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

1. INTRODUCTION AND MOTIVATION ................................................................. 1
   1.1 PRA Treatment of Dependent Failure ...................................................... 2
   1.2 ECA Philosophy Regarding CCF ............................................................. 3
   1.3 Definitions and Discussion ....................................................................... 4
   1.4 ECA Ground Rules for CCF Treatment .................................................. 7
      1.4.1 Deviations from Ground Rules ......................................................... 9
   1.5 CCF Examples ......................................................................................... 10
   1.6 Summary of Guidance ............................................................................ 14

2. DETAILED GUIDANCE FOR TREATMENT OF CCF ................................. 15
   2.1 Basic Principles of CCF Treatment in ECA ............................................ 15
   2.2 CCF Treatment Categories ................................................................. 16
      2.2.1 Observed Failure with Loss of Function of One Component in the CCCG .............................................. 16
      2.2.2 Observed Failures with Loss of Function of Two or More Components in the CCCG ................. 16
      2.2.3 Observed Failure with Loss of Function of One Component in the CCCG – Component not in SPAR Model .............................................................. 16
      2.2.4 Degradation in One or More Components in CCCG without Observed Failure .............................. 16
      2.2.5 Observed Unavailability of One or More Components in CCCG Due to Testing or Planned Maintenance .................................................. 17
      2.2.6 Observed Loss of Function of Components in CCCG Caused by the State of Other Components Not in the CCCG ........................................................... 17
      2.2.7 Observed Loss of Function of One or More Components in CCCG as a Result of Environmental Stress Caused by Failure or Degradation of Other Components outside Affected CCCG ...................................................... 17
      2.2.8 No Observed Failure or Degradation in the Affected CCCG ............... 18
   2.3 Cases where Guidance Might not Apply ................................................ 18
      2.3.1 CCCG Boundary Issues ................................................................. 18

3. Issues with Current CCF Modeling and Data Analysis Relevant to ECA .......... 19
   3.1 Issues with CCF Model ................................................................. 19
      3.1.1 CCF Model is not Causal ................................................................. 19
      3.1.2 BPM Employs a Symmetry Assumption ......................................... 20
      3.1.3 CCF is not Modeled Across Component or System Boundaries .......... 20
      3.1.4 Impact on More than One Failure Mode not Captured ...................... 20
      3.1.5 Conditional CCF Calculations in Models for Support System Initiating Events (SSIE) .......... 20
   3.2 Issues with Alpha-Factor Estimates ....................................................... 23
3.2.1 Treatment of Shared Components and Latent Human Errors ............................................... 24
3.2.2 Prior Distributions for Alpha Factors ................................................................................. 24
3.2.3 Estimates of Alpha Factors are not Plant-Specific ............................................................... 26
3.2.4 Treatment of Staggered Testing ............................................................................................ 26

4. Future Research ...................................................................................................................................... 28

4.1 Causal Failure Models ..................................................................................................................... 28
4.2 SSIE Models ................................................................................................................................... 29
4.3 Enhancements to NRC CCF Database .......................................................................................... 30
4.3.1 Prior Distribution for Alpha-Factors ..................................................................................... 30
4.3.2 Plant-Specific Alpha-Factor Estimates ................................................................................. 30
4.3.3 Adjusting Alpha-Factor Estimates ........................................................................................ 30
4.3.4 Effects of Testing Schemes on Estimators ............................................................................ 30

5. REFERENCES ....................................................................................................................................... 31

Appendix A ................................................................................................................................................. 33

Conditional Common-Cause Failure Probability Calculations ......................................................... 33
A.1 Review of Basic Parameter Model and Alpha-Factor Parameterization .................................... 33
A.2 Calculating Conditional Common-Cause Failure Probability .................................................... 35
A.2.1 Failure To Start ................................................................................................................... 37
A.2.2 Independent Failure To Start ............................................................................................... 38
A.2.3 Test or Preventive Maintenance Outage ............................................................................. 39

Appendix B ................................................................................................................................................. 40

Effects of Testing Schemes on Common-Cause Failure Parameters .................................................. 40
B.1 Common-Cause Failure Model Parameters ................................................................................ 40
B.2 Ways of Collecting Data ............................................................................................................... 41
B.2.1 Estimators when All m Components Are Demanded on Each Test .................................... 42
B.2.3 Estimators with Staggered Testing ...................................................................................... 44
B.3 Effect of Using the Wrong Formula ............................................................................................ 47
B.4 Proofs of Selected Results ............................................................................................................ 48

FIGURES

Figure 1 Illustration of difference between cause of failure and failure mechanism ......................... 3
Figure 2 Plot of 500 dependent failure times for two components from Marshall-Olkin shock model, showing simultaneous failure times caused by shared shocks occurring randomly in time ............... 5
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)..........................6

Figure 4 Circumferential crack in EDG flexible coupling.................................................................11

Figure 5 Lube oil lead from Y-strainer end cap on Dresden EDG 2/3 ..............................................12

Figure 6 Failed plastic end cap on Dresden EDG 2/3 lube oil strainer...........................................12

Figure 7 Reliability block diagram for two pumps in parallel, one normally running and one in standby 20

Figure 8 Markov model for two-pump configuration in Figure 7 ...................................................21

Figure 9 Reduced Markov model for two-pump CCCG, given that pump B has failed with potential for CCF of pump A........................................................................................................22

Figure 10 Example of Bayesian network causal model.................................................................29

Figure 11 Example fault tree for two failure modes and three components..................................36

TABLES

Table 1 CCF Data Used To Develop Alpha-Factor Prior Distribution.............................................24

Table 2 Component Failure Probabilities for Three-Component Example.....................................36

Table 3 Basic Event Probabilities for Three-Component Example...............................................36

Table 4 Quantified Minimal Cut Sets for Three-Component Example..........................................37

Table 5 Quantified Minimal Cut Sets and Conditional Probabilities for Three-Component Example, Given Observed Failure To Start of Component A.........................................................37

Table 6 Quantified Minimal Cut Sets and Conditional Probabilities for Three-Component Example, Given Observed Independent Failure To Start of Component A..................................39
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
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.
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASP</td>
<td>accident sequence precursor</td>
</tr>
<tr>
<td>BPM</td>
<td>basic parameter model</td>
</tr>
<tr>
<td>CCF</td>
<td>common-cause failure</td>
</tr>
<tr>
<td>CCCG</td>
<td>common-cause component group</td>
</tr>
<tr>
<td>CFR</td>
<td>Code of Federal Regulations</td>
</tr>
<tr>
<td>ECA</td>
<td>event and condition assessment</td>
</tr>
<tr>
<td>EDG</td>
<td>emergency diesel generator</td>
</tr>
<tr>
<td>FTR</td>
<td>failure to run</td>
</tr>
<tr>
<td>FTS</td>
<td>failure to start</td>
</tr>
<tr>
<td>HFE</td>
<td>human failure event</td>
</tr>
<tr>
<td>INL</td>
<td>Idaho National Laboratory</td>
</tr>
<tr>
<td>IR</td>
<td>inspection report</td>
</tr>
<tr>
<td>MCC</td>
<td>motor control center</td>
</tr>
<tr>
<td>MLE</td>
<td>maximum likelihood estimate</td>
</tr>
<tr>
<td>NRC</td>
<td>U.S. Nuclear Regulatory Commission</td>
</tr>
<tr>
<td>PORV</td>
<td>power-operated relief valve</td>
</tr>
<tr>
<td>PRA</td>
<td>probabilistic risk assessment</td>
</tr>
<tr>
<td>SAPHIRE</td>
<td>Systems Analysis Programs for Hands-On Integrated Risk Evaluations</td>
</tr>
<tr>
<td>SDP</td>
<td>significance determination process</td>
</tr>
<tr>
<td>SPAR</td>
<td>standardized plant analysis risk</td>
</tr>
<tr>
<td>SSIE</td>
<td>support system initiating event</td>
</tr>
</tbody>
</table>
Common-Cause Failure Analysis in Event and Condition Assessment

1. INTRODUCTION AND MOTIVATION

Event and condition assessment (ECA)\textsuperscript{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.

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.

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

\textsuperscript{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.
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.

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.

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. 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.
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.

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.

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.

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 probabilities, 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.

**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.
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

\[ n_i \]

In this equation, \( n_i \) 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 \( n_i \) 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.

(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.”

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; 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.

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.

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.

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.

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. 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.

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.

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](image)

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.
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
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.

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.

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.

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.
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

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.

2.2.2 Observed Failures with Loss of Function of Two or More Components in the CCCG

In this category, the event being analyzed involves the observed dependent failure of at least two components in a CCCG due to a shared cause, although not necessarily from the same failure mechanism (i.e., the failures do not have to involve the same subcomponents or piece parts). The individual inputs for those components that were failed in the event (associated basic events in the SPAR model) are set to “Multiple failure” in the ECA Workspace in SAPHIRE 8. As an example, if the observed events are failures to start of two motor-driven pumps in a CCCG, the two corresponding failure-to-start basic events that are an input to the CCF module for that CCCG in SAPHIRE 8 would be set to “Multiple failure” in the ECA Workspace.b

2.2.3 Observed Failure with Loss of Function of One Component in the CCCG – Component not in SPAR Model

In this situation, there are no alpha-factor estimates available in the NRC CCF database. The analyst will have to add the component to the SPAR model in accordance with the guidance in the RASP Handbook, including potential for CCF of the CCCG, and so estimates of alpha factors will be needed. Two options are available at present. First, the analyst could use the alpha-factor estimates for a similar supported component. As an example, if the component that failed was a motor-operated ventilation damper for a compartment containing a pump, and ventilation is required to cool the pump during operation, failure of the damper will lead to failure of the pump, and so the alpha-factor estimates for the pump could be applied to the CCCG containing the failed damper. The second option, in the case where there is no supported component, is to use the alpha-factor prior distribution in the NRC CCF database. As discussed in Sec. 3, this prior is based on CCCG size and is not component-specific. A third option, which will require further investigation, would be to use an average of the posterior alpha-factor distributions in the NRC CCF database.

2.2.4 Degradation in One or More Components in CCCG without Observed Failure

In this category the deficiency has led to an increased probability of failure for one or more components, but no actual failures involving loss of component function have been observed. The analyst

---

a The guidance is based on the ECA Workspace that should be available in SAPHIRE 8 by Summer 2011.
b This calculation conditions upon the union of $C_{ik}$ and higher-order CCF terms in the Basic Parameter Model (BPM). It is also possible to condition upon the intersection of the total failure probabilities by specifying each observed failures as “Failure with potential shared cause.”
enters the new estimated failure rate or probability for the associated basic events in the SPAR model. This is done by selecting the “New probability” option for each of the associated basic events in the ECA Workspace in SAPHIRE 8. Note that the adjustment to failure rate or failure probability should be done in consultation with experts at the NRC or INL. The calculation for this category, described in (Rasmuson & Kelly, 2008) and implemented in SAPHIRE 8, assumes that only one component in a CCCG is impacted, and the degradation is thus not shared with other components in the CCCG. If the degradation does affect more than one component in the CCCG, the analyst may have to create a new CCCG to capture this. This should be done in consultation with experts at the NRC and INL.

2.2.5 Observed Unavailability of One or More Components in CCCG Due to Testing or Planned Maintenance

Testing and planned maintenance can reduce the level of redundancy of a CCCG. SAPHIRE 8 recalculates CCF probabilities for this category under two assumptions. First, it is assumed that individual failures of components out for test or maintenance cannot be observed. Second, unavailability of a component due to test or maintenance does not affect the total failure rate or probability of other components in the CCCG. The details are described in (Rasmuson & Kelly, 2008). Note the emphasis on planned maintenance; corrective maintenance will be included in the categories described in Secs. 2.2.1 and 2.2.2. The analyst should set the basic events corresponding to out-of-service components in the SPAR model to “Out for Test and Maintenance” in the ECA Workspace in SAPHIRE 8. Note that some basic events represent test and maintenance directly as a failure mode (in addition to failure to start and failure to run). If a component in the CCCG is associated with one of these test and maintenance basic events in the SPAR model, then setting the test and maintenance basic event to “Out for Test and Maintenance” is sufficient (SAPHIRE will automatically adjust the values for the other failure modes as needed).

2.2.6 Observed Loss of Function of Components in CCCG Caused by the State of Other Components Not in the CCCG

Examples in this category include intersystem dependencies such as shared components and shared support systems, and human errors such as miscalibration. The distinguishing characteristic of this category is that the deficiency does not involve the dependent component whose function was lost. As discussed earlier, these types of dependencies are typically modeled explicitly in the fault tree logic of licensee PRAs, but may only be included implicitly in the estimates of alpha factors, rather than captured explicitly in a less detailed SPAR model. So the analyst must first determine the modeling status in SPAR: is the observed intersystem dependency modeled in the SPAR fault trees (explicit treatment), or is it included in the alpha-factor estimates for the affected CCCG (implicit treatment)?

If the dependency is not included explicitly in the SPAR models, there are two options for the analyst. The first is to enhance the SPAR model to include the dependency, in accordance with the guidance in the RASP Handbook. This is the recommended option, but may require assistance from INL, especially if it is necessary to revise alpha-factor estimates to avoid double counting the dependency. The second option is to map the observed failure into the fault tree for the affected CCCG. This option requires that the observed failure map into a CCCG in the affected system. If the dependency is included explicitly in the SPAR models, the analyst should set the associated basic event in the SPAR model to “Unknown failure” in the ECA Workspace in SAPHIRE 8.

2.2.7 Observed Loss of Function of One or More Components in CCCG as a Result of Environmental Stress Caused by Failure or Degradation of Other Components outside Affected CCCG

There are two cases to consider. In the first case, the failed components in the affected CCCG conform to required environmental qualifications. In other words, there is no performance deficiency associated with the affected CCCG. The guidance here is the same as for the intersystem dependency.
discussed in Sec. 2.2.6. In the second case, the failed components do not conform to required environmental qualifications. Here, the analyst should set the associated basic events in the SPAR model to “Multiple failure,” if more than one component is affected, or to “Failure with potential shared cause” if only one component is affected.

2.2.8 No Observed Failure or Degradation in the Affected CCCG

For this case, the unconditional CCF probability in the SPAR model is retained for the ECA.

2.3 Cases where Guidance Might not Apply

The essence of the guidance for treating CCF in ECA can be summarized as follows:

- If one component has failed as a result of an identified performance deficiency, model the observed failure by setting the associated basic event in the SPAR model to “Failure with potential shared cause.”

- If two or more components in a CCCG have failed, model the observed failures by setting their basic events to “Multiple failure.”

Other, less frequent possibilities are discussed in Sec. 2.2 above. There can be cases where this guidance may not apply directly. These exceptional cases are expected to be related to the CCCG boundary.

2.3.1 CCCG Boundary Issues

For cases in this category, in which the CCCG boundaries are inaccurate, the analyst should, with assistance from the INL, modify the SPAR model to correct the inaccuracies, in accordance with the guidance in the RASP Handbook to ensure that the base case SPAR model represents the as-built, as-operated plant. This should be done prior to mapping the observed condition into the SPAR model and calculating the conditional CCF probability.
3. Issues with Current CCF Modeling and Data Analysis Relevant to ECA

The CCF models used in PRA were not developed with ECA in mind. Thus, it is not surprising that issues arise with these models in their application to ECA. In this Section we describe a number of these issues, focusing on the alpha-factor model, and the supporting data and parameter estimation techniques for this model. In Section 4, we describe ongoing and potential future research that has the potential to alleviate these limitations.

3.1 Issues with CCF Model

In this section, we discuss issues associated with the Basic Parameter Model (BPM), focusing on the alpha-factor parameterization, as this is the consensus approach to CCF in the SPAR models.

3.1.1 CCF Model is not Causal

As discussed briefly in Section 1, the BPM and its various parameterizations such as the alpha-factor model do not incorporate causes of failure explicitly. The consensus model for CCF in PRA is thus parametric, and the parameters in this model 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 poor maintenance practices. The aleatory model used for CCF in the SPAR models is a straightforward extension of the binomial model used for failures on demand. In that model the unknown parameter is $p$, the probability of failure on demand. Note that $p$ in the binomial model is not specific to any particular cause of failure; rather, it is a lumped parameter, encompassing all possible causes of failure.

For CCF, the observed random variable is a vector of failure counts, ($n_1$, $n_2$, ..., $n_m$), where $n_k$ is the observed number of events in which $k$ components have failed, and $m$ is the number of redundant components in the CCCG. The aleatory model for this vector of event counts is the multinomial distribution, and the unknown parameter of the aleatory model is a vector whose components are usually denoted in PRA as $(\alpha_1, \alpha_2, ..., \alpha_m)$. These are the so-called alpha factors in the parameterization of the BPM used by the NRC. Like the analogous parameter $p$ in the binomial distribution, the alpha factors are lumped parameters, encompassing failure from a variety of causes rather than from any specific cause. For more details on the alpha-factor model, refer to (Mosleh, Rasmuson, & Marshall, 1998)

This approach to modelling CCF, because it is not causal, cannot provide the estimate needed for ECA; it can only provide an approximate answer, using the calculations of conditional CCF probability described in (Rasmuson & Kelly, 2008). In these calculations, one can condition upon the observed failure, and upon whether there is a potential for the cause of failure, which is unspecified in the BPM, to be shared with the redundant component. But it is not possible to condition directly upon the underlying cause of failure.

For example, using the alpha-factor model for CCF, in a CCCG of size two, where both components must fail to fail the CCCG, the unconditional failure probability ($Q_g$) for the CCCG is given as $\alpha_1^2 Q_1^2 + \alpha_2 Q_1$. When one component fails, and there is potential for shared common cause, the conditional probability for failure of the CCCG becomes $\alpha_1^2 Q_1^2 + \alpha_2 \approx \alpha_2$. If the failure were judged to have no potential for shared common cause the conditional failure probability of the CCCG would be $\alpha_1 Q_1$. Again, these are CCCG failure probabilities, conditional upon an observed failure; they are not, however, conditional upon a single observed cause of the failure, such as poor maintenance. Thus, because the CCF parameter estimates are not specific to a single cause, conditional CCF probabilities calculated using these estimates are approximate answers to the question being posed by the ECA. As a result, the conditional CCF probability, which is a function of the baseline CCF parameter values, may be either conservative or nonconservative, depending on the specific situation being modeled.
3.1.2 BPM Employs a Symmetry Assumption

A simplifying assumption of the BPM is that each component in a CCCG has the same total failure rate or failure probability, denoted by $\lambda_t$ and $Q_t$, respectively. This assumption is employed in the SPAR models, as well. If only one component in a CCCG is degraded, and thus has a different $\lambda_t$ or $Q_t$ than the other components in the CCCG, the symmetry assumption breaks down. SAPHIRE handles this using the method described in (Rasmuson & Kelly, 2008), which assumes that the cause of the degradation is not shared with the other components in the CCCG. If more than one component is degraded, the analyst may have to create a new CCCG containing the degraded components.

3.1.3 CCF is not Modeled Across Component or System Boundaries

The SPAR models, like most PRA models, incorporate CCF only within the CCCG boundaries, meaning that a CCCG does not include components of a different type in the same system, or components from more than one system. This is fundamentally a limitation of the available CCF database, which is too sparsely populated to allow estimation of CCF parameters outside the CCCG boundaries. Causes of failure, particularly those residing in the organization, are of course not limited by such boundaries. This makes the risk estimates for ECA approximate, and potentially nonconservative.

3.1.4 Impact on More than One Failure Mode not Captured

The current consensus CCF model is also tied to specific component failure modes (e.g., failure to start). A performance deficiency, such as poor maintenance or poor quality control, which results in a failure to start of a component in a CCCG, could also impact the CCF probability of multiple components in the CCCG failing to run as well. However, such an impact on an unobserved failure mode cannot be captured in the current parametric CCF models.

3.1.5 Conditional CCF Calculations in Models for Support System Initiating Events (SSIE)

It is becoming more common for fault trees to be used as models for the occurrence of initiating events caused by failures in certain support systems, such as component cooling water (CCW). These so-called SSIE models, which are being added to the NRC SPAR models for selected initiators, afford a direct estimate of the impact on initiating event frequency of failures in the support system. However, an accurate assessment of the impact requires conditioning CCF probability upon the observed failure. This issue has not been treated in the existing literature, to the best of our knowledge.

The approach that we propose is most easily understood, and appears to give the most accurate results, if we recast the SSIE fault tree as a Markov model. As a simple example, consider a portion of the system that consists of two pumps in parallel, one normally running, and the other in standby, ready to start and run should the running pump fail. A reliability block diagram for this arrangement is shown in Figure 7.

Figure 7 Reliability block diagram for two pumps in parallel, one normally running, one in standby

In terms of the BPM for CCF, the minimal cut sets of this configuration are $A_iB_i$ and $C_{AB}$. This portion of the system can be represented in terms of a Markov model, as shown in Figure 8. This model shows the four possible states of the two pumps:
(1) State 0: both pumps operational

(2) State 1: Pump A failed, pump B operating. Transition from State 0 to State 1 occurs at rate $\lambda_1$, the independent failure rate in the BPM.

(3) State 2: Pump B failed, pump A operating. Transition from State 0 to State 2 occurs at rate $\lambda_1$, the independent failure rate in the BPM.

(4) State 3: Both pumps failed. Transition from State 0 to State 3 occurs at rate $\lambda_2$, the rate at which two components fail due to CCF in the BPM. Transitions from States 1 or 2 occur at rate $\lambda_t = \lambda_1 + \lambda_2$.

Following the BPM, the failure rate of each pump is denoted as $\lambda_i$ and this is partitioned into $\lambda_1$ and $\lambda_2$. Repair of a failed component occurs at a constant rate $\mu$ (i.e., repair time is exponentially distributed with mean repair time $1/\mu$). Once State 3 is reached, the initiating event has occurred, and so no repair is modeled from that state.

Figure 8 Markov model for two-pump configuration in Figure 7

The salient outputs are the time-dependent probabilities of being in a given state, given that we started in a particular state at time $t = 0$. The equation for these state probabilities can be written most conveniently in vector form as

$$\dot{P} = MP \quad (1)$$

In this equation, $M$ is the Markov transition matrix, which in this example is

$$M_{ij}$$

is the transition rate from State $i$ to State $j$. The initiating event frequency is the rate at which the configuration enters State 3, which is given in terms of the time-dependent state probabilities by
The state probabilities are given by the solution to Eq. 3.1, which is

$$w(t) = \hat{\lambda}_2 P_0(t) + \hat{\lambda}_1 P_1(t) + \hat{\lambda}_i P_i(t)$$  \hspace{1cm} (2)

The state probabilities are given by the solution to Eq. 3.1, which is

$$P(t) = E e^{zt} E^{-1} P(t = 0)$$  \hspace{1cm} (3)

In this equation, $E$ is a matrix whose columns are the eigenvectors of $M$, $E^{-1}$ is the inverse of $E$, and $e^{zt}$ is a matrix whose diagonal elements are the exponentiated eigenvalues ($z$) of $M$, with 0 for each off-diagonal entry. $P(t = 0)$ is the vector of initial conditions.

In terms of the alpha-factor model, the failure rates are given by

$$\lambda_k = \frac{k \alpha_k \hat{\lambda}_z}{\sum_{j=1}^{m} j \alpha_j}$$  \hspace{1cm} (4)

where $m$ is the CCCG size (two in this example). Thus we have

For an ECA example, assume that pump B has failed. We are interested in the frequency with which we enter State 3, given the failure of pump B. We first consider a case where the failed pump can be repaired, with repair time treated via an exponential distribution, as above. In this case, the Markov transition matrix is unchanged, but we must vary the initial conditions to reflect the failure of pump B. We will treat the initial conditions probabilistically, consistent with the manner with which we treat an observed failure elsewhere in ECA. In other words, given failure of pump B, we will initially be in State 1 or 2 with probability $1 - P(A|B)$ and in State 3 with probability $P(A|B)$.

The conditional probabilities are calculated by SAPHIRE, using the approach described in (Rasmuson & Kelly, 2008). We find for this example that

![Figure 9 Reduced Markov model for two-pump CCCG, given that pump B has failed with potential for CCF of pump A](image)

The reduced transition matrix is
The rate at which State 3 is entered (i.e., the conditional initiating event frequency given failure of pump B with potential for CCF) is given by

\[ w(t) = \lambda t P_2(t) = \lambda t C \exp(-\lambda t) \]  

(5)

In this equation, \( C \) is a constant, determined from the initial conditions, which we treat probabilistically, as we did above. The conditional probabilities are calculated by SAPHIRE, using the approach described in (Rasmuson & Kelly, 2008). As above, we find that

Substituting into Eq. 3.5, we find a conditional initiating event frequency of

\[ \lambda t C \exp(-\lambda t) \]

### 3.2 Issues with Alpha-Factor Estimates

CCF data analysis is focused on estimating parameters in a parametric CCF model, such as the alpha factors. These parameter estimates involve ratios of failure counts, such as the maximum likelihood estimate (MLE) of \( \alpha_k \):

\[ \hat{\alpha}_k = \frac{n_k}{\sum_{j=1}^{m} n_j} \]  

(6)

In this equation, and similar equations for other CCF parameters, \( n_k \) is the number of actual failures, without regard to the failure cause, occurring within a time window determined by the PRA mission time, involving \( k \) components in a CCCG of size \( m \). Of course, there can be subjectivity in estimating the observed value of \( n_k \), leading to a subjective distribution over the possible observed values (termed an impact vector), or what is used more commonly, an average over this distribution, which leads to fractional counts as the observed value. For more on data uncertainties in CCF parameter estimation, including statistical treatment of these uncertainties, see (Siu N., 1990) and (Siu & Kelly, 1998). Regardless of such complications, \( n_k \) is an estimate of the actual failure count. Note, also, that estimates of alpha factors are not developed for each cause individually; failure counts from multiple causes are combined together in the estimate.

Once alpha-factor estimates are in hand, estimates of the \( Q_k \)s in the BPM can be calculated. The \( Q_k \)s are used in SAPHIRE to calculate probabilities for basic events that represent CCF in the SPAR models. For the usual assumption of staggered testing, the following equation is currently used by SAPHIRE to estimate \( Q_k \) (Mosleh, Rasmuson, & Marshall, 1998):

\[ \hat{Q}_k = \left(\sum_{m=1}^{k-1} \hat{\alpha}_i \hat{Q}_i \right)^{1/(m-1)} \]  

(7)

It is worth emphasizing again that in this equation, and other similar ones based on the BPM, the parameter estimates that appear in the equations are based on counting failures versus modeling causes of failures. Thus, the BPM is a data-driven parametric approach to modelling CCF. As a result, estimates of
CCF probabilities are determined only by component type and size (i.e., redundancy level) of the CCCG, with failure causes lumped together in the parameter estimates.

Because of the conditional CCF calculations employed in ECA, the quantitative risk metrics used in ECA can be quite sensitive to the estimates of the alpha factors and to the sensitivity of the equations for $Q_k$ to the testing scheme. We describe in the following subsections a number of issues related to the alpha-factor estimates and the dependence of the equation for $Q_k$ upon the testing scheme.

### 3.2.1 Treatment of Shared Components and Latent Human Errors

As discussed in Sec. 1, the licensee PRA may treat explicitly some dependencies that are treated implicitly via CCF in the associated NRC SPAR models. The two principal examples where this occurs are shared equipment and latent (pre-initiator) human failure events (HFE). Detailed licensee PRAs will typically capture these types of dependence explicitly in the structure of the system fault trees, for example by including a basic event representing instrument miscalibrations in the fault trees of all systems that depend on those instruments. The Boolean reduction of the linked fault trees preserves this dependency, with the basic event for the miscalibration error appearing as a first-order cut set for the failure of multiple components or systems.

The SPAR models are typically less detailed in this respect, and thus do not typically represent such dependencies explicitly in the system fault trees. To compensate, if such dependencies result in events involving multiple component failures, these events will be factored into the alpha-factor estimates, using equations such as 3.6. For ECA, the analyst must determine whether particular dependencies of these types are captured in the SPAR models explicitly, via fault tree basic events, or implicitly, via inclusion in the estimates of the alpha factors. If the results for an ECA are particularly sensitive to an estimated alpha-factor, the analyst may wish to have the INL derive an updated alpha-factor estimate that excludes such un-modeled dependencies.

### 3.2.2 Prior Distributions for Alpha Factors

The basis for the prior distribution in the NRC CCF database has not been published, and so we describe here the approach that was used to develop this prior. Currently, the prior distribution for alpha factors is a Dirichlet distribution, the multivariate generalization of the beta distribution, whose parameters are estimated using data from the period 1995-2005. This period was chosen because it was believed to be more representative of current plant conditions and practices than older data, which extends back to 1980.

The parameters of the Dirichlet prior are not component-specific, but are estimated from observed data for CCCG group sizes from 2 to 16. The total number of CCF events is the sum of so-called “complete” events, in which all components in the group fail, and “partial” events, in which a subset of the number of components in the group fail.

Especially for larger group sizes, the number of partial events is significantly larger than the number of complete events. Because it was felt that the number of complete CCF events may be under-represented, especially for larger group sizes, a statistical model was developed to estimate the number of “missing” complete events, and these were then added to the partial event counts for each group size. Table 1 shows the CCF data for the period 1995-2005. The statistical model used to augment the complete counts was a binomial distribution with parameters $n_i$ and $p_i$, where $i$ is the group size, $n_i$ is the number of complete CCF events, and $p_i$ is the probability of a complete CCF event.

**Table 1 CCF data used to develop alpha-factor prior distribution**

<table>
<thead>
<tr>
<th>Group size</th>
<th>Partial CCF events</th>
<th>Complete CCF events</th>
<th>Total CCF events</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>55</td>
<td>25</td>
<td>80</td>
</tr>
</tbody>
</table>
A logistic regression (also sometimes called a binomial regression) model was used to estimate $p_i$ for each group size:

$$\log\left(\frac{p_i}{1-p_i}\right) = a + bi, i = 2, 3, \ldots, 16$$  \hspace{1cm} (8)

The coefficients $a$ and $b$ were estimated via a least-squares approach, and the expected number of additional complete CCF events for group size $i$ is then given in terms of the estimates of $a$ and $b$ by

$$n_i \hat{p}_i = n_i\frac{\exp(\hat{a} + \hat{b}i)}{1 + \exp(\hat{a} + \hat{b}i)}$$  \hspace{1cm} (9)

These additional complete CCF events were added to the observed $n_i$ for each group size. Eq. 3.6 was then used to find the MLE of each $\alpha_k$, and this was treated as the mean of a constrained noninformative marginal prior for $\alpha_k$, which can be approximated by a beta distribution, see (Atwood, 1996) for more details. The first (second) parameter is approximately 0.5 for $\alpha_k < (>) 0.5$, and the sum of the two parameters, $\delta$, measures the dispersion of the distribution. Treating the MLE of $\alpha_k$ as the mean of the prior distribution, we have that $\delta_k = (\text{first parameter})/\alpha_k$.

This approach does not enforce the sum-to-unity constraint on the alpha factors for a given group size, which induces a correlation among the alpha factors. The Dirichlet distribution is the conjugate prior for the alpha-factors. It is a multivariate extension of the beta distribution. The Dirichlet parameters are denoted $\theta_k$, and the marginal distribution of each $\alpha_k$ is a beta distribution with first parameter $\theta_k$ and second parameter $\theta_t - \theta_k$, where $\theta_t = \Sigma \theta_j$. Thus, the marginal mean of each alpha-factor is $\theta_t/\theta_t$. Taking the MLE of each $\alpha_k$ as the mean, if $\theta_t$ were known, the parameters of the Dirichlet prior would be fully specified. The approach taken to specifying $\theta_t$ was to treat it as the geometric mean of the $\delta_k$s calculated above.
The prior parameters for the four reactor protection systems were developed in a similar way, although they are based on different datasets and the approach to developing the prior distribution did not supplement the number of complete CCF events with the expected complete event counts from the logistic regression model described above. The details can be found in NUREG/CR-5500, Vols. 2 (Westinghouse), 3 (General Electric), 10 (Combustion Engineering), and 11 (Babcock and Wilcox).

As discussed above, the alpha factor estimates fundamentally involve ratios of event counts, as in Eq. 3.6. For CCCGs with four or more redundant components, the event count data for \( n_m \) (representing failure of the entire CCCG) are extremely sparse; there are extremely few events involving failure of more than about 4 components.\(^a\)

The NRC CCF database actually performs Bayesian inference for the alpha factors, using a Dirichlet prior distribution. So Eq. 3.6 can be modified to give the posterior mean of each alpha factor as

\[
\hat{\alpha}_k = \frac{n_k + \theta_k}{\sum_{j=1}^{m} (n_j + \theta_j)}
\]

where \( \theta_k \) is the \( k \)th parameter of the Dirichlet prior for the alpha-factors. If \( n_k \) is zero, the posterior mean of \( \alpha_k \) is strongly influenced by \( \theta_k \).

Because of the sparsity of data, the prior distribution dominates the CCF parameter estimates for high-order CCCGs. In such cases, the data-based prior has difficulty replicating the observed data, and the parameters of the prior should be selected carefully. The analyst must remain aware of the influence of the prior on calculated quantities involving high-order alpha-factors, such as conditional CCF probabilities used in ECA. One recently developed approach for selecting Dirichlet prior distributions in such cases is described in (Kelly & Atwood, 2011).

### 3.2.3 Estimates of Alpha Factors are not Plant-Specific

The alpha-factor estimates in the CCF Parameter Estimation Update, which are used to calculate CCF probabilities in the SPAR models, are generic for a type of component. Because they are not plant-specific, they contribute to the approximate nature of ECA risk estimates. A review done by Karl Fleming for the Advisory Committee on Reactor Safeguards (Fleming K. N., 2003) raised this and some related issues regarding treatment of CCF. The other issues raised in (Fleming K. N., 2003) that are relevant to ECA were

- Need to treat asymmetric component configurations (discussed above);
- Lack of treatment of plant-to-plant variability in CCF parameter estimates, particularly for EDGs.

### 3.2.4 Treatment of Staggered Testing

In the nuclear power domain, nearly all failure events of most safety-related components are found during periodic tests rather than unplanned demands. The common testing schemes are

- Nonstaggered tests. For each test, the entire group of \( m \) components is tested, and the number of components that fail the test is recorded. Any failed components are repaired and the causes of the failures are removed. Therefore, the outcomes of distinct group tests are independent.

\(^a\) A search of the NRC CCF database for the period beginning in 1997 reveals only five so-called “complete failures” for group sizes of four or larger.
• Staggered tests with follow-up. The components in the group are tested one at a time, so that the entire cycle of $m$ components is tested periodically. If a component passes a scheduled test, nothing more is done until it is time for the next component to be tested. If, instead, a component fails its scheduled test, then all the other components are tested, and any failed components are repaired and their failure causes are removed.

• Staggered tests without follow-up. This is the same as above, except if a component fails its scheduled test, it alone is repaired. The other components are not tested until their scheduled times.

Across the U. S. nuclear power industry, a mixture of testing strategies appears to be in use. The vast majority of plants claim to use staggered testing, but some plants seem to use nonstaggered testing when it is more convenient. Moreover, some components, notably the large important ones such as pumps and diesel generators, have Technical Specifications requirements for follow-up after a component failure. However, other components, such as some valves, do not have such Technical Specifications, and follow-up is not necessarily performed for these components.

As discussed above, the probabilities of the CCF basic events in the SPAR models are a function of the $Q_k$s, which in turn are a function of the $\alpha_k$s. For staggered testing, Eq. 3.7 is used by the CCF module in SAPHIRE to calculate $Q_k$. A white paper by Cory Atwood and Dana Kelly (see App. B) has examined the mathematical foundations of this equation, and of Eq. 3.6 for the alpha-factor estimates, and has concluded that both of these equations may be in error.

The estimate of $\alpha_k$ may not be independent of the testing scheme, contrary to what has long been believed to be the case, and Eq. 3.6 may give conservative estimates for $\alpha_k$ if it is used with data collected under a staggered-testing scheme. Balancing this conservatism, Eq. 3.7 may be incorrect for staggered testing, and may give results for $Q_k$ that are too small by a factor of $k$. The net impact on ECA of these equations being incorrect remains to be examined.
4. Future Research

In this section, we describe research being considered to address some of the issues and limitations described in Sec. 3. We indicate in each case where the research is already underway, and an estimated time frame for completing the research. We will refer to the following time frames:

- Immediate: < 6 months
- Short term: 6 months – 2 years
- Intermediate term: 2-5 years
- Long term: > 5 years

Some or all of this research may be carried out in partnership with the Electric Power Research Institute, under a Memorandum of Understanding with the U. S. NRC.

4.1 Causal Failure Models

To directly address the question being asked in ECA, one needs a model that links equipment failures to their causes in a probabilistic fashion, allowing the analyst to estimate conditional probabilities of failure, given a particular cause such as poor maintenance. A Bayesian network is one such model. A Bayesian network is a type of probabilistic graphical model, first developed by Judea Pearl as a model for probabilistic reasoning by intelligent systems (Pearl J. , 1988). Specifically, a Bayesian network is a directed acyclic graph (DAG), in which nodes in the graph represent events of interest, and the edges connecting the nodes represent the directional influence of one event upon another. There are no loops in the graph, as an event cannot influence its own occurrence. An example of a Bayesian network was given in Figure 1, reproduced here for convenience. For theoretical details on Bayesian networks see (Pearl J. , 2009) and (Neapolitan, 2004). For a more practical treatment, including applications, see (Kjaerulff & Madsen, 2008) and (Pourret, Naim, & Marcot, 2008). For more general types of probabilistic graphical models, including Bayesian networks, (Koller & Friedman, 2009) is an excellent reference text.
Causal models have the potential to address the influence of organizational factors on equipment reliability, and to address intersystem failure potential. Some preliminary ideas for this type of model can be found in (Kelly, Shen, DeMoss, Coyne, & Marksberry, 2010). Research into this type of model is getting underway at the University of Maryland, sponsored by the U. S. NRC and led by Prof. Ali Mosleh. The modeling portion of this work is targeted for completion in the intermediate term; however, bringing such a model into production is expected to be a long-term effort, as substantial effort will likely be needed to develop an underlying database for quantification.

### 4.2 SSIE Models

The INL is exploring various approaches to ECA using the SSIE models being developed by NRC and EPRI under a Memorandum of Understanding. Currently, the models are in the form of fault trees, and produce minimal cut sets. This results in approximate answers in comparison with the answers provided by a Markov model. More work is needed to decide if better approximations can be obtained with the fault tree models, or whether it is feasible to use the Markov model directly. This research is categorized as short-term.
4.3 Enhancements to NRC CCF Database

4.3.1 Prior Distribution for Alpha-Factors

Because of the sensitivity of ECA risk metrics to the alpha-factor estimates that can result from the conditional CCF calculations, we plan to revisit the current data-driven approach to developing the prior distribution for the alpha factors that was described in Sec. 3. As discussed there, the current prior is based on CCCG size only, and is not component-specific. We will explore the possibility of component-specific priors, along with approaches that incorporate non-empirical information, such as the approach described in (Kelly & Atwood, 2011). This work is planned for the short term.

4.3.2 Plant-Specific Alpha-Factor Estimates

As discussed above, the alpha-factor estimates are not plant-specific, and the estimates do not reflect plant-to-plant variability. (Fleming K. N., 2003) suggested exploring treatment of such variability for certain components, such as EDGs. At this time, it is felt that the data are too sparse to support plant-to-plant variability modeling, so no research is planned in this area at present.

4.3.3 Adjusting Alpha-Factor Estimates

As discussed in Sec. 3, the NRC SPAR models tend to treat certain shared components and latent HFIs implicitly, whereas such dependencies would typically be treated explicitly in licensee PRA models. Including such events in the alpha-factor estimates can give conservative risk estimates if the dependence is modeled explicitly in the PRA. We plan to explore making it possible for the user to estimate the contribution of such events to the alpha-factor estimates, via the software interface to the NRC CCF database. We expect to complete this effort in the short term.

4.3.4 Effects of Testing Schemes on Estimators

Some review of the white paper mentioned above has already been performed. Additional reviews are planned for the immediate term. If the results described in App. B are found to be correct, work will be needed to revise the alpha-factor estimates in the NRC CCF database, and follow-on changes will need to be made in the SPAR models. This additional work, if needed, is planned for the short term.


Appendix A
Conditional Common-Cause Failure Probability Calculations

This appendix details the mathematics used by Systems Analysis Programs for Hands-On Integrated Risk Evaluations (SAPHIRE) 8 to calculate conditional common-cause failure (CCF) probabilities. It is taken from (Rasmuson & Kelly, 2008). Appendix B to the SAPHIRE 8 technical reference includes details of the SAPHIRE calculations themselves.

A.1 Review of Basic Parameter Model and Alpha-Factor Parameterization

A common-cause basic event (CCBE) is an event representing failure of a specific set of components in a common-cause component group (CCCG) resulting from a common cause. For example, in a CCCG of three redundant components labeled $A$, $B$, and $C$, the CCBEs are $C_{AB}$, $C_{AC}$, $C_{BC}$, and $C_{ABC}$. The first three events are CCF events involving only two components (e.g., $A$ and $B$), and the fourth is a CCF event involving all three components. Note that the CCBEs are only identified by the impact they have on specific sets of components within the CCCGs. Impact in this context is limited to “failed” or “not failed.” Note also that the cause of failure is not modeled explicitly, and a single CCBE may implicitly include several CCF mechanisms.

The complete set of basic events, including CCBEs, involving component $A$ in the three-component CCCG is as follows:

- $A_I$ = single independent failure of component $A$ (a basic event)
- $C_{AB}$ = failure of components $A$ and $B$ (and not $C$) from common causes
- $C_{AC}$ = failure of components $A$ and $C$ (and not $B$) from common causes
- $C_{ABC}$ = failure of components $A$, $B$, and $C$ from common causes

Component $A$ fails if any of the above events occur. Similar basic events are defined for components $B$ and $C$. The equivalent Boolean representation of total failure of components $A$, $B$, and $C$ is given by:

$$A_t = A_I \cup C_{AB} \cup C_{AC} \cup C_{ABC}$$
$$B_t = B_I \cup C_{AB} \cup C_{BC} \cup C_{ABC}$$
$$C_t = C_I \cup C_{AC} \cup C_{BC} \cup C_{ABC}$$

This representation of the total failure probability of a component in terms of independent and common-cause events is known as the basic parameter model (BPM). A further assumption of the BPM is that the terms in the above expansions of $A_t$, $B_t$, and $C_t$ are a partition. In other words, all of the terms in the expansion of a particular event (e.g., $A_I$) are mutually exclusive.

By definition in the BPM, events $A_I$, $B_I$, and $C_I$ are independent. Using this fact, and employing the rare event approximation, the failure probability of the two-out-of-three system is given by:

$$Pr(S) = Pr(A_I B_I) + Pr(A_I C_I) + Pr(B_I C_I) + Pr(C_{AB}) + Pr(C_{AC}) + Pr(C_{BC}) + Pr(C_{ABC})$$  \hspace{1cm} (A.1)

The BPM for CCF contains an underlying assumption of symmetry: the probabilities of similar events involving similar components (i.e., events in the same CCCG) are the same. This approach takes advantage of the physical symmetries associated with identical redundant components in reducing the number of parameters that need to be quantified. For example, in the above equation it is typically
assumed that:

\[ \text{Pr}[A_i] = \text{Pr}[B_j] = \text{Pr}[C_j] = Q_1 \]
\[ \text{Pr}[C_{AB}] = \text{Pr}[C_{AC}] = \text{Pr}[C_{BC}] = Q_2 \]
\[ \text{Pr}[C_{ABC}] = Q_3 \]

In other words, the probability of occurrence of any basic event within a given CCCG is assumed to depend only on the number and not on the specific components in that basic event. This is called the symmetry assumption.

With the symmetry assumption and using the notation just introduced, the CCCG failure probability under the rare event approximation can be written as:

\[ Q_s = 3Q_1^2 + 3Q_2 + Q_3 \]  

(A.3)

\[ Q_{(m)}^k = \text{probability of a CCBE involving } k \text{ specific components in a CCCG of size } m, (1 \leq k \leq m). \]  

In terms of the \( Q_{(m)}^k \)s, the total failure probability of a component, \( Q_t \), can be written as:

\[ Q_t = \sum_{k=1}^{m} \binom{m-1}{k-1} Q_{(m)}^k \]  

(A.4)

In the standard approach to the BPM, \( Q_t \) is conserved as CCCG redundancy changes. However, \( Q_{(m)}^k \) varies as the level of redundancy (\( m \)) changes.

The alpha-factor model develops CCF probabilities from a set of failure ratios and the total component failure probability (\( Q_t \)). The parameters of the model are:

- \( Q_t \) = total failure probability of each component from all independent and CCF events
- \( \alpha_k \) = fraction of the total number of failure events that occur in the CCCG that involve the failure of \( k \) components from a common cause

Using these parameters, depending on the assumption regarding the way components in the CCCG are tested, the probability of a CCBE involving failure of \( k \) components in a CCCG of \( m \) components is given by the following:

For a staggered testing scheme (see Chapter 3 for a discussion of the potential inaccuracy of this equation):

\[ Q_{(m)}^k = \frac{1}{m-1} \frac{\alpha_k}{k-1} Q_t \]  

(A.5)

For a nonstaggered testing scheme or if there is no testing scheme:

\[ Q_{(m)}^k = \frac{k}{m-1} \frac{\alpha_k}{k-1} Q_t \]  

(A.6)

\[ a \] This and the following equations apply to the failure rate, \( \lambda_t \), for normally running components.
where
\[ \alpha_i = \sum_{k=1}^{m} k \alpha_k . \] (A.7)

As an example (assuming staggered testing), the probabilities of the basic events of the three-component CCCG are written as:

\[ Q_1^{(3)} = \alpha_1 Q_t \]
\[ Q_2^{(3)} = \frac{1}{2} \alpha_2 Q_t \]
\[ Q_3^{(3)} = \alpha_3 Q_t \] (A.8)

A.2 Calculating Conditional Common-Cause Failure Probability

Consider a CCCG of size three. We denote the components by \(A\), \(B\), and \(C\). We will consider two CCF-susceptible failure modes—failure to start, denoted by \(S\), and failure to run, denoted by \(R\). The \(S\) and \(R\) can be a superscript, subscript, or a regular letter, depending upon the context. We will present the details of the calculation for this case to illustrate how the result depends upon the underlying BPM and associated simplifying assumptions, the definition of conditional probability, and the alpha-factor parameterization of the BPM.

Using the BPM, we define the total failure to start of component \(A\) by the following equation:

\[ A_t^S = A_s \cup S_{AB} \cup S_{AC} \cup S_{ABC} \] (A.9)

Where
\(A_t^S\) = Total Failure to start of component \(A\) from all causes
\(A_s\) = Failure to start of component \(A\) from independent causes
\(S_{AB}\) = Failure of components \(A\) and \(B\) to start due to common causes
\(S_{AC}\) = Failure of components \(A\) and \(C\) to start due to common causes
\(S_{ABC}\) = Failure of components \(A\), \(B\), and \(C\) to start due to common causes

We will assume that this representation of \(A_t^S\) constitutes a partition. Similarly, we define total failure to start of components \(B\) and \(C\) by the following equations:

\[ B_t^S = B_s \cup S_{AB} \cup S_{BC} \cup S_{ABC} \]
\[ C_t^S = C_s \cup S_{AC} \cup S_{BC} \cup S_{ABC} \] (A.10)

We define total failure to run of each component (component \(A\) is shown) by a similar equation:

\[ A_t^R = A_r \cup R_{AB} \cup R_{AC} \cup R_{ABC} \] (A.11)
The success criterion we will consider is that one of the three components must function. Thus, to have failure of the system, all three components must fail. They can fail to start or fail to run. Figure 11 shows the fault tree. Note that this is not typical of most PRA fault trees, as it has been expanded to include all elements of the BPM, which are needed for the exact solution. Table 2 lists the failure probabilities for the failure-to-start and failure-to-run modes, including CCF parameters. Table 3 lists the basic event failure probabilities produced by the alpha-factor parameterization of the BPM, assuming staggered testing.

Table 4 shows the quantified cut sets. Note that cut sets such as $S_{AB}S_{AC}$ have not been included, as discussed above. However, other similarly structured cut sets, such as $R_{AC}S_{BC}$ are included, because each term is a contributor to the total failure probability of a component to run or start, respectively. Hence, to conserve the total probability of failure for each component, these terms must be included. The total failure probability for the three-train CCCG is $1.24 \times 10^{-4}$.

![Figure 11 Example fault tree for two failure modes and three components](image)

### Table 2 Component Failure Probabilities for Three-Component Example

<table>
<thead>
<tr>
<th>Basic Event</th>
<th>Failure Probability</th>
<th>Basic Event</th>
<th>Failure Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>QT</td>
<td>5.000E-03</td>
<td>QT</td>
<td>1.193E-02</td>
</tr>
<tr>
<td>$\alpha_1$</td>
<td>0.98195</td>
<td>$\alpha_1$</td>
<td>0.97029</td>
</tr>
<tr>
<td>$\alpha_2$</td>
<td>0.0134</td>
<td>$\alpha_2$</td>
<td>0.0223</td>
</tr>
<tr>
<td>$\alpha_3$</td>
<td>0.00465</td>
<td>$\alpha_3$</td>
<td>0.00741</td>
</tr>
</tbody>
</table>

### Table 3 Basic Event Probabilities for Three-Component Example

<table>
<thead>
<tr>
<th>Basic Event</th>
<th>Failure Probability</th>
<th>Basic Event</th>
<th>Failure Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-S</td>
<td>4.910E-03</td>
<td>A-R</td>
<td>1.16E-02</td>
</tr>
<tr>
<td>B-S</td>
<td>4.910E-03</td>
<td>B-R</td>
<td>1.16E-02</td>
</tr>
<tr>
<td>C-S</td>
<td>4.910E-03</td>
<td>C-R</td>
<td>1.16E-02</td>
</tr>
<tr>
<td>S-AB</td>
<td>3.350E-05</td>
<td>S-AB</td>
<td>3.350E-05</td>
</tr>
<tr>
<td>S-AC</td>
<td>3.350E-05</td>
<td>R-AB</td>
<td>1.33E-04</td>
</tr>
<tr>
<td></td>
<td></td>
<td>R-AC</td>
<td>1.33E-04</td>
</tr>
</tbody>
</table>

Figure 11 Example fault tree for two failure modes and three components
Table 4  Quantified Minimal Cut Sets for Three-Component Example

<table>
<thead>
<tr>
<th>Cut set</th>
<th>Cut set Probability</th>
<th>Cut set</th>
<th>Cut set Probability</th>
<th>Cut set</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2.325E-05</td>
<td>S-ABC</td>
<td>16</td>
<td>2.797E-07</td>
</tr>
<tr>
<td>3</td>
<td>1.561E-06</td>
<td>A-R, B-R, C-R</td>
<td>17</td>
<td>2.797E-07</td>
</tr>
<tr>
<td>4</td>
<td>1.543E-06</td>
<td>B-R, R-AC</td>
<td>18</td>
<td>2.797E-07</td>
</tr>
<tr>
<td>5</td>
<td>1.543E-06</td>
<td>C-R, R-AB</td>
<td>19</td>
<td>1.645E-07</td>
</tr>
<tr>
<td>6</td>
<td>1.543E-06</td>
<td>A-R, R-BC</td>
<td>20</td>
<td>1.645E-07</td>
</tr>
<tr>
<td>8</td>
<td>6.607E-07</td>
<td>A-R, B-R, C-S</td>
<td>22</td>
<td>1.184E-07</td>
</tr>
<tr>
<td>9</td>
<td>6.607E-07</td>
<td>A-S, B-R, C-R</td>
<td>23</td>
<td>4.455E-09</td>
</tr>
<tr>
<td>10</td>
<td>6.530E-07</td>
<td>B-S, R-AC</td>
<td>24</td>
<td>4.455E-09</td>
</tr>
<tr>
<td>11</td>
<td>6.530E-07</td>
<td>C-S, R-AB</td>
<td>25</td>
<td>4.455E-09</td>
</tr>
<tr>
<td>13</td>
<td>3.886E-07</td>
<td>C-R, S-AB</td>
<td>27</td>
<td>4.455E-09</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Total</td>
<td>1.244E-04</td>
</tr>
</tbody>
</table>

A.2.1  Failure To Start

We now estimate the conditional failure probability of the CCCG given that component $A$ fails to start, and this failure has the potential to be shared with the other two components in the CCCG. To obtain the cut sets for the numerator of the calculation, we construct a fault tree with the top event in Figure 1 ANDed with $A^c$. Table 5 lists the 22 cut sets for this case along with the numerical results. Note that, among these results, are cut sets such as \{A-S, R-ABC\}. This cut set may appear odd, as it seems to imply that component $A$ both fails to start and fails to run. However, R-ABC is a contributor to the total failure-to-run probability of components $B$ and $C$. This probability has not been changed by the failure of component $A$ to start, so such terms remain in the results.

The conditional CCF probability is obtained by dividing each cut set’s probability by the total failure-to-start probability of component $A$ (i.e., 0.005). The last column of Table 5 contains the results. The total conditional CCF probability is equal to $5.400 \times 10^{-3}$.

Table 5  Quantified Minimal Cut Sets and Conditional Probabilities for Three-Component Example, Given Observed Failure To Start of Component $A$

<table>
<thead>
<tr>
<th>No.</th>
<th>Cut Set</th>
<th>Cut Set Probability</th>
<th>Conditional Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Event</td>
<td>Failure Rate 1</td>
<td>Failure Rate 2</td>
</tr>
<tr>
<td>---</td>
<td>------------------</td>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>1</td>
<td>S-ABC</td>
<td>2.325E-5</td>
<td>4.65E-03</td>
</tr>
<tr>
<td>2</td>
<td>A-S, B-R, C-R</td>
<td>6.607E-7</td>
<td>1.32E-04</td>
</tr>
<tr>
<td>3</td>
<td>A-S, R-BC</td>
<td>6.530E-7</td>
<td>1.31E-04</td>
</tr>
<tr>
<td>4</td>
<td>A-S, R-ABC</td>
<td>4.340E-07</td>
<td>8.68E-05</td>
</tr>
<tr>
<td>5</td>
<td>B-R, S-AC</td>
<td>3.886E-7</td>
<td>7.77E-05</td>
</tr>
<tr>
<td>6</td>
<td>C-R, S-AB</td>
<td>3.886E-7</td>
<td>7.77E-05</td>
</tr>
<tr>
<td>7</td>
<td>A-S, B-S, C-R</td>
<td>2.790E-7</td>
<td>5.58E-05</td>
</tr>
<tr>
<td>8</td>
<td>A-S, B-R, C-S</td>
<td>2.790E-7</td>
<td>5.58E-05</td>
</tr>
<tr>
<td>9</td>
<td>A-S, S-BC</td>
<td>1.645E-07</td>
<td>3.29E-05</td>
</tr>
<tr>
<td>10</td>
<td>B-S, S-AC</td>
<td>1.645E-07</td>
<td>3.29E-05</td>
</tr>
<tr>
<td>11</td>
<td>C-S, S-AB</td>
<td>1.645E-07</td>
<td>3.29E-05</td>
</tr>
<tr>
<td>12</td>
<td>A-S, B-S, C-S</td>
<td>1.184E-07</td>
<td>2.37E-05</td>
</tr>
<tr>
<td>13</td>
<td>A-S, C-R, R-AB</td>
<td>7.575E-09</td>
<td>1.52E-06</td>
</tr>
<tr>
<td>14</td>
<td>A-S, B-R, R-AC</td>
<td>7.575E-09</td>
<td>1.52E-06</td>
</tr>
<tr>
<td>15</td>
<td>R-AB, S-AC</td>
<td>4.455E-09</td>
<td>8.91E-07</td>
</tr>
<tr>
<td>16</td>
<td>R-BC, S-AC</td>
<td>4.455E-09</td>
<td>8.91E-07</td>
</tr>
<tr>
<td>17</td>
<td>R-AC, S-AB</td>
<td>4.455E-09</td>
<td>8.91E-07</td>
</tr>
<tr>
<td>18</td>
<td>R-BC, S-AB</td>
<td>4.455E-09</td>
<td>8.91E-07</td>
</tr>
<tr>
<td>19</td>
<td>A-S, C-S, R-AB</td>
<td>3.206E-09</td>
<td>6.41E-07</td>
</tr>
<tr>
<td>20</td>
<td>A-S, B-S, R-AC</td>
<td>3.206E-09</td>
<td>6.41E-07</td>
</tr>
<tr>
<td>21</td>
<td>R-ABC, S-AC</td>
<td>2.961E-09</td>
<td>5.92E-07</td>
</tr>
<tr>
<td>22</td>
<td>R-ABC, S-AB</td>
<td>2.961E-09</td>
<td>5.92E-07</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td><strong>2.699E-5</strong></td>
<td><strong>5.400E-3</strong></td>
</tr>
</tbody>
</table>

### A.2.2 Independent Failure To Start

Conditioning upon an independent component failure (i.e., a failure with no potential for shared common-cause mechanisms with other components in the CCCG) is the exception, rather than the rule. Since this is an independent failure we condition on $A_i$ rather than $A_r$.

Equation 12 derives the numerator cut sets for the conditional probability that the CCCG fails, given that component $A$ has failed independently. In deriving this result, we have applied the assumption that the BPM constitutes a partition of each failure mode. This leads to the elimination of cut sets such as $A_i S C_1 R C_{AB}^s$. 

---

Draft
Table 6 shows the results of applying this calculation to our size three example above.

<table>
<thead>
<tr>
<th>No.</th>
<th>Cut Sets</th>
<th>Cut Set Probability</th>
<th>Conditional Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A-S, B-R, C-R</td>
<td>6.607E-07</td>
<td>1.35E-04</td>
</tr>
<tr>
<td>2</td>
<td>A-S, R-BC</td>
<td>6.530E-07</td>
<td>1.33E-04</td>
</tr>
<tr>
<td>3</td>
<td>A-S, R-ABC</td>
<td>4.340E-07</td>
<td>8.84E-05</td>
</tr>
<tr>
<td>4</td>
<td>A-S, B-S, C-R</td>
<td>2.797E-07</td>
<td>5.70E-05</td>
</tr>
<tr>
<td>5</td>
<td>A-S, B-R, C-S</td>
<td>2.797E-07</td>
<td>5.70E-05</td>
</tr>
<tr>
<td>6</td>
<td>A-S, S-BC</td>
<td>1.645E-07</td>
<td>3.55E-05</td>
</tr>
<tr>
<td>7</td>
<td>A-S, B-S, C-S</td>
<td>1.184E-07</td>
<td>2.41E-05</td>
</tr>
<tr>
<td>8</td>
<td>A-S, C-R, R-AB</td>
<td>7.575E-09</td>
<td>1.54E-06</td>
</tr>
<tr>
<td>9</td>
<td>A-S, B-R, R-AC</td>
<td>7.575E-09</td>
<td>1.54E-06</td>
</tr>
<tr>
<td>10</td>
<td>A-S, C-S, R-AB</td>
<td>3.206E-09</td>
<td>6.53E-07</td>
</tr>
<tr>
<td>11</td>
<td>A-S, B-S, R-AC</td>
<td>3.206E-09</td>
<td>6.53E-07</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>2.61E-06</td>
<td>5.32E-04</td>
</tr>
</tbody>
</table>

A.2.3 Test or Preventive Maintenance Outage

In this case, the condition is that one component in a CCCG is out of service for preventive maintenance or testing. We will again consider a CCCG of size three, with components designated A, B, and C, and a one-of-three success criterion. We will assume that component C is unavailable as a result of preventive maintenance and that it is not in a failed state (as it would be if the maintenance outage were for corrective maintenance). Although component C is out for preventive maintenance and thus cannot itself fail, the potential exists for causes and coupling factors still to be shared between component C and the other components in the CCCG. That is, C_{AC}, C_{BC}, and C_{ABC} have not occurred, but they could occur. Events C_{AC} and C_{ABC} now represent causes that have the potential to fail components A and C, or A, B, and C, respectively. Another perspective is that removing component C from service has not affected the total failure probability for either of the other two components, and the total failure probability, by the BPM, includes terms such as C_{AC}, C_{BC}, and C_{ABC}. Since component C is unavailable, but not failed, the cut sets for this case reduce to {A_B, B_i}, {A_i, C_{BC}}, {B_i, C_{AC}}, {C_{AB}}, and {C_{ABC}}. Quantification of these cut sets in terms of the BPM yields:

\[
\Pr(A_i \cap B_i \cap C_i \mid C_m) = Q_1^2 + 2Q_1Q_2 + Q_2 + Q_3 \\
\approx Q_1^2 + Q_2 + Q_3
\]  

(A.13)

where C_m denotes that component C is unavailable because of testing or preventive maintenance.
Appendix B
Effects of Testing Schemes on Common-Cause Failure Parameters

This appendix provides details from the white paper prepared by Corwin Atwood and Dana Kelly on the statistical foundations of the basic parameter model (BPM) and alpha-factor parameterization. Specifically, this appendix treats these models from a statistical viewpoint, laying out the statistical distributions of the various failure counts under various testing strategies and assumptions.

Only failures on demand are considered; this appendix does not consider standby failures, in which failures become more likely as time passes since the last test. Some other issues of practical importance are also not considered. These include heterogeneity (variability in the parameter values for different data sources) and inference for a group of one size based on data from groups of different sizes. The focus of this appendix is to develop statistical distributions for the common-cause failure (CCF) data under various testing strategies and to find the resulting maximum likelihood estimates (MLEs) of the model parameters, noting any problems encountered along the way.

B.1 Common-Cause Failure Model Parameters

The model contains $m$ identical standby components that are occasionally demanded to operate and may succeed or fail. The parameters are based on the assumption that all $m$ components in the group are demanded at once; this is the typical scenario in a probabilistic risk assessment (PRA) analysis. We emphasize here that these parameters are constants, independent of whatever methods may be used to gather data or to estimate them.

The basic parameters are defined for $1 \leq k \leq m$ as:

$$Q_k$$ is the probability that a particular set of $k$ components (and no other components) fails when all $m$ components are demanded.

The definition often includes the phrase “fails due to a common cause.” This is sometimes ignored because of the difficulties of identifying the cause, interpreting the proximate and root causes, and finding this information in the event reports.

Implicit in the definition is the assumption that $Q_k$ depends on $k$, and only on $k$, not on the particular $k$ components being considered. Therefore, the probability that exactly $k$ components fail, but not any particular specified set of $k$ components, is:

$$\binom{m}{k} Q_k$$  \hspace{1cm} (B.1)

The binomial coefficient is the number of distinct $k$-component subsets that can be formed from a total of $m$ components.

Likewise the following is a parameter, interpreted as the probability that $k$ components fail, given that at least one component fails, when all $m$ components are demanded:
\[ \alpha_k = \frac{\binom{m}{k} Q_t}{\sum_{j=1}^{m} \binom{m}{j} Q_j} \]  

(B.2)

An alternative interpretation is that \( \alpha_k \) is the long-term fraction of \( k \)-component failure events, among all events having at least one failed component; this still assumes that all \( m \) components are demanded in each event.

Finally, the overall probability that a specific component fails when all \( m \) components are demanded is denoted \( Q_t \). In terms of the \( Q_j \)s, it is given by:

\[ Q_t = \sum_{k=1}^{m} \binom{m-1}{k-1} Q_k \]  

(B.3)

Like the \( Q_j \)s, \( Q_t \) is a parameter of the model.


\[ Q_t = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_t \]  

(B.4)

where \( \alpha_t = \sum \alpha_k \), and \( \alpha_k \) and \( Q_t \) are defined by Equations B.2 and B.3. Equation B.4 follows from the definitions of \( \alpha_k \) and \( Q_t \). It allows the parameters \( Q_t \) to be found from the \( \alpha_k \)s and \( Q_t \). The final section of this appendix gives a more concise proof of Equation B.4 than that presented in NUREG/CR-4780.

### B.2 Ways of Collecting Data

In the nuclear power domain, nearly all failure events of most safety-related components are seen on periodic tests rather than on unplanned demands. The common testing schemes are described below.

- **Nonstaggered tests.** For each test, the entire group of \( m \) components is tested, and the number of components that fail the test is recorded. Any failed components are repaired and the causes of the failures are removed. Therefore, the outcomes of distinct group tests are independent. In any set of such data, let \( N_D \) denote the number of group tests, corresponding to \( m*N_D \) tests of individual components.

  In fact, the tests are normally not perfectly simultaneous. Instead a component is isolated and tested. Immediately afterward the component is again put in service and the next component is isolated and tested. It is assumed that this process is a good surrogate for an unplanned demand in which all components are demanded in a truly simultaneous fashion.

- **Staggered tests with followup.** The components are tested one at a time, so that the entire cycle of \( m \) components is tested periodically. If a component passes a scheduled test, nothing more is done until it is time for the next component to be tested. If, instead, a component fails its scheduled test, then all the other components are tested, and any failed components are repaired...
and their failure causes are removed. The cycle is assumed to start over on the date of the next scheduled test.\footnote{This is a simplifying assumption; in reality, there may be a variety of testing schemes. However, for the binomial distribution in Equation B.5, the number of component demands must be specified in advance; thus, an assumption has to be made about the number of demands. The actual number of component demands should not differ greatly from the assumed value of $m^*N_D$ at any rate.} In a data set, let $N_D$ denote the number of scheduled cycles of tests, corresponding to $m^*N_D$ scheduled tests of individual components.

- **Staggered tests without followup.** This is the same as above, except if a component fails its scheduled test, it alone is repaired. The other components are not tested until their scheduled times.

Across the nuclear power industry, a mixture of testing strategies seems to be used. The vast majority of plants claim to use staggered testing, but some plants seem to use nonstaggered testing when it is more convenient. Moreover, some components, notably the large important ones, such as pumps and diesel generators, have technical specifications that require followup after a component failure. However, other components, such as some valves, do not have such technical specifications, and followup is not necessarily performed for these components.

The sections below will show how the distributions of failure counts depend on the testing strategies. In particular, the fraction of observed $k$-component failure events out of all observed failure events depends on the testing strategy. Staggered testing with followup gives relatively fewer observed single failures, and relatively more observed multiple failures, than does nonstaggered testing. This means that the observed fraction of failure events involving $k$ components is not necessarily an unbiased estimator of the parameter $\alpha_k$—it depends on the testing strategy.

### B.2.1 Estimators when All $m$ Components Are Demanded on Each Test

Let $n_k$ be the number of failed components when all $m$ components are demanded. To emphasize that this is under the assumption that all $m$ components are demanded (typically from nonstaggered testing), we will write this as $n_k^{\text{NS}}$, where the letters NS stand for “nonstaggered.”

In the work below, especially where the notation becomes thick, it will be helpful to keep in mind that superscripts such as NS are used only for quantities that depend on the testing strategy. The parameters ($Q_k$, $\alpha_k$, and $Q$) are constants, independent of the method of data collection, so they do not get superscripts. Only quantities that depend on data—the failure counts $n_k$ and the parameter estimates, such as $\hat{Q}_k$—have superscripts to indicate the testing strategy that underlies the data.

The notation $n_k^{\text{NS}}$ can also be used if the data come from unplanned demands, assuming that each such demand is a demand on the entire group of $m$ components. If there are $N_D$ such demands of the full group (nonstaggered tests or unplanned demands or both), the probability distribution of $n_k^{\text{NS}}$ is:

$$n_k^{\text{NS}} \sim \text{binomial}
\left(N_D, \binom{m}{k}Q_k\right)$$

The justification of Equation B.5 is as follows. Because $n_k^{\text{NS}}$ is the number of events in which exactly $k$ components fail, out of $N_D$ independent demands on the full group, $n_k^{\text{NS}}$ must have a binomial($N_D, r_k$)
distribution for some probability \( r_k \). Because the probability that exactly \( k \) components fail is \( \binom{m}{k} Q_k \), it follows that \( r_k = \binom{m}{k} Q_k \), proving Equation B.5.

Based on Equation B.5, the MLE of \( Q_k \) is:

\[
\hat{Q}_k^{NS} = \frac{n_k^{NS}}{\binom{m}{k} N_D}
\]  

(B.6)

As a generalization of Equation B.5, the joint distribution of \( (n_0^{NS}, n_1^{NS}, ..., n_m^{NS}) \) is multinomial. The \( m+1 \) values of \( n_k^{NS} \) sum to \( N_D \). The superscript \( NS \) emphasizes that this is the distribution when all \( m \) components experience a demand essentially simultaneously. Excluding the successes, the joint distribution of \( (n_1^{NS}, ..., n_m^{NS}) \), conditional on the sum \( n_1^{NS} + ... + n_m^{NS} \), is multinomial, with corresponding parameters \( (\alpha_1, ..., \alpha_m) \).

The MLE of \( \alpha_k \) can be found in two equivalent ways. One is to use the multinomial distribution of \( (n_1^{NS}, ..., n_m^{NS}) \). The other is to replace the \( Q_k \) parameters in Equation B.2 by their estimates in Equation B.6 and perform an algebraic cleanup. Either method shows that the MLE of \( \alpha_k \) is:

\[
\hat{\alpha}_k^{NS} = \frac{\sum_{j=1}^{m} n_j^{NS}}{\sum_{j=1}^{m} n_j^{NS}}
\]  

(B.7)

Again, the \( NS \) superscript emphasizes that this is the MLE based on data in which all \( m \) components are demanded simultaneously. The expression on the right side of Equation B.7 is the sample fraction of \( k \)-component failure events, out of all failure events occurring in nonstaggered testing. It is an intuitively natural estimate of the long-term fraction of such events, \( \alpha_k \).

The MLE of \( Q_t \) can be found by replacing each \( Q_k \) in Equation B.3 by its MLE, using Equation B.6. After some algebraic manipulation, this yields:

\[
\hat{Q}_t^{NS} = \sum_{k=1}^{m} kn_k^{NS} / (mN_D)
\]  

(B.8)

This has the intuitive interpretation that \( \hat{Q}_t^{NS} \) = (number of component failures)/(number of component demands). This is difficult to derive directly from the likelihood of the individual component failures because the components do not necessarily fail independently of each other on a single group demand. NUREG/CR-4780 derives Equation B.8 as Equation C.46.

There is a theorem which states that the MLE of \( f(\text{parameters}) = f(\text{MLEs of the parameters}) \) for any function \( f \). Therefore, Equation B.4 is valid if one substitutes the MLEs on both sides.
This can also be verified by substituting the MLEs, given by Equations B.6, B.7, and B.8, into Equation B.4 and performing algebraic simplification.

\[ \hat{Q}_k^{NS} = \frac{k}{m-1} \frac{\hat{\alpha}_k^{NS}}{\hat{\alpha}_i^{NS}} \hat{Q}_i^{NS} \]  
(B.9)

B.2.3 Estimators with Staggered Testing

We make the important assumption here that the outcomes of separate tests are independent. That is, if a component is tested and it succeeds, this has no effect on the probability that the next component will succeed or fail when its scheduled test is performed. On the other hand, if a component is tested and it fails, and followup tests of the other components are performed, these are not regarded as separate tests, but as a single, virtually simultaneous demand on the whole group.

B.2.3.1 Staggered Testing without Followup

For systems with staggered testing but no followup tests following failure of a component, great care is necessary. The issue is that \( \alpha_k \) cannot be estimated if multiple failures are impossible to observe. It is an error to simply count every observed failure as a single failure. It underestimates the number of failures that are parts of multiple failures and overestimates the number of single failures, and thus \( \alpha_1 \) if Equation B.6 is applied naively. Unless the data source gives good reason for determining the number of failed components in any observed failure event, the observed failures can be used for estimating \( Q_t \), but not for quantifying probabilities of multiple failures.

B.2.3.2 Staggered Testing with Followup

This testing strategy does not demand all \( m \) components, except when the first component tested (the “scheduled component”) fails. Many of the notations below will include the superscript \( S \), for “staggered” testing, to emphasize that they apply to the present situation and not to the situation when all \( m \) components are tested essentially simultaneously. This will contrast with the superscript \( NS \), for “nonstaggered,” used above. It will be seen below that crucial formulas differ, depending on the testing strategy. The probability that a scheduled component fails and that a total of \( k \) of the \( m \) components fail is:

\[ Q_k \binom{m-1}{k-1} \]

This is because \( Q_k \) is the probability that a particular set of \( k \) components fails on demand, and there are \( \binom{m-1}{k-1} \) distinct (mutually exclusive) sets of \( k \) components that include the scheduled component.

Let \( n_k^S \) be the number of failure events with \( k \) failed components that are found through staggered testing with followup. Every scheduled test of a component gives an opportunity for \( k \) components to fail, the scheduled component and \( k-1 \) other components in the group. Therefore, in \( N_D \) cycles of \( m \) scheduled component tests,

\[ n_k^S \sim \text{binomial} \left( mN_D, \binom{m-1}{k-1} Q_k \right) \]  
(B.10)
Therefore, the MLE of $Q_k$ is:

$$\hat{Q}_k^S = \frac{n_k^S}{\binom{m-1}{k-1} m N_D}$$  \hspace{1cm} (B.11)

This differs from Equation B.6, which uses data from nonstaggered testing. Both $\hat{Q}_k^{NS}$ and $\hat{Q}_k^S$ are unbiased estimators of the parameter $Q_k$ that is defined above. However, $\hat{Q}_k^{NS}$ uses $n_k^{NS}$, obtained from data in which every demand is a simultaneous demand of all $m$ components, and $\hat{Q}_k^S$ uses $n_k^S$, obtained from data based on a different testing strategy.

NUREG/CR-4780 is, in our opinion, somewhat mistaken about this. It derives Equation B.11 as its Equation C.71. It then states, in Equation C.72, that:

$$\frac{\hat{Q}_k^S}{\hat{Q}_k^{NS}} = \frac{1}{k}$$

This equation is true only if the number of $k$-component failures is the same under both testing strategies: $n_k^S = n_k^{NS}$. In fact, it can be shown from Equations B.5 and B.10 that the expected (or mean) values of the $n_k$s satisfy:

$$\frac{E(n_k^S)}{E(n_k^{NS})} = k,$$

so we do not expect $n_k^S = n_k^{NS}$ very often. Since $\hat{Q}_k^{NS}$ and $\hat{Q}_k^S$ are both unbiased estimators of the same quantity, it seems more likely that each estimator is larger than the other about half the time.

Now consider estimation of $Q_t$. The probability that a scheduled component fails when tested is $Q_t$. The sum:

$$\sum_{k=1}^m n_k^S$$

is the total number of times that a scheduled component fails in the $m N_D$ scheduled component tests. Therefore,

$$\sum_{k=1}^m n_k^S \sim \text{binomial}(m N_D, Q_t)$$  \hspace{1cm} (B.12)

The MLE of $Q_t$ follows from Equation B.10, giving the estimate based on staggered data:

$$\hat{Q}_t^S = \frac{\sum_{k=1}^m n_k^S}{m N_D}$$  \hspace{1cm} (B.13)

In words, this is $\hat{Q}_t^S = \frac{\text{(number of failures on scheduled tests)}}{\text{(number of scheduled tests)}}$. Next, let us consider estimation of the alpha factors. A generalization of Equation B.10 is that the joint distribution of $(n_1^S, \ldots, n_m^S)$, conditional on the sum $\sum_{k=1}^m n_k^S$, is multinomial, with:

$$\sum_{k=1}^m n_k^S \sim \text{multinomial}(m N_D, (Q_1, \ldots, Q_m)).$$
\[
\frac{(m-1)Q_k}{\sum_{j=1}^{m}(m-1)Q_j} = \frac{(m-1)Q_k}{Q_i}
\]

as the probability corresponding to \(n_i^k\). This quantity is analogous to, but different from, the alpha factor defined by Equation B.2. For want of a better name, we call this quantity a “zeta factor”:

\[
\zeta_k = \frac{(m-1)Q_k}{Q_i}
\]

(B.14)

Recall that \(Q_k\) and \(Q_i\) are parameters, defined independently of how the data are collected. Since \(\zeta_k\) is a function of these parameters, it can be regarded as a (derived) parameter. Therefore, none of the terms in Equation B.14 have superscripts. Their definitions do not depend on data.

The above paragraph says that, conditional on the sum \(\sum_{1 \leq m} n_{i}^{S} = (n_{1}^{S}, \ldots, n_{m}^{S})\) is multinomial, with corresponding parameters \((\zeta_{1}, \ldots, \zeta_{m})\). It follows that the MLE of \(\zeta_{k}\) is:

\[
\hat{\zeta}_{k}^{S} = \frac{n_{k}^{S}}{\sum_{j=1}^{m}n_{j}^{S}}
\]

(B.15)

We remark that \(\hat{\zeta}_{k}^{S}\), the estimate of the parameter \(\zeta_{k}\), depends on data, and so has an \(S\) superscript to show that the estimate uses failure counts from staggered testing.

The expression on the right side in Equation B.15 is the sample fraction of \(k\)-component failures, out of all failure events found by staggered testing. It has the same form as the MLE of \(\alpha_{k}\) given in Equation B.7, but the counts here are from staggered rather than nonstaggered testing. Therefore, \(\sum_{j=1}^{m} n_{j}^{S} / \hat{\alpha}_{j}^{S}\) is the MLE of \(\zeta_{k}\) as defined by Equation B.14, not the MLE of \(\alpha_{k}\) as defined by Equation B.2.

How, then, does one find the MLE of \(\alpha_{k}\) with data from staggered testing? One way is to substitute the MLEs \(\hat{Q}_{k}^{S}\) for the \(Q_{k}\)s in Equation B.2. This yields:

\[
\hat{\alpha}_{k}^{S} = \frac{n_{k}^{S} / k}{\sum_{j=1}^{m}(n_{j}^{S} / j)}
\]

(B.16)

The superscript \(S\) indicates that this estimate of \(\alpha_{k}\) is based on data from staggered testing.

A second way is to estimate the zeta factors in the natural way using Equation B.15 and then convert the estimates into estimates of the alpha factors. To convert results involving \(\zeta_{k}\) to results involving \(\alpha_{k}\), the following relation is useful:
This is proved from Equations B.2 and B.14, treating the denominators in those two equations as constants because they do not depend on \( k \). The constant of proportionality in Equation B.17 can be sidestepped in practice by using the facts that:

\[
\sum_{k=1}^{m} \alpha_k = 1 \quad \text{and} \quad \sum_{k=1}^{m} \zeta_k = 1.
\]

Therefore, if the zeta factors have known or estimated numerical values, set:

\[
\alpha'_k = \zeta_k / k
\]

for each \( k \), and then normalize by setting:

\[
\alpha_k = \frac{\alpha'_k}{\sum_{j=1}^{m} \alpha'_j}
\]

By this use of Equation B.17, if the MLEs of the zeta factors have been found, the MLEs of the alpha factors can be constructed. This is an alternative to the use of Equation B.16.

Finally, consider formulas to estimate \( Q_k \) based on estimates of other parameters. Rearrangement of Equation B.14 allows one to express \( Q_k \) in terms of \( \zeta_k \) and \( Q_t \):

\[
Q_k = \frac{1}{m - 1} \left( \sum_{j=1}^{k} \frac{1}{\alpha_j} \right) \zeta_k Q_t.
\]

NUREG/CR-5485 gives the same equation, labeled Equation 5.6 in that publication, except \( \zeta_k \) is called \( \alpha_k \). This is incorrect. NUREG/CR-5485 certainly uses Equation B.15 to estimate \( \zeta_k \) (which it calls \( \alpha_k \)), but it does not explicitly state the formula to use for estimating \( Q_k \) with data from staggered testing. The equation here may be used to estimate \( Q_k \) if Equations B.15 and B.13 are used to estimate \( \zeta_k \) and \( Q_t \).

A way to estimate \( Q_k \) based directly on the estimates of the \( \alpha_k \)s and \( Q_t \) is to substitute the correct estimates (from Equations B.16 and B.13) into Equation B.4, obtaining:

\[
\hat{Q}_k^s = \frac{k}{m - 1} \frac{\hat{\alpha}_k^s}{\hat{\alpha}_t^s} \hat{Q}_t^s
\]

This is justified by the theorem about MLEs mentioned in connection with Equation B.9. In summary, Equation B.4 is valid for the parameters, and Equations B.9 and B.18 are the corresponding equations in terms of estimators under the two kinds of testing.

### B.3 Effect of Using the Wrong Formula

The parameter \( \alpha_k \) is defined in Equation B.2, based on a process in which all \( m \) components are demanded simultaneously. It seems to be widely believed that the sample fraction of \( k \)-component failure events:
is the MLE of $\alpha_k$ regardless of whether the data come from staggered or nonstaggered testing. It has been shown above that the sample fraction is the MLE of $\alpha_k$ only when the data come from nonstaggered testing. What is the effect of using Equation B.19 when the testing is staggered? (Of course, here we only consider staggered testing with followup. As stated above, staggered testing with no followup cannot be used at all to estimate the alpha factors.)

Equation B.16 shows that for large $k$, $\alpha_k$ is smaller than $\zeta_k$, and for small $k$ the inequality is reversed. (A proof of this claim is given in the final section of this appendix.) Therefore, the sample fraction from staggered testing,

$$\frac{n_k}{\sum_{j=1}^{m} n_j}$$

which equals $\hat{\zeta}_k$, overestimates $\alpha_k$ for large $k$ and underestimates $\alpha_k$ for small $k$. Therefore, from a risk perspective, the sample fraction is a conservative estimator.

Now consider $Q_t$. It is clear that with data from staggered testing, if Equation B.8 is used instead of the correct Equation B.13, then the estimate will be too large. Therefore, using the wrong estimator for $Q_t$ is also conservative.

If data are mixed, some coming from staggered testing with followup and some from nonstaggered testing, the conservatism seen above remains, but it is less strong. This may seem completely obvious, but the final section of this appendix provides mathematical proofs of this fact.

### B.4 Proofs of Selected Results

**Proof of Equation B.4**

Equation B.2 defines $\alpha_k$ as

$$\alpha_k = \frac{k}{m} \alpha_t Q_t$$

Because:

$$\binom{m}{k} = \frac{m}{k} \binom{m-1}{k-1}$$

This can be rewritten as:
\[
\alpha_k = \frac{\frac{m}{k}(m-1)Q_k}{\sum_{j=1}^{m} \binom{m}{j}Q_j}
\]

which can be rearranged as:

\[
\frac{k}{m} \alpha_k \sum_{j=1}^{m} \binom{m}{j}Q_j = \binom{m-1}{k-1}Q_k
\]

Summing with respect to \( k \) gives:

\[
\frac{1}{m} \sum_{k=1}^{m} k \alpha_k \sum_{j=1}^{m} \binom{m}{j}Q_j = \sum_{k=1}^{m} \binom{m-1}{k-1}Q_k
\]

The three summations can be rewritten in somewhat simpler terms. The leftmost summation is defined as \( \alpha_t \), and the rightmost summation is defined as \( Q_t \) in Equation B.3. The final summation is the denominator in the definition of \( \alpha_k \), Equation B.2, and so can be rewritten. Therefore, substituting gives:

\[
\frac{1}{m} \sum_{k=1}^{m} k \alpha_k \frac{\binom{m}{k}Q_k}{\alpha_k} = Q_t
\]

Using Equation B.20 here results in:

\[
\frac{1}{m} \sum_{k=1}^{m} k \alpha_k \frac{\binom{m}{k}Q_k}{\alpha_k} = Q_t
\]

which is the equation we wished to prove.

Proof that for small \( k \), \( \alpha_k \geq \zeta_k \) and for large \( k \) the inequality is reversed

From Equation B.17 we have:

\[
k \alpha_k = C \zeta_k
\]

for some proportionality constant, \( C \). Because \( k \) takes values from 1 to \( m \), we have:

\[
\alpha_k \leq C \zeta_k \leq m \alpha_k
\]

Now sum over \( k \), obtaining:

\[
\sum_{k=1}^{m} \alpha_k \leq C \sum_{k=1}^{m} \zeta_k \leq m \sum_{k=1}^{m} \alpha_k
\]

Because the alphas sum to 1 and the zetas sum to 1, this chain of inequalities reduces to \( 1 \leq C \leq m \). The exact value of \( C \) presumably depends on the particular numbers. However, if \( k \leq C \), Equation B.21 states that \( \alpha_k \geq \zeta_k \), and if \( k \geq C \), Equation B.21 states that \( \alpha_k \leq \zeta_k \), as claimed.