INEEL/CON-99-00375
PREPRINT

IDAHO NATIONAL ENGINEERING & ENVIRONMENTAL LABORATORY

General Electric Reactor Protection System Unavailability, 1984 – 1995

S. A. Eide (INEEL)
M. B. Calley (INEEL)
C. D. Gentillon (INEEL)
T. Wierman (INEEL)
H. Hamzehee (USNRC)
D. Rasmuson (USNRC)

August 22, 1999 – August 25, 1999

PSA '99

GENERAL ELECTRIC REACTOR PROTECTION SYSTEM UNAVAILABILITY, 1984 – 1995

Steven Eide, Michael Calley, Cindy Gentillon, and Thomas Wierman
Idaho National Engineering and Environmental Laboratory
P.O. Box 1625
Idaho Falls, ID 83415
(208) 526-3797

Hossein Hamzehee and Dale Rasmuson

U.S. Nuclear Regulatory Commission
11545 Rockville Pike
Rockville, MD 20852
(301) 415-6228

ABSTRACT

An analysis was performed of the safety-related performance of the reactor protection system (RPS) at U.S. General Electric commercial reactors during the period 1984 through 1995. RPS operational data were collected from the Nuclear Plant Reliability Data System and Licensee Event Reports. A risk-based analysis was performed on the data to estimate the observed unavailability of the RPS, based on a fault tree model of the system. Results were compared with existing unavailability estimates from Individual Plant Examinations and other reports.

I. INTRODUCTION

Operational experience of the U.S. General Electric RPS from 1984 through 1995 was studied and documented in the report *Reliability Study: General Electric Reactor Protection System, 1984 - 1995.*[1] The analysis focused on the ability of the RPS to automatically shut down the reactor given a plant upset condition requiring a reactor trip while the plant is at full power. RPS spurious reactor trips or component failures not affecting the automatic shutdown function were not considered. Systems added as part of the anticipated transient without scram (ATWS) mitigation effort were not included in the analysis.

The General Electric RPS is a complex control system comprising numerous electronic components that combine to provide the ability to produce an automatic or manual rapid shutdown of the nuclear reactor, known as a reactor trip or scram. In spite of its complexity, the General Electric RPS can be roughly divided into four segments – channels, trip system, hydraulic control units (HCUs) and related components, and rods – as shown in Figure 1. The rods segment includes the control rods and associated control rod drives (CRDs). General Electric RPSs typically have 120 to 190 control rods and associated CRDs. The HCU segment includes the HCU components: scram pilot solenoid-operated valves (SOVs), scram inlet and outlet air-operated valves (AOVs), and scram accumulator. There is one HCU for each control rod and CRD combination. The HCU segment also includes the scram discharge volume (SDV) and two backup scram SOVs controlling instrument air to the scram air header. For the trip system, all but one of the General Electric plants have relay-based trip systems. Clinton, a boiling water reactor 6 (BWR/6) design, is the only General Electric plant to have a solid-state trip system. Finally, all of the designs have four channels.

RPS Segments			
Channels	Trip System	HCU and Related Components	Rods
4 channels (A – D, sometimes termed A1, A2, B1, and B2)	2 trip systems (A and B), relay-based or solid state; scram logic and backup scram logic	120 to 190 HCUs, 1 or 2 SDVs	120 to 190 CRDs and associated control rods

Figure 1. Segments of General Electric RPS.

The analysis of the General Electric RPS was based on the Peach Bottom 2 plant design, which is a BWR/4 design. This configuration is representative of the General Electric plant designs except for Clinton, which has a solid-state trip system. The General Electric RPS includes many different types of trip signals. The trip signals include various neutron flux indications, reactor pressure and level, primary containment pressure, and others. For this study, two of the trip signals were modeled: reactor vessel high pressure and low water level.

The trip system portion of the RPS includes two systems or trains, A and B. Channels A and C feed into trip system A, and channels B and D feed into trip system B. A scram signal is generated if one of two channel sensors associated with each of the two trip systems detects a scram condition. This is termed a one-out-of-two-twice logic. Given a scram signal, the two SOVs in each HCU cut off the air supply to the scram inlet and outlet valves, causing them to open. (The air supply to all the HCUs is also cut off through the backup scram logic, which opens backup scram SOVs that control the air supply to the air header.) This allows the CRD to drive the control rod up into the core. In order for the control rod to insert into the core, drive water is drained into the SDV. For the RPS to fail, one of the trip systems and the backup scram system must fail, a sufficient number of channel failures must occur, or a sufficient number of control rods must fail to insert. Since only two diverse trip signals were modeled, 1 of 2 channels for each trip system for each of the two trip signals must fail. It was assumed that 33% or more of the 185 Peach Bottom 2 control rods must fail to fully insert (in a random pattern). A sensitivity study was conducted to determine the impact on RPS unavailability from this assumption.

Testing of the General Electric RPS can be summarized by RPS segment (Figure 1). Generally, the RPS channels are functionally tested every three months, with the channel being placed in a bypass condition during the test. Weekly manual scram (or automatic actuator) tests cover the trip system logic. The HCUs, control rods, and associated CRDs are tested every refueling or 18 months. Also, 10% of these are tested every four months while the plant is at power.

II. SYSTEM FAULT TREE

A system fault tree was constructed for the Peach Bottom 2 (BWR/4) RPS design. The level of detail in the fault tree includes sensor/transmitters, trip units and switches, relays, SOVs, AOVs, scram accumulators, control rods and CRDs, and the SDV. As noted previously, two trip signals were included in the fault tree, even though at least three signals are typically generated for plant upset conditions. A sensitivity study was conducted to determine the impact on RPS unavailability if three trip signals had been modeled.

Common-cause failures (CCFs) across similar components were explicitly modeled in the RPS fault tree. In general, CCF events were defined to involve sufficient failures of the component type to fail the RPS. Lower-order CCF events, which must be combined with random component failures to cause an RPS failure, were not included in the fault tree. Results of the fault tree quantification were reviewed to ensure that the exclusion of lower-order CCF events did not significantly impact the results.

Test and maintenance outages and associated RPS configurations were modeled for channel outages. For channel outages, the channel was assumed to be placed into a bypass condition, rather than a tripped mode.

The Peach Bottom 2 (BWR/4) RPS fault tree model included approximately 70 basic events, of which approximately 20 were CCF events. Approximately 4,000 cut sets were generated when the fault tree model was solved using the SAPHIRE computer code. [2]

III. DATA REVIEW AND ANALYSIS

U.S. General Electric RPS performance during the period 1984 through 1995 was assessed by reviewing Licensee Event Reports and the Nuclear Plant Reliability Data System (NPRDS) reports. Thirty-four U.S. General Electric nuclear power plants were covered in the study. Approximately 7,000 reports were identified. Of these 7,000, approximately 600 involved actual component failures (independent or CCF) applicable to this study.

The data review process involved at least two independent reviews of each event report by knowledgeable engineers. Each event was characterized by safety function impact (fail-safe, non-fail-safe, or unknown) and degree of failure (complete failure, no failure, or unknown). This resulted in a three-by-three matrix, with nine different bins into which an event could be placed, as indicated in Figure 2. This classification scheme resulted in one bin with non-fail-safe, complete failures of components. Three other bins may also contain such events, but lack of information from the event report did not allow the analysts to determine whether the events were non-fail-safe, complete failures.

	Safety Function Impact		
	Non-fail-safe, complete failure [a]	Unknown safety function impact, complete failure [b]	Fail-safe, complete failure [c]
Failure Complete-ness	Non-fail-safe, unknown complete-ness [b]	Unknown safety function impact, unknown completeness [b]	Fail-safe, unknown complete-ness [c]
	Non-fail-safe, no failure [c]	Unknown safety function impact, no failure [c]	Fail-safe, no failure [c]

a. Events in this bin receive weights of 1.0.
b. Events in these bins receive weights of <1.0.
c. Events in these bins are not applicable.

Figure 2. Data classification scheme.

The data analysis considered events from these four bins (shaded bins in Figure 2), using a weighting scheme to account for the uncertainty in the unknown events.

Data analysis for the component failures involved several steps:

1. Demand count and exposure time estimation
2. Statistical analysis of data subgroups to identify differences
3. Component unavailability estimation
4. CCF event unavailability estimation
5. Trending with time evaluation.

The component demand counts were estimated from plant scram histories (for those components demanded by a scram), and testing intervals (generally weekly, every three months, or every 18 months).

Statistical analysis of data subgroups was performed to identify differences in component performance resulting from plant mode (at power or shutdown), time period (1984 – 1989 versus 1990 – 1995), or type of demand (scram or test). The data from the selected data subgroup were then analyzed to determine component failure probabilities or rates.

Results of the data analysis to determine component failure probabilities or rates are presented in Figure 3. The numbers of component failures listed in Figure 3 are generally subsets of the total number of failures identified in the data review. For example, if the data subgroup analysis indicated a significant difference in component performance between 1984 – 1989 and 1990 – 1995, then only the 1990 – 1995 data were used. In general, the resultant component failure probabilities and rates are comparable with existing estimates.[3 through 5]

Quantification of the CCF events in the fault tree was performed using the alpha factor method outlined in the report *Common-Cause Failure Database and Analysis System: Event Definition and Classification*.[6] Only CCF events associated with the General Electric RPS during the period 1984 through 1995 were used in the quantification process. Several steps were required in the overall CCF evaluation:

1. Characterization of CCF data (component group size, impact vector, shared cause and timing factors, and failure completeness factor)
2. Characterization of CCF events modeled in the fault trees (component group size and required number of component failures)
3. Development of alpha factor equations for each of the CCF events modeled
4. Development of an appropriate prior for the alpha factors
5. Mapping up or down of CCF data to match the component group sizes modeled in the fault trees
6. Quantification of CCF event probabilities using component-specific CCF data and the prior.

Selected results of the CCF event quantification process are presented in Figure 4. In general, the CCF event probabilities reflect multipliers (from the alpha factor equations) of 0.002 to 0.09 on the component failure probabilities. These multipliers are influenced by the specific failure criterion (minimum number of component failures required and size of component group), strength of the component-specific CCF data, and the prior distribution for the alpha factors obtained from the General Electric CCF data. In general, there were very few complete CCF events (where all the components in the group fail due to a common cause). Also, there were no complete CCF events in the higher-order group sizes.

Trending analysis over time was performed for the component failure probabilities and the number of CCF events. None of the 11 component types exhibited significant increasing or decreasing trends over time with respect to failure probabilities.

The number of CCF events reported each year dropped over the period 1984 – 1995. This is the result of two component types exhibiting decreasing trends over time. The remaining nine exhibited no trends. Therefore, none of the component types exhibited increasing numbers of CCF events over time. Most of the component trends (or lack of trends) were supported by a limited number of CCF events.

IV. RESULTS

The General Electric RPS fault tree was quantified using the basic event data presented in Figures 3 and 4. The resultant RPS mean unavailability (failure probability upon demand) is 5.8E-6, assuming no credit for operator action. This result is for the Peach Bottom 2 (BWR/4) RPS design, which is considered to be representative of most BWRs. If credit is taken for the operator to actuate the manual scram switch, then the mean unavailability drops to 2.6E-6. Dominant failures involve CCFs of the HCU and backup scram SOVs, channel trip units (bistables), control rods and CRDs, trip system contactor relays, and channel relays. CCF events contribute over 99% to the RPS unavailability.

The General Electric RPS unavailability results can be broken down into contributions by each of the four segments. These breakdowns are presented in Figure 5.

Component Type	Number of Failures [a]	Number of Demands or Hours	Failure Probability or Rate [b]	Basic Event Description
HCU accumulator	1 (0.5)	43883	2.2E-5	HCU accumulator fails to discharge upon demand to assist the control rods to insert into the core
HCU scram inlet or outlet AOV	1 (1.0)	522306	2.9E-6	HCU scram inlet or outlet AOV fails to open upon demand
Trip unit (bistable)	7 (4.0)	15026	2.9E-4	Channel trip unit (bistable) bails to trip at its setpoint
Level sensor/ transmitter	10 (4.9)	6750	7.7E-4	Channel reactor vessel level sensor/transmitter fails to detect a low level and send a signal to the trip unit
Pressure sensor/ transmitter	0 (0.0)	8753	5.7E-5	Channel reactor vessel pressure sensor/ transmitter fails to detect a high pressure and send a signal to the trip unit
Manual scram switch	0 (0.0)	38469	1.3E-5	Manual scram switch fails to operate upon demand
Control rod and associated CRD	6 (2.7)	62365	5.0E-5	Control rod or associated CRD fails to insert fully into core upon demand
Level switch	4 (3.3)	6075	6.1E-4	Channel (SDV high level) process switch fails to detect a high level and send an appropriate signal to the relay
HCU scram pilot SOV or backup scram SOV	84 (50.1)	77845	7.0E-4	HCU scram pilot SOV (or backup scram SOV) fails to cut off and vent air supply to AOVs
Relay	13 (10.8)	579677	1.9E-5	Channel or trip system relay fails to de-energize upon demand

a. Includes uncertain events and CCF events. The number in parentheses is the weighted average number of failures, resulting from the inclusion of uncertain events in Figure 2 (shaded bins).
b. The failure probability or rate calculation involves a complex simulation process to account for potential non-fail-safe, complete failure events (the three bins in Figure 2 with the "b" footnote). However, the probability can be approximated by the expression (n+0.5)/(D+1), where n is the weighted number of failures (in parentheses in column 2) and D is the number of demands. The failure rate can be approximated by the expression (n+0.5)/T, where T is the time in hours.

Figure 3. General Electric RPS component failure probabilities.

Component Type	Number of CCF Events	Component Failure Probability	CCF Event Probability	CCF Event Description
HCU accumulator	3	2.2E-5	1.1E-7	CCF 33% or more of 185 HCU accumulators fail
HCU scram inlet or outlet AOV	2	2.9E-6	6.9E-9	CCF 33% or more of 370 HCU scram inlet/outlet AOVs fail to open
Trip unit (bistable)	4	2.9E-4	3.1E-6	CCF specific 4 or more of 8 channel bistables
Level sensor/ transmitter	16	7.7E-4	7.1E-5	CCF specific 2 or more of 4 level sensor/transmitters
Pressure sensor/ transmitter	2	5.7E-5	4.9E-6	CCF specific 2 or more of 4 pressure sensor/transmitters
Manual scram switch	0	1.3E-5	7.7E-7	CCF of 2 of 2 manual scram switches
SDV level switch	0	6.1E-4	3.1E-5	CCF specific 2 or more of 4 SDV level switches
Control rod and associated CRD	22	5.0E-5	2.5E-7	CCF 33% or more of 185 control rod/CRDs
HCU scram pilot and backup scram SOV	21	7.0E-4	1.7E-6	CCF 33% or more of 370 HCU scram pilot SOVs and 2 of 2 backup scram SOVs
Relay	11	1.9E-5	3.8E-7	CCF specific 4 or more of 8 trip system relays

Figure 4. Selected General Electric RPS CCF event probabilities.

	RPS Unavailability	
RPS Segment	No Credit for Manual Scram by Operator	Credit for Manual Scram by Operator
Channel	3.4E-6 (58%)	1.4E-7 (5%)
HCU and related	1.9E-6 (32%)	1.9E-6 (71%)
Trip system	3.8E-7 (6%)	3.8E-7 (14%)
Rod	2.5E-7 (4%)	2.5E-7 (10%)
Total RPS	5.8E06	2.6E-6

Figure 5. General Electric RPS unavailability by segment.

Channel CCF failures dominate, contributing 58.0% to the total. However, this drops to only 5% of the total if credit is taken for manual scram by the operator. HCU related CCF failures contribute 32%. However, this increases to 71% if credit is taken for manual scram. The trip system contributes 6%, while the rod/CRDs contribute 4%.

Finally, uncertainty results are presented in Figure 6. These uncertainty results incorporate only data uncertainties. They do not include any modeling uncertainties. Sensitivity studies were conducted to address certain modeling issues, such as the failure criterion for control rod/CRDs, use of two rather than three reactor trip signals in the fault tree, and others. In general, the sensitivity studies indicated that the data uncertainty results cover most of the modeling uncertainties. However, the choice of prior distribution for the alpha factors in the CCF calculations can significantly impact the RPS unavailability results.

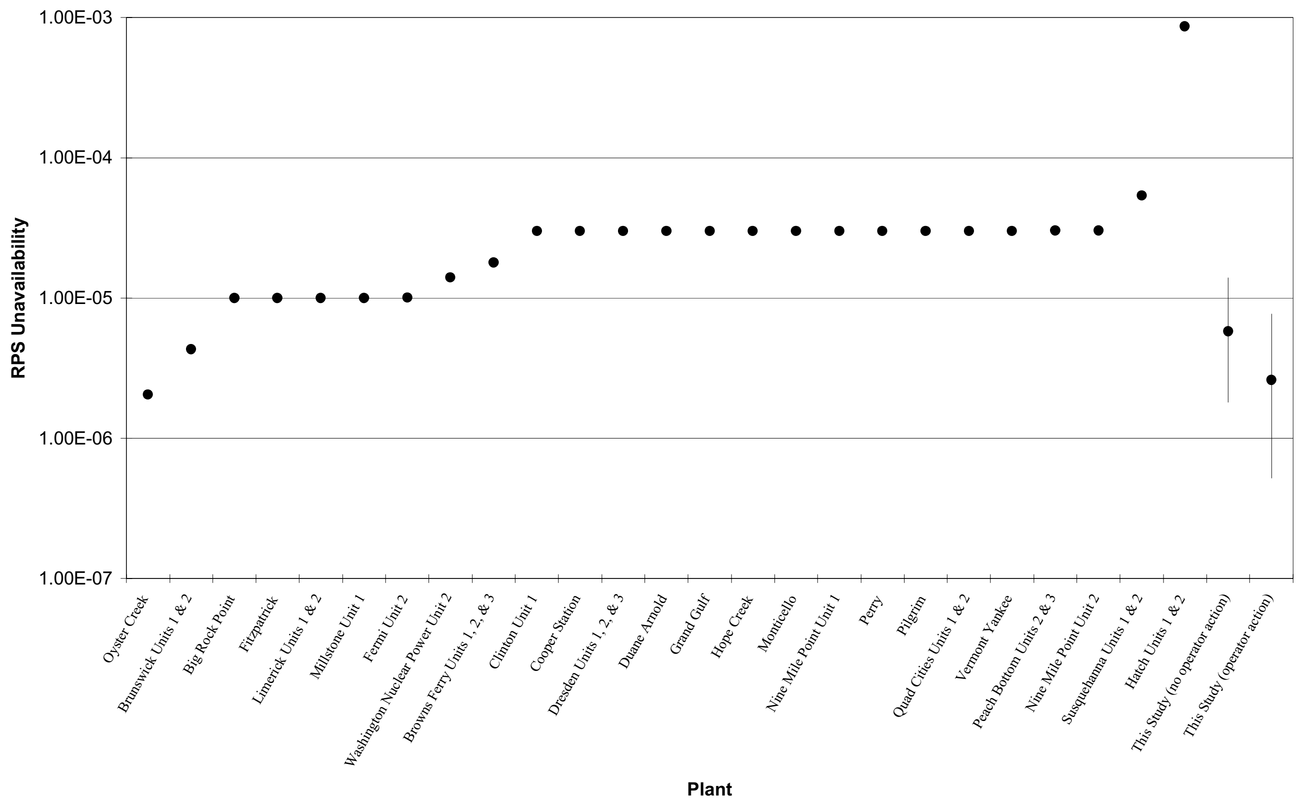
The General Electric RPS unavailabilities obtained from the 1984 – 1995 data are compared with Individual Plant Examination (IPE) estimates in Figure 7. The IPE RPS estimates range from approximately 1.0E-6 to 1.0E-3. Because of the lack of detailed information in the IPE submittals, it is not clear which estimates included credit for operator action. The uncertainty ranges obtained in this study do not cover most of the IPE range of RPS unavailabilities. The RPS results obtained from this study are generally significantly lower than many of the IPE RPS unavailability estimates.

	Unavailability			
RPS Case	5^{th} Percen-tile	Median	Mean	95^{th} Percen-tile
No manual scram	1.8E-6	4.6E-6	5.8E-6	1.4E-5
Manual scram	5.2E-7	1.6E-6	2.6E-6	7.7E-6

Figure 6. General Electric RPS uncertainty results.

V. DISCUSSION AND INSIGHTS

CCF events contribute over 99% to the RPS unavailabilities obtained in this study. Quantification of the CCF events in the RPS fault trees is a complex process. The channel and trip system portions of the RPS fault tree contain component group sizes ranging from two to 12, while the HCU and rod portions contain group sizes of 185 and 370. Separate priors for the alpha factors were developed for the channel and trip system



Note: The ranges shown for this study are the 5th and 95th percentiles. All other data points are mean values.

Figure 7. General Electric IPE RPS unavailabilities.

component CCFs and for the HCU and rod component CCFs. These priors were based only on General Electric RPS component CCFs. The priors were then updated using CCF data specific to the component in question. In several cases the component-specific CCF data were sparse, resulting in a strong influence by the prior. However, this RPS CCF quantification is believed to be the most comprehensive and component-specific effort to date. The effort would not have been possible without the methodology outlined in the report *Common-Cause Failure Database and Analysis System: Event Definition and Classification*.

Several insights were obtained from this study:

1. CCF events involving the HCU SOVs (and backup SOVs) contribute 32% to the overall RPS unavailability. The most significant historical event, involving the use of improper seating material and affecting all of the HCU SOVs, occurred in 1984. Two similar types of SOV CCF events occurred in 1994 but did not affect as many of the components. Several events involving improper use of liquid thread sealant also caused significant CCF events. It is believed that the requirement to test 10% of the control rods each four months helped discover these problems (developing over time) before they developed into catastrophic failures.

2. The backup scram portion of the RPS may be an important contributor to the low RPS unavailability, based on sensitivity studies conducted as part of this project and uncertainties associated with the SOV failure characteristics. (Without the backup scram logic, only a specific two of eight trip system relay failures are needed to fail the RPS, rather than a specific four of eight if the backup scram system is modeled.) The backup scram SOVs are classified as non-safety-related, and these valves are not part of the NPRDS reportable scope for the General Electric RPS. Therefore, no failure data were collected for these valves. Also, it is not clear how often these valves are tested, and what their failure probabilities are. This study assumed these valves are tested every

18 months during shutdown, and that their failure characteristics are similar to the HCU SOVs. These assumptions need to be verified.

3. The trends in component failure probabilities and numbers of CCF events are generally flat over the period 1984 through 1995. Therefore, existing RPS surveillance and maintenance practices and industry lessons learned programs have been effective in preventing increasing failure probabilities.

4. There were significant SDV problems in the early 1980s involving both drainage of SDVs and level instrumentation, dominated by the 1980 Browns Ferry Unit 3 failure of 76 of 185 control rods to insert. Data collected during the period 1984 through 1995 indicate that SDV instrumentation failure probabilities are similar to other RPS trip instrumentation. Also, only one inadvertent filling of the SDV while a plant was at power was identified during the period. Finally, the RPS fault tree quantification indicates that SDV events leading to failure of the RPS contribute less than 1% to the overall RPS unavailability. Therefore, early SDV-related problems in General Electric RPSs are no longer dominant contributors to RPS unavailability.

VI. ACKNOWLEDGMENTS

This study was sponsored by the U.S. Nuclear Regulatory Commission, Office for Analysis and Evaluation of Operational Data. The authors would like to acknowledge the support and suggestions from S. Mays of the U.S. Nuclear Regulatory Commission, and D. Prawdzik and S. Conroy of the Idaho National Engineering and Environmental Laboratory for technical support. Finally, technical reviews by A. Kolaczkowski and J. Minarick of Science Applications International Corporation and A. Mosleh of the University of Maryland contributed substantially to the content and quality of the effort.

VII. REFERENCES

1. S. A. Eide et al., *Reliability Study: General Electric Reactor Protection System, 1984 – 1995*, NUREG/CR-5500, Vol. 3, U.S. Nuclear Regulatory Commission, Washington, D.C. (May 1999).

2. K. D. Russell et al., *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 5.0*, NUREG/CR-6116, Vol. 1, U.S. Nuclear Regulatory Commission, Washington, D.C. (December 1993).

3. W. P. Sullivan, *Technical Specification Improvement Analyses for BWR Reactor Protection System*, NEDC-30851P, General Electric Company (May 1985).

4. S. A. Eide et al., *Generic Component Failure Data Base for Light Water and Liquid Sodium Reactor PRAs*, EGG-SSRE-8875, Idaho National Engineering and Environmental Laboratory, Idaho Falls, ID (February 1990).

5. R. R. Fullwood et al., *ATWS: A Reappraisal Part I: An Examination and Analysis of WASH-1270, "Technical Report on ATWS for water-cooled Power Reactors,"* EPRI NP-251, Electric Power Research Institute, Palo Alto, CA (August 1976).

6. F. M. Marshall et al., *Common-Cause Failure Database and Analysis System: Event Definition and Classification*, NUREG/CR-6268, Vol. 2, U.S. Nuclear Regulatory Commission, Washington, D.C. (June 1998).