsite power system undependability and a frequency of failure of offsite power. The undependability of the onsite system is the probability it will fail to start or continue to run for the mission. The onsite system undependability was calculated for missions up to 30 h after a loss of onsite power, and the expected number of station blackouts was calculated for durations of 0-0.5, 0.5-8, and 8-24 h. Results of a sensitivity study were used to identify significant contributors to unreliability, and costs of improvements were estimated.

TECHNICAL APPROACH

Design Review

The configuraton of diesel generators at all of the operating plants was reviewed and tabulated. From this tabulation, five generic and eighteen plant specific success-logic configurations representative of typical onsite power system designs were constructed. The five generic success-logic configurations are the following: 1-of-2, 1-of-3, 2-of-3, 2-of-4, and 2-of-5. The success logic configuraiton is the number of diesel generators required for successful cooling of the reactor out of the number of diesels available.

Because of the potential consequences of the loss of two plant systems simultaneously, interactions with other plant systems were reviewed. The only significant interactions are with the plant service-water system, dc power sytem, and the offsite power system.

Many water-cooled engines are dependent on the plant service-water system, but air-cooled engines or engines with a dedicated water cooling system are not dependent on plant service-water. If the cooling subsystem fails, the diesel can run only a few minutes at full load before it overheats. Air-cooled diesels can continue to supply ac power even though the service-water system is unavailable.

For most nuclear plants, diesel generator control power is supplied by a plant IE (safety system) battery; a few diesel generators have batteries dedicated to control the diesel engine and the generator. However, diesel generators with dedicated batteries are not independent of a plant IE battery because control power to the generator output breaker is from plant batteries. Failure of a plant IE dc power source will cause failure of the associated diesel generator output breaker to function regardless of the presence of a dedicated diesel battery.

At some plants there is a potential interaction between the onsite and offsite power systems through the dc system. Such an interaction occurred at Millstone 2 when loss of the "A" battery resulted in the loss of switchyard breaker control power and loss of a diesel generator. Loss of the "A" battery resulted in loss of dc control power to one diesel generator and to breakers in the onsite and offsite power systems.

Operating Experience Review

There were 1522 diesel generator events categorized for the years 1976-1980, of which 813 were LERs and the remainder were from other sources, mostly NUREG-0737 questionnaire responses. There were 418 primary and secondary failures, 85 autostart failures, and 1019 nonfailures. Primary failure is an intrinsic or end-of-life failure, and secondary failure is an extrinsic or externally caused failure. the definitions of failure, autostart failure, and nonfailure follow:

Failure: A test or emergency demand during which the diesel generator did not or would not, if offsite ac power were lost, supply sufficient ac power to the emergency bus.

Autostart failure: An event that would be a failure except that power is restored to the emergency bus within a few minutes by operator action.

Nonfailure: All events that were not primary, secondary, or autostart failures.

The average probability of failure to start was calculated from a standby failure rate, as shown in Eq. 1.

$$P_{av} = \lambda T/2 \qquad (1)$$

where P_{av} is the average probability of failure to start, λ is the standby failure rate, and T is the technical specification test interval. An industry-average value of the probability of failure to start is 0.025. This was used in all of the generic studies, but plant specific values were used to estimate the plant specific failure probabilities.

The average probability of diesel failure on demand was also calculated for tests, losses of offsite power, and other automatic starts not for testing. These data and results are presented in Table I. The average probability of failure on demand, 0.019, is less than the average standby failure probability, 0.025. For a diesel that has a lot of starts unevenly spaced throughout the year, which is the case for many diesels, the standby failure rate is more conservative than the average failure on demand. Therefore the standby failure probability was used in the reliability calculations.

There is little data for failure to run for long periods of time because most diesel generator tests are for 1 h, but there have been periodic or special tests that last longer than 1 h. The rate of failure to run was calculated from tests that were scheduled to last longer than 6 h. The number of failures that occurred during these tests was divided by the cumulative run-time. There were 314 tests scheduled, 9 failures, and 3754 h of run-time. The failure rate is 2.4×10^{-3} failures/h. This value was used in all of the reliability calculations.

There were 59 human-error events that caused or had the potential to cause simultaneous unavailability of two or more diesel generators. Maintenance errors caused all but one of these events. Therefore diesel generator maintenance procedures of several plants were reviewed to determine how they might to contributing to human error. The procedures were graded and separated into three categories based on guidelines such as the details in checklists, test after maintenance, checks for return to normal after tests, and the clarity of the procedures. Procedures in caregory I were the best and those in III the worst. Procedures from 35 plants were evaluated. Nine were in category I, 16 in category II, and 10 were in category III.

The BFR computer code[6] was used to calculate human-error failure rates. The group of plants in categories I and II had lower human-error failure rates than those in category III. This correlation indicates that procedure quality affects the human error CCF rate. In addition to a CCF failure rate attributed to procedures, there is a generic human-error failure rate to which all plants are subject. The human-error failure rate used in this reliability study is the sum of the generic rate and the specific rate assigned for the quality of the procedures. The range of human-error CCF is in Table II. Diesel configuration also affects the human error CCF rate.

There were 12 events that caused or had significant potential to cause a CCF attributed to hardware. These events were classified into six failure modes of which two are applicable to all plants and four to specific groups of plants. The two generic failure modes to which all plants are susceptive are fuel blockage or extreme room temperature. The four plant specific failure modes are the following: (1) water in the fuel system, (2) lack of effective corrosion inhibitor in the engine jacket-water, (3) service-water system blockage, and (4) loss of air-start air pressure through interconnecting lines.

The BFR computer code was used to calculate a failure rate for each of these six categories. A CCF rate attributed to hardware is calculated by adding the generic rate to those of each failure mode applicable to a specific plant. Diesel configurations also affects the hardware CCF rate. The range of hardware CCF probabilities is shown in Table II.

The generic estimate of a mean-time-to-repair (MTTR) is the average of the repair times for primary and secondary failures. Plant specific values are used for the 18 plants studied in detail. Of the 418 primary and secondary failures, repair times were reported for 312. The mean is 36h and the standard deviation 135h. The median is 8h. Distribution of these repair times is shown in Fig. 3.

Unavailability of diesel generators because of scheduled maintenance during reactor operation contributes to onsite system unreliability. The average unavailability of a diesel is 0.006. When this average is used, it contributes insignificantly to the onsite system unreliability. However, extensive scheduled maintenance, including overhauls, performed during reactor operation at some plants contributes significantly to unreliability. There were three diesels unavailable during losses of offsite power, as shown in Table I, but all three occurred while the reactors were shut down.

Failure probabilities for dc systems,[7] plant service water systems,[3] and offsite power systems[1] were obtained from other reports. The failure probabilities for these systems are given in Table II.

Reliability Analysis

The results of a sensitivity analysis for specific plants are given in Table III. Plant specific cases are analyzed rather than generic cases because increased reliability will be plant-by-plant. The changes in the failure probabilities are to realistic probabilities that have been achieved by some operating plants. The decrease in the initial unavailability for most changes is approximately 2; there are no feasible changes that will decrease the onsite unavailability by a factor of 10,

Cost of Onsite System Improvements

The costs of several methods to improve the onsite system are presented below. Possible improvements must be evaluated for each plant. Only the direct costs of the modifications are estimated. Indirect costs, such as the cost of additional reactor downtime, may add as much as $500,000 per day.

Independent diesel failure probability cannot be significantly reduced for the nuclear industry, but plants with independent failure probabilities much higher than average may achieve a significant reduction in independent failure probability and system unavailability. Several methods to reduce the independent failure probability and the associated costs are as follows: install air dryers on the air-start system, $100,000 per diesel; install gaskets on relay cabinets, $10,000 per diesel; periodic overhaul of the governors, $6000 per diesel.

Improving maintenance procedures will reduce human-error CCF probability. The cost of rewriting a maintenance procedure is approximately $5000 per procedure.

Three hardware modifications that will reduce CCF probability are the following: install a drain on the bottom of the fuel day tank, $10,000 per diesel; remove connections between independent air-start systems, $5000 per diesel; add an effective corrosion inhibitor to the diesel engine jacket-water, $500 per diesel per year.

Scheduled maintenance during reactor operation contributes to onsite system unreliability. Some plants do not schedule diesel generator downtime during reactor operation while others have scheduled maintenance unavailability equal to six times the industry-average. The cost of deferring scheduled maintenance may be the expense of hiring additional maintenance staff. Also, deferring scheduled maintenance may increase the independent failure probability. Because of these factors, scheduling of maintenance has to be evaluated on a plant specific basis. Service water cooled diesel generator reliability is significantly reduced because of the plant service water failure probability and T&M unavailability. However, costs are not included for two reasons: (1) modifications to change a diesel from water-cooled to air-cooled would be very difficult, and an improvement in reliability would not be certain; and (2) suggestions to modify the service water system are not within the scope of this study.

RESULTS AND CONCLUSIONS

The onsite system reliability will have to be improved plant-by-plant rather than by generic improvements. Therefore, the frequency of station blackout and the undependability of the onsite power system was estimated for several designs using plant specific data. The important contributors to onsite power system undependability was found to be plant specific. Independent diesel generator failure was the important contributor for most of the 18 plants modeled. Other important contributors were common-cause failure because of hardware failure or human-error, unavailability because of scheduled maintenance, and cooling subsystem undependability. A sensitivity analysis of several specific plants was performed to quantify the increases in reliability that can be attained for several possible improvements. The costs for some of these improvements was estimated.

Reduction of the industry-average independent diesel generator failure probability will be small because there are no dominant failure modes. Three failure modes, which caused ~17% of all diesel generator failures, are dirt and moisture on relays and switches, contaminated oil in the governor and governor setpoint error, and moisture in the air-start system. Contribution to failure by these failure modes may be reduced by improved design and maintenance. Some diesels may have a failure mode that is causing a large number of failures for that diesel. If this failure mode were reduced, the onsite system unavailability may be reduced significantly.

Common-cause failure for some plants is a significant contributor to onsite system unreliability. Diesel generator CCF potential is increased by the following design features: no drain from the bottom of the fuel day tank; inadequate corrosion inhibitor in jacket-water; and connections between independent air-start systems.

Human-error contribution to CCF is also significant. Maintenance and test procedures that are difficult to understand, do not include review of maintenance, and do not include a verification test after maintenance, contribute to the probability of CCF by human-error.

Scheduled maintenance at a few plants is a significant contributor to onsite system unavailability. Rescheduling preventive maintenance should be carefully evaluated to determine if the onsite system unavailability can be reduced.

There is also potential for increasing diesel generator reliability by improving the service-water system availability.

REFERENCES

1. F. H. Clark, "Loss of Offsite Power at Nuclear Power Plants," (to be published as a NUREG/CR report).

2. R. E. Battle and D. J. Campbell, "Reliability of Emergency AC Power Systems at Nuclear Power Plants," (to be published as NUREG/CR report).

3. A. M. Kolaczkowski and A. C. Payne, "Station Blackout Accident Analyses," (to be published as a NUREG/CR report).

4. Millstone 2, NRC Docket No. 50-336, LER 81-005, Event date 1/2/81.

5. C. L. Atwood and W. J. Suitt, "User's Guide to BFR, A Computer Code Based on the Binomial Failure Rate Common Cause Model," EGG-EA-5502, Idaho National Engineering Laboratory (   ).

6. P. W. Baranowsky, A. M. Kolaczkowski, and M. A. Fedele, "A Probabilistic Analysis of DC Power Supply Requirements for Nuclear Power Plants," NUREG-0666 (1981).

Table I. Comparison of test and emergency start demand data

Category	Demands	No. of primary and secondary failures on demand	Probability of primary or secondary failure on demand	No. of autostart failures on demand	Probability of autostart failure on on demand	No. of DGs unavailable for T&M	T&M unavailability
Test	13,665	253	0.019	55	0.004	—	0.006
Loss of offsite power	78	2	0.026	2	0.026	3	0.038
All actual demands	539	14	0.026	5	0.009	3	0.006

Table II. Probability or frequency of basic events in failures

Basic event description	Range of plant specific initial unavailability or frequency		
	Low	Average	High
Diesel Generator			
Independent failure	8.2×10^{-3}	2.5×10^{-2}	1×10^{-1}
CCF attributed to hardware	3.6×10^{-5}	4.0×10^{-4}	1.18×10^{-3}
CCF attributed to human-error	7.2×10^{-5}	7.8×10^{-4}	3.7×10^{-3}
T&M	1×10^{-5}	6×10^{-3}	4.5×10^{-2}
DC Power System			
Independent failure	1×10^{-5}	1×10^{-4}	1×10^{-3}
CCF	1×10^{-6}	1×10^{-5}	1×10^{-4}
Service Water			
Independent failure	2×10^{-4}	2×10^{-3}	2×10^{-2}
CCF	8×10^{-6}	8×10^{-5}	8×10^{-4}
T&M	1×10^{-4}	2×10^{-3}	4×10^{-2}
Offsite Power			
Plant centered losses	9.2×10^{-2}/y	2.5×10^{-1}/y	
Area wide storms	1.3×10^{-2}/y	2.7×10^{-1}/y	
Area wide blackouts	1.3×10^{-2}/y	2.4×10^{-1}/y	

Table III. Onsite system sensitivity analysis

Basic event plant, and success logic	Basic event failure probability changed		Onsite system unavailability changed	
	From	To	From	To
Independent failure				
Plant A, 2-of-3	8.2×10^{-2}	4.1×10^{-2}	4.8×10^{-2}	3.1×10^{-2}
Plant B, 1-of-2	5.9×10^{-2}	3.0×10^{-2}	4.2×10^{-3}	2.1×10^{-3}
Hardware CCF				
Plant C, 2-of-5	1.8×10^{-3}	8.6×10^{-5}	2.5×10^{-3}	0.8×10^{-3}
Plant D, 1-of-3	6.0×10^{-4}	2.4×10^{-5}	7.2×10^{-4}	1.5×10^{-4}
Human-error CCF				
Plant E, 1-of-2	8.8×10^{-4}	3.4×10^{-4}	1.5×10^{-3}	1.0×10^{-3}
T&M unavailability				
Plant F, 2-of-3	4.5×10^{-2}	0	4.8×10^{-2}	2.5×10^{-2}

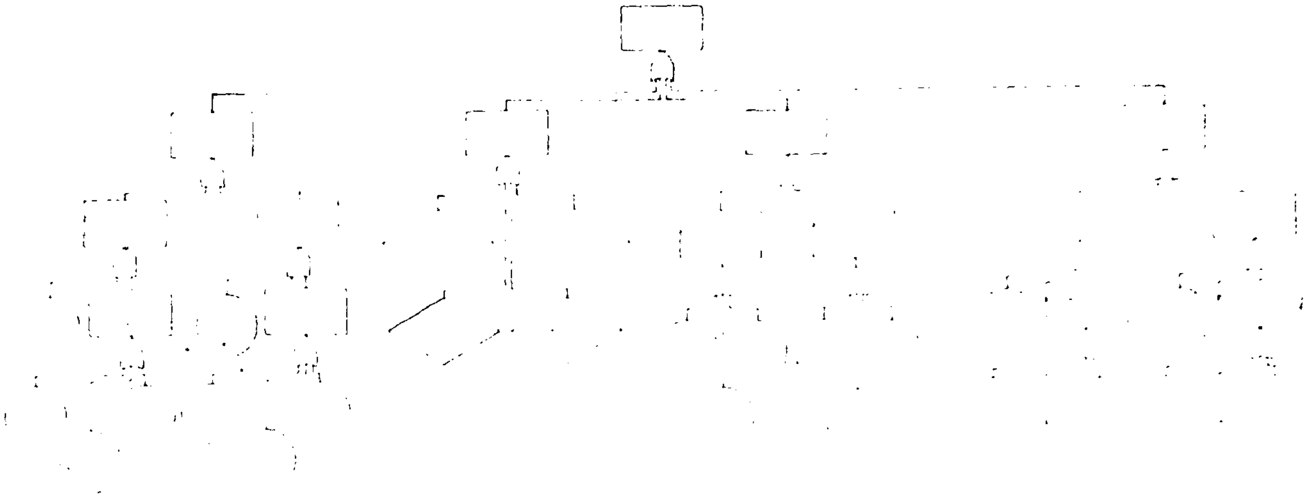

Fig 1. Fault tree for 1-of-2 success logic.

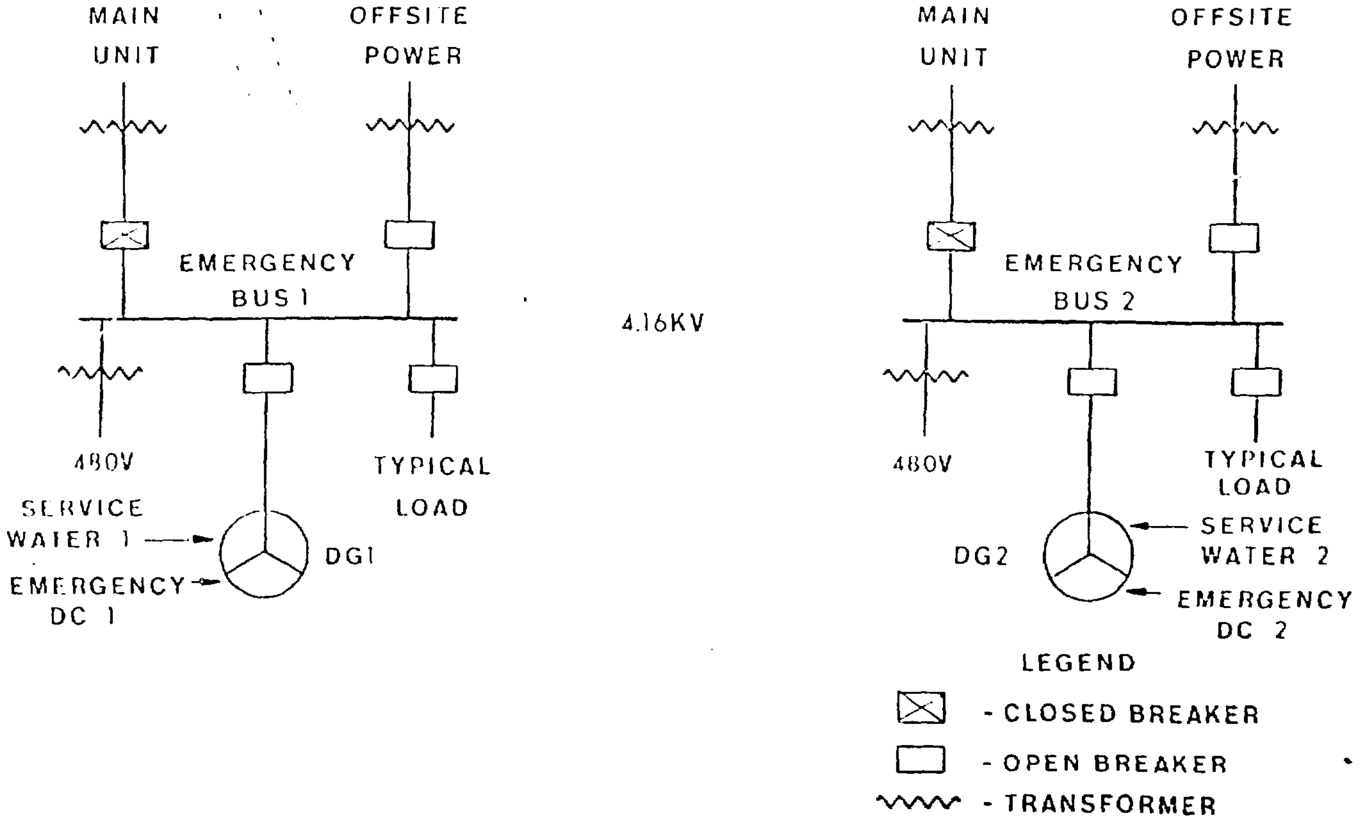

Fig 2. Typical emergency ac power system