Evaluation of Service Water Pumps P-7A and P-7B Failure Rates Following Failure of Pump P-7C

1.0 Introduction

Palisades experienced failure of couplings on the P-7C service water pump on two occasions. The first occurred about 110 days after installation of couplings made of a material that was susceptible to inter-granular stress corrosion cracking (IGSCC). After replacement of the couplings with similar material, another failure occurred approximately 670 days later. Post failure analysis by Lucius Pitkin Incorporated (LPI) determined the failure mechanism and indicated that the other service water pump couplings were susceptible to similar failure mechanisms. Shortly thereafter, all service water pump couplings were replaced with a material less susceptible to IGSCC failure and testing of the couplings for the P-7A and P-7B pumps was conducted to determine their as-found condition and estimate their expected lifetime had they been allowed to run to failure.

This evaluation examines the conditions discovered by that inspection and the assessment of potential crack growth rates (CGR) for the P-7A and P-7B pump couplings. Based on the as-found condition information provided in the LPI report [1], an estimate of the degraded failure to run rate for each pump was developed. A convolution distribution for the joint probability of failure was derived from the individual pump failure to run rates. This represents the probability of failure of both pumps as a function of time since the couplings were initially installed.

Following failure of pump P-7C, the probability that the two remaining pumps would fail to run can be assessed for any particular time period by subtracting the convolution failure probability at the time of failure of P-7C and the convolution probability of failure at some time thereafter. The key time period of interest is either the repair time for the P-7C pump, or the Technical Specification (TS) allowed outage time whichever is smaller. In this case, the TS allowed outage time of 3 days was used in this evaluation even though the actual time to repair the pump was shorter. This represents a minor conservatism in the analysis that is not expected to affect the result or conclusions appreciably.

2.0 Evaluation

There are three stages to failure of a coupling due to IGSCC. These are crack initiation, crack growth to a through wall condition, and critical fracture (failure of the material). The last of these occurs rapidly compared to the other two and is conservatively assumed to occur immediately upon crack growth to a through wall state. The crack growth rate (CGR) is a constant over time once initiated, while the crack initiation rate varies over time.

As noted in the LPI report [1]:

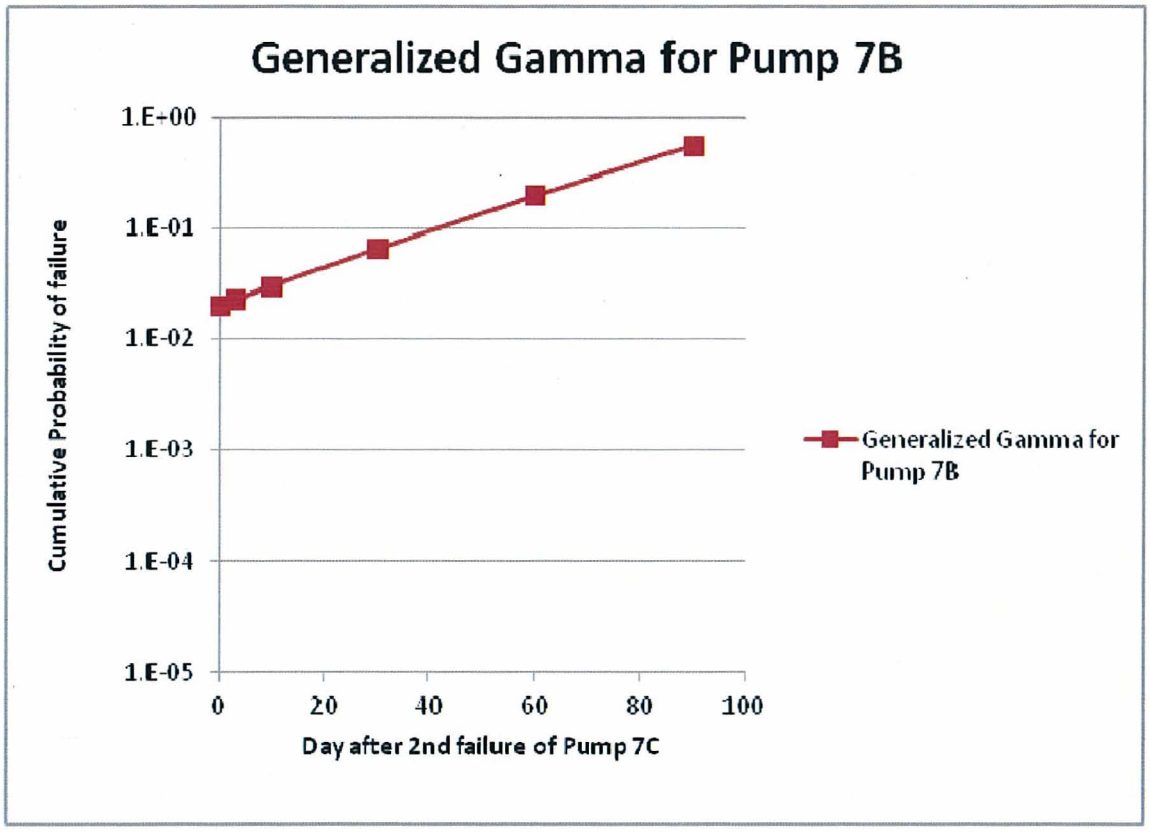
> *"The time to failure of a susceptible material in a given environment is dependent on the applied tensile stress, as can be seen in Figure 3-7 (not shown here). The plot compares applied stress or load to the logarithm of exposure time in an environment and illustrates the time to failure increases significantly with decreasing applied stress. The crack propagation time, t_{cp} is taken to be the difference between the time of failure, t_f, minus the time of initiation, t_{in}. The time at failure is typically known. However, the time of initiation is highly alloy-environment and applied stress dependant and thus is an unknown without specific test data. The initiation time is also highly dependent upon pre-existing flaws that may have been introduced during heat treatment or thread fabrication. Therefore, predicting initiation time is difficult. Unless there are preexisting flaws, a distribution of 80% initiation and 20% propagation is considered reasonable for the life of a component subject to SCC process as suggested by Figure 3-8 (not shown here)."*

To determine the expected life of the non-failed couplings due to IGSCC, three cases for the CGR were postulated in the LPI report [1] based on the P-7C pump history for the first failure (the shortest time between installation and failure which leads to the highest CGR estimation).

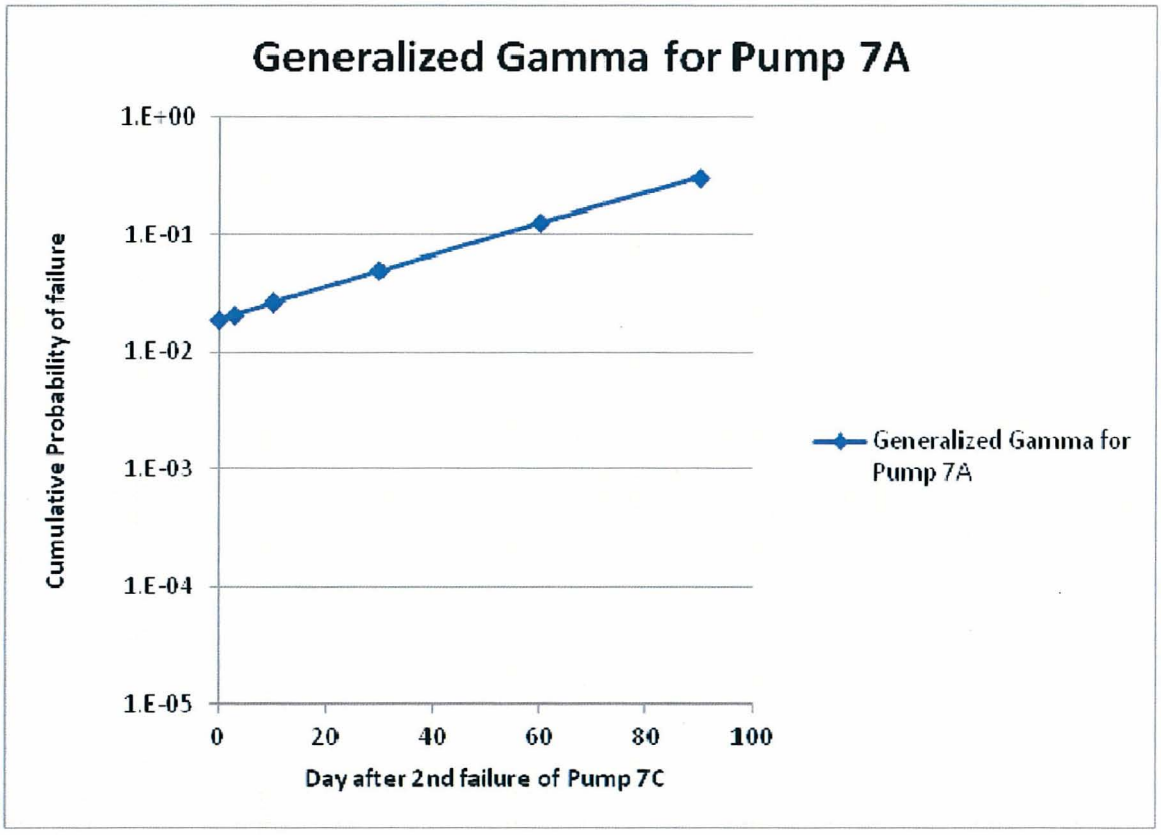
Case 1 involved using the crack growth rate based on generic data associated with crack growth rates for this type of material in distilled water (2.3E-04 in/hr). This produced an expected life of about 90 days if a crack was initiated at the time of installation. Case 2 assumes that half of the observed life of the first P-7C coupling failure was spent in crack initiation and half of the time was spent in crack growth. This case results in a CGR of 3.81E-04 in/hr. Case 3 involved the assumption that a pre-existing crack had occurred at the time of coupling installation for the first P-7C coupling failure (the one with the shortest time to failure) and resulted in a CGR of 1.91E-04 in/hr.

The LPI report [1] indicates that the P-7C pump couplings failed initially after about 110 days of operation with the new coupling material in place and the second failure occurred at about 670 days after the first failure with similar coupling material in place. As the CGRs in this evaluation are all based on the shortest time to failure for the P-7C pump, using these CGRs to estimate the remaining life of the as-found coupling for P-7A and P-7B represents a conservative estimate based on the as-found conditions.

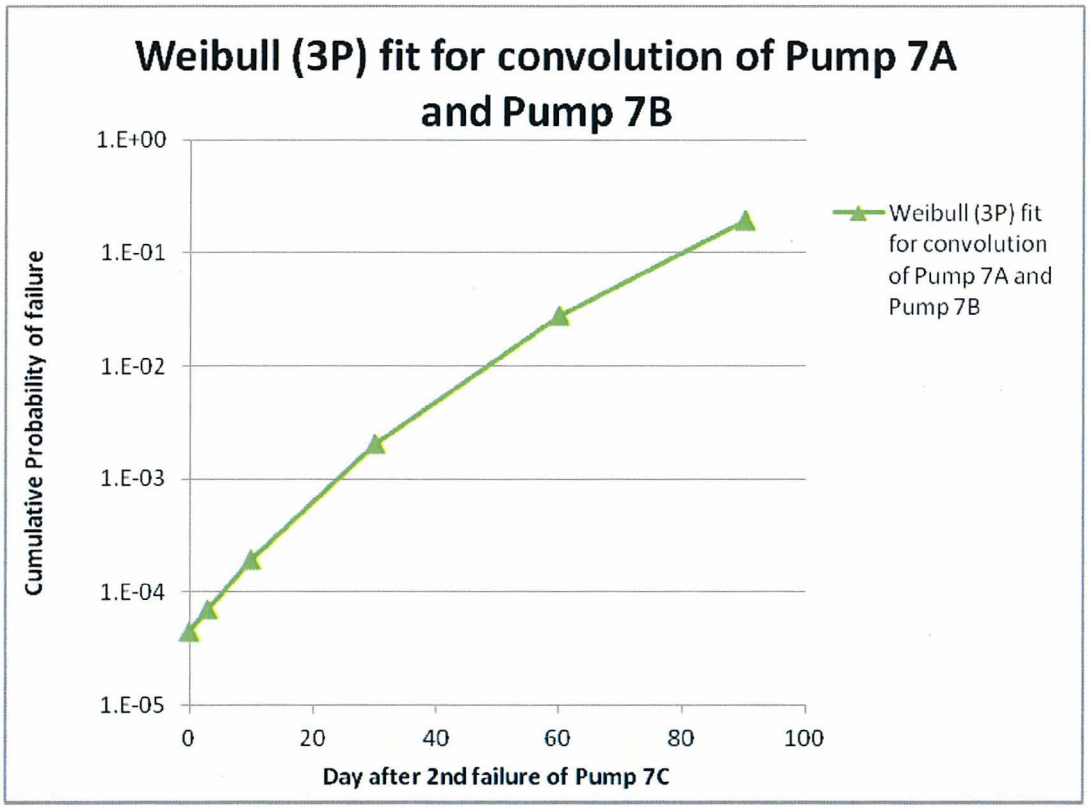
To evaluate the failure to run rate for the P-7B pump, the actual condition of the worst coupling was used to estimate the remaining life. The worst coupling exhibited cracks with a depth of 0.132 inches with a total wall thickness 0.5 inches. Using the CGRs from the three cases noted above, the LPI report estimated remaining life for this coupling. A Generalized Gamma distribution was fit for this data and is shown below. Weibull++7 software package is used to fit this data [2].



For the P-7A couplings, there were no indications of crack initiation apparent from the examination of the material after the failure of the P-7C coupling. As a conservative estimation of the remaining life of these couplings, the LPI report [1] assumed that a crack would initiate at the time the coupling was removed for inspection. Thus, the estimated remaining life is based on the CGRs from the three cases noted above and an assumption that cracks existed which were not observed in the as-found condition of the couplings. Using this conservative assumption, a Generalized Gamma distribution was fit for this data and is shown below. Weibull++7 software package is used to fit this data [2].

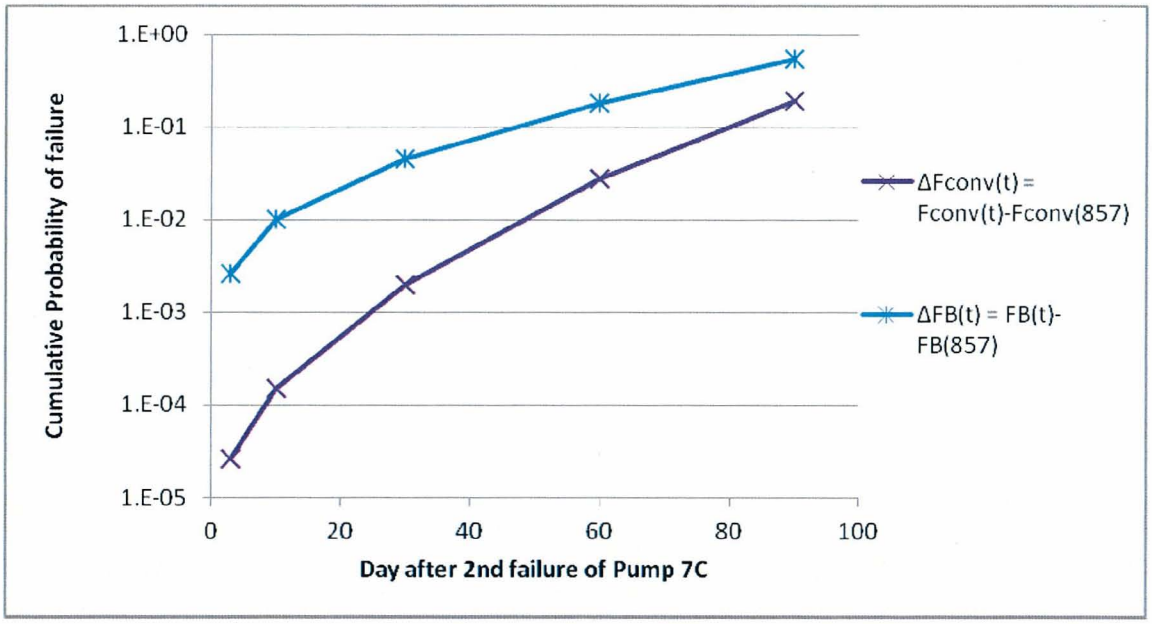


To estimate the probability that both the P-7A and P-7B couplings would fail within the 3 day time window allowed by Technical Specifications, a convolution of these two failure rates produced the joint failure probability curve shown below. By looking at the joint failure probability at the time of the P-7C failure and the joint failure probability 3 days later, the difference is the probability that both P-7A and P-7B would fail some time during that 3 day period. That value is 2.65E-05. The figure below shows the convolution curve. The convolution was simulated using OpenBugs [3] and the result of the OpenBugs was fitted to a closed form distribution using EasyFit software package [4] .



The convolution curve generated above is based on the fact that while the mechanisms that cause a higher than normal failure rate for service water pump couplings are common, the rate at which they affect each pump is not. That is, while each has a higher than normal failure rate, the failure rate for each is different and statistically independent. The worst case scenario would involve a complete dependence between the failure rates for both pumps. This is tantamount to using the worst failure rate for either pump as the rate at which both pumps fail.

The actual evidence of the difference in time between the failure of the P-7C couplings and the as-found conditions of the P-7A and P-7B couplings demonstrates that this worst case scenario is simply not valid. Nevertheless, assuming complete dependence between the two failure rates results in a probability of total loss of service water during the 3 day allowed outage time of 2.61E-03. The figure below shows the "delta" curve for the convolution curve and the complete dependence curve as a function of time.

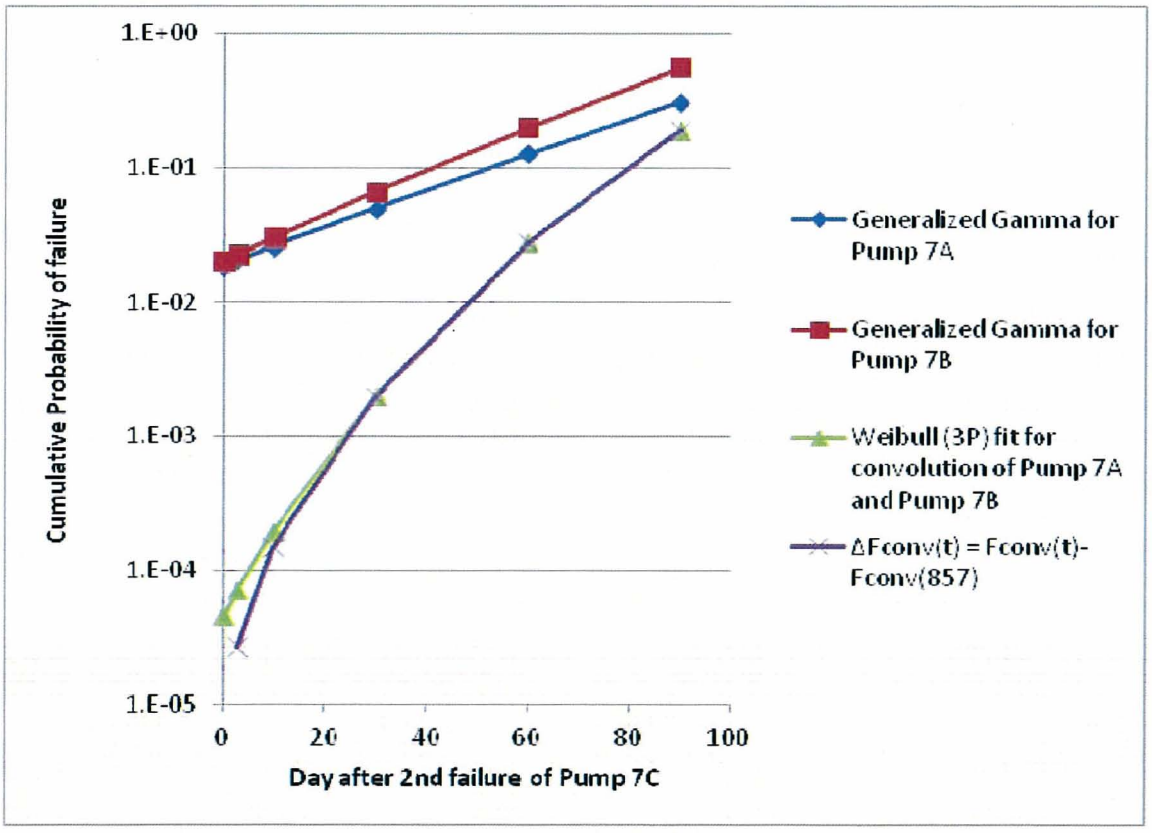


3.0 Summary

Using the as-found condition of the P-7A and P-7B pump couplings and conservative assumptions about the crack growth rate (based on the shortest time to failure of the P-7C pump), an estimate of the remaining life for these couplings was provided by the LPI report [1]. From that information, a distribution for the failure to run rate was produced by fitting a Generalized Gamma distribution to that data.

A convolution of the resulting failure rate curves produced a curve representing the probability of failure of both the P-7A and P-7B couplings as a function of time after the couplings were initially installed. Comparing the probability at the time of P-7C failure and the probability three days later (based on the TS allowed outage time) demonstrates that the likelihood of a total loss of service water during that interval was small.

The figure below is a combination of the degraded failure rates based on as-found conditions along with the convolution curve for those failure rates. It also includes the "delta" curve which shows the difference between the convolution curve value at the time of P-7C failure and the convolution curve at various times after P-7C failure. This evaluation indicates that the likelihood of total loss of service water following failure of the P-7C pump was low for a considerable period of time following the failure of the P-7C pump even with degraded failure rates in the remaining pump couplings.



4.0 References

1. F11358-LR-001 Rev. 0, "Past Operability Assessment of Service Water Pumps P-7A and P-7B associated with As-found Evaluation of Pump Shaft Couplings – Palisades Nuclear Plant", Lucius Pitkin, Inc., September 28, 2011
2. Weibull++ 7 website, http://www.reliasoft.com/Weibull/index.htm
3. OpenBUGS website http://www.openbugs.info/w/FrontPage
4. EasyFit website, http://www.mathwave.com/

5.0 Appendices

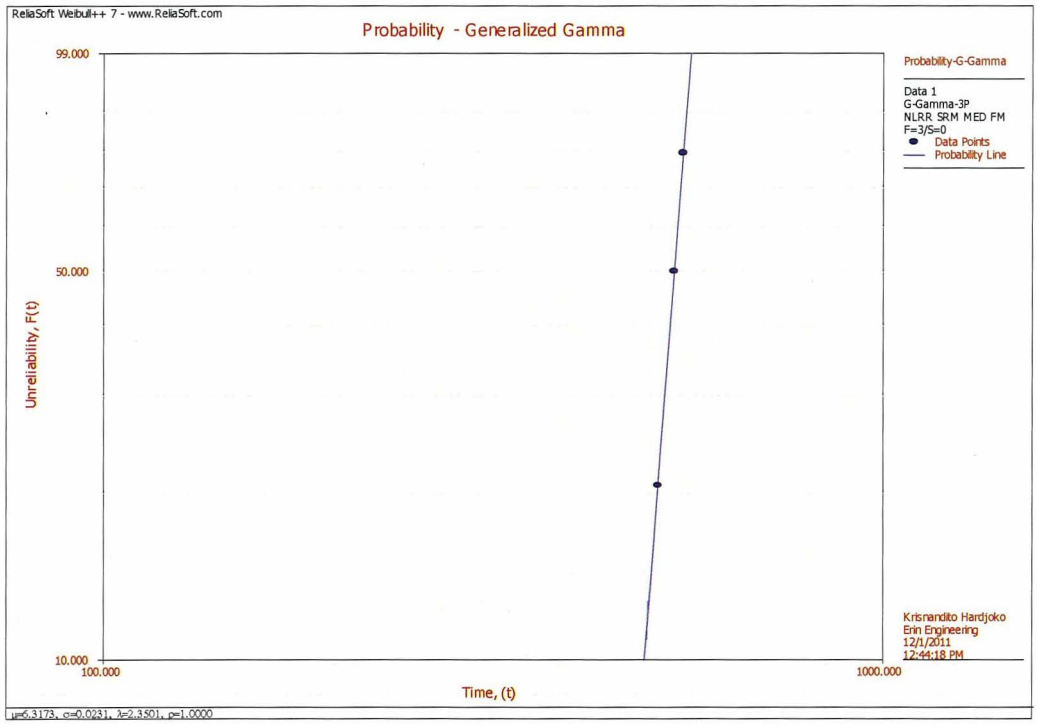
Appendix A, Convolution Input and Output (7 pages)

Development of probability of failure curve of coupling pump 7A and 7B

Estimated Time to Failure use to develop probability of failure curve of coupling pump 7B

Input for Weibull++ 7 (Pump 7B)

Coupling	Time to Failure
11-P7B-6K Case 1	552.5
11-P7B-6K Case 2	515
11-P7B-6K Case 3	574

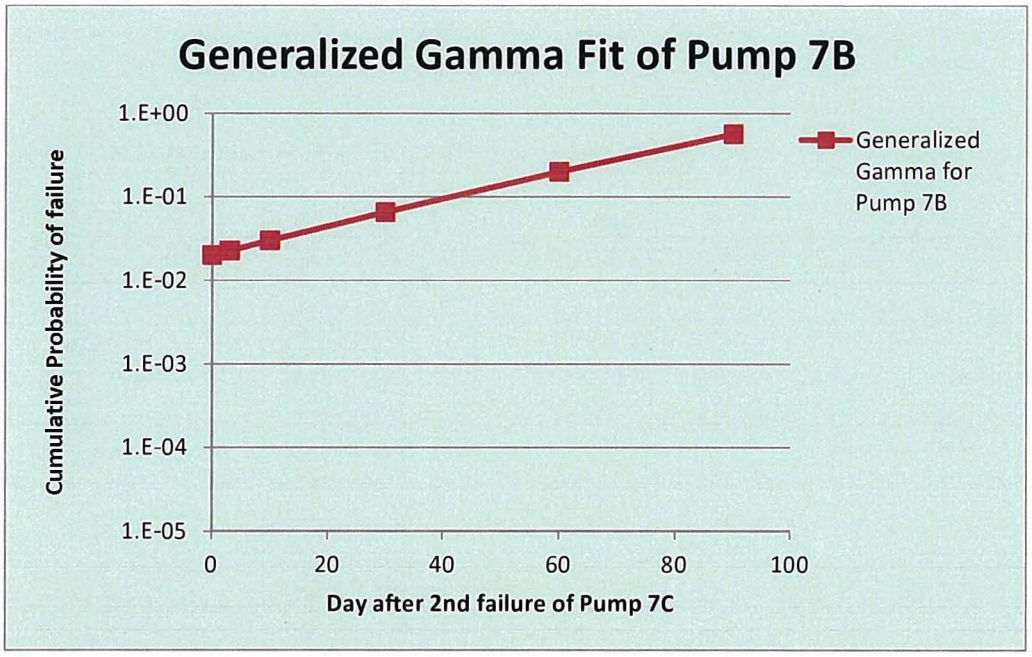


Curve Fitting Result to Generalized Gamma Distribution for Pump 7B

Output from Weibull++ 7: Generalized Gamma Distribution with μ=6.3173, σ=0.0231 and λ=2.3501

Use StatAssist that part of EasyFit software package to calculate cumulative probability of failure

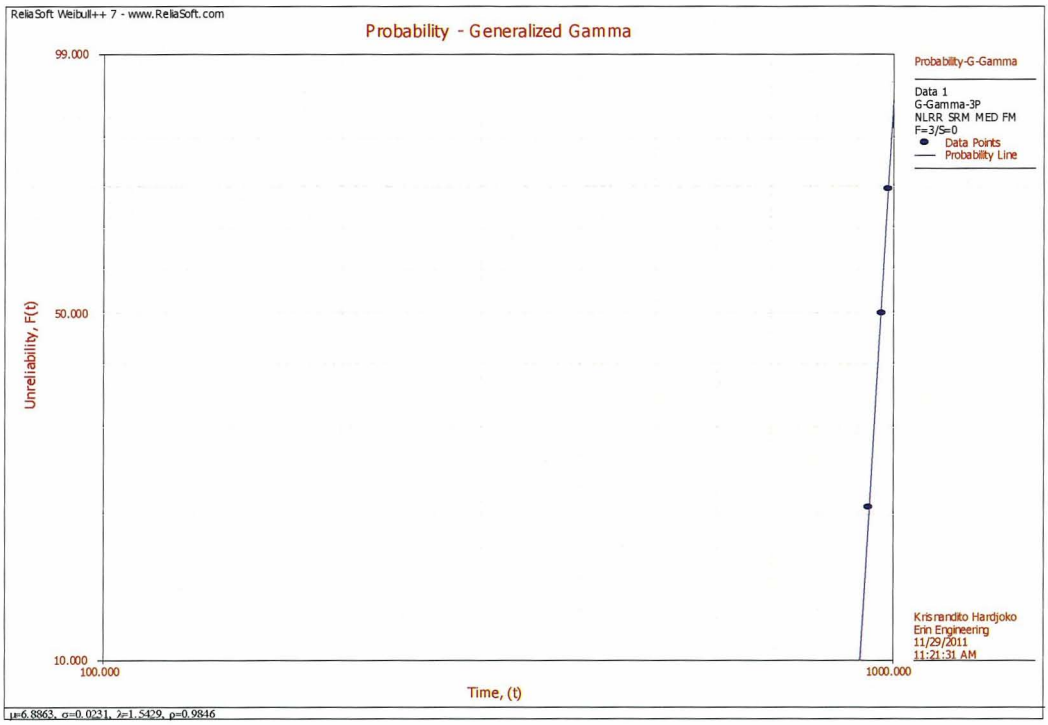
	F(857)	F(860)	F(867)	F(887)	F(917)	F(947)
Day since the failure of Pump 7-C for the 2nd time	0	3	10	30	60	90
Generalized Gamma for Pump 7B where $F(t)=F_B(t-403)$	2.02E-02	2.28E-02	3.02E-02	6.57E-02	1.99E-01	5.64E-01



Cumulative Probability of Failure for Pump 7B

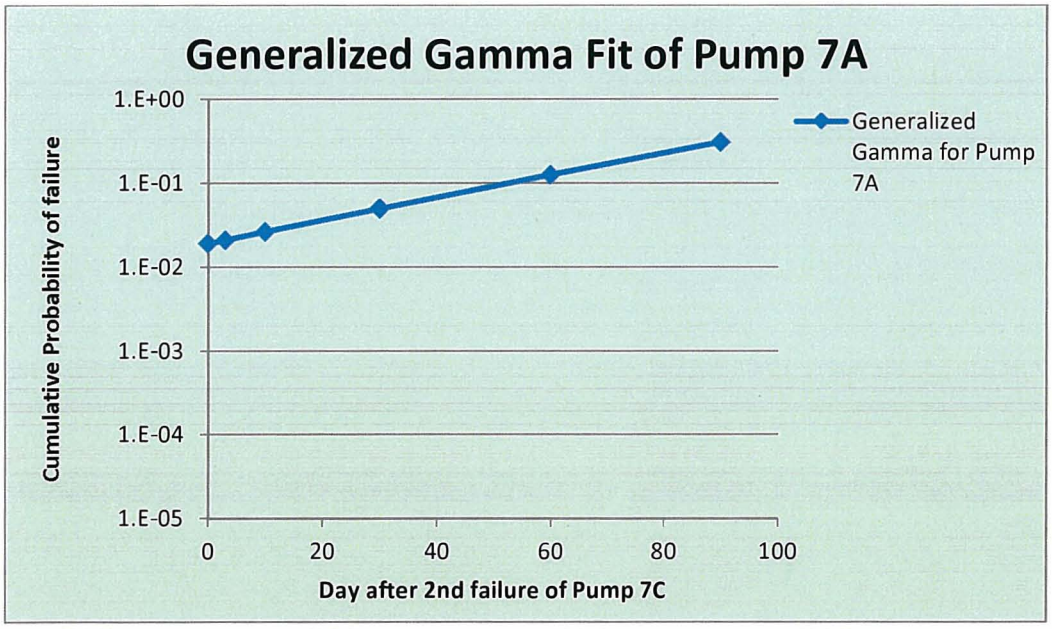
Input for Weibull++ 7 (Pump 7A)

Coupling	Time to Failure
11-P7A-6K Case 1	966.3
11-P7A-6K Case 2	931
11-P7A-6K Case 3	985



Curve Fitting Result to Generalized Gamma Distribution for Pump 7A

Output from Weibull++ 7: Generalized Gamma Distribution with μ=6.8863, σ=0.0231 and λ=1.5429



Cumulative Probability of Failure for Pump 7A

Use StatAssist that part of EasyFit software package to calculate cumulative probability of failure

	F(857)	F(860)	F(867)	F(887)	F(917)	F(947)
Day since the failure of Pump 7-C for the 2nd time	0	3	10	30	60	90
Generalized Gamma for Pump 7A	1.89E-02	2.09E-02	2.62E-02	4.96E-02	1.26E-01	3.07E-01

Convolution of Pump 7A and Pump 7B

- Simulate Pump 7A time to failure with Pump 7B time to failure+403 days.
- Take the longest time to failure among Pump 7A and 7B for each data generation
- Generate 100000 data
- Use OpenBugs to do convolution
- Fit the 100000 convolution result to a curve.

Input for OpenBugs

```
#new
model{
ta~dggamma(ra,mua,betaa)
tb~dggamma(rb,mub,betab)

tnb<-tb+403
tcomb<-max(ta, tnb)
}
list(ra=0.42, mua=0.001008503  , betaa= 66.73, rb=0.181, mub=0.001775 , betab= 101.81)
```

		mean	**sd**	**MC_error**	**val2.5pc**	**median**	**val97.5pc**	**start**
sample								
ta	956.8	35.83	0.1106	865.7	964.5	1004.0	1001	100000
tb	532.8	27.96	0.09087	459.6	540.3	565.4	1001	100000
tcomb	966.0	22.23	0.07175	917.2	966.4	1004.0	1001	100000
tnb	935.8	27.96	0.09087	862.6	943.3	968.4	1001	100000

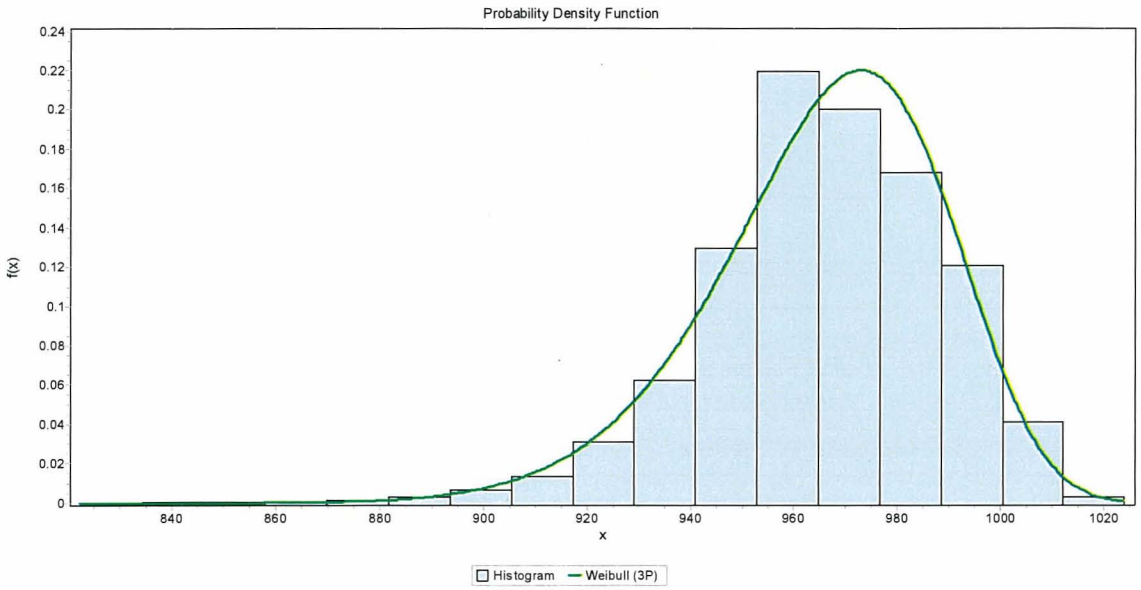
Output of OpenBugs

	mean	sd	MC_error	val2.5pc	median	val97.5pc	sample
time to failure pump 7A	956.8	35.83	0.1106	865.7	964.5	1004	100000
time to failure pump 7B	532.8	27.96	0.09087	459.6	540.3	565.4	100000
time to failure pump 7B + 403 days	935.8	27.96	0.09087	862.6	943.3	968.4	100000
time to failure convolution pump 7A & 7B	966	22.23	0.07175	917.2	966.4	1004	100000

Output point from OpenBugs and input for EasyFit

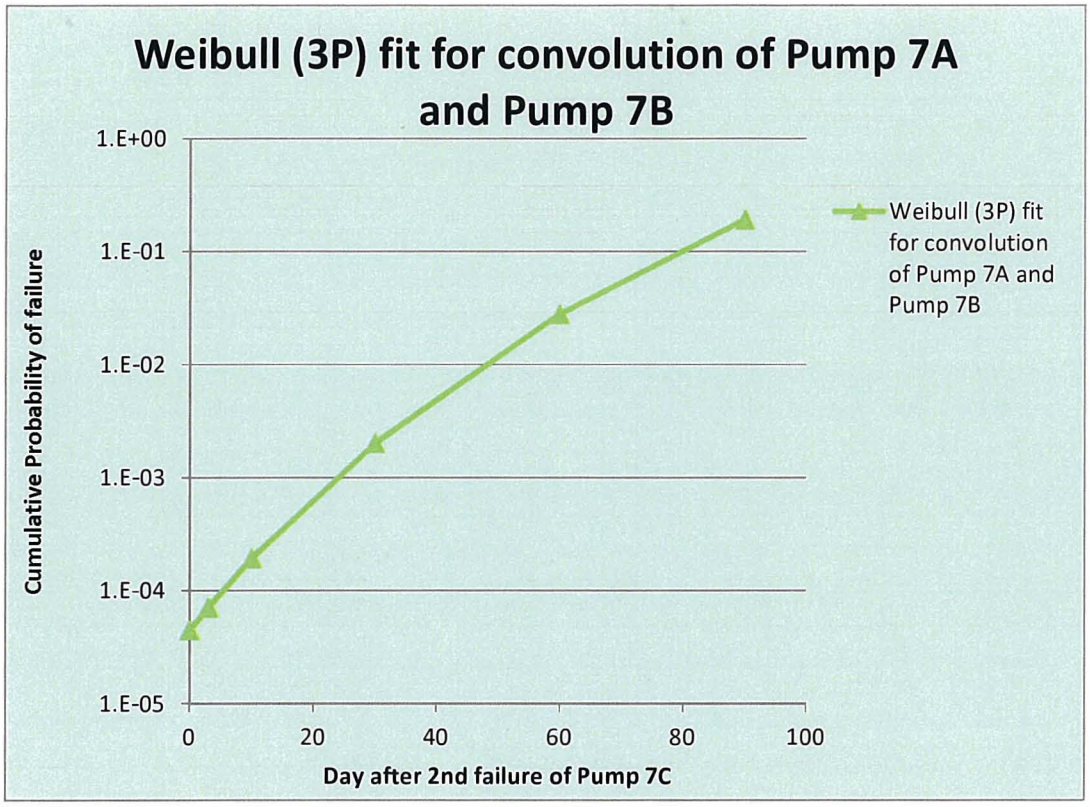
OpenBugs simulation output and input for E

Weibull (3P) fit the best to the convolution result.



Curve Fitting Result to Weibull (3P) Distribution for Convolution Result

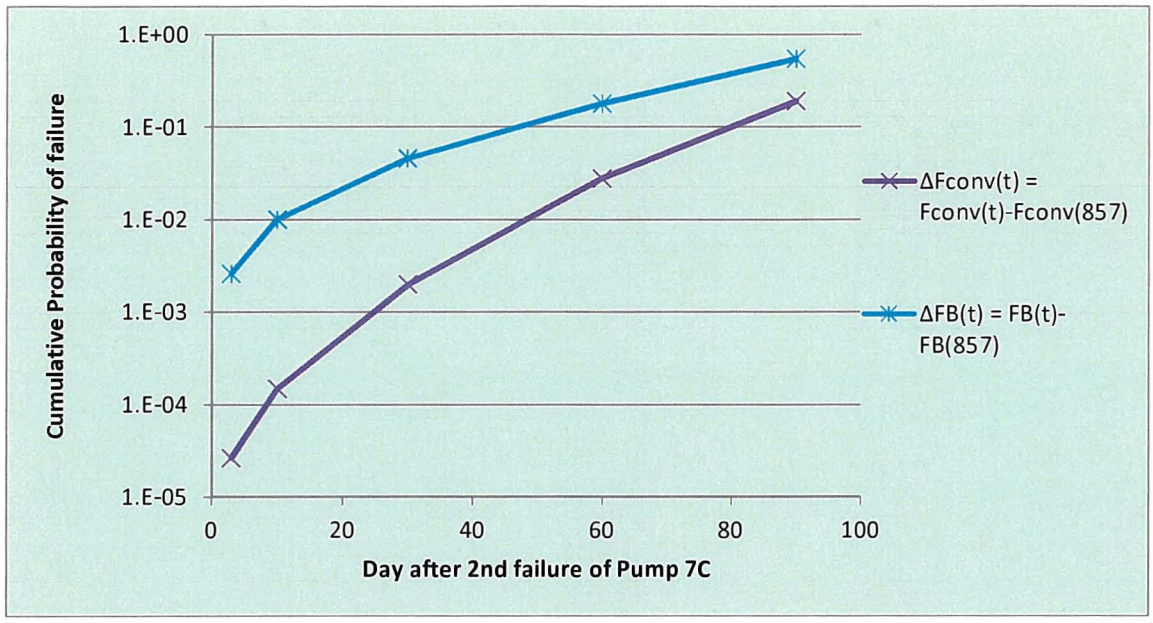
Output from Easy Fit: Weibull (3P) with parameter α=8.630243967, β=172.4086991, and γ=803.0072566



Cumulative Probability of Failure for Convolution of Pump 7A and Pump 7B

Summary of Cumulative Probability of Failure for Pump 7A, Pump 7B and Convolution Result

	F(857)	F(860)	F(867)	F(887)	F(917)	F(947)
Day since the failure of Pump 7-C for the 2nd time	0	3	10	30	60	90
General Gamma for Pump 7A	1.89E-02	2.09E-02	2.62E-02	4.96E-02	1.26E-01	3.07E-01
General Gamma for Pump 7B	2.02E-02	2.28E-02	3.02E-02	6.57E-02	1.99E-01	5.64E-01
Weibull (3P) fit for convolution of Pump 7A and Pump 7B	4.45E-05	7.10E-05	1.93E-04	2.01E-03	2.77E-02	1.90E-01



Probability of Both Pump 7A and Pump 7B Fail Since the Pump 7-C Failed for the 2nd time. The blue curve assumed completely dependent to the worst pump (pump 7B) and the purple curve assumed pump 7-A and 7-B completely independent

Probability of Both Pump 7A and Pump 7B Fail Since the Pump 7-C Failed for the 2nd time

	F(857)	F(860)	F(867)	F(887)	F(917)	F(947)
Day since the failure of Pump 7-C for the 2nd time	0	3	10	30	60	90
$\Delta F_B(t) = F_B(t)-F_B(857)$	0.00E+00	2.61E-03	9.98E-03	4.55E-02	1.79E-01	5.44E-01
$\Delta F_{conv}(t) = F_{conv}(t)-F_{conv}(857)$	0.00E+00	2.65E-05	1.48E-04	1.97E-03	2.77E-02	1.90E-01

Common-Cause Failure Analysis in Event and Condition Assessment: Guidance and Research

Song-Hua Shen, NRC
Don Marksberry, NRC
Gary DeMoss, NRC
Kevin Coyne, NRC
Dale M. Rasmuson (NRC, retired)

Dana L. Kelly, INL
John A. Schroeder, INL
Curtis L. Smith, INL

ABSTRACT

Event and condition assessment is an application of probabilistic risk assessment in which observed equipment failures, degradations, and outages are mapped into the risk model to obtain a numerical estimate of risk significance, which can then be used in other applications, such as the Significance Determination Process. Past experience has shown that conditional common-cause failure (CCF) probability is often a substantial contributor to the risk significance of a performance deficiency. However, guidance for assessing CCF potential has been lacking. Because of this lack of guidance, considerable resources have been expended in efforts to demonstrate an absence of CCF potential, often by scrutinizing piece-part differences across redundant trains instead of focusing on the higher organizational or programmatic issues that were the real cause of the observed failure. Piece parts have often been the object of scrutiny in efforts to declare an observed failure "independent," meaning that no potential existed for CCF of redundant components. Such scrutiny of piece parts is counter to the Significance Determination Process guidance in Inspection Manual Chapter 0308, "Reactor Oversight Process (ROP) Basis Document," which states, "The performance deficiency should most often be identified as the proximate cause of the degradation. In other words, the performance deficiency is not the degraded condition itself, it is the proximate cause of the degraded condition."

This NUREG offers guidance for assessing CCF potential at the level of the observed performance deficiency, provides essential definitions of technical terms, and describes the treatment of CCF for a number of categories of component failures and outages. It also describes technical issues with both the consensus CCF model used in probabilistic risk assessments conducted in the United States and the associated parameter estimates and the data upon which they are based. The NUREG closes with a summary of future research intended to address these issues.

CONTENTS

FIGURES

TABLES

FOREWORD

The U.S. Nuclear Regulatory Commission's Division of Risk Analysis in the Office of Nuclear Regulatory Research develops and manages research programs relating to probabilistic risk assessments (PRAs), human factors, and human reliability analysis. The division assesses U.S. operational safety data and reliability information to determine risk-significant insights and trends, which allows us to focus on the risks most important to protecting public health and safety.

A general conclusion from PRAs of commercial nuclear power plants is that common-cause failures (CCFs) are significant contributors to the unavailability of safety systems. Especially in event and condition assessment (ECA), an observed performance deficiency has the potential to fail multiple components in a relatively short time period. CCF in ECA has to be analyzed at the level of the observed performance deficiency. In other words, the assessment of the potential for multiple dependent equipment failures in ECA should not be constrained by an assumption that CCF requires failure of the same piece part or subcomponent because of the same failure mechanism. Instead, this assessment should focus on the higher organizational or programmatic issues that were the real cause of the observed failure.

This NUREG offers guidance for assessing CCF potential at the level of the observed performance deficiency, provides essential definitions of technical terms, and describes the treatment of CCF for a number of categories of component failures and outages. It also describes technical issues with both the consensus CCF model used in PRAs conducted in the United States and the associated parameter estimates and the data upon which they are based. The NUREG closes with a summary of ongoing and future research intended to address these issues.

Richard Correia, Director
Division of Risk Analysis Office of
Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission

1.) This initial discussion of the proposed approach to conduct common cause analysis under the premise that it not be constrained to the same piece part or subcomponent or the same failure mechanism, is contrary to any existing PRA methodology for conducting common cause analysis.

This document attempts to move the concept of cross cutting issues into the PRA model which may or may not be consistent with the approach to implement common cause contribution in the model. A principal issue is the guidance provided does not include any direction to provide a basis to support the conclusion that the performance deficiency is directly tied to the component failures being observed and that all common cause failures identified would be expected to occur within the PRA mission time of a single event. The approach is to elevate the definition of performance deficiency to the broadest definition that can be shown to encompass the event in question. The elevated description then makes the assertion that many other common cause failures beyond those identified would be possible and not necessarily constrained to the common cause group of the component(s) failed in the event under consideration.

For example, the following is from IM 0308 Attachment 3:

> "The staff is responsible to define licensee performance deficiencies. Where the proximate cause of multiple degraded conditions is the same, there is likely to be only one finding (based on the identified performance deficiency related to the proximate cause) and the risk impact of the collective degraded conditions (including any overlapping conditions) is then appropriately used as the basis for the SDP result. However, this concept could be taken to an extreme of defining all licensee performance deficiencies as "management weakness" or something similarly fundamental. Doing so would then cause all degraded conditions to be manifestations of a single and possibly never-ending finding, would make unnecessary the need for an Action Matrix, and may require the staff to devise a continuous risk meter or similar substitute for the Action Matrix. Thus, a "floor" was set for the implementation of this concept that is consistent with the ROP framework, in that no performance deficiency should be defined at a level associated with the ROP cross-cutting issues (i.e., human performance, safety-conscious work environment, and problem identification and resolution) or more

fundamentally. Although artificially setting this "floor" may create a philosophical inconsistency with use of a probabilistic thinking framework (i.e., if there is really a known common-cause effect taking place, then it should be explicitly acknowledged in a probabilistic model), it remains necessary for practical reasons as long as the Action Matrix continues in its present form. Concerns about possible insufficient regulatory responses arising from this approach are also mitigated as noted below."

It is considered this documents premise is inconsistent with the above.

This documents approach goes on to state, given the definition of the performance deficiency, the current assignments in the PRA model for common cause grouping may no longer be applicable, and the failure mechanisms considered as the common element of group failure are no longer a constraint on the number of components that would be the target group for common cause failure. The issue is that the definition of the performance deficiency at this high level ('POOR MAINTENANCE PROCESS') represents an unbounded characterization of commonality among a group of components. This would allow cross system groupings, and grouping of dissimilar components, into much larger common cause groups. There is no guidance that mandates the development of a technical basis that would establish the connection of the specific observed failure(s) to the entire common cause group.

2.) The summary discussion in the foreword also states that it describes technical issues; with the consensus CCF model used in PRAs, and the associated parameter estimates and data upon which they are based. The principal issue with this description is the industry has developed several standards (ASME / ANS) to establish a baseline consistent methodology of implementing risk assessment.

Plants are required to undergo review by external organizations to establish the degree of implementation/compliance with these standards. The authors herein have determined that the current standards are inadequate and infer that the implementation of this approach provides a method of quantifying risk assessments that will correct these deficiencies.

The guidance provided is a proposed means of correcting issues with the current consensus model without having been subjected to the same process of development as the current standards. Moreover, any issues with the current standards should be resolved within the standards process prior to issuing contrary guidance. If there are legitimate issues with the ASME/ANS standard process, it needs to be corrected first.

ACKNOWLEDGMENTS

This report benefited from the discussions and comments of A. Mosleh, P. Aggignani, L. Criscione, C. Hunter, J. Lane, A. Salomon, and See-Meng. Wong.

The authors would like to acknowledge the technical contributions of Dr. Corwin Atwood to Appendix B.

ABBREVIATIONS

ASP	accident sequence precursor
BPM	basic parameter model
CCF	common-cause failure
CCCG	common-cause component group
CFR	*Code of Federal Regulations*
ECA	event and condition assessment
EDG	emergency diesel generator
FTR	failure to run
FTS	failure to start
HFE	human failure event
INL	Idaho National Laboratory
IR	inspection report
MCC	motor control center
MLE	maximum likelihood estimate
NRC	U.S. Nuclear Regulatory Commission
PORV	power-operated relief valve
PRA	probabilistic risk assessment
SAPHIRE	Systems Analysis Programs for Hands-On Integrated Risk Evaluations
SDP	significance determination process
SPAR	standardized plant analysis risk
SSIE	support system initiating event

Common-Cause Failure Analysis in Event and Condition Assessment

1. INTRODUCTION AND MOTIVATION

Event and condition assessment (ECA)[a] is an application of probabilistic risk assessment (PRA) in which observed equipment failures, degradations, and outages are mapped into the risk model to obtain a numerical estimate of risk significance. Such an assessment can be either prospective, as when utilities use PRA as an aid in planning and scheduling equipment maintenance, or retrospective, such as in the Nuclear Regulatory Commission's Significance Determination Process (SDP) and Accident Sequence Precursor (ASP) Program. In this report, we focus on retrospective assessments intended to estimate the risk significance of degraded conditions, such as equipment failure caused by a deficiency in a maintenance process.

However, it is important to understand that the analyst is estimating a *conditional* risk metric (e.g., the conditional probability of core damage) for the event. Because the actual event did not lead to core damage, the event is not modeled exactly as it transpired because this would lead to a conditional core damage probability of zero. Instead, observed failures are mapped into the PRA model, but successes are treated probabilistically; the analyst accounts for the possibility that equipment that functioned successfully might, with some probability, fail to function, and that equipment that was not demanded in the actual event could have been demanded for some scenarios and also have a probability of failure. Thus, failure probabilities are left at their nominal values or are conditioned as necessary to reflect the details of the event.

3.) This discussion is somewhat vague. When an event happens and core damage does not occur, the conditional probability of core damage is zero. What is being computed is the likelihood that, if such an event or similar event were to occur again under the same boundary conditions that existed when the actual event occurred, that additional failures would have occurred to produce core damage. The key is the probability of what happened is not being evaluated, but what could happen if the event were to occur again.

As an example, many if not most retrospective ECAs in the U.S., are done as part of the NRC's SDP, which is intended to evaluate the risk significance of inspection findings that pertain to an observed deficiency in licensee performance. Therefore, the ECA's main purpose is to quantify the risk significance of the event caused by the deficiency, using a PRA model (U. S. Nuclear Regulatory Commission, 2006). As an example, if the deficiency that led to an observed failure were poor quality control, then the ECA would estimate the risk significance of the observed equipment failure caused by this deficiency, and the analysis includes a *probabilistic* treatment of failures that were not actually observed, but could have been, because multiple equipment items could have been impacted by the deficiency (decreased reliability due to susceptibility to the same cause). Because nuclear plants utilize redundant safety equipment, the risk significance of such a deficiency will often be strongly influenced by the potential for dependent failure of this redundant equipment. Thus, a crucial term in the ECA risk equation is the conditional probability that remaining redundant components could fail, given that one or more such components were failed as a result of the identified performance deficiency. This probability is obtained by calculating a conditional common-cause failure (CCF) probability using the inputs to the PRA model.

4.) When an event occurs and the cause of the event is determined, the conditional probability of it being a common cause failure or independent failure is either 1 or 0. There may be uncertainty in determining this, so one might assign some probability that it was a common cause using engineering judgment, but this should not be compared with CCF model parameters.

Past SDP experience has shown that conditional CCF probability is often a significant contributor to the risk significance of the deficiency. In addition, guidance for assessing CCF potential has been lacking. Due to this lack of guidance, considerable resources have been expended in efforts to demonstrate an absence of CCF potential, often by scrutinizing differences among subcomponents and

piece parts across redundant trains instead of focusing on the higher organizational or programmatic issues that were the real cause of the observed failure. Piece parts have often been the object of scrutiny in efforts to declare the observed failure "independent," meaning there was no potential for CCF of

[a] We will not distinguish, except where it is technically necessary to do so, between an "event," which involves the occurrence of a PRA initiating event, and a "condition," which involves degradation of components for some period of time, but without the occurrence of an initiating event.

5.) The guidance above states that, while common cause contribution has been shown to be a significant contributor in past Event and Condition Assessments (ECA), there have been issues in not appropriately characterizing the common cause potential *perceived* to be associated with the observed events. The approach states the problem is related to being overly specific in the statement of the performance deficiency which restricts the focus of the risk assessment.

Therefore, the deficiency description should be elevated and broadened to a level commensurate with the definition of the cornerstone or the general requirements of the Quality Assurance Program Elements. While this is appropriate in the context of determining the possible association of several different events into a depiction of broader organizational issues, it also raises two concerns:

1. Statements of performance deficiencies at this level result in unbounded issues which makes it difficult to impossible to demonstrate issue resolution.

2. The association of component failures from several different events that have been encompassed by this broadened deficiency definition may not have not been shown to be connected by a direct common cause.

The issue is that deficiency definitions at this level are self fulfilling with respect to any group one would choose to create. The definitions become so vague that anything can be postulated to belong to the group.

Almost all equipment failures that have ever occurred could be lumped into a single group as long as we are willing to discuss causes at the proposed level (e.g. poor maintenance processes). In addition, the depiction of the deficiency in this broader characterization to assess several different events that occurred over some extended period of time ignores any correlation that would have established the probability of the different events occurring within a single event response.

PRA models have not been developed to accommodate this type of assessment of organizational issues and there is no data to support the quantification, as is being proposed in this document. This type of assessment has historically been a qualitative determination of the level of significance of the possible impacts of several disparate but similar events.

Current PRA models are not developed with the capability to perform this type of assessment. To now provide a methodology that would superimpose this type of assessment onto a PRA would be subject to subjective determinations, and gross over or underestimation of the risk contribution.

redundant components. Such scrutiny of piece parts is counter to the SDP guidance in (U. S. Nuclear Regulatory Commission, 2006), which states, "The performance deficiency should most often be identified as the proximate cause of the degradation. In other words, the performance deficiency is not the degraded condition itself, it is the proximate cause of the degraded condition." The inspector should exercise care to ensure that the performance deficiency is not focused too specifically on a particular subcomponent or piece part. For example, a deficiency related to an inadequate vendor design basis for short-time inrush current on a circuit breaker might better be worded to refer simply to an inadequate vendor design basis, without adding the specific details as to the components that were affected. One of the primary motivations for this NUREG is to elaborate on the performance deficiency issue, and to provide clear guidance for conditioning CCF probability in ECA.

6.) It is unclear what is meant by "proximate cause". This should be better defined.

1.1 PRA Treatment of Dependent Failure

Since the publication of WASH-1400, PRA studies have recognized the importance of dependent failure as a means of defeating designed-in redundancy and diversity. In treating dependent failure of hardware components, WASH-1400 employed the term *common mode failure*, defined as:

Multiple failures which are dependent, thereby causing the joint failure probability to increase. The multiple failures are common mode or dependent because they result from a single initiating cause, where "cause" is used in its broadest context.

7.) Per the ASME/ANS PRA standard CCF is defined as:

common cause failure (CCF): a failure of two or more components during a short period of time as a result of a single shared cause.

This definition brings in the concept of short time which is only implied in the WASH-1400 definition. Note that the term was changed from common mode to common cause because the cause was the key to defining the failures in the same short time interval – failure modes can be common but at different times they are not common cause failures.

WASH-1400 elaborates on what can constitute a cause of dependent failure, noting that a cause can be "one of a number of possibilities: a common property, a common process, a common environment, or a common external event." While WASH-1400 used the term common mode failure to encompass all types of dependence, later PRAs categorized dependent failures largely based on how they were treated in PRA models. The PRA Procedures Guide (U.S. Nuclear Regulatory Commission, 1983) describes nine different types of dependent failure, summarizing these in three categories: *common cause initiating events* (now called external hazards), *inter-system,* and *inter-component* dependencies. External hazards (e.g., earthquake) produce dependent failures of equipment through spatial interactions; such dependencies are treated through special analysis techniques. An example of inter-system dependence, which is generally captured in the PRA fault trees and event trees, is dependence of front-line systems on shared support systems. These can be thought of as *hard-wired* dependencies that are a result of system design. Inter-component dependencies, which are not captured explicitly in the PRA models, span a wide range, and may include common design, manufacture, testing, maintenance, environment, and many others. The PRA Procedures Guide (U.S. Nuclear Regulatory Commission, 1983) referred to this last dependence category as *common cause failure* (CCF), and U.S. PRAs since that time have followed this convention, defining CCF as the failure of multiple redundant components, within the mission time window of the PRA, as a result of a shared cause. However, as noted by (Bedford & Cooke, 2001), dependent failure treatment in PRA remains "an issue around which much confusion and misleading terminology exist."

Part of the confusion, particularly with respect to ECA, stems from a focus on the manner in which the cause is manifested at a piece-part level, that is, the failure mechanism.

8.) Failure at the "piece part" level is not the same as a failure mechanism. The confusion occurs in the use of CCF models for the purposes they were not intended for.

As discussed above, such a focus is counter to existing SDP guidance in (U. S. Nuclear

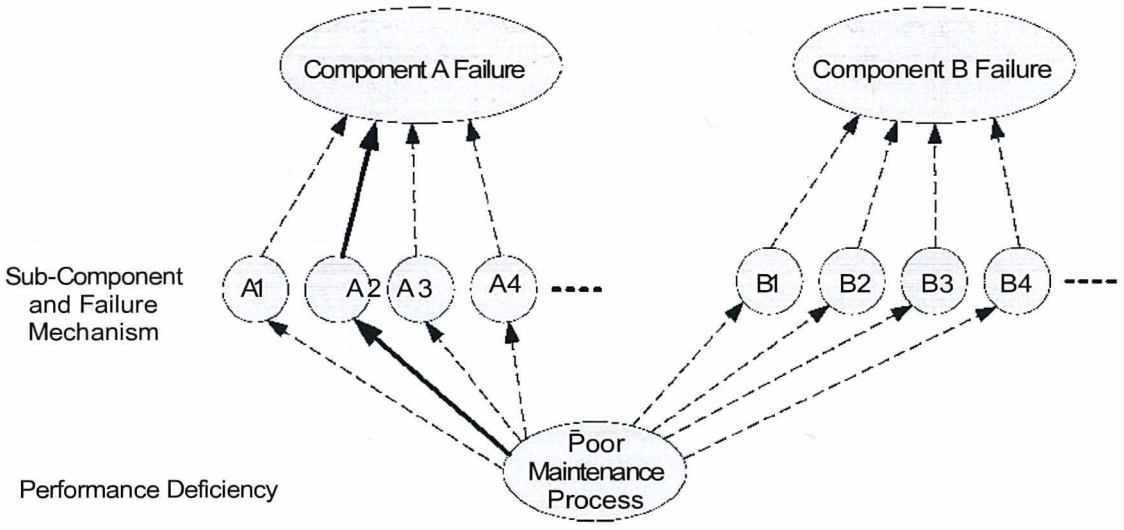
Regulatory Commission, 2006). For example, if the shared cause of failure is a deficiency in a maintenance process, the manner in which the deficiency is manifested across components may vary. In other words, two components could fail in the same *mode* due to CCF, with the *shared cause* being the deficiency in the maintenance process, but the *failure mechanism* at the subcomponent or piece-part level might not be the same. CCF does not require that the failure *mechanism* be identical, only that the *cause* of failure is shared. This concept is illustrated graphically in Figure 1.

9.) This discussion does not make it clear that the times of the multiple failures must be synchronized. A failure due to poor maintenance practice and noting that the maintenance practice is shared by redundant components does not meet the definition of common cause. Poor maintenance practice could just as easily lead to higher independent failure rates than increased CCF potential.

10.) In the discussion of the PRA Treatment of Dependent Failure section 1.1, the argument is made that once the definition of the performance deficiency is elevated to a broader scope description, this is sufficient basis for expanding the existing common cause grouping to include any number of diverse components because they can be shown to be encompassed by the all-inclusive definition. Creating deficiency descriptions at this level creates a condition in which almost any failure that ever occurred could be considered part of the group because the over generalized cause statement cannot be proven incorrect. Consequently, this allows the focus to be shifted away from the actual component failures and their direct causes. Attempts to over generalize these conditions to estimate the risk of organizational weakness has not been the purview of PRA modeling and should not be.

The PRA model focus has been, and should continue to be, on maintaining the reliability of components credited in mitigating analyzed events. At no point has there been any discussion of the need to develop a basis for the connection of these events under one common theme. While it is appropriate to characterize events similar to the examples provided as poor maintenance processes as an example for the purpose of aggregating against the ROP cornerstones, or the broadly defined QA areas, it is not necessarily true that the elements of the maintenance processes are all necessarily failed or failed to the same degree.

Also, the failure to correctly implement a procedural requirement one time does not guarantee failure on the next occurrence. This must be demonstrated by providing evidence that the procedural requirement is routinely violated and that evidence exists in implementation of other procedures as well. Even in the case of additional examples, any suspect increase in risk should be restricted to the cases where the evidence is provided. Otherwise, the generalized statements of performance deficiency result, as was done in this document, in an overall indictment of an entire process which was not supported by any factual information. This is the very issue that was raised in the SDP process to be avoided because of the likely gross over estimation of the risk significance.



Poor Maintenance Process is the observed performance deficiency
A2 is the observed failure mechanism of a specific sub-component due to the observed performance deficiency.
B2 is the same failure mechanism of the same sub-component of component B.
A1, A3, A4, ---- and B1, B3, B4, ---- are the other failure mechanisms may be caused by the same performance Deficiency.

11.) This model would apply equally well to maintenance causing increased independent failure rates or increased common cause potential. The model should include the time element.

Figure 1 Illustration of difference between cause of failure and failure mechanism

1.2 ECA Philosophy Regarding CCF

CCF is included in the PRA because analysts have long recognized that many factors, such as the poor maintenance process in the previous example, which are not modeled explicitly in the PRA, can defeat redundancy or diversity and make failures of multiple similar components more likely than would be the case if these factors were absent. The effect of these factors on risk can be significant. For practical reasons related to data availability, the PRA community has estimated the CCF probability of similar components using ratios of failure counts collected at the component level, without regard to failure cause. Since CCF probabilities are thus based on composite parameters from a cause perspective, the baseline risk estimate of PRAs is felt to be correct in an average sense. While use of conditional CCF probability in ECA can be imprecise because of lack of specificity at the cause level, this document will go on to show that it is important to consider (rather than ignore) this conditional probability, and suggest ways that the approach can be improved.

12.) An equally, or more important reason, is that causes are too numerous to mention and difficult to codify. The causes described here are general cause categories and are not defined sufficiently to determine the type of cause.

Often, factors such as poor maintenance processes are part of the environment in which the components are embedded, and are not intrinsic properties of the components themselves. The conditioning of CCF probability on observed failures in ECA allows the PRA to provide an approximate insight as to the risk significance of these implicit environmental or organizational factors; CCF is the principal means (human reliability analysis being the other) by which current PRAs can assess the impact

of organizational factors on risk, however approximate the assessment may be. As was mentioned above, CCF is modeled parametrically (i.e., the treatment is statistical rather than explicit) in PRA, using what can be considered to be a consensus model, as defined in (Drouin, Parry, Lehner, Martinez-Guridi, LaChance, & Wheeler, 2009). In this consensus model, the CCF parameter values are estimated from a combination of past events, which had a variety of causes. Thus, the CCF parameter values are not specific to a single cause, such as a poor maintenance process. As a result, the conditional CCF probability, which is a function of the baseline CCF parameter values, might be either conservative or nonconservative, depending on the specific situation being modeled. In addition, while some causal factors, such as poor maintenance processes, can impact multiple systems, the state of the practice in U. S. PRA does not include models of intersystem CCF, only CCF within a redundant group of components in a single system. From this perspective, the conditional CCF probability could be nonconservative.

13.) The idea of a conditional CCF probability is not carefully defined. Conditional CCF probability is not related to MGL or ALPHA factors. ALPHA factors are correlative and should not be used as surrogate conditional probability values. Moreover, as cited in this document ALPHA factors can be conservative or nonconservative. So if ALPHA factors are applied as surrogate conditional probabilities, the conclusion is unclear.

1.3 Definitions and Discussion

Because of the confusion in terminology mentioned by (Bedford & Cooke, 2001), we will define some necessary terms as clearly as possible. These definitions are in general accord with wider PRA usage.

Dependent failure: The joint probability of two or more components failing is not equal to the product of the individual probabilities of failure when the failures are dependent. For hardware, the joint probability of failure is typically larger in the case of dependence than the product of the individual probabilties, and this is the reason for concern with dependent failure in the PRA. Note: to be of concern in the calculation of risk, multiple failures have to occur within the mission time window; however, *dependent failures do not have to be simultaneous.*

14.) Stating the dependant failures must occur within the mission time window is somewhat vague. There are situations where the mission time might be long – months. If the mission time is short and the independent failure rate is high, multiple failures in short time intervals are not necessarily CCF.

Common cause failure: When two or more components fail within the PRA mission time window as a result of a shared cause. *The failure mechanisms do not have to be shared.* In other words, the subcomponent or piece part that fails does not have to be the same; it is the *cause* of failure that is shared. Various stochastic models of CCF have been developed over several decades. A few of these, such as the Marshall-Olkin model (Marshall & Olkin, 1967) and the binomial failure rate adaptation of that model (Vesely, 1977), are *shock models*, meaning that dependent failures are due to shocks that affect multiple components simultaneously. The common cause shocks are randomly distributed in time in these models. In such models, the failure times of components affected by common cause shocks are simultaneous, as shown in Figure 2, taken from (Kelly D. L., 2007). Thus, shock models cannot, without modification, represent more general causes of dependent failure that do not lead necessarily to simultaneous failures.

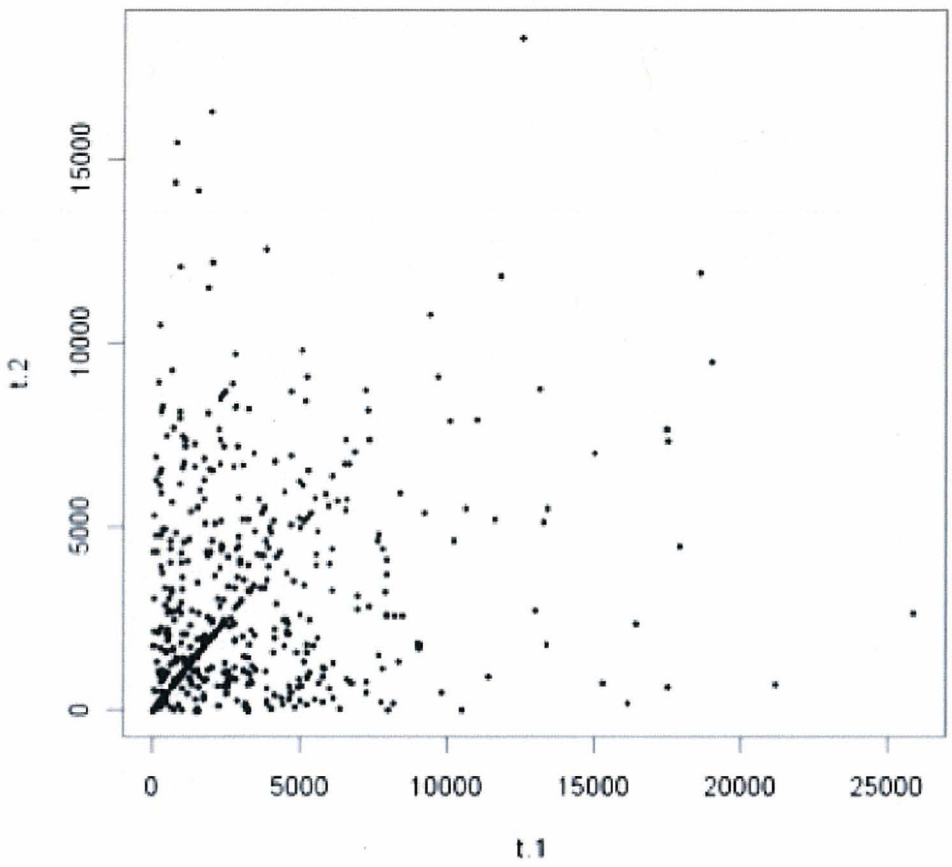


Figure 2 Plot of 500 dependent failure times for two components from Marshall-Olkin shock model, showing simultaneous failure times (those along the line *t.2* = *t.1*) caused by shared shocks occurring randomly in time, from (Kelly D. L., 2007)

However, the most commonly used PRA models of CCF (e.g., alpha-factor model) are not shock models. Furthermore, the requirement that failures be simultaneous in order to count as CCF is overly restrictive; a shared cause such as poor maintenance might generally cause the failure times of affected components to be positively correlated, without giving rise to exactly simultaneous failures, as shown in Figure 3, taken from (Kelly D. L., 2007).

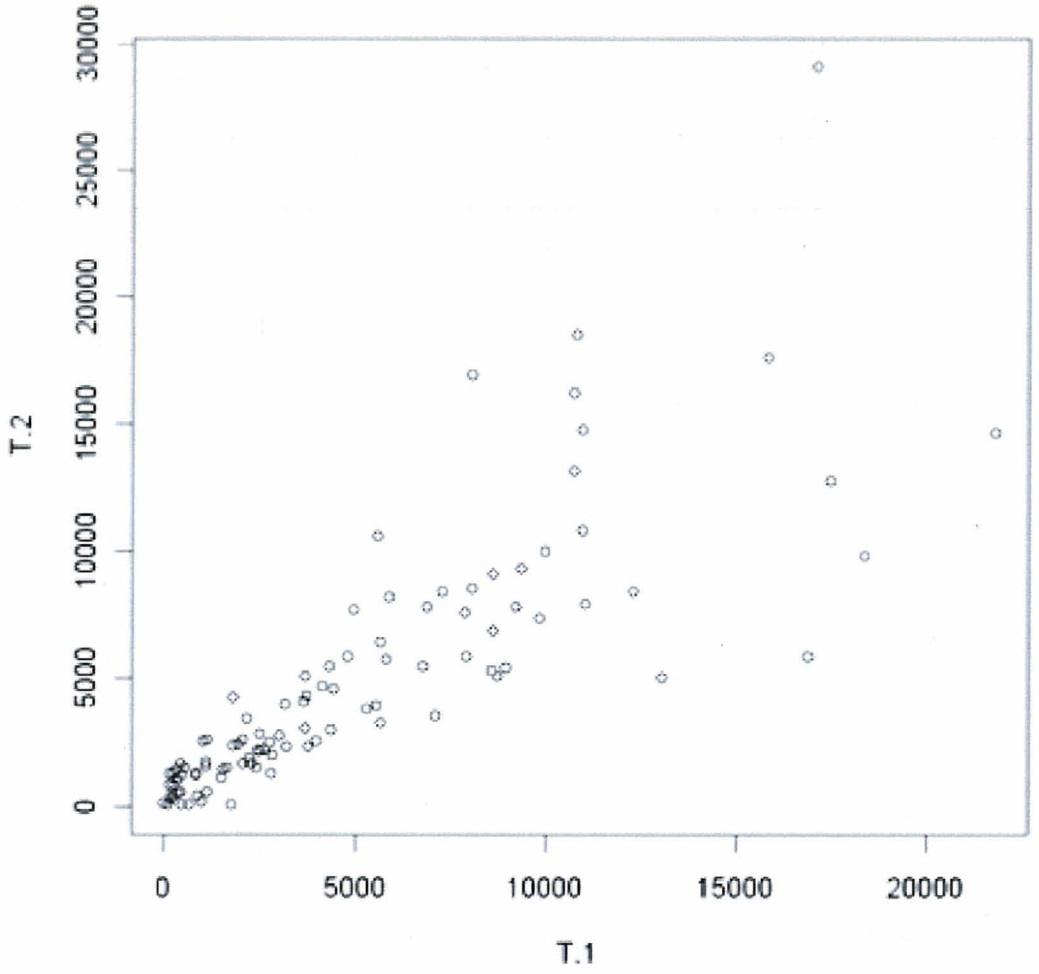


Figure 3 Scatterplot of 100 dependent failure times for two components, showing positive correlation of failure times, but without the simultaneous failures that would be produced from a shock model, taken from (Kelly D. L., 2007)

Common-cause component group (CCCG) : This is defined in (Mosleh, Fleming, Parry, Paula, Worledge, & Rasmuson, 1988) as "A group of (usually similar) components that are considered to have a high potential of failing due to the same cause." We would revise this definition slightly to say simply that the components share a potential for failing due to the same cause; the potential for failure does not need to be high. In fact, typical CCF probabilities are quite low; in a CCCG of size two, if we have observed a failure of one component, the conditional probability that the second component fails due to the same cause is < 0.05.

Assignment of components to CCCGs is part of the qualitative analysis of CCF done for the PRA. A description of the qualitative analysis can be found in (Mosleh, Fleming, Parry, Paula, Worledge, & Rasmuson, 1988). If components have been placed into a CCCG as part of the PRA model development, one can assume that a potential for dependent failure exists among the components. As a result, if a component in a CCCG fails as a result of a performance deficiency, potential for CCF exists with other components in the CCCG unless the boundaries of the CCCG can be shown to be inaccurate.

Common mode failure: Term used by WASH-1400 to describe dependent failures of all kinds. This term was later applied to a variety of different conditions, and this has led to confusion. One usage of the term that is heard occasionally today, which we do not encourage, is for failures caused by a shared component, or by a latent human error, where this dependence is not modeled explicitly in the PRA. Because the NRC Standardized Plant Analysis Risk (SPAR) models contain less detail than a typical licensee PRA and the primary function of the NRC CCF database is to support the SPAR models with CCF parameter estimates, such events are classified as common cause failures in the NRC CCF database. This is due to the boundary definitions of PRA components developed for the NRC CCF database and the fact that few latent human errors are included explicitly in the SPAR models. For more information on the NRC CCF database, see (Wierman et al., 2007).

Independent failure: In one sense, an independent failure is just a failure whose probability is not influenced in any way by other failures or successes that may have occurred. Thus, the joint probability of failure of two or more component can be written as the product of the individual (more formally, marginal) failure probabilities; this is the mathematical definition of stochastic independence. However, independent failure is a term that is sometimes applied in a more specialized sense when estimating parameters of CCF models, such as the alpha-factor model. The parameter estimates of these models are based fundamentally on observed (and inferred) failure counts. For example, a commonly used estimate in the alpha-factor model is

---

In this equation, n_k is the number of events involving the failure of k redundant components in a CCCG of size m. For $k = 1$, the events involve only one component; such events are referred to as *independent* counts. If the presence of a shared failure cause guaranteed failure of all components sharing that cause, the term would be apt, as observed single failures would by necessity imply the absence of a shared cause. However, this is not the case in reality; a shared cause might only increase the joint probability of multiple failures (per the definition of dependent failure above). Hence, a more appropriate term for n_1 might be *individual failures*.

Failure memory approach: The aim of using PRA for ECA is to assess probabilistically what else could have happened in the event, but which did not happen, that would have resulted in core damage. So failures are remembered and successes are forgotten. Thus, observed failures are mapped into the PRA model, but successes are treated probabilistically: the analyst accounts for the possibility that equipment that functioned successfully or was not demanded in the actual event might, with some probability, fail to function. Thus, failure probabilities are left at their nominal values or are conditioned as necessary to reflect the details of the event. For more details see App. A to Vol. 1 of the RASP Handbook and (Hulsmans, De Gelder, Asensio, & Gomez, 2001).

1.4 ECA Ground Rules for CCF Treatment

This section presents the fundamental approach for treating CCF of redundant components in an ECA risk calculation, when one or more of the redundant components are not available due to a deficiency in licensee performance. In past analyses, assessments of CCF were made in varying ways due to the lack of clear guidance for making the assessment. This section attempts to eliminate or at least significantly reduce this variability by presenting clear and simple guidelines for the assessment, which are consistent with what CCF represents in terms of dependent failure, as described above. We also discuss some deviations from the guidelines, which address limitations in current PRA modeling. A more detailed discussion can be found in Sec. 2.

There are three basic ground rules for treatment of CCF in ECA. We list these rules, along with some discussion. Some examples are provided later in this Section.

(1) The shared cause is the deficiency identified in the Inspection Report, which led to the observed equipment failure. For example, if the deficiency were poor quality control, which could affect other redundant components in the CCCG, then a potential for CCF would be judged to exist. The shared cause of failure at this level is the quality control deficiency. Note that the shared cause should be considered in a broad sense, and not necessarily limited to what was written in the Inspection Report, in order to ensure that the potential for CCF is considered appropriately.

15.) This rule does not address the time element. If redundant components share a deficiency, it does not mean that the deficiency will increase the likelihood of a CCF.

For example, the incandescent light bulb;

- All light bulbs share the same deficiency which explains why almost 100% of failures occur due to the same failure mechanism – thermal fatigue of the filament,
- However 99.999+% of all cases of light bulb failure due to this mechanism are independent failures. Many cases of shared deficiency can be explained by an increased failure rate.

(U. S. Nuclear Regulatory Commission, 2006) has the following to say regarding a performance deficiency: "...it is important to recognize that discernable (sic) risk increases come from degraded plant conditions, *both* material *and procedure/process in nature* [emphasis added], and that the performance deficiency should most often be identified as the proximate cause of this degradation. In other words, the performance deficiency is not the degraded condition itself, it is the proximate cause of the degraded condition. This determination of cause does not need to be based on a rigorous root-cause evaluation (which might require a licensee months to complete), but rather on a reasonable assessment and judgement of the staff."

16.) The guidance states that the performance deficiency is not the degraded condition itself but it's the proximate cause of the degraded condition. Note that 'degraded condition' has crept into the guidance. PRAs do not typically analyze the impact of degraded conditions. More importantly the guidance states that the determination of cause does not need to be based on rigorous root cause evaluation but can be based on 'reasonable assessment and judgment of the staff'. Given the possible implications of the findings associated with the performance deficiency, a statement that rigorous evaluation is not required is not consistent with potential consequences of such a judgment.

Emphasis was placed on degradations in procedures and processes in this quote to help discourage overly narrow descriptions of a performance deficiency, focusing on specific subcomponents or piece parts and thus diluting the larger impact of such a deficiency on risk. It is preferable to state that a performance deficiency was "poor maintenance practices" rather than ""poor maintenance practices associated with installing bearings in the correct orientation." Other examples: "failure to correct a condition adverse to quality" instead of "failure to correct a condition adverse to quality associated with lube oil systems;" the licensee failed to develop and implement scheduled preventive maintenance, as required by Technical Specifications" instead of "the licensee failed to develop and implement scheduled preventive maintenance, as required by Technical Specifications for Agastat E7000 series time delay relays in the emergency diesel generator (EDG) 2B protective logic;" "failure to identify the cause of a significant condition adverse to quality" instead of "failure to identify corrosion on the turbine-driven auxiliary feedwater pump governor control valve stem."

The effect of this ground rule is that the analyst will use the conditional probability of CCF, given the observed component failure. In applying this ground rule, we are treating the shared cause *probabilistically*. This treatment is consistent with how other events are handled in ECA, relying on the failure memory approach. For example, if we observe failure of one component in a CCCG of size two, we know that the other component did not fail during the event, but still we do not set its failure probability to zero, as it might have failed; likewise, unless conditions exist that would prevent the cause (e.g., good maintenance practice) of failure from being shared, a *potential* for CCF is judged to be present.

17.) The guidance states that given the failure of one component in a common cause group, the analyst will use the conditional probability of CCF, given the observed component failure. It is recognized that while one or more additional failures do not occur during an event is not a guarantee that addition common cause failures could not have occurred. This guidance precludes any consideration of facts that could discount or substantially reduce the probability of common cause failure.

In addition, consideration of possible random failure of components that were known to be successful during the event response is not considered the same as arriving at the conclusion that the conditions necessary for a common cause failure of multiple components is present.

One can question whether this treatment gives a best estimate of risk or a conservatively large estimate. Continuing with the example of a poor maintenance practice, which might be shared among components but which resulted in the failure of only one component in the event, failing to consider the potential (i.e., probabilistic) impact of observed poor maintenance on the other components in the CCCG by not calculating a conditional CCF probability is the same mistake as setting the failure probabilities of the other components to zero, on the basis that they did not fail during the event. Doing so would be inconsistent with the failure memory approach employed in ECA. Likewise, if it was only chance that prevented multiple components from being impacted by the common maintenance practice, then declaring the observed failure to have no potential for shared common cause would not give a best estimate of risk; it would give a nonconservatively low estimate because the impact of the poor maintenance practice (i.e., its potential to defeat redundancy) is not properly reflected in the risk model.

The estimate provided under the assumption of an observed independent failure gives full probabilistic credit to the remaining redundant components, which might not be warranted.

(2) For ECA, arguments about the time window are irrelevant, and essentially go against the failure memory concept. Simply testing the redundant components cannot provide proof that multiple dependent failures would not occur within the mission time window, as the failure memory concept does not allow credit for successful operation, and there is no guarantee that multiple components could not fail during the mission time window. To put it another way, chance alone cannot be relied upon to eliminate CCF potential from an ECA, based on failure timing. Of course, for data analysis purposes, CCF failures are of concern when they occur during the mission time of the PRA, which for internal hazard groups is generally 24 hours. This is the time window used in estimating parameters in CCF models, in which observed failure counts are used.

18.) This is counter to the ASME/ANS standard definition of CCF. The time element is key to what makes a failure common cause.

19.) The guidance regarding the impact of the time window for common cause failure or 'chance' conditions states that consideration of the time window for common cause failure is irrelevant and contrary to the 'failure memory concept'. Further the guidance states that 'simply' testing redundant components cannot provide proof that multiple dependent failures would not occur within the mission time would not occur within the mission time window.

However, it has been long standing practice that upon discovery of a failed risk significant component, that redundant component(s) be immediately tested to verify that the failure is not present in those components. Implicit in this evaluation is an assumption that the tested components are available for the mission time. If we are to accept the premise that redundant components cannot be proven to NOT be subject to common cause failure during the mission time, then it is unclear why plants are not required to shutdown immediately upon discovery of a failure of a risk significant component that can be characterized as a cause which can result in common cause failure.

Further, the guidance discounts the benefit of staggered testing which is a planned evolution based on the premise that such testing provides for early detection of conditions and implementation of corrective actions to minimize the potential for common cause failure. Again the impact of staggered testing is left to the judgment of the analyst to decide whether common cause failures could have occurred during the PRA mission time.

The potential for multiple dependent failures within the mission time window is taken into account in the NRC CCF data collection effort, via a timing factor. This data collection effort examines past events involving failures of components in a SPAR CCCG. Because most failures are discovered during testing, and much testing is done on a staggered basis, multiple dependent failures may be separated in calendar time by weeks or months, a period of time much longer than the PRA mission time. In these cases,

judgment is applied as to whether such failures would have occurred during the mission time window, had the failures been the result of an actual PRA demand.

20.) For normally operating systems, judgments about time windows can be made when the failures are self announced.

In the data collection effort, the judgment about timing produces a conditional probability that the failures would have occurred within the mission time window, given that the failures were the result of an actual PRA demand. In contrast, ECA is usually focused on a *single* failure, and is concerned with the probability that multiple dependent failures during a recurrence of this event could fall within the PRA mission time window

(3) Credit for programmatic actions to mitigate CCF potential (staggering equipment modifications, etc.) should be applied *qualitatively* during the enforcement process and not incorporated into the numerical risk result. In other words, strong defenses against coupling factors can mitigate CCF potential, but such mitigation is to be addressed qualitatively during the enforcement process rather than quantitatively in the ECA. Qualitative consideration of such factors might allow, for example, a low "White" finding to be changed to "Green."

1.4.1 Deviations from Ground Rules

Because typical PRAs do not model components to the piece-part level, it is possible that some failure causes cannot be shared among components that are redundant from the perspective of the PRA model. In other words, from a high level perspective such as component type and function, components may be placed into the same CCCG in the PRA, but there may be differences at a lower level that are important to take into consideration. Conditioning CCF probability on the assumption of a potential shared cause in this case could produce an unnecessarily conservative estimate of risk. As an example, consider the failure of the EDG 1A feeder breaker described in Calvert Cliffs Inspection Report (IR) 2006012. While the NRC SPAR model for Calvert Cliffs places the EDGs in the same CCCG, EDG 1A, being air-cooled, is a unique design from the other EDGs, and employs radiator cooling fans, which contribute to the inrush current. The other EDGs are water-cooled and have no corresponding short-time overcurrent trip on the breakers feeding the auxiliary MCCs. Thus, depending on the specifics of the ECA, the analyst might need to treat EDG 1A separately from the other EDGs. However, caution should be exercised in revising CCCG boundaries, because typical performance deficiencies, which reflect organizational problems, such as poor maintenance, can couple the EDGs despite the design differences.

21.) The guidance recognizes the potential for over-estimating the risk significance of common cause failure by applying a particular failure mode to a common cause group in a PRA model where the failure does not apply to all components within the common cause group. It is not unusual for common cause groupings to be present in a PRA model for a limited set of failure mechanisms that apply to the group, but a full set of failure mechanisms typical of the component type may not be applicable to all components within the group.

However, the guidance cautions against alteration of common cause group boundaries to accommodate these design differences as the characterization of the performance deficiency as a broader based problem can 'couple' the components despite any design differences that could preclude common cause failure of components within the group.

The Palisades model has separate common cause groupings for which design differences come in to play.

A second category where the ground rules may not strictly apply is also related to the level of detail in the PRA model. In this case, the licensee PRA may have explicit treatment of some dependencies that are treated implicitly via CCF in the associated NRC SPAR models. Two examples are shared equipment and latent (pre-initiator) human failure events (HFE). For example, the deficiency might apply to a power supply control processor that is shared among all steam generator power-operated relief valves (PORV), where this dependency is modeled explicitly in the fault trees of the licensee's PRA, but is not included in the fault trees of the associated SPAR model. In this case, an event in which a failure of the shared control processor led to multiple dependent PORV failures would be captured in the NRC CCF data collection effort, and would contribute to alpha-factor estimates used to calculate CCF probability of the PORVs in the SPAR model. Rather than calculating a conditional CCF probability for the remaining

PORVs, an alternative treatment of a deficiency involving the shared control processor might be to modify the SPAR fault trees to capture this dependency explicitly, allowing better comparison to the licensee PRA. The other generic example related to level of detail is latent HFEs (e.g., miscalibrations). These are not treated comprehensively in the SPAR models, and again are captured indirectly by including such events in the alpha-factor estimates.

1.5 CCF Examples

We include in this chapter some selected examples of CCF that have resulted in an ECA. Note that none of these events are coded as CCF events in the current version of the NRC CCF database.[a] This is because each event involved failure of only a single component. Failures of single components are added to the CCF database only infrequently, when there is judged to be incipient failure of at least one other component in the CCCG. Such events are assigned a fractional count in estimating the alpha factors for the associated CCCG.

22.) The guidance here suggests that events described in the examples provided are not currently considered common cause failure in the current version of the NRC CCF database and that they will be added in a future update. This represents another example of the implication of deficiencies in other processes that are theorized to underestimate the actual CCF parameters.

Moreover, the guidance suggests that analyses of events that involve these deficiencies will be within the SDP process via implementation of this (NUREG) process without having first addressed the issues in the underlying processes (ASME/ANS).

Hatch EDG Coupling Failure (EA-09-054, SIR 2008008))

Cracking in the engine-to-generator flexible coupling for EDG 1B caused severe vibration during a 24-hour load run. The EDG was secured and declared to be inoperable following troubleshooting. Similar cracking was found in the flexible couplings of the other EDGs, and as a result EDG 1C was also declared inoperable. An example of the cracking is shown in Figure 4. Such cracking had been first observed by the utility in 1988, 20 years before the event. At that time, the cracking was not viewed as being indicative of coupling degradation. In fact, the observations of cracking were not even documented. No consideration was given to industry experience with cracking of EDG flexible couplings, and no condition report was written for the cracking observed in 1988. Taking all of this into account, the performance deficiency in the IR for the 2008 event was against 10 CFR 50 App. B, Criterion XVI, which requires that measures be established to promptly identify and correct conditions adverse to quality.

The utility determined the root cause of the cracking to be age-related hardening of the rubber in the flexible coupling between the engine and the generator. This cause was shared with the couplings in the other EDGs because they were similar in age, manufacture, operational and environmental conditions, and were subject to the same maintenance and testing program. Despite the shared cause, an argument for not treating this as a CCF was presented. This argument was based on a claimed low likelihood that multiple couplings would fail within the PRA mission time window for EDG operation. The low likelihood portion of the argument was based in turn on predicted failure times using a regression model developed from *ex situ* testing of the EDG couplings, and on the lower cumulative run times of the other EDGs.

23.) There is not enough information in this example to properly evaluate. Were the failures observed here used to revise the failure rate estimate? Evaluating the CCF parameter must also include a look at the failure rate as it is used before judging the adequacy of the model.

There are numerous problems with this argument, but regardless of these problems the argument is counter to the guidance provided above because the potential for CCF exists at the level of the identified performance deficiency. Furthermore, the failure memory approach does not credit

[a] As a result of discussion during a March 2011 meeting, these events will be

included in future revisions of the database.

successful tests. Thus, an ECA of this event should use conditional probabilities of CCF for the remaining EDGs, given the observed failure to run.

Figure 4 Circumferential crack in EDG flexible coupling

Dresden EDG Strainer Plug Failure (IR 2009005)

EDG 2/3 was 25 minutes into a monthly surveillance run in June 2009 when an oil leak on the turbo lube oil system Y-strainer end cap required EDG shutdown. The leak is shown in Figure 5. This was caused by failure to replace a plastic shipping plug on the recently installed strainer with a metal end cap (see Figure 6). The utility had not ordered the metal cap, and receipt inspection and subsequent maintenance activities failed to identify and correct the problem. The strainer on EDG 2/3 had been replaced in 2008 because of wear on the strainer blowdown caps, which may have been caused by the use of improper tools. The root causes of the failure were judged to be failure to order proper parts and failure to detect the problem during receipt inspection and subsequent maintenance and testing (i.e., a material control deficiency).

Inspection found that the other four EDGs had metal end caps installed on their Y-strainers, which had not been replaced, and this was the basis for an argument that this constituted an independent failure of EDG 2/3. This argument conflates the *cause* of failure (inadequate material control, and not just of lube oil strainers) with the *manifestation* of the cause (failed plastic shipping plug). As discussed above, CCF does not require failure of identical piece parts, only that the *cause* of failure be shared, which it was in this case. A material control deficiency can affect multiple items in EDGs and other important plant components, increasing the joint failure probability of these components. In this example, the material control deficiency was discovered because of the strainer failure. It is possible that other important components in the plant were impacted by this deficiency, but focusing too much on the manifestation of the cause at the piece-part level can underestimate the risk

significance of the deficiency.

24.) In the discussion of the Dresden event, the argument by the licensee is discredited based on the elevation of the performance deficiency description to 'inadequate material control'. This description allows for the arbitrary inclusion of a broader scope of components that results in substantially higher risk significance. At issue in this example is; does any factual information to support a conclusion that the broader group of components was subject to an elevated level of risk from specific performance deficiencies which could impact their performance, exist?

The original deficiency was appropriately characterized as a failure to order proper parts and failure to detect the problem during receipt inspection (i.e. a material control deficiency in the broader context) with respect to one diesel generator. However, all other diesel generators had the appropriate part installed and no other material control deficiencies were identified with respect to any of the other diesel generators. In fact, the example states that because of the elevated description of the deficiency all other diesel generators become suspect and assigned increased probability of failure as a group.

The example argues that because of the elevated description, the issue is now about any other possible failure mechanisms that could result from inadequate material control 'not just lube oil strainers' (the original issue) without having any evidence that material control deficiencies currently exist that could result in failure of the remaining diesel generators. There is a certain level of guilt by association and implication in this approach.

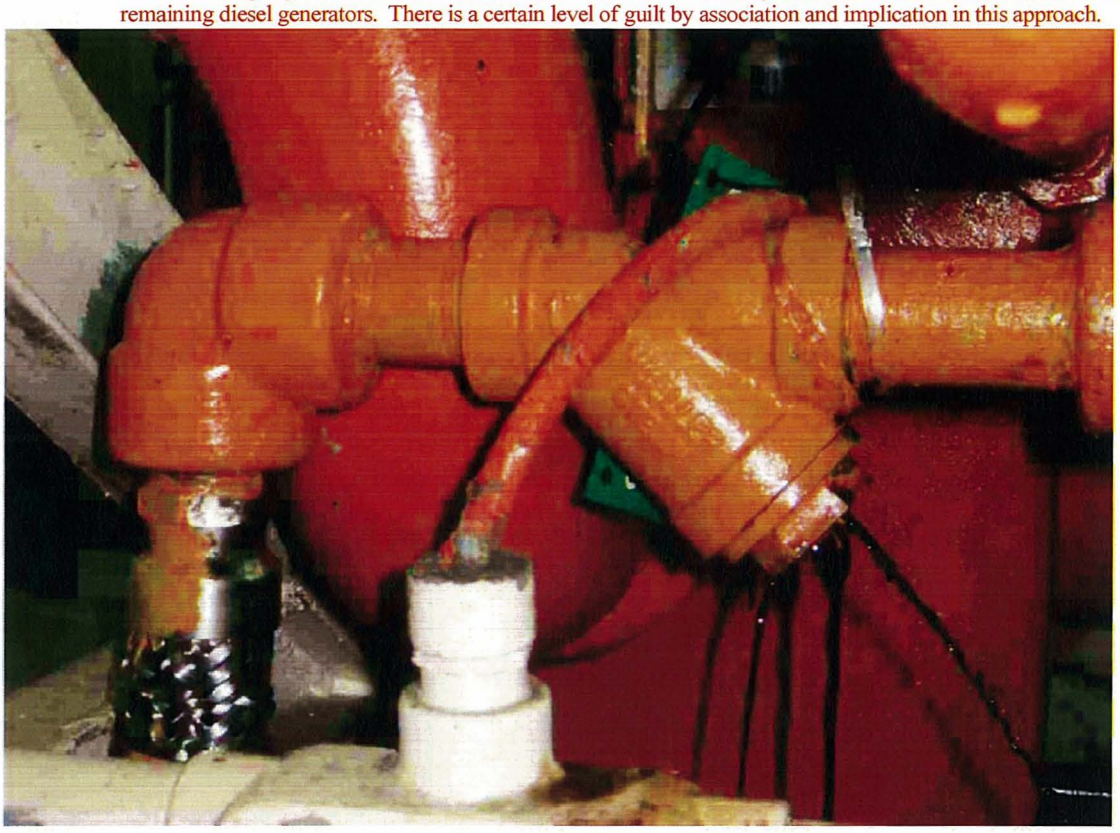


Figure 5 Lube oil lead from Y-strainer end cap on Dresden EDG 2/3

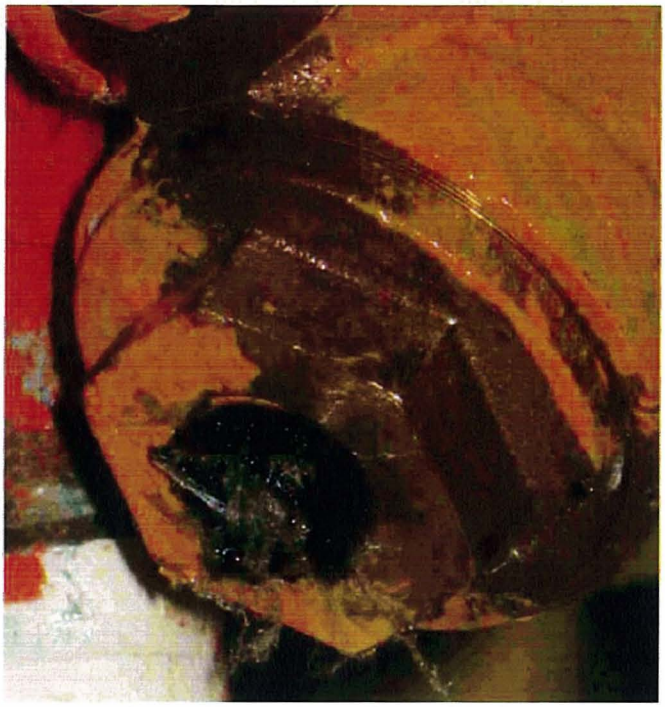


Figure 6 Failed plastic end cap on Dresden EDG 2/3 lube oil strainer

Farley Residual Heat Removal (RHR) Motor-Operated Valve (MOV) Failure (EA-07-173)

An encapsulated MOV in the suction line from the containment sump to RHR pump 2A failed to stroke fully open on two occasions in 2006 and 2007. The specific root cause of failure could not be identified clearly, but the performance deficiency was failure to promptly identify and correct conditions adverse to quality (10 CFR 50, App. B, Criterion XVI). One candidate root cause was corrosion, caused by high humidity in the valve encapsulation. Another was hammerblow forces on the valve torque switch, with this cause not being shared among the redundant valves, because they had different actuator configurations.

At the level of the performance deficiency, which was failure to adequately identify an equipment problem and take appropriate corrective actions, the argument at the piece-part level is no longer relevant. The identified deficiency, which is an organizational problem, can lead to an increased probability of multiple equipment failing. In this specific instance, the problem manifested itself in failure of a single MOV in the RHR system, but from a probabilistic perspective the problem could have been manifested in multiple dependent failures, so the risk evaluation would use the conditional CCF probability for the other valves in the CCCG.

Calvert Cliffs EDG Failure (IR 2006012)

The feeder breaker to EDG 1A tripped in 2006 due to a low design set point. The performance deficiency was identified as an inadequate vendor design basis for short-time inrush current on the feeder breaker to EDG 1A auxiliary motor control centers (MCC). The EDG arrangement at Calvert Cliffs is somewhat unique in that EDG 1A is a very different design than the other three. EDG 1A, being air-cooled, uses radiator cooling fans, whereas the other three EDGs are water-cooled. The radiator fans on EDG 1A contribute to the short-time inrush current; the other EDGs do not even have a short-time overcurrent trip on the feeder breakers to their auxiliary MCCs.

However, despite these differences, the defined EDG common cause component group in the Calvert Cliffs PRA includes both the single air-cooled diesel and the three water-cooled diesels. Although the specific failure manifestation of the performance deficiency was associated with a unique feature of the EDG 1A, all four EDGs share numerous common attributes that can introduce the potential for common cause failure, including EDG support systems other than cooling and maintenance and testing practices. For this reason, the performance deficiency should be viewed in the broader sense of a failure of the licensee to adequately verify design basis information supplied by a vendor, rather than in the more narrow sense of only being associated with breaker current trip settings. In this case, the specific regulatory violation was cited against 10 CFR 50, Appendix B, Criterion III for inadequate design control, a deficiency that has potential to propagate to other EDG trains. Therefore, this event had the potential to affect other trains within the common cause component group and the risk assessment should include consideration of CCF potential.

> 25.) In the Calvert Cliffs example, a diesel generator experienced a failure due to a design feature unique to that diesel. This diesel incorporates a fan cooled radiator for engine cooling. The other diesel engines are water cooled and do not experience the additional in-rush current from the radiator fans on diesel start. This design feature represents a diversity of design that offsets at least some level of contribution from common cause failure as a consequence of a support system failure.
>
> However, the guidance establishes the position that while the particular mechanism is NOT shared among the component group, it is sufficient to argue that other failure mechanisms exist between components within the group and therefore the existence of this uncorrelated failure is a basis to elevate the risk impact of common cause failure of the group is justifiable. If this approach holds, then any benefit from diversity of design is negated. This type of argument represents a self-fulfilling prophecy. One can always argue that while a particular failure mechanism is not shared within the common cause group the presence of other failure mechanisms that could be considered shared is an appropriate basis for increasing the common cause probability of the group as a consequence of the existence of this unshared failure mechanism.

Comanche Peak EDG Failure Due to Paint (IR 2007008, EA-08-028)

EDG 1-02 failed to start during a monthly surveillance test in 2007. Troubleshooting revealed two fuel rack linkage/metering rods bound by paint. The painting had occurred immediately after the last successful surveillance test. The performance deficiency was failure to adequately implement maintenance procedures, which require post-painting verification of equipment functionality. One might argue that this was a random independent failure because the redundant EDG had not been painted. However, this appeared to be pure chance; because of the procedural breakdown (the procedure is a CCF defense mechanism), the other EDG could easily have been painted before finding the problem on EDG 1-02. Preventing CCF requires *deliberate* defenses against coupling factors among redundant components; in this case the defense mechanism was the maintenance procedure, which was not correctly implemented.

26.) In the Comanche Peak example, a diesel generator had been painted immediately after a successful surveillance test and apparently failed the next surveillance test due to a failure to assure that the painting did not impact the functionality of the painted components. The performance deficiency was failure to adequately implement maintenance procedure(s). This approach implements the 'chance' argument. The information provided only identifies a single occurrence of the failure to implement this aspect of the procedure. The 'chance' argument is predicated on the possibility that the other diesel might have been painted between subsequent diesel tests.

Given painting of diesel components is not considered a routine activity, this appears to be an overestimation of the probability of the second diesel becoming subject to the same condition. While it cannot be argued that this is impossible, the question is how probable was it? But, the process discounts conditions which would support lower probability of a common cause event. The argument provided also assumes that the isolated occurrence of the failure to implement the procedure represents a condition that guarantees future failure, and no credit can be considered for the procedure to prevent a second occurrence of the failure.

1.6 Summary of Guidance

In summary, the three ECA ground rules are:

(1) The shared cause is the performance deficiency identified in the Inspection Report.

(2) For ECA, arguments about the time window are irrelevant, and essentially go against the failure memory concept.

(3) Defenses against CCF are to be addressed qualitatively during the enforcement process rather than quantitatively in the ECA.

CCF is the principal means by which PRA can quantify the contribution to risk of crosscutting organizational issues. As noted above, with current CCF models this quantification is an approximation, and might either under- or overestimate the actual contribution in specific situations. If the performance deficiency is related to issues rooted in the organization, such as procedures or control of maintenance, some level of dependence is likely among affected components (more than the failed component are affected), and the CCF probability for these components in the PRA should be conditioned on the observed failure and the presence of a shared cause of dependent failure. Looking for differences in how a failure cause is manifested at a subcomponent or piece-part level, in addition to consuming resources, is almost certain to underestimate the risk associated with such a deficiency; differences can always be found at a low enough level. The only case where these general ground rules might not apply would appear to be issues with the CCCG boundary. However, if the shared cause is rooted in an organizational performance deficiency, the ground rules are expected to be generally applicable.

27.) Sections 1.4 – 1.6 of the draft NUREG describe the ECA (Event and Condition Assessment) ground rules for treatment of a component failure in a common cause group. The general approach described is that any component that fails will have some impact on the common cause group failure probability regardless of the

timing of the failures or the failure mechanism. This implies that essentially all failures may impact common cause group failure probability.

For example, pump 'A' fails due to cause 'X', and pump 'B', a redundant pump, fails 5 years later due to cause 'Y. Following the draft NUREG guidance, these failures could be treated as a common cause due to any performance deficiency. The performance deficiencies could be the same preventive maintenance was performed, or the pumps have a similar design, or they are in the same room, or they operate at the same temperature, etc. etc.

A further example could be a group of redundant components have been installed in a plant for 30 years. Over that period there have been 3 failures spaced 10 years apart. This data would typically be used to update the random failure probability for the components, but does not result in evidence that warrants an increase in the common cause failure probability simply because the components have the same design characteristics or operating environment.

NUREG/CR-6268 and NUREG/CR-4780 when defining common cause factors state:

> *"The concept of a shared cause of malfunction or change in component state is the key aspect of a CCF event. The use of the word "shared" implicitly includes the concept of coupling factor or mechanism. In addition, the reference to a time interval between failures acknowledges the reliability significance of these events. Multiple component failures from a shared cause, but without affecting mission requirements, in a period required for performance are of little or no significance from a reliability point of view. It is the correlation of failure times and their simultaneity in reference to the specified mission time that carries their reliability significance. Often when the same cause is acting on multiple components, failure times are also closely correlated."*

NUREG/CR-6268 further defines the timing factor for announced failures as within three times the PRA mission time.

There is no discussion in the draft NUREG of when plant specific evidence may be applied to update random failure probability when performing an ECA. The failures in the above examples would be more appropriately treated as an increase in the random failure probability. The components may constitute a common cause group, but if they are unreliable, this will be reflected in their individual random failure probabilities.

2. DETAILED GUIDANCE FOR TREATMENT OF CCF

In this section we expand upon the high-level guidance introduced above. We provide guidance for CCF treatment within SAPHIRE 8 of a number of cases that can be encountered with varying frequency in ECA. We also give more detailed discussion of deviations from this guidance that may be encountered. However, as stated above, such deviations are expected to be infrequent.

2.1 Basic Principles of CCF Treatment in ECA

We begin with the basic principles that underlie the detailed guidance that is to follow.

(1) CCF represents all implicit intercomponent dependencies. To reiterate from earlier, CCF is included in the PRA because many factors, such as poor maintenance practices, which are not modeled explicitly in the PRA, can defeat redundancy and make failures of multiple redundant components more likely than would be the case if these factors were absent. These factors often reside in the organizational environment in which the components are embedded, and are not intrinsic properties of the components themselves.

(2) The treatment of such intercomponent dependencies is probabilistic. The unconditional probabilities associated with CCF basic events in the PRA represent joint dependent failure probabilities of similar components that have been placed into a CCCG on the basis that shared causes of dependent failure exist. ECA requires these CCF probabilities to be conditioned upon observed failures of components in the CCCG. As a simple example, assume a CCCG contains three redundant valves. If one valve is already failed, the unconditional probability of three valves failing dependently must be replaced by the conditional probability that the remaining two valves fail dependently, given that one valve has already failed. This conditional probability of two

valves failing will obviously be higher than the unconditional probability that all three valves fail.

(3) The parameters in the probabilistic CCF models are not estimated for specific causes of failure. CCF parameter estimates are based on counting component failures, with these failures due to an array of different causes. Thus, the alpha-factor estimates in the NRC CCF database are based on events spanning a range of causes, and there are currently no means to condition a CCF probability upon a particular cause of failure using these estimates. Thus, with the current consensus CCF modeling approach, the best that can be done is to condition CCF probability upon failures observed in the event being analyzed.

(4) All identified performance deficiencies (typically in an IR) that result in failure of one or more components in a CCCG have the potential for CCF. Exceptions to this principle are expected to be infrequent in practice, and will most often be related to issues with the CCCG boundaries. We discuss potential exceptions in more detail below.

(5) ECA relies on the failure memory approach, and gives no credit to observed successful equipment operation. This treatment of CCF is consistent with how other events are handled in ECA. This principle governs the issues of testing and mission time window. A successful operability test of redundant components in the CCCG in which a failure was observed does not reduce the conditional CCF probability of CCF of the remaining components to zero. For ECA, arguments about the time window are irrelevant, and essentially go against the failure memory concept. Again, the failure memory concept does not allow credit for successful operation, and there is no guarantee that multiple components could not fail during the mission time window.

(6) With respect to defenses against CCF, such as staggering maintenance on redundant components, such defenses must be deliberate and effective in order to break dependence. To put it another way, chance alone cannot be relied upon to eliminate CCF potential from an ECA. The effect of such defenses on risk is to be considered qualitatively in during the enforcement phase rather than quantitatively in the ECA.

2.2 CCF Treatment Categories

In this section we describe categories of events that are expected to span the spectrum of cases encountered in ECA. Guidance is given for CCF treatment in each of these categories using the ECA Workspace in SAPHIRE 8.[a] See App. C for examples that illustrate the ECA Workspace. SAPHIRE 8 calculates conditional CCF probabilities for each category, using the approach described in (Rasmuson & Kelly, 2008).

2.2.1 Observed Failure with Loss of Function of One Component in the CCCG

28.) There is no basis for the approach of using the alpha factor in the baseline PRA model as an estimate for the conditional probability that an event is a CCF. The CCF model is being implemented in a manner that it was never intended to be used for. The alpha factor is correlative and not a conditional probability. Again this surrogate use of an alpha factor may be driven by the goal of creating a fast and dirty conditional probability value but any conclusion is suspect.

In this category, which is probably the most commonly encountered one in ECA, the event being analyzed involves the observed failure of one component in a CCCG. The corresponding basic event in the SPAR model is set to "Failure with potential shared cause" in the ECA Workspace in SAPHIRE 8. This will be the case regardless of the outcome of an operability test on the other components in the CCCG. This treatment is also generally independent of differences among the components in the CCCG at the subcomponent or piece-part level; exceptions will be infrequent and will typically involve CCCG boundary issues, which should be resolved via modifications to the SPAR model, with assistance from the INL, before carrying out the conditional CCF calculation, as discussed below.

29.) This treatment arbitrarily brings in some knowledge to update the PRA model and excludes others. If it is determined that the remaining components are not affected by the cause of the first failure, it should be modeled as an independent event.

NO ADDITIONAL COMMENTS

ATTACHMENT 1

SDP PHASE 3 ANALYSIS

To calculate the exposure time, Section 2.1 of Volume 1 of the Risk Assessment of Operational Events (RASP) Handbook was used. The RASP Handbook states that the exposure time is the duration period of the failed or degraded structure, system, or component (SSC) being assessed that is reasonably known to have existed and includes repair time. For the P-7C pump, the exposure time was one year (the maximum allowable time used in risk analyses), based upon the new stainless steel material for the couplings for all three SW pumps being in place since at least mid-May 2010. The P-7C pump failed on August 9, 2011, at 1201 hours and was returned to service on August 12, 2011, at 0309 hours following successful post-maintenance surveillance testing. Thus, the repair time was approximately 63 hours. There is no recovery credit in this analysis.

This analysis divided the exposure time into two segments:

- The exposure time with the P-7C SW pump not failed (for approximately one year), but with an increased failure-to-run (FTR) rate for all three SW pumps.

- The exposure time when the P-7C SW pump was failed (approximately 63 hours), with an increased FTR rate for SW pumps P-7A and P-7B.

The SRA used the Palisades Standardized Plant Analysis Risk (SPAR) model (version 8.17 dated June 20, 2011), and the SAPHIRE 8 version 8.0.17 software.

The Palisades SPAR model was modified using the Events and Conditions Assessment (ECA) workspace with the following changes:

- A revised FTR rate for the three SW pumps was obtained using statistical analysis, i.e., a Bayesian update with a Jeffreys non-informative prior. The two observed failures of the SW pumps over a total run-time of 40509 hours for the three SW pumps (since the new stainless steel couplings were installed until the failure of the P-7C pump on August 9, 2011) was used. The revised FTR rate for the three SW pumps was 6.17E-5/hour.

- A revised initiating event frequency (IEF) for a loss of service water (IE-LOSW) was obtained based on an approximate method recommended by Idaho National Laboratory (INL). To estimate a new IEF for the LOSW event, the existing SW system fault tree was solved with the nominal SW pump FTR failure rate (3.9E-6/hour), and then again with the new FTR rate (6.17E-5/hour). The ratio of the SW system unavailability with the new rate to that of the system unavailability with the old rate was then calculated. The IEF for the LOSW was then increased by this ratio.

  1.) The approach for revising the IE-LOSW uses a ratio of calculated unavailability from a mitigation system fault tree and then multiplying by the existing IE frequency. This method would not be capable of meeting the ASME/ANS PRA Standard Supporting Requirements IE C-9 and IEC-10 as it combines fault trees for system unavailability with a model for initiating event analysis. However, it is recognized that SPAR modeling utilizes conservative