U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG-2225

Basis for the Treatment of Potential Common-Cause Failure in the Significance Determination Process

Office of Nuclear Regulatory Research

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Library at www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and Title 10, "Energy," in the *Code of Federal Regulations* may also be purchased from one of these two sources.

1. **The Superintendent of Documents**
   U.S. Government Publishing Office
   Washington, DC 20402-0001
   Internet: bookstore.gpo.gov
   Telephone: (202) 512-1800
   Fax: (202) 512-2104

2. **The National Technical Information Service**
   5301 Shawnee Road
   Alexandria, VA 22312-0002
   www.ntis.gov
   1-800-553-6847 or, locally, (703) 605-6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

Address: **U.S. Nuclear Regulatory Commission**
Office of Administration
Multimedia, Graphics, and Storage & Distribution Branch
Washington, DC 20555-0001
E-mail: distribution.resource@nrc.gov
Facsimile: (301) 415-2289

Some publications in the NUREG series that are posted at NRC's Web site address www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852-2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036-8002
www.ansi.org
(212) 642-4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractorprepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG-2225

Basis for the Treatment of Potential Common-Cause Failure in the Significance Determination Process

Manuscript Completed: September 2018
Date Published: September 2018

Prepared by:
A. Mosleh[1]
K. Coyne
C. Hunter
S. Shen

[1]University of California, Los Angeles
Samueli School of Engineering
7400 Boelter Hall
Los Angeles, CA 90095

Christopher Hunter, NRC Project Manager

Office of Nuclear Regulatory Research

ABSTRACT

Event and condition assessment is an application of probabilistic risk assessment in which observed equipment failures, degradations, and outages are mapped into a risk model to obtain a numerical estimate of risk significance. These retrospective assessments are used in regulatory applications, such as the Significance Determination Process (SDP), Accident Sequence Precursor Program, and Incident Investigation Program. In the SDP, which is the focus for this report, the identified performance deficiency is mapped in the risk model by adjusting the failure probability of the affected (i.e., nonconforming) component. In addition, the probability of common-cause failure (CCF) is adjusted to reflect the performance deficiency that could have affected all redundant components in the affected system (i.e., within the same common-cause component group in the risk model). Experience has shown that increased potential for CCF is often a substantial contributor to the risk significance of a performance deficiency.

This NUREG documents the basis for the treatment of CCF potential at the level of the observed performance deficiency within the scope of the SDP, describes important technical terms associated with CCF modeling and how these terms relate to event and conditional assessments versus base probabilistic risk assessment modeling, and provides examples of CCF potential for actual conditions. It also describes the basic assumptions and key principles for treating CCF of redundant components in SDP risk assessments when one or more of the redundant components are failed or functionally degraded due to a deficiency in licensee performance. This report does not introduce new methods for CCF and is intended to summarize the U.S. Nuclear Regulatory Commission's philosophical basis for treating CCF within retrospective risk assessments performed as part of the SDP.

FOREWORD

The U.S. Nuclear Regulatory Commission's (NRC) 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 the agency to focus on the risks most important to protecting public health and safety. A general conclusion from operating experience and PRAs of commercial nuclear power plants is that common-cause failures (CCFs) are significant contributors to the unavailability of safety systems. This conclusion is not surprising as CCF can defeat the redundancy designed into critical safety systems. As a result, experience has shown that the evaluation of the risk contribution of potential CCF often can strongly influence the results of Significance Determination Process (SDP) risk assessments performed under the NRC's oversight and enforcement program.

Although the treatment of CCF potential as described in this NUREG has been in practice for several years in SDP risk assessments, it is often the subject of debate in discussions between the NRC and licensee risk analysts. In particular, questions have been raised repeatedly about conditions under which failures can be considered to be *independent* (i.e., with a cause not capable of being shared across redundant trains) and the likelihood of additional failures of redundant equipment given an observed degraded condition. In particular, these questions have often focused on the appropriate definition of a performance deficiency within the context of a CCF shared cause and related coupling factor, simultaneity of potential CCF failures, applicability of operating experience collected by the NRC, and the relevance of observed successful operation of redundant equipment following identification of the degraded condition. The purpose of this NUREG is to document the basis for the NRC's longstanding approach to addressing these issues within the context of the SDP.

This report represents the contributions of many individuals. In addition, significant input on the treatment of CCF potential in SDP risk assessments was provided by external stakeholders through their feedback on the draft version of this NUREG [see the *Federal Register Notice* published on November 2, 2011 (NRC, 2011)]. Based on the feedback provided, the report was revised significantly to enhance the presentation and ensure technical clarity. Responses to these comments can be found in NRC Response to Public Comments on Draft NUREG XXXX, "Common Cause Failure Analysis in Event and Condition Assessment: Guidance and Research, Draft Report for Comment," dated February 2018 (NRC, 2018).

TABLE OF CONTENTS

ACKNOWLEDGMENTS

Special appreciation is expressed to the following experts who have made significant contributions in the development of this report:

- Don Marksberry [U.S. Nuclear Regulatory Commission (NRC)]
- John Schroeder [Idaho National Laboratory (INL)]
- Mike Calley (INL)
- Jeff Circle (NRC)
- Gary DeMoss (formerly with NRC)
- Dana Kelly (formerly with INL)
- Laura Kozak (NRC)
- Zhegang Ma (INL)
- Jeffrey Mitman (NRC)
- John Nakoski (NRC)
- Dale Rasmuson (NRC retired)
- Martin Sattison (formerly with INL)
- Sunil Weerakkody (NRC)
- See-Meng Wong (NRC retired)

ABBREVIATIONS AND ACRONYMS

CCBE	common-cause basic event
CCF	common-cause failure
CCCG	common-cause component group
CFR	*Code of Federal Regulations*
ECA	event and condition assessment
EDG	emergency diesel generator
EPIX	Equipment Performance and Information Exchange
HFE	human failure event
IMC	inspection manual chapter
INL	Idaho National Laboratory
LER	licensee event report
MOV	motor-operated valve
NRC	U.S. Nuclear Regulatory Commission
NPRDS	Nuclear Plant Reliability Data System
PORV	power-operated relief valve
PRA	probabilistic risk assessment
SDP	Significance Determination Process
SPAR	standardized plant analysis risk

1 INTRODUCTION

1.1 Purpose and Scope

The primary purpose of this NUREG is to document the basis for the treatment of common-cause failure (CCF) potential at the performance deficiency level in quantitative risk assessments performed as part of the Significance Determination Process (SDP). Due to the special considerations of how licensee performance deficiencies are defined within the U.S. Nuclear Regulatory Commission's (NRC's) enforcement program, the information provided in this report pertains to risk assessments performed as part of the SDP. The applicability of this information to the treatment of CCF in risk assessments performed in conjunction with other NRC programs [e.g., Accident Sequence Precursor Program and Management Directive 8.3, "NRC Incident Investigation Program," dated June 24, 2014 (NRC, 2014)] should be considered on a case-by-case basis due to differences in program objectives.

Significant risk contributors are typically found when dependencies exist between components. Risk drivers can emerge from a known performance deficiency in which a deficient design or operations affecting a component can also influence redundant components. The potential for failures arising from dependencies is often difficult to identify and, if neglected in the event and condition assessment (ECA), may result in an underestimation of the risk.

The modeling of CCFs is included in probabilistic risk assessments (PRAs) because many factors (e.g., poor maintenance process) that are not modeled explicitly in the PRA can defeat redundancy and make failures of redundant components more likely. These factors are part of the physical and human/organizational environment in which the components are embedded and are not intrinsic properties of the components themselves. The effect of these factors on plant risk can be significant.

The conditioning of CCF probability on observed failures in SDP risk assessments 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 some of the impact of organizational factors on risk, however approximate the assessment may be.

Past SDP experience has shown that conditional CCF probability is often a significant contributor to the risk significance of the performance deficiency. Consequently, considerable resources have been expended in attempts to demonstrate an absence of CCF potential, often by successfully testing redundant equipment after the event or by scrutinizing differences among subcomponents and *piece parts*[1] across redundant trains. Often, these attempts have not focused on the higher organizational/programmatic deficiencies that were the *proximate* cause of the observed failure or that could have allowed the degradation to propagate to redundant equipment. In particular, piece parts have often been the object of scrutiny in efforts to show that redundant equipment did not have similar piece parts in order to declare the observed failure as *independent*, meaning there was no increased potential for CCF of redundant components.

[1] In this context, piece parts are the individual parts that make up a subcomponent and generally refer to the specific part that that was degraded or failed. Common examples of piece parts include relay contacts, springs, limit switches, valve stems, or motor shafts.

Higher organizational deficiencies, defined in terms of the *proximate* cause of the observed degradation, are the focus of the SDP.[2]

The NRC acknowledges that there are limitations with the treatment of CCF within the current PRA framework and that assessments that are more realistic would require further research and development of refined methods and databases. These limitations can sometimes result in either underestimating or overestimating the calculated risk in ECA. Until such methods are developed, the NRC has made the process-based decision on how CCF potential should be treated in risk assessments performed as part of the SDP. This *philosophy* of the treatment of CCF potential in SDP risk assessments has been used by NRC analysts for the past few years.[3] Therefore, the purpose of this NUREG is to document the basis for how CCF potential is treated in SDP risk assessments and to formally communicate this basis to both internal and external stakeholders.

1.2 Common-Cause Failure Modeling Background

Since the publication of WASH-1400, "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," issued October 1975 (NRC, 1975), 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 follows:

> 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. In NUREG/CR-2300, "PRA Procedures Guide," issued January 1983 (NRC, 1983), nine types of dependent failures are described, summarized in three categories: *common-cause initiating events* (e.g., external or internal hazards), *intersystem* dependencies, and *intercomponent* dependencies:

(1) *Common-cause initiating events* produce dependent failures of equipment through spatial interactions or shared response to an event or condition; such dependencies are treated through special analysis techniques.

(2) *Intersystem dependencies* are events or failure causes that create interdependences among the probabilities of failure for multiple systems. Stated another way, intersystem dependences cause the conditional probability of failure for a given system along an accident sequence to be dependent on the success or failure of systems that precede it in the sequence. An example of intersystem 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.

---

[2] Within the SDP, the term *proximate* refers to cause at the performance deficiency level.

[3] Similar guidance on the treatment CCF potential in ECA was introduced into Volume 1, "Internal Events," of the Risk Assessment of Operational Events Handbook, Revision 2.0, issued January 2013 (NRC, 2013).

(3) *Intercomponent dependencie*s span a wide range of factors and may include common design, manufacturer, testing, maintenance, environment, and many others. The PRA Procedures Guide (NUREG/CR-2300) refers to this last dependence category as CCF. Modern PRAs generally have followed this convention, defining CCF as the failure of multiple redundant components, within the mission time of the PRA, as a result of a shared cause. This definition framed the scope of the CCF analysis guidebook [NUREG/CR-4780, "Procedures for Treating Common-Cause Failures in Safety and Reliability Studies," issued January 1988 (NRC, 1988)], that further elaborated on characteristic of CCF events and introduced methods to account for CCF in PRA, including techniques for data analysis and model parameter estimation.

The treatment of CCFs in PRAs and reliability studies is well established in the literature and in practice. NUREG/CR-4780 documents a concerted effort of the NRC and the Electric Power Research Institute to unify the basic principles underlying CCF analysis. An update to this study, NUREG/CR-5485, "Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment" (NRC, 1998), was completed in November 1998.

1.3 Focus of Significance Determination Process Risk Assessments

Risk assessments performed as part of the SDP are examples of a retrospective application in which PRA is used to obtain a numerical estimate of the risk significance of a licensee performance deficiency. According to Inspection Manual Chapter (IMC) 0308, Attachment 3, "Significance Determination Process Technical Basis," dated June 16, 2016 (NRC, 2016a)—

> If a relationship between a degraded condition and a performance deficiency is identified, the inspection staff must describe how the licensee performance deficiency was the proximate cause of the degraded condition. In other words, the performance deficiency is not the degraded condition itself, it is the proximate cause of the degraded condition. The determination of cause does not need to be based on a rigorous root cause evaluation (which might take a licensee months to complete), but rather on a reasonable assessment and judgment of the staff. The term "proximate cause" is intended to describe a cause that was a significant contributor to the occurrence of the degraded condition. In addition, there could be several additional causal factors that contribute, either in parallel or in series logic, to the occurrence of the degraded condition; however, only a single proximate cause needs to be linked to the performance deficiency. Once the staff has described how a licensee performance deficiency is the proximate cause of a degraded condition, the SDP, via applicable attachments and appendices, estimates the safety or security significance of the degraded condition.

The SDP places an emphasis on degradations in procedures and processes (what the SDP defines as *proximate* causes) to help discourage overly narrow descriptions of a performance deficiency that focus on specific subcomponents or piece parts and thus diminish the larger impact that such deficiency can have on risk. For issues involving quality control of safety-related equipment or processes, the performance deficiency is typically defined to be consistent with the governing criterion in Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities."

For example, it is preferable to state that a performance deficiency was "inadequate test control" rather than "inadequate test control practices associated with postmaintenance testing following

installation of bearings," or "failure to correct a condition adverse to quality" instead of "failure to correct a condition adverse to quality associated with emergency diesel generator lube oil systems." Other examples include "failure to develop and implement scheduled preventive maintenance" instead of "failure to develop and implement scheduled preventive maintenance for Model ABC time delay relays in the emergency diesel generator (EDG) 2B protective logic," and "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."

Another way to look at the performance deficiency is the action that the NRC expects the licensee would take to correct the nonconforming action. For example, a missing page from an emergency operating procedure should result in the performance deficiency to be defined as "inadequate procedure control," and the expected action by the licensee to correct this deficiency should be more than merely replacing the correct page in emergency operating procedure books. The expected action may be a thorough review of procedure control practices and an audit of a sample of procedures for not only incorrect pages but also other potential errors, such as noncompliance with procedure review and approval processes. The missing page in this example could be substituted with a noncompliant piece part in any component in other examples, in which performance deficiency would be defined not at the piece-part level but at the higher process level at which the corrective action would be most effective in preventing reoccurrence and the potential for CCF (instead of just replacing the nonconforming part).

As will be discussed in the following sections, this concept of identifying the proper level of the performance deficiency will be important in the treatment of CCF potential for SDP risk assessments.

2 TREATMENT OF COMMON-CAUSE FAILURE POTENTIAL IN SIGNIFICANCE DETERMINATION PROCESS RISK ASSESSMENTS

2.1 Differences between Common-Cause Failure Modeling in Probabilistic Risk Assessment and Treatment of Common-Cause Failure Potential in Significance Determination Process Risk Assessments

Common-cause failures are often an important risk contributor when performing ECA, which is an application of PRA where equipment failures, degradations, and outages are mapped into the risk model to obtain a numerical estimate of their risk significance. Such assessments can be either prospective, as when utilities use their PRAs as an aid in planning and scheduling equipment maintenance, or retrospective, as when obtaining the risk significance of a degraded condition or initiating event. This NUREG focuses on the treatment of CCF potential in retrospective assessments performed as part of the SDP. These SDP risk assessments are intended to estimate the risk significance of a degraded condition (e.g., component failure) caused by a licensee performance deficiency (e.g., deficiency in a maintenance process), as well as the risk significance of the potential degradation of defense strategies in place to prevent the failure of all redundant components resulting from the cause being shared through an existing coupling factor.

During a retrospective risk assessment, the analyst is estimating a *conditional* risk metric (e.g., the conditional probability of core damage) for the event or equipment condition. This numerical risk estimate is conditioned on the equipment failures, degradations, and outages that existed during the period of interest. Because the actual event did not lead to core damage, the event is not modeled exactly as it transpired. Instead, observed failures are mapped into the PRA model and successes and failures of events beyond the event being assessed are treated probabilistically. For example, the analyst accounts for the possibility that equipment that functioned successfully during the actual event might, with some probability, fail to function. In addition, equipment that was not demanded during the actual event could have been demanded in other scenarios and have a probability of failure. Thus, failure probabilities are left at their base PRA values or are conditioned as necessary to reflect the details of the event.[4]

It is important to note that much of the past research on CCF has been focused on the modeling of CCFs in base PRA models, including the corresponding data collection and parameter estimation. As such, the state-of-practice for treatment of CCF in ECA is less mature. In addition, specific programs and processes may dictate different assumptions and approaches.

According to NUREG/CR-5485 and other reports on CCF, there are several key concepts that apply to the identification and evaluation of CCF events for CCF modeling and parameter estimation in PRAs, including the following:

- root cause
- coupling factor and shared cause
- timing of failures
- failure modes
- common-cause component groups (CCCGs)

[4] This analytic method is sometimes termed the *failure memory approach*, since failures are specifically modeled in the analysis (remembered), but successes are treated probabilistically (typically by the base PRA failure probabilities).

- common-cause basic events and the alpha-factor model
- alpha-factor model and conditional CCF probability

The following sections explain the differences in how these key concepts are used in base PRA model applications and SDP risk assessments. Some of these key concepts used to model CCF in base risk models may also be applicable in ECA.

2.1.1 Root Cause vs. Proximate Cause

According to NUREG/CR-5485—

> CCFs result from the coexistence of two main factors: a susceptibility for components to fail or become unavailable due to a particular *root cause*[5] of failure, and a *coupling factor*[6] (or coupling mechanism) that creates the condition for multiple components to be affected by the same cause.

Table 4-1 of NUREG/CR-5485 provides the following examples of root causes:

- lack of attention during maintenance and/or deficiency in the written procedure
- error in design realization and failure to realize that proof testing was not adequately simulating real demand conditions
- error or ambiguity in maintenance procedure
- inadequate training and lack of motivation
- inadequate training of installation crew and deficiency in installation procedures

Table 4-1 also provides examples of *proximate* causes (e.g., corrosion from moisture or high humidity, equipment failure, maintenance error, and vibration). It is noted in NUREG/CR-5485 that *proximate* causes are "symptoms of the root cause" and their relatively generic nature "does not in itself necessarily provide a full understanding of what led to that condition." However, the CCF data collection and parameter estimation used in base PRA model applications typically use the *proximate* cause. This is largely due to necessity. According to NUREG/CR-6268, "Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding," Revision 1, issued September 2007 (NRC, 2007):[7]

> The root cause is the basic reason why components fail. Correction of a root cause can prevent recurrence. The identification of root cause, therefore, can be tied to the implementation of defenses. The root cause may be determined to be the trigger event or the conditioning event. Often, failure investigations do not determine the root causes of failures even though this determination is crucial for judging defense adequacy. Additionally, the utility failure reports (LERs, EPIX reports, and NPRDS reports) often do not identify the actual root cause.

---

5 "Root cause is the most basic reason or reasons for the component failure, which if corrected, would prevent recurrence. The concept of root cause helps to understand why a component(s) fails."

6 "Coupling factor is a set of factors characterizing why and how a failure is systematically induced in several components."

7 The CCF database is a data collection and analysis system that includes a method for identifying CCF events and coding and classifying those events for use in CCF studies, as well as a computer system for storing and analyzing the data. Additional information on the NRC CCF database can be found at http://nrcoe.inel.gov/resultsdb/CCFDB/.

> Therefore, the failure cause coded into the CCF database is usually the proximate cause.

The purpose of SDP risk assessments is to determine the risk significance of an identified performance deficiency (i.e., the *proximate* cause per IMC 0308, Attachment 3); therefore, the CCF potential is evaluated at this level. As an example, consider an SDP risk assessment of a licensee performance deficiency associated with poor maintenance practices that led to a component failure. Although the performance deficiency resulted in a single component failure, the same poor maintenance practices *could have been applied* to other redundant component(s) in the same system. The emphasis is on "could have been applied" and not that the poor maintenance practices were observed to have been applied to redundant components. This distinction is important for understanding the differences between PRA and ECA applications. The SDP risk assessment estimates the risk significance of the observed component failure and the *probability* that redundant component(s) (that did not fail during the actual event) could have an increased failure probability due to the licensee performance deficiency. Because nuclear power plants utilize redundant safety system trains, the risk significance of such a deficiency will often be strongly influenced by the potential for failure of redundant components due to a cause shared between components as a result of a coupling factor. Thus, a crucial element of the SDP risk assessment is the conditional probability that remaining redundant components (i.e., components in the same CCCG) could have failed, given that one or more such components were failed as a result of the identified performance deficiency. Again, the emphasis is on the potential of the performance deficiency to cause redundant components to fail and is not necessarily related to the observed characteristics of the failure. As will be discussed later, this probability is obtained by calculating a conditional CCF probability using the inputs to the PRA model.

2.1.2 Shared Cause and Coupling Factor

According to NUREG/CR-5485—

> The concept of a shared cause resulting in malfunction, or change in component state, is the key aspect of a CCF event. The use of the word "shared" implicitly includes the concept of a coupling factor or mechanism.

A failure of several components to function may occur as a result of a single specific event or shared cause. Such failures may simultaneously affect several different items important to risk. The cause may be a design deficiency, manufacturing deficiency, an operating or maintenance error, a natural phenomenon, a human-induced event, or an unintended cascading effect from any other operation or failure within the plant.

A coupling factor is the condition or mechanism through which multiple components are affected (or coupled) by the same cause. Coupling factors can be based on attributes, such as hardware quality (manufacturing, installation), design (component part, system configuration), maintenance (schedule, procedure, staff), operation (procedure, staff), and environment (external, internal).

Regardless of whether the application is parameter estimation or an SDP risk assessment, CCF failures (or CCF potential) require a shared caused that is linked via a coupling factor. The potential differences between applications stem from the level of the coupling factor; that is, the shared cause and associated coupling factor are broader in scope in the SDP application as compared to the parameter estimation application.

Another aspect that has complicated past SDP risk assessments stems from limiting the focus of the cause at a piece-part level. As noted previously, such a narrow focus is counter to existing SDP guidance in IMC 0308, Attachment 3 and fails to account for other possible failure mechanisms that could be triggered by the same shared cause. For example, if the cause of the performance deficiency is an inadequate maintenance process, the manner in which the deficiency is manifested across redundant components within the same CCCG may vary and depends on the existence of a coupling factor that allows multiple components to be affected by the same shared cause. In other words, two components *could* fail in the same *mode* due to CCF (e.g., failure to start or failure to open), with the same *shared cause* (e.g., deficiency in the maintenance process because the components are coupled by a shared 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 2-1.

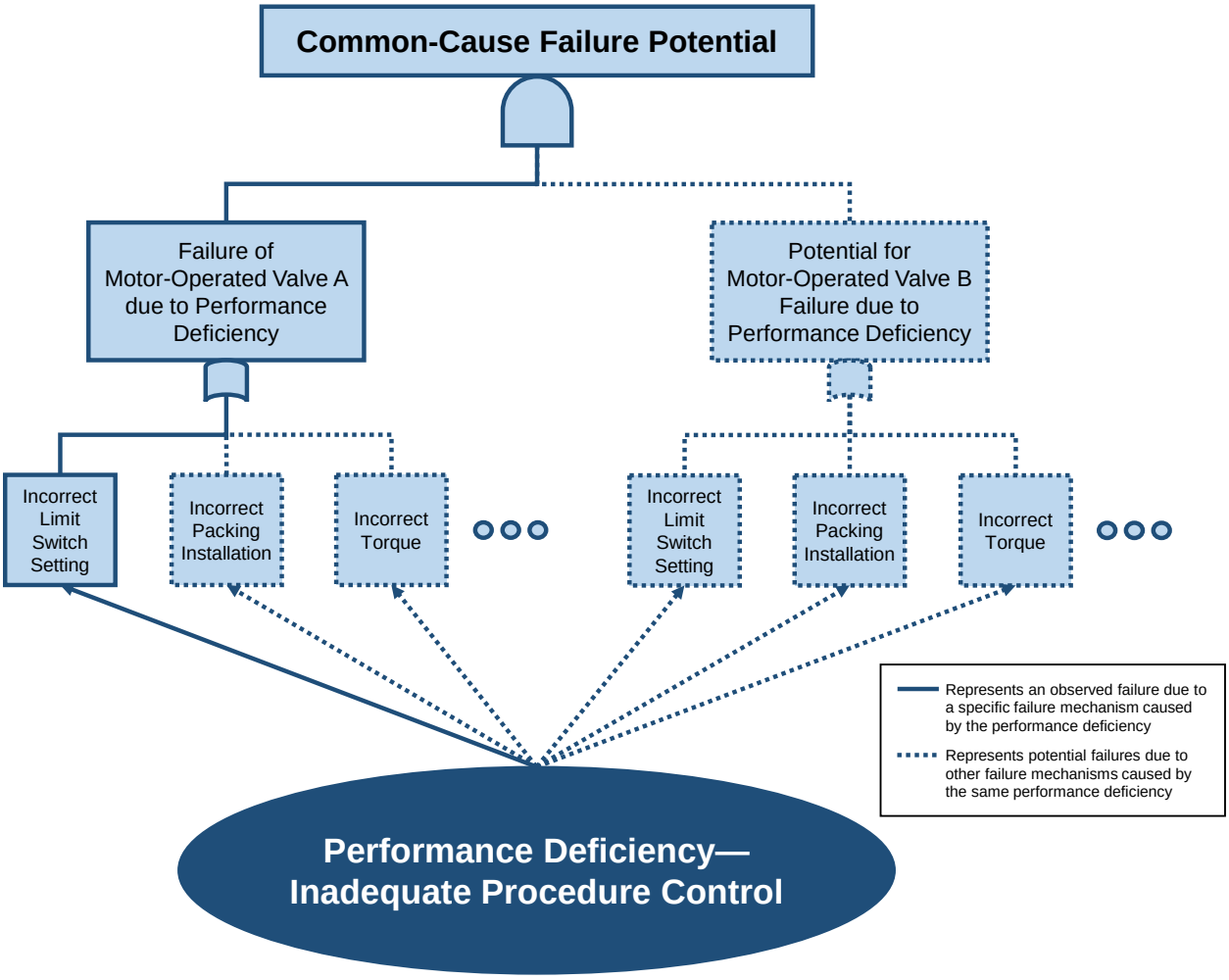


Figure 2-1 Illustration of common-cause failure in performance level.

This example (Figure 2-1) shows the potential for CCF in an SDP risk assessment given a performance deficiency, inadequate procedure control, which resulted in the failure of motor operated value (MOV) A due to incorrect setting of the limit switch. One potential CCF mechanism is for the performance deficiency to introduce the same failure mechanism in MOV B

(i.e., incorrect limit switch setting). In addition, the performance deficiency could potentially cause a CCF through a different failure mechanism of MOV B (e.g., inadequate procedure control potentially resulting in incorrect packing installation for MOV B coincident with the observed incorrect limit switch setting on MOV A). Therefore, ruling out the observed failure mechanism on MOV B (i.e., by verifying that the MOV B limit switch setting is correct) as part of the performance deficiency followup does not eliminate the potential for CCF due to other possible piece-part/failure mechanism combinations.

2.1.3 Timing of Failures

Defining CCF in terms of the timing is an important aspect of developing CCF parameters for PRA applications. The American Society of Mechanical Engineers/American Nuclear Society (ASME/ANS) PRA standard (ASME/ANS, 2013) defines CCF as—

> A failure of two or more components during a short period of time as a result of a single shared cause.

In this context, the term *short period of time* is meant to be synonymous with the mission time, if the mission time is sufficiently short (e.g., 24 hours). According to NUREG/CR-5485—

> Multiple component failures due to a shared cause that do not affect the mission requirements are of little or no significance from a PRA point of view.

In addition, NUREG/CR-6268 states that redundant failures are identified as CCF events if—

> The period of the failures is within or near the PRA mission time.[8]

Operating experience shows that when redundant components fail due to a shared cause (i.e., actual CCFs), times of failure are often closely correlated; however, *dependent failures do not have to be simultaneous in a literal sense*. Certain CCF parametric models such as the multivariate exponential distribution (Marshall and Olkin, 1967) and the binomial failure rate adaptation of that model (Vesely, 1977), also known as *shock models*, may imply the assumption of simultaneity, but such assumptions should not be viewed as a required characteristic of CCFs. The most commonly used PRA models of CCF (e.g., alpha-factor and multiple Greek letter models) are not shock models. Furthermore, the requirement that failures be simultaneous in order to count as a CCF is overly restrictive; a shared cause such as poor maintenance might generally result in the failure times of affected components to be positively correlated, without giving rise to exactly simultaneous failures. These points are further elaborated in (Kelly, 2007).

Often, the issue of timing surfaces during testing of redundant component(s) that are within the same CCCG of a component (or components) that failed. It is standard practice in SDP risk assessments that credit is not provided for equipment that successfully operates (during either the event or subsequent testing) for its PRA mission time. For example, when performing an SDP risk assessment for a condition that resulted in the failure of an EDG, the redundant EDG(s) are tested to ensure operability per plant technical specifications. If the redundant EDG(s) are tested and shown to be operable, they would not be assumed in the SDP risk assessment as successful. Therefore, the associated failure probabilities would not be set to zero but would remain at their base PRA values. If credit were provided for the successful operation of plant equipment, the risk for any operational event or equipment degradation that does not result in core damage would be

[8] A timing factor (with a value of 1, 0.5, 0.1, or 0) is assigned to CCF events based upon a PRA mission time and when the failure is identified.

zero and not provide a meaningful input into the NRC's oversight programs. Analogously, for a failed component, successful testing of redundant components within the same CCCG is not credited in eliminating increased CCF potential.

2.1.4 Failure Modes

A review of the actual CCFs that have occurred at U.S. nuclear power plants reveals that a shared cause usually fails redundant component(s) in the same failure mode. In this context, *functional mode* refers to the failure mode modeled in the PRA (e.g., failure to open, failure to run), not the specific failure mechanism. In SDP risk assessments, potential CCFs are assumed to have the same failure modes even though the coupling factor at the *proximate*-cause level does not necessarily lead to the same failure mode. Given how CCF is typically modeled in the base PRA, including the NRC's Standardized Plant Analysis Risk (SPAR) models, this is a necessary simplification for ECA.

2.1.5 Common-Cause Component Groups

A key step in modeling CCF in PRAs is the identification of the CCCGs. According to NUREG/CR-5485, a CCCG is—

> A group of (usually similar [in mission, manufacturer, maintenance, environment, etc.]) components that are considered to have a high potential for failure due to the same cause or causes.

The assignment of components to CCCGs is part of the qualitative analysis of CCF performed for the PRA (a description of the qualitative analysis is found in NUREG/CR-5485). Most CCCGs are limited to redundant components within the same system. In addition, some CCCGs may even be limited to functions within the system.[9] If components were 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 due to a performance deficiency, increased potential for CCF due to the shared proximate cause exists with other components in the CCCG. While the identification of CCCGs is outside the scope of this NUREG, it is important to note that because CCF potential evaluated as part of SDP risk assessments is at the *proximate*-cause level, the coupling factors at this level naturally extend to identical (or similar) components across CCCGs. However, this extension ventures into the intersystem CCF, which is beyond the current state-of-practice and available data. (This is an example of where the state-of-practice CCF modelling is potentially nonconservative.)

2.1.6 Common-Cause Basic Events and the Alpha-Factor Model

Within a PRA model, CCF events are included in the system logic model (typically fault trees) in terms of common-cause basic events (CCBEs). According to NUREG/CR-5485—

> CCBE is an event representing failure of a specific set of components in a CCCG resulting from a common cause.

[9] For example, a two-train system may have identical check valves on the pumps' suction and discharge with two different CCCGs comprising the two suction check valves and two discharge valves.

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.

In the context of this NUREG, the *unit of analysis* (i.e., basic events) in current PRA systems' analysis is generally defined at the component level. The unit of analysis should be defined in a manner consistent with the operating experience data that are used to calculate failure probabilities. This applies to the treatment of CCFs as well. CCBEs are only identified by the impact they have on specific sets of components within the defined CCCGs. Impact in this context is limited to component functional states such as *failed* or *not failed*; that is, the causes of failures are not modeled explicitly and any given CCBE implicitly covers all applicable causes of CCF events.

Using a symmetry assumption, the probability of occurrence of any CCBE within a given CCCG depends only on the number and not on the specific components in that basic event. Defining $Q^{(m)}_k$ as the probability of a CCBE involving *k* specific components in a CCCG of size *m* ($1 \le k \le m$), the total failure probability of a component, Q_t, can be written as:

$$Q_t = \sum_{k=1}^{m} \binom{m-1}{k-1} Q_k^{(m)} \qquad (1)$$

Where $\binom{m-1}{k-1} = \frac{(m-1)!}{(k-1)! \cdot (m-k)!}$

The alpha-factor model (Mosleh and Siu, 1987) 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 causes

α_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, the probability of a CCBE involving failure of *k* components in a CCCG of *m* components is calculated. For example, for a staggered testing scheme:[10]

$$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \alpha_k Q_t \qquad (2)$$

As an example, the probabilities of the basic events of CCCG of two components A and B are written as:

$$Q_1 = \alpha_1 Q_t \qquad (3)$$

$$Q_2 = \alpha_2 Q_t \qquad (4)$$

[10] The details of a nonstaggered testing scheme may be found in NUREG/CR-5485.

Therefore, for a 1-out-of-2 system success criterion, the failure probability of the CCCG is written as:

$$P(AB) = (Q_1)^2 + Q_2$$

$$= (\alpha_1 Q_t)^2 + \alpha_2 Q_t \quad (5)$$

The term Q_1 represents the probability of failure of redundant (individual) components within the CCCG, independent of other failure events (i.e., CCBEs) of the CCCG. Such single failure events are also referred to as an *independent* failure. An independent failure probability is not influenced in any way by other failures or successes that may have occurred. Thus, the joint probability of the independent failure of two or more components can be written as the product of the individual failure probabilities, as seen for example in equation 5 in the term $(Q_1)^2$. This is the mathematical definition of stochastic independence. The term Q_2 represents the probability of failure of redundant components within the CCCG due to a shared cause. This failure is referred to as a *dependent* failure (i.e., CCF).

2.1.7 Alpha-Factor Model and Conditional Common-Cause Failure Probability

A challenge in SDP risk assessments is that an observed component failure or degradation is only one of the possible manifestations of the performance deficiency to result in an increased potential for a CCF event. The current component-oriented PRA state-of-practice does not generally include specific mechanisms for component failure. Consistent with this level of modeling, the PRA community has estimated the CCF probability of similar components using ratios of failure counts collected at the component level, without regard to the failure mechanism. Since CCF probabilities are thus based on composite parameters from a cause perspective, the baseline risk estimate of PRAs is only correct in an aggregate sense. At this aggregate level, the conditional probabilities of CCF given the observed failure of a single component and determined performance deficiency are approximated by the use of aggregate CCF parameters. For example, for a CCCG of two components *A* and *B* (from equation 5), the conditional probability, given failure of one, is calculated using:

$$P(AB \mid A \text{ due to specific deficiency}) = \alpha_1 Q_t + \alpha_2 \quad (6)$$

The conditional CCF probability (α_2) can be imprecise within ECA because of a lack of specificity at the causal level (i.e., CCF parameter values are estimated from past events, which have a variety of causes). Because the CCF parameter values are not specific to a single cause (e.g., poor maintenance process), the conditional CCF probability might be either conservative or nonconservative for an SDP risk assessment, depending on the specific situation being modeled.[11] In addition, while some failure causes, such as poor maintenance processes, can impact multiple systems, the current state-of-practice in PRA does not include models of intersystem CCF, instead focusing on CCF within a redundant group of components in a single system. From this perspective, the conditional CCF probability could be nonconservative.

[11] The NRC has sponsored research at the University of Maryland and Idaho National Laboratory to expand the capability of evaluating CCF parameters (i.e., alpha factors) at the causal level. The use of the causal alpha-factor method [see (O'Connor and Mosleh, 2015) for additional information] could be applied in SDP risk assessments on a case-by-case basis, depending on the availability of data and resources (including time). Use of the causal alpha-factor method could lead to increase or decrease in risk significance depending on the identified cause.

The fact remains that current CCF models and operating experience data collection practices allow two alternatives: (1) use aggregate CCF conditional probabilities, which may be conservative or nonconservative depending on the specifics of the event or (2) consider the increased CCF potential as negligible (i.e., keep the applicable CCF event as its base PRA model probability). This latter approach would underestimate the risk significance of the identified performance deficiency and the potential impact of defenses against CCF.

2.2 Examples of Potential Common-Cause Failures

This section discusses selected examples of potential CCF that were derived from inspection findings.

2.2.1 Emergency Diesel Generator Failure Due to Paint

An EDG failed to start during a monthly surveillance test. Troubleshooting revealed two fuel-rack linkage/metering rods bound by paint. The painting had occurred immediately after the last successful surveillance test. An inspection found that the other EDG within the CCCG had not been recently painted.

The *proximate* cause of the failure, which was reflected in the identified performance deficiency, was judged to be the failure to adequately implement maintenance procedures that require postmaintenance verification of equipment functionality. Because these requirements applied to all components within the defined CCCG, this *proximate* cause had a coupling factor across all redundant components in the defined CCCG.

One might argue that this was a random (i.e., independent) failure because the other EDG had not been painted. However, this argument narrowly focuses on the *manifestation* of the specific (observed) failure mechanism (parts bounded by paint) rather than the potential for coupling of the *proximate* cause (inadequate verification of equipment functionality following a maintenance activity—not just following a painting activity) across all redundant components in the CCCG.

In this case, the procedural breakdown defeated the CCF defense mechanism of performing a functional verification of an EDG following painting (or another maintenance activity). It was by chance that the degradation was discovered during an unrelated surveillance test. A different maintenance schedule may have allowed all EDGs in the CCCG to be painted (or other maintenance activities) without a functional verification, leading to a potential for a complete loss of function. 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.[12]

The *potential* for CCF does not require the *potential* failure of identical piece parts, only that the *cause* of failure be shared, which it was in this case. A maintenance control deficiency can affect multiple subsystems (or piece parts) in EDGs, increasing the joint failure probability of these components.

2.2.2 Emergency Diesel Generator Strainer Plug Failure

An EDG was 25 minutes into a monthly surveillance run when an oil leak on the turbo-charger lube oil system Y-strainer end cap required the EDG to shutdown. An investigation revealed that

[12] Refer to NUREG/CR-5460, "A Cause-Defense Approach to the Understanding and Analysis of Common Cause Failures," issued March 1990 (NRC, 1990), for further discussion on defenses against CCFs.

the oil leak resulted from a damaged plastic shipping plug on the strainer. This plastic plug was not replaced with a metal end cap when the strainer on the EDG was replaced a year earlier. The utility had failed to order the metal cap, and receipt inspection and subsequent maintenance activities failed to identify and correct the problem. Inspection found that the other four EDGs within the CCCG had metal end caps installed on their Y-strainers.

The *proximate* causes of the failure were judged to be failure to order proper parts and failure to detect the problem during receipt inspection. The performance deficiency was determined to be inadequate procurement document control for safety-related equipment (10 CFR Part 50, Appendix B, Criterion IV). Because these requirements applied to all plant equipment, this *proximate* cause had a coupling factor across all redundant components in the defined CCCG.

One might argue that this was a random (i.e., independent) failure of a single EDG because the other strainers had never been replaced. However, this argument narrowly focuses on the *manifestation* of the specific (observed) failure mechanism (damaged plastic shipping plug) rather than the *potential for coupling* of the *proximate* cause (inadequate material control of any subcomponent or piece part within the CCCG—not just lube oil strainers) across all redundant components in the CCCG.

In this case, the breakdown in the procurement document control process defeated the CCF defense mechanism of performing a proper order review and receipt inspection. A different maintenance schedule may have allowed all EDG oil coolers (or another subcomponent or piece part) in the CCCG to be replaced without proper parts processing, leading to a potential for a complete loss of function. Preventing CCF requires deliberate defenses against coupling factors among redundant components; in this case, the defense mechanism was the procurement document control process, which was not properly implemented.

The *potential* for CCF does not require the *potential* failure of identical piece parts, only that the *cause* of failure be shared, which it was in this case. A procurement document control deficiency can affect multiple subsystems (or piece parts) in EDGs, increasing the joint failure probability of these components.

2.2.3 Emergency Diesel Generator Flexible Coupling Failure with Degradations in Other Couplings

Cracking in the engine-to-generator flexible coupling for an EDG caused severe vibration during a 24-hour load run. The EDG was secured and declared inoperable. Similar cracking was found in the flexible couplings of the other EDGs, and as a result, an additional EDG was declared inoperable. Similar cracking had been observed by the utility in 1988, 20 years before the current event. At that time, the cracking was not viewed as being indicative of flexible coupling degradation. 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. The utility later determined that the root cause of the observed failure mechanism (i.e., cracking of the flexible coupling) was age-related hardening of the rubber in the flexible coupling.

The *proximate* cause was judged to be the failure to promptly identify and correct conditions adverse to quality. The performance deficiency was determined to be an inadequate implementation of a corrective action program. While these requirements applied to all plant equipment, this *proximate* cause had a coupling factor with all redundant components within the defined CCCG.

Since similar cracking was observed in identical flexible couplings of the redundant EDGs, the degradation was not random. However, one might argue that this was still a random (i.e., independent) failure because the observed degree of degradation of other flexible couplings would not have resulted in simultaneous failures. This argument narrowly focuses on the *manifestation* of the specific (observed) failure mechanism (cracking found in the flexible couplings) rather than the *potential for coupling* of the *proximate* cause (failure to promptly identify and correct a condition adverse to quality) across all redundant components in the CCCG.

In this case, the performance deficiency defeated the CCF defense mechanism of promptly identifying and correcting conditions adverse to quality. It was only by chance that the degree of degradation of the flexible couplings of the redundant EDGs did not result in additional failure(s). Different circumstances (e.g., different failure mechanism) could have resulted in the redundant EDGs in the CCCG to fail simultaneously (due to the failure of other subcomponents or piece parts), leading to a complete loss of function. Preventing CCF requires deliberate defenses against coupling factors among redundant components; in this case, the defense mechanism was the corrective action program, which was not properly implemented.

3 BASIC ASSUMPTIONS AND KEY PRINCIPLES FOR COMMON-CAUSE FAILURE TREATMENT IN THE SIGNIFICANCE DETERMINATION PROCESS

Based on the discussion in Section 2, this section presents basic assumptions and key principles for treating CCF of redundant components in SDP risk assessments when one or more of the redundant components are failed or functionally degraded due to a deficiency in licensee performance.

3.1 Basic Assumptions

The following are a list of basic assumptions that underlie the key principles described in Section 3.2:

- ***CCF represents all implicit dependencies within the defined CCCG.*** 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. Some of these factors reside in the organizational environment in which the components are embedded, and they are not intrinsic properties of the components themselves.

- ***The treatment of such 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 common coupling factors exist. In context of an SDP risk assessment, these CCF probabilities are conditioned upon observed failures of components in the CCCG.

- ***The parameters in the current probabilistic CCF models are not estimated for specific failure mechanisms.*** CCF parameter estimates are normally based on counting component failures that have occurred 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. With the current consensus CCF modeling approach, the best that can be done is to condition CCF probability upon the functional failure observed in the event being analyzed, rather than the specific cause of that failure.

- ***All identified performance deficiencies that result in the failure of one or more components in a CCCG have the potential for CCF provided that at least one coupling factor for the deficiency can be identified.*** Exceptions to this principle are expected to be infrequent in practice and are expected to be rare cases related to issues with the CCCG boundaries or unmodeled dependencies (e.g., preinitiator human errors).

- ***For observed successful equipment operation, SDP risk assessments do not provide credit to screen out the potential CCF*****.** This treatment of CCF is consistent with how other events are handled in SDP risk assessments. This assumption covers 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 probability of CCF of the remaining components to zero, as there is no guarantee that multiple components could not fail during the mission time.

3.2 Key Principles

Using the basic assumptions provided in Section 3.1, the following key principles were developed for evaluating potential for CCF in SDP risk assessments given an observed failure(s) associated with a licensee performance deficiency.

3.2.1 Potential for CCF is treated at the performance deficiency (i.e., *proximate* cause) level

The SDP assesses the performance deficiency (*proximate* cause) of the degraded condition (IMC 0308, Attachment 3), not the degraded condition itself. Therefore, the organizational impact of the performance deficiency can propagate to other components within the common cause component group (CCCG) through the existing coupling factors. As such, a performance deficiency can result in the failure of other components within the CCCG by any potential failure mechanism or by any piece-part failure related to the *proximate* cause. Defining the performance deficiency (i.e., the shared cause of a potential CCF) at the *proximate*-cause level (rather than by the specific observed failure mechanism) better captures the organizational aspects of the performance deficiency.

For example, consider the failure of a safety-related valve caused by the corrosion of the valve stem due to the improper selection of the stem material for the system environment. Assume that the stem failure was due to the failure to implement adequate design measures for the selection and review of suitability for materials that are essential for the safety function of the valve. Consequently, the inspectors identify the failure to implement adequate design control measures (10 CFR Part 50, Appendix B, Criterion III) as the licensee performance deficiency. The effect of this key principle is that the SDP risk assessment assumes that this performance deficiency (i.e., inadequate design control measures) could affect other redundant valves within the same CCCG by failure mechanisms related to inadequate design control, and thus, a *potential* for CCF would exist.

Another important effect of this key principle is that failures caused by a performance deficiency to components that are part of a defined CCCG are not treated as "independent" (i.e., having no potential for resulting in a CCF failure) in the SDP risk assessment. This is not to be confused with data collection activities that will make the determination of whether an observed failure is considered "independent" or is an actual CCF for the purposes of data coding and parameter estimation.

3.2.2 The alpha factor method is used by the NRC to calculate all CCF probabilities

The alpha factor method is a state-of-practice CCF method consistent with the ASME/ANS PRA Standard, is used by the NRC, and is one of the CCF methods used within the nuclear industry. The alpha factor method aligns with the current NRC data collection practices and allows for efficient estimation of base PRA CCF probabilities. In addition, the alpha factor method is designed to provide revised CCF probabilities that can be "conditioned" on an observed component failure within the defined CCCG.[13] The calculation of revised CCF probabilities using a reformulation of the basic parameter model, which the Systems Analysis Programs for

[13] In this context, the term "conditioned" refers to changes that are made to the alpha factor model CCF mathematical equation to reflect the probability(s) of other failures in the CCCG conditional on the occurrence of the observed failure(s), which results in a higher failure likelihood of redundant components due to the potential shared caused. The alpha parameters that appear in the resulting formulation do not directly represent conditional failure probabilities and are not revised in any way.

Hands-On Integrated Risk Evaluations (SAPHIRE) automatically performs using the NRC SPAR models, follows the process shown in Appendix E of NUREG/CR-5485. While there is potential for these revised CCF probabilities to be either conservative or nonconservative, the alternative of maintaining the CCF probabilities at their base PRA values (i.e., not conditioned upon the observed failure) will always underestimate the risk significance of identified performance deficiencies.

3.2.3 Demonstration of functionality of redundant components within the same CCCG does not eliminate or reduce the potential for CCF

Extent-of-condition evaluations or testing of redundant components is often mentioned to show that there is no CCF potential (beyond the base PRA CCF probability) given an observed failure. These extent-of-condition evaluations or testing measures are needed to verify the operability of redundant component(s) to establish compliance with technical specifications. However, these measures cannot be used to show that potential CCF is reduced or eliminated in SDP risk assessments. In fact, CCF likelihood estimates for most typical components, even when conditioned upon the observed failure, would show a very low likelihood for the occurrence of an actual CCF event. Therefore, the normal expectation is that extent of condition testing would show that the redundant equipment was functional. However, if credit were provided for such extent of condition measures in the SDP, the risk assessment would fail to account for the small, but potentially risk significant, chance that the performance deficiency could propagate to the redundant train(s). Therefore, such credit would be inconsistent with the established failure memory approach, which assumes that observed successes during an operational event still have a failure potential in a retrospective risk assessment.

It has sometimes been argued that, for a given observed failure mechanism, the rate of degradation could not result in failure of redundant components in the CCCG within the PRA mission time. Although an actual CCF does require that multiple failures occur within the mission time, the simultaneity of failures is accounted for in the estimation of CCF model parameters.[14] Furthermore, mission-time arguments against using the conditional CCF probability are often focused on the specific observed failure mechanism and do not account for the potential of other failure mechanisms arising from the same performance deficiency, which could also result in the potential for CCF. Therefore, the degradation rate or time to failure of the observed failure mechanism is not considered in the evaluation of potential for CCF of redundant components within the same CCCG.

3.2.4 Potential for CCF is limited to redundant components within the same CCCG

Coupling factors between components within same CCCG in the base PRA are presumed to exist because the CCCGs should have been evaluated with the factors defined in the ASME/ANS PRA Standard. Even though some CCF coupling factors are not limited by CCCG boundaries, modeling of intersystem CCF is beyond the current state-of practice in nuclear power plant PRAs.

---

[14] The mission time as the time window of CCF events is also used in estimating parameters in CCF models based on observed failure counts. In fact, the potential for multiple dependent failures within the mission time is taken into account in the NRC CCF data collection effort, via a timing factor (NUREG/CR-6268). Also note that the occurrence of demand-based CCF events (e.g., CCF failures associated with standby equipment) are considered in parameter estimates if the failure would have been likely to occur within the same PRA mission time even if the actual observed failures occurred over a longer time interval (e.g., if the failures were observed during subsequent testing intervals).

Therefore, potential CCF must be limited to redundant components within the same CCCG. (Note: the limitation of potential CCF to components within the same CCCG is potentially nonconservative.)

3.3 Deviations from Key Principles

Because a typical PRA does not model components to the piece-part level, it is possible that some *proximate* 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. In these cases, the CCCG may have been defined in a simplified manner that does not account for these component differences. Conditioning CCF probability on the assumption of a common coupling factor in this case could produce an unnecessarily conservative estimate of risk. However, caution should be exercised in revising CCCG boundaries, because typical performance deficiencies, which reflect organizational problems such as poor maintenance, can affect the equipment within the CCCG despite the design differences. Because the *proximate* cause is defined at a higher level than the piece-part failure mechanism, it is expected that situations requiring this deviation would be extremely rare.

A second category where the key principles may not strictly apply is also related to the level of detail in the PRA model. For example, a licensee's 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 that is not explicitly modeled in the PRA and latent (preinitiator) human failure events (HFEs). For example, consider a power supply that is shared among all steam generator power-operated relief valves (PORVs), where this dependency is not explicitly included in the fault trees of the associated SPAR model. In this case, failure of the shared power supply (that would lead to multiple dependent PORV failures) could be captured by the PORV CCF basic event. However, in order to accurately model the impact of a performance deficiency that led to failure of the power supply, the analyst should modify the PRA model to capture this dependency explicitly. The other generic example related to level of detail is preinitiator or latent HFEs (e.g., miscalibrations). These are not treated comprehensively in some PRA models and again are captured indirectly by including such events in the alpha-factor estimates. In this latter case, it is preferable to explicitly add the associated preinitiator or latent HFEs to the PRA logic rather than relying on a qualitative argument.

A third category of potential deviations may arise for rare and exceptional circumstances where licensee defenses for CCF are not captured in historical operating experience and, therefore, not reflected in current CCF parameter estimates. This should not include routine state-of-practice CCF defenses have been implemented by licensees for many years and are reflected in current CCF parameter estimates. Examples of these routine CCF defenses include staggering of equipment modifications and testing, installation of diverse piece-parts, use of different maintenance staff, and standard quality assurance practices. In order for this deviation to apply, the risk analyst must determine that the CCF defense goes beyond the current state-of-practice, has not been widely implemented, and therefore is not already reflected in current CCF parameter estimates.

4 SUMMARY

This NUREG documents the basis for the treatment of CCF potential at the level of the observed performance deficiency within the scope of the SDP, describes important technical terms associated with CCF modeling and how these terms relate to event and conditional assessments versus base probabilistic risk assessment modeling, and provides examples of CCF potential for actual conditions. It also describes the basic assumptions and key principles for treating CCF of redundant components in SDP risk assessments when one or more of the redundant components are failed or functionally degraded due to a deficiency in licensee performance. This report does not introduce new methods for CCF and is intended to summarize the U.S. Nuclear Regulatory Commission's philosophical basis for treating CCF within retrospective risk assessments performed as part of the SDP.

Risk assessments performed as part of the SDP place an emphasis on higher organizational/programmatic deficiencies that were the *proximate* cause of the observed failure or that could have allowed the degradation to propagate to redundant equipment degradations in procedures and processes. If the performance deficiency is related to issues rooted in the organization, such as procedure or maintenance control, some level of dependence exists among affected components (more than the failed component are affected). The current state-of-practice of CCF modeling limits this dependency to redundant components within the same CCCG. Given an observed failure, the CCF probability for redundant components should be conditioned on the performance deficiency and the presence of a CCF coupling factor that could have led to a dependent failure. This "conditioning" of the applicable CCF probability must be at the performance deficiency level because of the scope of the SDP.

5 REFERENCES

10 CFR Part 50 — U.S. Code of Federal Regulations, "Domestic Licensing of Production and Utilization Facilities," Part 50, Chapter I, Title 10, "Energy."

ASME/ANS, 2013 — American Society of Mechanical Engineers/American Nuclear Society, "ASME RA-Sb-2013—Addenda to ASME/ANS RA-S–2008 Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications," September 2013.

Kelly, 2007 — Kelly, D.L., "Using Copulas to Model Dependence in Simulation Risk Assessment," *2007 ASME International Mechanical Engineering Congress and Exposition*, Seattle, WA, 2007.

Marshall and Olkin, 1967 — Marshall, A., and Olkin, I., "A multivariate exponential distribution," *Journal of the American Statistical Association*, 62 (317): 30–44.

Mosleh and Siu, 1987 — Mosleh, A., and Siu, N., "A Multi-Parameter, Event-Based Common-Cause Failure Model," *Proceedings of the Ninth International Conference on Structural Mechanics in Reactor Technology*, Lausanne, Switzerland, August 1987.

NRC, 1975 — U.S. Nuclear Regulatory Commission, "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," NUREG-75/014 (WASH-1400), October 1975.

NRC, 1983 — U.S. Nuclear Regulatory Commission, "PRA Procedures Guide," NUREG/CR-2300, Volumes 1 and 2, January 1983.

NRC, 1988 — U.S. Nuclear Regulatory Commission, "Procedures for Treating Common-Cause Failures in Safety and Reliability Studies," NUREG/CR-4780, Volumes 1 and 2, January 1988.

NRC, 1990 — U.S. Nuclear Regulatory Commission, "A Cause-Defense Approach to the Understanding and Analysis of Common Cause Failures," NUREG/CR-5460, March 1990.

NRC, 1998 — U.S. Nuclear Regulatory Commission, "Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment," NUREG/CR-5485, November 1998.

NRC, 2007 — U.S. Nuclear Regulatory Commission, "Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding," NUREG/CR-6268, Revision 1, September 2007.

NRC, 2011	U.S. Nuclear Regulatory Commission, "Common-Cause Failure Analysis in Event and Condition Assessment: Guidance and Research, Draft Report for Comment," *Federal Register*, Vol. 76, No. 212, November 2, 2011, pp. 67764–67765.
NRC, 2013	U.S. Nuclear Regulatory Commission, "Risk Assessment of Operational Events Handbook," Volume 1, "Internal Events," Revision 2.0, January 2013.
NRC, 2014	U.S. Nuclear Regulatory Commission, "NRC Incident Investigation Program," Management Directive 8.3, June 2014.
NRC, 2016	U.S. Nuclear Regulatory Commission, "Significance Determination Process Technical Basis," Inspection Manual Chapter 0308, Attachment 3, June 16, 2016.
NRC, 2018	U.S. Nuclear Regulatory Commission, "NRC Response to Public Comments on Draft NUREG XXXX, 'Common Cause Failure Analysis in Event and Condition Assessment: Guidance and Research, Draft Report for Comment,'" February 2018.
O'Connor and Mosleh, 2015	O'Connor, A., and Mosleh, A., "A General Cause Based Methodology for the Analysis of Common Cause and Dependent Failures in Systems Risk and Reliability Assessments," *Reliability Engineering and System Safety*, 145: 341–350.
Vesely, 1977	Vesely, W.E., "Estimating Common-Cause Failure Probabilities in Reliability and Risk Analysis: Marshall-Olkin Specialization," Idaho National Laboratory, 1977.

NRC FORM 335
(12-2010)
NRCMD 3.7

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER
(Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG-2225

2. TITLE AND SUBTITLE

Basis for the Treatment of Potential Common-Cause Failure in the Significance Determination Process

3. DATE REPORT PUBLISHED

MONTH	YEAR
September	**2018**

4. FIN OR GRANT NUMBER

5. AUTHOR(S)

A. Mosleh[1], K. Coyne, C. Hunter, and S. Shen

6. TYPE OF REPORT

Technical

7. PERIOD COVERED (Inclusive Dates)

8. PERFORMING ORGANIZATION - NAME AND ADDRESS (If NRC, provide Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)

[1]University of California, Los Angeles
Samueli School of Engineering
7400 Boelter Hall
Los Angeles, CA 90095

Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

9. SPONSORING ORGANIZATION - NAME AND ADDRESS (If NRC, type "Same as above", if contractor, provide NRC Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address.)

Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

10. SUPPLEMENTARY NOTES

C. Hunter

11. ABSTRACT (200 words or less)

Experience has shown that increased potential for common-cause failure (CCF) is often a substantial contributor to the risk significance of a performance deficiency. This NUREG documents the basis for the treatment of CCF potential at the level of the observed performance deficiency, provides essential definitions of technical terms and how these traditional CCF parameter terms relate to event and conditional assessments, describes the treatment of CCF for a number of categories of component failures and outages, and provides several examples of assessing CCF potential for actual conditions. It also describes technical issues with both the current CCF models used in probabilistic risk assessments conducted in the United States and the associated parameter estimates and the data upon which they are based. This report does not introduce new methods for CCF and is intended to summarize the U.S. Nuclear Regulatory Commission's philosophical basis for treating CCF within retrospective risk assessments performed as part of the Significance Determination Process.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)

Common-cause failure, CCF, Significance Determination Process, SDP, alpha factor

13. AVAILABILITY STATEMENT

unlimited

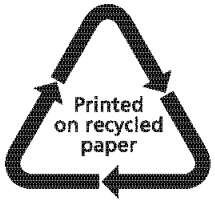
14. SECURITY CLASSIFICATION

(This Page)
unclassified

(This Report)
unclassified

15. NUMBER OF PAGES

16. PRICE



Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMSSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS

NUREG-2225

Basis for the Treatment of Potential Common-Cause Failure in the Significance Determination Process

September 2018