Dependent Failure Analysis
of
NPP Data Bases*

Susan E. Cooper, Ernest V. Lofgren (SAIC)
Pranab K. Samanta, See-Meng Wong (BNL)

ABSTRACT

A technical approach for analyzing plant-specific data bases for vulnerabilities to dependent failures has been developed and applied. Since the main purpose of this work, to aid in the formulation of defenses to dependent failures, is different than that for other dependent failure analyses, the approach of this analysis is also critically different. For instance, component failures have been defined to include all types of component function loss (e.g., catastrophic, degraded, incipient). Also, the determination of component failure dependencies has been based upon identical failure mechanisms rather than failure modes. Consequently, in the context of this study, both the definition of component failure and a categorization scheme for component failure mechanisms are used to identify clusters of component failures which are termed common failure mechanism (CFM) events.

Motor-operated valves (MOV) in two nuclear power plant data bases have been analyzed with this approach. The analysis results include seven different failure mechanism categories; identified potential CFM events; an assessment of the risk-significance of the potential CFM events using existing probabilistic risk assessments (PRAs); and postulated defenses to the identified potential CFM events.

1.0 Introduction

The purpose of this work is three-fold: 1) to gain a better understanding of nuclear power plant (NPP) vulnerability to dependent component failures, 2) to identify early indications (i.e., precursors) of dependent failures in order to institute timely preventive measures (i.e., defenses), and 3) to assess the suitability of plant-specific data bases for each of the previous purposes. The analysis of plant-specific data bases for early indications of dependent failures is the cornerstone of the overall technical approach developed and used.

* Work performed under the auspices of the U.S. Nuclear Regulatory Commission.

MASTER

The predictive purpose of this analysis required a different technical approach than has been employed in other analyses of dependent component failures. For instance, in dependent failure analyses for probabilistic risk assessments (PRAs), common cause failures (CCFs) are defined to be component failures (in the same failure mode) which are catastrophic and are due to common causes (which are usually not explicitly identified). This analysis of dependent failures differs from PRA analyses in two major ways: 1) component "failure" is defined to include all types of component function loss (e.g., catastrophic, degraded, and incipient failures) and 2) commonality in component failures is determined by identical failure mechanisms. As defined in this study, failure mechanisms are closely related to the root causes of component failures (e.g., see Reference 1). This close link to the ultimate causes of component failures allows the postulation of defenses to identified dependent failures.

Definitions of key terminology and the key features of the technical approach are discussed in Section 2. The discussion of analysis results, consisting of failure cause categories, identified CFM events, and postulated defenses, follows in Section 3.

2.0 Technical Approach

This study's technical approach for detecting component failure dependencies is centered around the analysis of plant-specific data bases for nuclear power plants (NPPs). The basic steps of the approach are:

- 1) select component data for analysis,
- 2) analyze and re-classify data base entries as either failures or non-failures (and, for the purposes of the risk evaluation (see #5 below), also separate catastrophic and non-catastrophic failures,
- 3) establish failure mechanism categories based upon the component failure descriptions given in the data base, then categorize the component failures by these failure mechanisms,
- 4) identify time-grouped component failures of the same failure mechanism category and define such groups as potential common failure mechanism (CFM) events, and
- 5) assess the risk significance of the identified potential CFM events.

The critical features of steps 1, 3, 4, and 5 of are discussed below following the definition of several key terms.

2.1 Definition of Terms

The appropriate application of the technical approach used in this study and the understanding of its results depend upon the definition of several key terms. Most of these terms have already been mentioned or implied in the above introduction but will be expanded upon in this section. The terms discussed below are: failure, dependent failure, catastrophic and non-catastrophic failures, failure mechanism, and common failure mechanism (CFM) events.

A component failure, as mentioned above, is defined in this study as any loss of component function. This general definition encompasses a spectrum of degraded component conditions, including the incipient impairment of a component's ability to perform its function. In this study, the determination of component failure was based upon the information given in the maintenance work record data bases analyzed and the judgment of the analyst. Ideally, this information would consist of failure cause descriptions, generated upon discovery of the component failure, and descriptions of work performed. Furthermore, since the maintenance records used generally followed the convention of assigning the failure of supporting equipment (e.g., circuit breakers) to the component it serves, this study includes such failures with the definition of failure for a specific component.

Reference 2 defines nine types and three categories of dependent failures, including dependent initiators and dependent system and component failures, which are all characterized as dependent, multiple, concurrent failures. Following the terminology of Reference 2, this study focuses upon intercomponent dependencies, specifically those which involve physical interactions (e.g., failure mechanisms) or human interactions (i.e., human errors) since they can be detected in maintenance record data bases. In addition, by focusing upon these two types of dependencies, the analysis of this study parallels the more familiar common cause failure analysis performed for PRAs.

As pointed out in the previous section, the distinction between catastrophic and non-catastrophic failures is made in this study primarily to support the assessment of the risk-significance. This assessment, which is described in a later section of this chapter, relies upon the comparison of this study's results with the results of PRAs. Since PRAs are based upon the premise that failures include only catastrophic, or complete and total, losses of component function, this study separates catastrophic and non-catastrophic (e.g., degraded, incipient) component failures so that their relative contributions to the number of identified dependent failures can be determined. Hence, a risk perspective, which preserves the predictive purpose of this study, can be gained from the use of PRAs without misconstruing this study's results for non-catastrophic dependent failures.

As stated above, one of the critical differences between this dependent failure analysis and others is that this study focuses upon component failure mechanisms rather than failure modes, as defined in the PRA community. Failure modes are generalized ways

by which components can fail either on demand or while in operation and which are characterized by the state of the component when it fails (e.g., failures to start or run, failures to open or close). In order to illustrate the relationship between failure mechanisms and modes, failure mechanisms could be described as the ways by which components can fail in a particular mode. However, the relationship between failure mechanisms and failure modes cannot be generalized further. For instance, a single failure mechanism for a component may impact more than one failure mode and several failure mechanisms can impact the same failure mode. In this study, the purpose of using failure mechanisms is to establish a closer relationship with proximate causes (e.g., root causes) of component failures, as they are documented in maintenance record data bases. Component failure mechanisms established in this way will be dependent upon component type and, in some cases, may be dependent upon the specific system or operating environment and upon the specific plant's maintenance "environment." As a result, it may be appropriate to define different categories of failure mechanisms for different component types, system types (e.g., standby or normally operating), environments (e.g., raw or treated water), and plants.

The definition of "common failure mechanism (CFM) event" used in this study is composed of two critical pieces: the definition of "failure," discussed above, and the definition of "common mechanism." The definition of "common mechanism," in turn, is composed of three parts: 1) the commonality of failure mechanism category, 2) the similarity in component design and/or function, and 3) the proximity of failures in time. In this study, a cluster of component failures satisfying this definition is termed a potential common failure mechanism (CFM) event and the failures which comprise the event are called common mechanism failures. The first basis for the "common mechanism" definition is the failure mechanism categorization scheme, step #3 in the basic technical approach discussed above. Secondly, common failure mechanism events are conjectured to occur for components which have similar designs and which serve a similar or common function. Failures of components in the same system (i.e., intra-system failures) can satisfy this definition but some component failures between different systems, with similar functions, (i.e., inter-system failures) may also be appropriate. The third part of the "common failure mechanism event" definition, an assumed appropriate time window, is discussed further in Section 2.3. Potential CFM events identified in this study should be verified at the plant site through the analysis of original work order requests or interviews of maintenance and engineering personnel before they can be labeled other than "potential" events.

2.2 Data Selection

In the technical approach of this study, decisions regarding the appropriateness of data involve the selection of maintenance record data bases, systems, component types, and specific components to be analyzed. The important factors determining this appropriateness for the purposes of this study are discussed below. Further weeding of the information in the data bases is typically required even after the selection of appropriate data is complete, involving, for instance, the elimination of preventive maintenance records and the

separation of component types (e.g., MOVs, AOVs, etc.). These other possible data selection subtasks are usually data-base-specific and, hence, will not be further discussed here.

Three basic factors influenced the selection of data for analysis: 1) the quantity of available data, 2) the quality of available data (i.e., is there enough information in the data base to perform the analysis?), and 3) the relevance to risk of available data. The amount of data for analysis, from the standpoint of statistical significance, should be a critical factor in all data selection decisions. In this study, the risk relevance of components was based upon their inclusion in PRA analyses (e.g., PRA documentation such as simplified P&IDs, component lists, etc.) or their roles played in some of the key safety system functions typically modeled in PRAs for mitigating accidents. Consideration of both quantity and risk-relevance lead to the decision to limit the scope of this pilot study to motor-operated valves, a relatively large component population compared to other component types, in safety systems of nuclear power plants. Discussion of the respective influence of data base information content and risk-significance upon which data bases to select and which safety systems, safety-related functions, and specific MOVs to include in the analysis is given below.

In selecting data bases for this study, the most critical criteria is the quality or the information content of a data base. In particular, the amount of information contained in the failure cause descriptions, and work performed descriptions when available, must be sufficient to allow the development of the failure mechanism categories. For example, in this study, data bases for three nuclear power plants, denoted as Plants X, Y, and Z, were initially considered for analysis. Both maintenance records and NPRDS data were available for Plant X. However, both Plant X and Z's maintenance records were rejected because of inadequate failure cause information, leaving only two of the four data bases as suitable for the data analysis scheme developed. Hence, application of this data base suitability criteria demonstrates that having access to plant maintenance records is not a guarantee that the developed data analysis strategy can be applied; not all NPPs may be able to use this approach as it is intended.

In selecting specific MOVs for inclusion in the data analysis, preference was given to those MOVs which were determined to have risk-significance based upon their inclusion in PRA analyses or their roles played in some of the key safety system functions typically modeled in PRAs for mitigating accidents. Hence, the low pressure injection (LPI), high pressure injection (HPI), auxiliary feedwater (FW), and service water (SW) systems were selected for this pilot study. Due to the sparsity of data for Plant X, the containment spray (CT) system was added to this list of systems to be analyzed. Additionally, risk-significant motor-operated valves were defined as those MOVs which are required in the functions for injection or recirculation, Reactor Coolant Pump (RCP) seal injection or cooling, containment spray injection or recirculation functions, or service water cooling for such components as HPI and LPI pumps, LPI heat exchangers, and diesel generator jackets. Of less importance, but included in this study, are MOVs involved in the long-term or

shutdown cooling function of the LPI system. More leniency in the definition of risk-significance MOVs was required in the case of the Plant X data base due to the sparsity of Plant X MOV data. Hence, for Plant X, data available for any MOV in the selected safety systems was used.

2.3 The Failure Mechanism Categorization Scheme: Development and Application

As indicated above, the development, and subsequent application, of the failure mechanism categorization scheme is central to the study's purpose to aid in the formulation of possible defenses to potential CFM events. Applying the categorization scheme to data base entries determined to be component failures is straightforward, and, therefore, not discussed further here, if the failure mechanism categories are developed as described below.

The most critical aspect of the failure mechanism categorization scheme development is the accurate correspondence with the failures which are actually present in the data base(s) being used. In order to be able to establish this basis for the categorization scheme, all data entries in the maintenance record data base(s) must be reviewed prior to the determination of failure and non-failure assignments. Since, as stated above, the failure mechanisms categories are likely to be dependent upon component type, system type (e.g., standby or normally operating), and operating environment (e.g., raw or treated water), these data selection decisions also should have been made prior to reviewing data base entries for the purpose of determining appropriate mechanism categories. In this study, the data selected consisted of only one component type (i.e., motor-operated valves) and several systems, which were largely similar in operating environment, test and surveillance frequencies, and, most importantly, function (i.e., directly or indirectly required for accident response). Consequently, only one scheme of failure mechanism categories was developed. While reviewing data entries for more than one plant, the data analyst should also be sensitive to the potential need for plant-specific failure mechanisms due to differing plant maintenance "environments." The review of data base information for the development a failure mechanism categorization scheme which is useful for both early detection and possible defense against CFM events also includes the following additional criteria:

- consideration of all maintenance activities contained in the data base with the exception of preventive maintenance (e.g., corrective maintenance as well as modifications, tests, etc.),
- consideration of all failure classifications used in the data base,
- consideration of logical component breakdowns which are compatible or related to maintenance specializations (e.g., mechanical, electrical), and

- close correspondence with proximate causes of failures (i.e., root causes).

2.4 Common Failure Mechanism (CFM) Events: Definition and Identification

In this study, the identification of common failure mechanism events involved the following five final steps:

- 1) the assignment of a "discovery date" to each identified failure, using the work order initiation date, preferably, or the work start date,
- 2) the definition of an appropriate time window in order to complete the component, system, and plant-specific definition of a CFM event,
- 3) the plotting of failure data by failure mechanism and system as a function of time,
- 4) the postulation of intra-system CFM events, using the time-line plots for each system separately to identify clusters of failures which are due to the same mechanism and which occur within the adopted time window, and
- 5) the postulation of inter-system CFM events by similarly comparing the time-line plots of different systems.

Steps 3, 4, and 5 are straightforward and are illustrated in the presentation of results in Section 3.0. The assignment of failure discovery dates and the assumption of an appropriate time window for defining CFM events, however, are discussed further below. Note that, in following the above steps for CFM event identification, another difference is created between the CFM events identified in this study and the common cause failures that might be identified in PRA studies. The definition of a CFM event is not limited to, as is the definition of a common cause failure, the failures of components which are on redundant trains of a system, performing exactly the same function (e.g., low pressure cold leg injection MOVs on Trains A and B). In this study, two or more failures of any components which are part of a system's major flowpath can be termed a CFM event if all parts of the CFM event definition are satisfied.

One of the crucial tasks in the identification of CFM events is determining the time of component failure, or the "discovery" date. Maintenance work record data bases typically contain several dates related to the repair and return to service of a failed component. From data base to data base, there are variations in which dates are reported and what relationship these dates have to when a component failure actually occurred. As stated above, a work order initiation date, if available, is preferred to a work start date so far as best estimating the discovery date of a component failure. However, uncertainties

and inaccuracies in the determination of discovery dates are likely even when work order initiation dates are used due to, for instance, the lack of timeliness in reporting (and/or documenting) component failures and the practice of checking of similar components on alternate trains when a component failure, occurs (i.e., cross-train checking).

The third part of the "common failure mechanism event" definition, as was discussed in Section 2.1, is an assumed appropriate time window. For the systems (primarily safety systems) and component type investigated in this study, all failures of similar components and common failure mechanism category were assumed to be common mechanism failures when they were separated in time by one month or less. This assumption regarding the proximity of failures is based upon the fact that, typically, the shortest time between tests (and, therefore, discovery of failures) of safety system components in nuclear power plants is one month. However, this assumption neglects the possibility that false identifications of CFM events can occur because of the practice of testing components of similar type and function when a failure is discovered. The maintenance record data bases analyzed for this study verified that this maintenance practice is relatively common. Due to this common (probably industry-wide) practice, and the resultant possibility of false CFM event identification from maintenance records, it is recommended that the potential CFM events identified in this study be verified at the plant site through the analysis of original work order requests or interviews of maintenance and engineering personnel before they should be labeled other than "potential" events. Identified potential inter-system CFM events should also be validated.

2.5 Assessment of CFM Event Risk-Significance

Risk-significance, defined in terms of PRA results (i.e., core melt frequency), is determined in this study based upon existing PRA information or general knowledge regarding PPA analysis techniques. The foundation for such determinations is the appropriate selection of systems and components for inclusion in the analysis (see Section 2.2, Data Selection). Assuming that the data selection process included consideration of PRA risk concepts, the risk-significance of the potential CFM events identified with this technical approach can be assessed with the following four steps:

- 1) separate CFM events which are composed of all catastrophic failures from those which are composed of non-catastrophic failures, either exclusively or in combination with catastrophic failures,
- 2) compare the component failures comprising CFM events with the elements of the minimal cutsets for all dominant sequences produced in a PRA and note the resulting matchups,

- 3) re-construct minimal cutset elements which may have been truncated from the PRA results due to low probability (i.e., review system diagrams to determine other combinations of component failures which result in failure of system function),
- 4) develop a hierarchy of risk-significance based upon: a) whether or not the identified CFM events match up with elements of minimal cutsets and b) whether or not the identified CFM events contain all catastrophic failures or some combination of catastrophic and non-catastrophic failures.

The hierarchy of Step 4 can be represented as a matrix of the risk-significant considerations regarding potential CFM events. The catastrophic component failures of, by definition, catastrophic potential CFM events are risk-significant since these failures should be represented in the PRA data base. The inclusion of these dependent catastrophic failures in the PRA data set would result in larger component failure probabilities than if only independent failures are included. Since the failure data used in PRAs are typically lumped by component type, the failure probabilities for all components of the same type which are included in the PRA model could be larger than that based upon independent failures only (i.e., the random failure rate) because of these dependent failures. As a consequence of larger component failure probabilities contained in the PRA data set, the probability of core melt calculated in the PRA study is likely to be larger than would have been otherwise. In a similar fashion, the non-catastrophic component failures which comprise a non-catastrophic potential CFM event can be viewed as precursors to catastrophic, dependent failures and, therefore, less risk-significant than catastrophic dependent failures. The risk-significance of CFM event/minimal cutset matchups is based upon the fact that, typically, each minimal cutset in a PRA study consists of probabilities of independent component failures only. (The exceptions are those cutsets which contain common cause failures.) The probability of core melt represented by minimal cutsets which are comprised of only independent component failures must be increased to account for dependent component failures. Matchups of the dependent component failures comprising a potential CFM event with elements of a minimal cutset indicates a potential need to increase the PRA's reported core melt frequency to reflect increases in the probabilities of contributing minimal cutsets. In summation, the most risk-significant potential CFM events are those comprised of catastrophic component failures which match up with elements of minimal cutsets. The successively less risk-significant potential CFM events are: non-catastrophic CFM events which match up with minimal cutsets, catastrophic CFM events which do not match up with minimal cutsets, and non-catastrophic potential CFM events which also do not match up with minimal cutsets.

Another difference between the potential CFM events and common cause failures (CCFs) is evident when identifying matchups of CFM events with minimal cutsets. Common cause failures are included in PRA models, and their results, only for components (of the same type) which serve the same function on redundant trains of a system.

Examples of two valid CCFs involving MOVs for a low pressure injection (LPI) system (which has no cross ties between its two injection trains) would include the Train A and B pump suction MOVs and the Train A and B cold leg injection MOVs. In contrast, common failure mechanism (CFM) events are composed of any combination of component failures (of the same type) which fail the function of the system. Hence, in addition to the valid CCF combinations of MOV failures, a potential CFM event for the combination of the LPI system's Train A pump suction and Train B cold leg injection MOV failures, and vice versa, is also appropriate.

3.0 Results

The technical approach described in the previous section was applied to the data bases, systems, and components which were determined as part of the data selection task. Analysis of the selected motor-operated valve (MOV) failures of the low pressure injection (LPI), high pressure injection (HPI), emergency feedwater (EFW), and service water (SW), and containment spray (CT) systems produced the following results:

- MOV failure mechanism categories,
- identified potential CFM events,
- assessments of risk-significance for identified potential CFM events, and
- postulated defenses to identified potential CFM events.

3.1 MOV Failure Cause Categories

Seven categories of failure mechanisms were developed for MOV failures. These categories are representative of the failures contained in the maintenance record data bases for the selected systems of the two plants analyzed. The MOV failure mechanism categories are:

- leakage (packing or seat),
- binding,
- torque/limit switch (TS/LS) failures,
- motor/operator failures,
- external events,
- plugging (applicable to the SW system only), and
- other.

As noted in this list, plugging failures, usually manifested by internal corrosion, were only applicable to the SW system due to its operating environment (i.e., raw rather than borated water). The "other" category was used for all failures which could not be categorized elsewhere. By design, there were very few "other" failures (i.e., none in the Plant X data base and three in the Plant Y data base).

3.2 Identified Potential CFM Events

Following the analysis and categorization steps described in the sections above, the MOV failure data for Plants X and Y were plotted as described in Section 2.4. Examples of such time-line plots, chosen for the relatively large number of failures represented, are shown in Figures 1 - 3. Using these plots, and the documentation of discovery dates when necessary, clusters of MOV failures on any horizontal line representing a failure mechanism were identified as potential CFM events. The results of such identifications are discussed below.

Based upon the potential CFM events identified for all failure mechanisms, Table 1 shows the number of potential CFM events, the total number of MOV failures, and number of MOV dependent failures, or common mechanism failures, and the ratio of dependent to total number of failures for both Plants X and Y. (Leakage failures are indicated separately since all such failures were judged to be less risk-significant than failures of other categories. This judgment was based upon the functions, and failure modes, of the MOVs included in the data set.) This table indicates that the numbers of identified potential CFM events are significant for both plants, although the number of CFM events for Plant Y is greater than that for Plant X by a factor of 3. Similarly, the numbers of dependent and independent Plant Y MOV failures and the fraction of dependent failures are larger than the Plant X statistics. Table 2, however, shows that the number of catastrophic CFM events are nearly the same for Plants X and Y. Also, the four categories of failure mechanisms having the most numerous identified potential CFM events are the same for both plants: leakage, torque/limit switch failures, binding, and motor/operator failures. In fact, with the exception of leakage failures, the Plant X and Plant Y numbers of identified potential CFM events for these four categories are almost identical.

Among the results for Plant Y are two unusual CFM events, both of which occur in July 1986. Nearly all of the Plant Y TS/LS MOV failures occur during this time frame, resulting in one huge inter-system CFM event which can be broken down into smaller intra-system CFM events involving all of the Plant Y systems studied. Similarly, a relatively large number of the motor/operator MOV failures, encompassing all four Plant Y systems, occur in July 1986. Further investigation of these large inter-system potential CFM events is necessary in order to explain their occurrence. Whatever the reason for these potential CFM events, the analysis of this study indicates that degradation of components, such as that described in July 1986 maintenance records of the Plant Y data base, can be risk-significant.

3.3 Risk-Significance of Identified CFM Events

Matrices of identified potential CFM events were constructed as described in Section 2.5. Two examples of such matrices, selected specifically because of the relatively large number CFM events included, are shown in Tables 3 and 4. Based upon the hierarchy discussed in Section 2.5, the matrices constructed for Plants X and Y revealed

Figure 1a. MOV failures of the Plant Y low pressure injection system.

Figure 1b. MOV failures of the Plant Y low pressure injection system.

Figure 2a. MOV failures of the Plant Y high pressure injection system.

Figure 2b. MOV failures of the Plant Y high pressure injection system.

Figure 3a. MOV failures of the Plant Y service water system.

Figure 3b. MOV failures of the Plant Y service water system.

Table 1. Total Number of Common Mechanism Failure (CFM) Events, Contrasted to the Total Number of Failures and Number of Failures in CFM Events for Plants Y and X With and Without Leakage Failures.

Plant		Number of CFM Events (w/o Leakage)	Total Number of Failures (w/o Leakage)	Number of Common Mechanism Failures (w/o Leakage)	Fraction of Failures that Are Common Mechanism (w/o Leakage)
Plant X	1984-1987 (4 years)	8 (5)	45 (35)	21 (14)	0.467 (0.40)
Plant Y	1984-1989 (5 years)	21(8)	176 (108)	139 (80)	0.790 (0.741)

Table 2. Breakdowns of the Number of CFM Events for Plants X and Y: Catastrophic Versus Non-Catastrophic and the Categories of Torque/Limit Switch, Leakage, Binding, and Motor/Operator Failures.

	Number of CFM Events (w/o Leakage)					
Plant/Total	Catastrophic	Non-Catastrophic	TS/LS	Leakage	Binding	Motor/Operator
Plant X 8 (5)	4 (4)	4 (1)	3	3	2	0
Plant Y 21* (8)*	5 (5)	18 (5)	3	13	1	2

* Some non-catastrophic CFM events are formed which could be considered part of catastrophic CFM events. Since the non-catastrophic events are not unique, they are not counted in the total.

that only two potential CFM events for Plant Y and only one for Plant X are ranked as most risk-significant (i.e., top left in matrix). The two most risk-significant CFM events for Plant Y involve MOV failures in the SW system due to torque/limit switch- and external event-caused failures, respectively (shown in Tables 3 and 4). The Plant Y TS/LS failures, shown in Table 3, involve SW MOVs which provide cooling water to the two emergency diesels while the external event-caused CFM event involves the failure of all four SW MOVs which provide cooling to the containment fan coolers. The Plant X risk-significant CFM event involves failure of both LPI Hot Leg isolation MOVs which are required for the shutdown cooling function. In addition, several potential non-catastrophic CFM events which correspond with elements of cutsets (i.e., the next most risk-significant category: top right) were found in the risk-significant matrices for Plant Y. These Plant Y potential CFM events include three cutset matchups with potential CFM events formed by Plant Y leakage failures, three cutset matchups with Plant Y binding failures, fourteen cutset matchups with Plant Y torque/limit switch (TS/LS) failures, and one cutset matchup with Plant Y motor/operator failures. In contrast, all Plant X potential CFM events, other than the torque/limit switch CFM event discussed above, fall in the least risk-significant (i.e., bottom right) category.

3.4 Postulated Defenses to Identified CFM Events

Based upon the results of the dependent failure analysis performed in this study, a variety of defensive actions can be recommended which may reduce a plant's vulnerability to MOV common failure mechanism events. The defensive actions or strategies given in this section have been developed primarily with the evidence from the Plant Y and X data bases concerning the numbers of MOV CFM events and fractions of MOV failures which are due common mechanisms. In addition, lower level failure cause (i.e., potential root cause) information derived from the failure cause and work performed descriptions in the data bases was drawn upon to formulate the defensive strategies. Since, as indicated in a previous section, vulnerabilities by failure cause to common failure mechanism events may be plant-specific, defenses to CFM events may also be plant-specific. Hence, while the defensive strategies given here are intended to be generic to both Plant Y and Plant X, whether or not they may be generically applicable to other nuclear power plants has not been established by this study.

The defenses developed in this study are shown in Table 5. The table shows the suggested defenses, the potential effect of the defensive actions, and the failure mechanism categories which are expected to be impacted. Recommended defenses include additional preventive maintenance actions, increased surveillances or inspections (formal or informal), design improvement, procedural improvements, increased training, and programmatic improvements. The defenses are expected to result in either improved detection or prevention of common failure mechanism events. Associated with the defenses and their possible effects are suggestions for the most likely failure causes to be impacted, as evidenced by the failure cause and work descriptions in the Plant Y and Plant X data bases. In keeping with the results of this study regarding the important failure mechanisms from

Table 3. Plant Y Common Failure Mechanism Events
Categorized by Risk for Torque/Limit Switch Failures.

	Catastrophic Failures	Non-Catastrophic Failures
In Cutsets	<p>* SW Event</p> <p>SW10 (86-1-13, 86-1-23)</p> <p>SW11 (86-1-13)</p>	<p>1. LPI Cutset (86-7-3)</p> <p>LP9, LP5, LP8</p> <p>2. EFW Cutset (86-7-3)</p> <p>FW9, FW15</p> <p>3. SW/EFW Cutset</p> <p>SW2 (86-7-17)</p> <p>FW4 (86-7-3)</p> <p>4. SW/LPI Cutsets</p> <p>a. SW2 (86-7-17)</p> <p>LP5 (86-7-3)</p> <p>b. SW2 (86-7-17)</p> <p>LP8 (86-7-3, 86-7-17)</p> <p>LP9 (86-7-3)</p> <p>5. LPI/EFW Cutsets (86-7-3)</p> <p>a. LP5</p> <p>FW4</p> <p>b. LP5</p> <p>FW4</p> <p>FW15</p> <p>* 1. LPI Events</p> <p>a. LP7 (86-7-3, 86-7-17)</p> <p>LP8 (86-7-3)</p> <p>b. LP4 (86-7-17)</p> <p>LP5 (86-7-3)</p> <p>c. LP9 (86-7-3)</p> <p>LP11 (86-7-17)</p> <p>d. LP11 (86-7-17)</p> <p>LP8 (86-7-3, 86-7-17)</p> <p>* 2. HPI Event</p> <p>HP2 (86-7-3, 86-7-17)</p> <p>HP1 (86-7-3)</p> <p>HP4 (86-7-3)</p> <p>HP5 (86-7-17)</p> <p>* 3. EFW Event</p> <p>FW2 (86-7-3, 86-7-17)</p> <p>FW1 (86-7-3)</p> <p>** HPI Event (86-7-3)</p> <p>HP7, HP8, HP9, HP10, HP11</p>
Not In Cutsets	<p>1. LPI/SW (86-7-17)</p> <p>a. LP8</p> <p>b. SW1</p> <p>SW11</p> <p>2. SW/EFW Event</p> <p>SW8 (86-12-12)</p> <p>FW4 (86-12-20)</p>	<p>1. 86-7-3 Event *</p> <p>LP3</p> <p>HP14</p> <p>SW15</p> <p>FW5</p> <p>FW12</p> <p>2. 86-7-17 Event *</p> <p>LP2</p> <p>SW5</p> <p>SW4</p> <p>SW7</p>

* Should be in cutsets

* The two events in July are considered as a single CFM event.

** Potential initiating event.

**Table 4. Plant Y Common Failure Mechanism Events
Categorized by Risk for External Events.**

	Catastrophic Failures	Non-Catastrophic Failures
In Cutsets	*SW Cutset (88-10-11) SW15, SW16, SW17, SW18	
Not in Cutsets		

* Should be in cutsets

the standpoint of the frequency and risk-significance of potential CFM events, it can be observed that most of the defensive actions in Table 5 focus upon minimizing the potential for common failure mechanism events due to TS/LS-, leakage-, motor-operator-, and binding-caused failures.

Although complete analysis of the lower level failure cause information in the Plant Y and Plant X data bases was beyond the scope of this project, this information suggested specific actions for increased preventive maintenance, surveillances and inspections, design improvement, training, procedures, and programmatic improvements. In the Plant Y data base, for instance, the numerous packing leak-related work requests, representing a significant investment of resources, suggest that some cost-effective strategy of replacing packing through the preventive maintenance, as opposed to corrective maintenance, program might be worthwhile. Similarly, the Plant Y data base supports the idea of between-test or during maintenance surveillances or inspections as possible vehicles for the early detection of valve degradations which have visually observable symptoms (e.g., drips from packing leaks; boron precipitation in the LPI and HPI systems as evidence of packing or seat leaks and as a possible precursor to binding; and corrosion- or wear-related seat leaks, binding, or SW plugging). Inspection of similar MOVs following discovery of seriously degraded or incorrectly maintained equipment, evidently already practiced in instances such as severe corrosion of Plant Y valve internals, could be beneficially extended to torque switches or limit switches which are found to be out of tolerance. The recurrence of some Plant Y and Plant X binding failures (e.g., handwheel operator cover interference with moving parts) and TS/LS and motor/operator failures (e.g., wires burnt due to proximity of internal space heater) might be avoided through improvement of MOV design. Training for recognition of the visually observable symptoms of valve degradation would support the inspection/surveillance defense mentioned above as well as support component condition monitoring tasks. According to the both data bases, specific training in the area of electricity fundamentals may be effective in reducing or eliminating the contributors to TS/LS- and motor/operator-caused failures (e.g., missing ground wires, reversed motor leads, open circuits, improperly crimped wires, missing TS limiter plate). Similarly, both data bases provide evidence that maintenance procedure enhancement could reduce maintenance errors of both commission and omission related to all failure causes (e.g., missing packing, missing bolts, over-torquing, electrically-related maintenance errors). Overall, maintenance programs, both preventive and corrective, might be improved diagnosis, planning, and scheduling through the use of: 1) component condition monitoring, tracking, and trending; 2) reporting of better failure cause descriptions; 3) better communication with site organizations outside maintenance, such as engineering; and 4) use of root cause analysis for important and/or chronic failures. For instance, the Plant Y single catastrophic plugging failure, one of several plugging failures which had "discovery dates" two years before repair, illustrates the need for improved understanding of potential failure mechanisms in conjunction with maintenance planning and scheduling.

Table 5. Possible CFM Defenses, their Effects, and Impacted Failure Mechanisms Based Upon Plant Y and Plant X Data Bases

Possible Common Failure Mechanism Event Defense	Potential Effect	Possible Failure Mechanisms Impacted
Regular, planned replacement of packing.	Prevention of packing leaks.	Packing leaks.
Between-test surveillance or inspection. Training of all field personnel to recognize failure cause symptoms.	Early detection of packing leaks, boron precipitation-caused binding; corrosion, wear or boron precipitation-caused seat leaks; and plugging.	Packing and seal leaks, binding, and plugging.
Surveillance for vibration.	Early detection of vibration induced failures.	Torque/limit switch, motor/operator.
Inspection of similar valves when one is found degraded or incorrectly maintained	Prevention/early detection of failures caused by either degradation or human error.	All failure causes.
Design improvement program under utility/mannufacturer/vendor guidance.	Prevention/early detection of design related failures.	Binding, torque/limit switch, motor/operator.
Functional testing included in the post-maintenance process prior to control room release.	Detection/prevention of maintenance-caused failures.	Torque/limit switch, motor/operator, binding to over-torquing.
Calibration procedures which include specific instructions, setpoints, and functional testing.	Prevention/detection of human-caused failures.	Torque/limit switch.

**Table 5. Possible CFM Defenses, their Effects, and Impacted Failure Mechanisms Based Upon Plant Y and Plant X Data Bases
(Continued)**

Possible Common Failure Mechanism Event Defense	Potential Effect	Possible Failure Mechanisms Impacted
<p>Maintenance procedures which include the following features:</p> <ul style="list-style-type: none"> o More specific instructions, o Inclusion of equipment/materials lists, o Independent checking, and o Human-factoring. 	Prevention of maintenance-caused failures.	All failure causes, but especially binding due to over-torquing, torque/limit switch, motor/operator.
<p>Training for all maintenance personnel regarding fundamentals of electricity and the function of electrical piece-parts.</p>	<p>Improved detection of contributing failure causes.</p> <p>Prevention of maintenance-caused failures.</p>	Torque/limit switch, motor operator.
<p>Component condition monitoring, tracking, trending.</p> <p>Use of failure cause descriptions in the work order data base which include best-estimates of failure cause and a description of work performed.</p> <p>Communication between maintenance and engineering regarding work order requests.</p> <p>Root cause analysis of important component failures.</p>	Improved planning and scheduling of both corrective and preventive maintenance (i.e., prevention of catastrophic failures) based upon improved understanding of failure causes and mechanisms (i.e., detection).	All failure causes, but especially corrosion- or wear-caused seat leakage, binding, and plugging.

4.0 Summary and Conclusions

Based upon the experience of this study, the applications of this technical approach for the analysis of dependent failures can be beneficial in putting together a strategy for preventing common failure mechanism events through early detection of degraded component functions. This study verified that plant data bases can be used to detect indications of common failure mechanism events since a significant number of potential CFM events were identified in both data bases used in this study. In addition, analysis of both plants' data bases revealed noteworthy risk-significance by virtue of potential CFM event matchups with elements of cutsets in respective PRAs. These assessments of CFM event risk-significance were demonstrated to be useful in prioritizing efforts to develop defensive actions to CFM events. Finally, since the application of this approach is straightforward and generic once failure mechanism categories are developed, similar insights can be gained from the analysis of other plants, systems, and component types using this technical approach.

REFERENCES

1. D. G. Satterwhite et. al., Root Causes of Component Failures Program: Methods and Applications, NUREG/CR-4616, December 1986.
2. PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, NUREG/CR-2300, Vol.1, January 1983.