ANS PSA 2008 Topical Meeting - Challenges to PSA during the nuclear renaissance
Knoxville, Tennessee, September 7–11, 2008, on CD-ROM, American Nuclear Society, LaGrange Park, IL (2008)

SOME COMPONENT INSIGHTS FROM ANALYZING NRC'S COMMON-CAUSE FAILURE DATABASE

Dale M. Rasmuson
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001
dale@rasmuson.net

Ali Mosleh
Center for Risk and Reliability
University of Maryland
College Park, MD 20742
mosleh@umd.edu

Thomas E. Wierman
Idaho National Laboratory
Idaho Falls, ID 83415-3250
thomas.wierman@inl.gov

ABSTRACT

This paper summarizes key insights from studies of common-cause failures (CCF) of emergency diesel generators (EDGs), motor-operated valves (MOVs), motor-driven pumps (MDPs), and circuit breakers (CBs) from 1980 to 2005. The data studied were derived from the Nuclear Regulatory Commission's CCF database, which is based on U.S. commercial nuclear power plant event data. The insights are the result of an in-depth review of the CCF data. Trends of the annual number of CCF events show that the number of events has been decreasing over time. The insights can help to focus inspection and utility maintenance activities.

Key Words: common-cause failure insights, emergency diesel generators, motor-operated valves, pumps, circuit breakers

1 INTRODUCTION

This paper provides a summary of insights related to common-cause failure (CCF) events for emergency diesel generators (EDGs), motor-operated valves (MOVs), motor-driven pumps (MDPs), and circuit breakers (CBs). The insights for U.S. plants are derived from information captured in the common-cause failure (CCF) database maintained for the U.S. Nuclear Regulatory Commission (NRC) by the Idaho National Laboratory (INL). The database contains CCF-related events that have occurred in U.S. commercial nuclear power plants reported in licensee event reports (LERs) and reports to the Nuclear Plant Reliability Data System (NPRDS) and the Equipment Performance and Information Exchange (EPIX) system maintained by The Institute for Nuclear Plant Operations (INPO).

The CCF data contain attributes about events that are of interest in the understanding of: completeness of the failures, occurrence rate trends of the events, sub-system affected (if applicable), causal factors, coupling or linking factors, event detection methods, and manufacturer. Distributions of these CCF characteristics and trends were analyzed and individual events were reviewed for insights. The information presented in this paper can help focus inspections on the more risk-important aspects of CCF events. Utilities can also use the information to help focus maintenance and test programs such that CCF events are minimized.

The CCF event data collected, classified, and compiled in the CCF database provide a unique opportunity to go beyond just estimation of CCF frequencies to gain more engineering insights into how and why CCF events occur. The data classification employed in the database was designed with this broader objective in mind. The data captured include plant type, system component, piece parts, failure causes, mechanisms of propagation of failure to multiple components, and functional and physical failure modes. Other important characteristics such as defenses that could have prevented the failures are also included.

2 COMMON-CAUSE FAILURE EVENT DATA SOURCE

The CCF event collection effort uses event data from operating U.S. commercial nuclear power plants (NPP). The evaluation presented in this paper is based on the operating experience from 1980 through 2005. The data sources used in the CCF data collection include: (1) LERs, 1980 to 2005, (2) NPRDS, 1980 to 1996, and (3) EPIX, 1997 to 2005. The CCF data collection and analysis system consists of (1) CCF event identification methodology, (2) event coding guidance, and (3) a software system to estimate CCF parameters. The systems and components contained in the CCF Database are mainly the important components and systems contained in probabilistic risk analysis (PRA) models. The data collection period is from 1980 through 2005. The number of CCF events in the database for this period is over 1700. The number of complete CCF events is over 240. A complete CCF is an event in which all components affected are in the failed (as opposed to degraded) state, fail within a short time period, and have the same shared cause.

The CCF event identification process includes reviewing failure data to screen and identify independent and CCF failure events. The following four criteria must be met for an event to be classified as resulting from a common cause:

- Two or more individual components must fail or be degraded, including failures during demand, inservice testing, or from deficiencies that would have resulted in a failure if a demand signal had been received;
- Two or more individual components must fail or be degraded in a select period of time such that success during the PRA mission would not be certain;
- The component failures or degradations must result from a single shared cause and coupling mechanism; and
- The component failures are not due to the failure of equipment outside the established component boundary.

The CCF event coding process provides guidance for the analyst to consistently code events. The CCF events undergo a quality assurance review by outside parties. Any differences are reviewed and the differences reconciled before the events are added to the database.

Additionally, the CCF events are stored in a format that allows PRA analysts to review the events and develop understanding of how they occurred.

A software system stores CCF events and independent failure counts, and automates parameter estimations for CCF probability models used in PRAs. The system employs two quantification models: the alpha factor and the multiple Greek letter method. These models are used throughout the nuclear industry. The software system and data are shared with utilities under an agreement with INPO. The users of the database provide feedback on the software system and any errors they may find in a particular event in the database.

The computer software produced for this project uses the impact vector method introduced in References 1 and 2 and further refined in References 3 – 6. The basic information needed for understanding and coding a CCF event is based on the physical characteristics of the event, and is recorded in the following fields in the database: a component degradation parameter for each component in the specified group of similar components, the timing factor (which is a measure of the time between the failures), and the shared cause factor (which measures the analyst's uncertainty about a shared cause). These are defined and explained in References 3 and 5. Other coded fields include the proximate cause (a characterization of the condition that is readily identified as leading to failure of the components), coupling factor (a factor characterizing why and how a failure is systematically induced in several components), failure mode, and the number of affected components.

3 GENERAL INSIGHTS

General CCF insights from the CCF database are available on the a are on the Reactor Operational Experience Results and Databases webpage [7]. These insights include graphs and trends based on all events in the database.

One important trend, shown in Figure 1, is that of the yearly CCF event occurrence rate. It has decreased over the years.

4 COMPONENT-SPECIFIC INSIGHTS

In this section we present some insights for four component types – emergency diesel generators, motor-operated valves, motor-driven pumps, and circuit breakers. References 8 – 11 contain detailed insights for the four components based on information from 1980 through 2000. A summary of selected CCF insights is presented in [12]. Table I contains a count of the CCF events and the complete CCF events and the percent failure for the specific component failure modes.

Table I Summary Statistics

Area	Emergency Diesel Generators	Motor-Driven Pumps	Motor-Operated Valves	Circuit Breakers
No. of Events	155	308	163	136
No. of Complete CCF Events	26	70	26	4
Failure to Start	41%	47%	—	—
Failure to Run	59%	53%	—	—
Failure to Open	—	—	61%	43%
Failure to Close	—	—	39%	57%

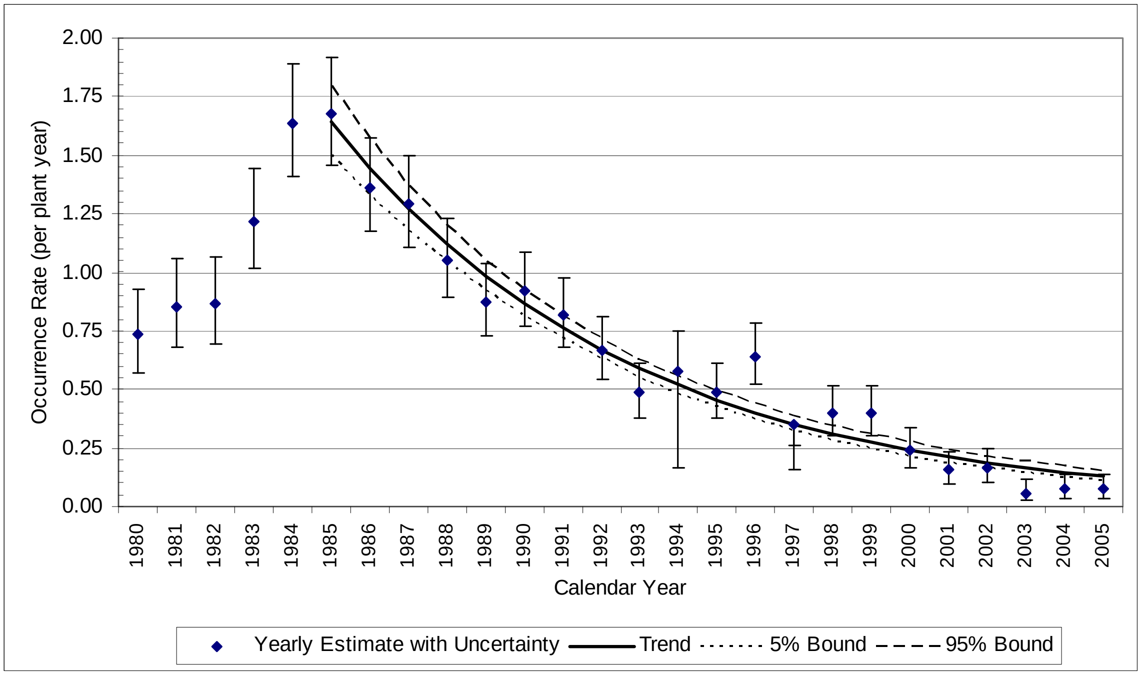

Figure 1. Annual occurrence rates and trends for all CCF events

4.1 Proximate Causes

In the context of the present discussion about CCF data coding, the *cause* of a failure event is a condition or combination of conditions to which a change in the state of a component can be attributed. It is recognized that the description of a failure in terms of a single cause is often too simplistic. For example, for some purposes it may be adequate to identify that a pump failed because of high humidity. However, to develop a complete understanding of the potential for multiple failures, it is necessary to identify why the humidity was high and why it affected the pump, e.g., it is necessary to identify the ultimate reason for the failure. There are many different paths by which the ultimate reason for failure could be reached. The sequence of events that constitutes a failure path, or failure mechanism, is not necessarily simple. As an aid to evaluating failure mechanisms, it is helpful to consider the following concepts (cf. NUREG/CR-5460).

A **proximate cause** associated with a component failure event is a characterization of the condition that is readily identifiable as having led to the failure. In the pump example above, humidity could be identified as the proximate cause. The proximate cause is usually easy to identify and is adequate for identifying and classifying CCF events for data coding. However, the proximate cause can be regarded as a symptom of the failure cause and does not necessarily provide a complete understanding of what led to that failed condition. As such, the proximate cause may not be the most useful characterization of failure events for the purposes of identifying appropriate corrective actions or for event assessment. Figure 1 contains the proximate cause hierarchy and their descriptions used to code the CCF events.

FAILURE CAUSE

- Design/Construction/Manufacture
  - Design Error
  - Manufacturing Error
  - Installation/Construction Error
  - Design Modification Error
- Operational/Human Error
  - Accidental Action
  - Inadequate/Incorrect Procedure
  - Failure to Follow Procedure
  - Inadquate Training
  - Inadequate Maintenance
- External Environment
  - Fire/Smoke
  - Humidity/Moisture
  - High/Low Temperature
  - Electromagnetic Field
  - Radiation
  - Bio-organisms
  - Contamination/Dust/Dirt
  - Acts of Nature
    - Wind
    - Flood
    - Lightning
    - Snow/Ice
- Internal to Component
  - Normal Wear
  - Internal Environment
  - Early Failure
- State of Other Component
  - Supporting System
  - Inter-connection
- Unknown
- Other

Design/Construction/Installation/Manufacture Inadequacy. This category encompasses actions and decisions taken during design, manufacture, or installation of components both before and after the plant is operational.

Operational/Human Error (Plant Staff Error). Represents causes related to errors of omission and commission on the part of plant staff. An example is a failure to follow the correct procedure. This category includes accidental actions, and failure to follow procedures for construction, modification, operation, maintenance, calibration, and testing. It also includes ambiguity, incompleteness, or error in procedures for operation and maintenance of equipment. This includes inadequacy in construction, modification, administrative, operational, maintenance, test, and calibration procedures.

External Environment. Represents causes related to a harsh external environment that is not within component design specifications. Specific mechanisms include electromagnetic interference, fire/ smoke, impact loads, moisture (sprays, floods, etc.), radiation, abnormally high or low temperature, and acts of nature.

Internal to Component. This is associated with the malfunctioning of something internal to the component. Internal causes result from phenomena such as normal wear or other intrinsic failure mechanisms. It includes the influence of the internal environment of a component. Specific mechanisms include erosion/ corrosion, vibration, internal contamination, fatigue, and wear-out/end of life.

State of Other Component. The component is functionally unavailable because of failure of a supporting component or system. For example, an air supply line to a valve breaks or a fuse in a control circuit blows. CCF events exclude those events that have dependencies that would reasonably be expected to be modeled in an IPE or PRA.

Unknown. This cause category is used when the cause of the component state cannot be identified.

Other. This cause category is used when the cause cannot be attributed to any of the previous cause categories. This category is most frequently used for cases of setpoint drift.

Figure 2. Proximate cause hierarchy

Figure 3 shows the proximate cause distribution for the four components. The dominant proximate cause for all for components is internal to component, followed by design and human/operations.

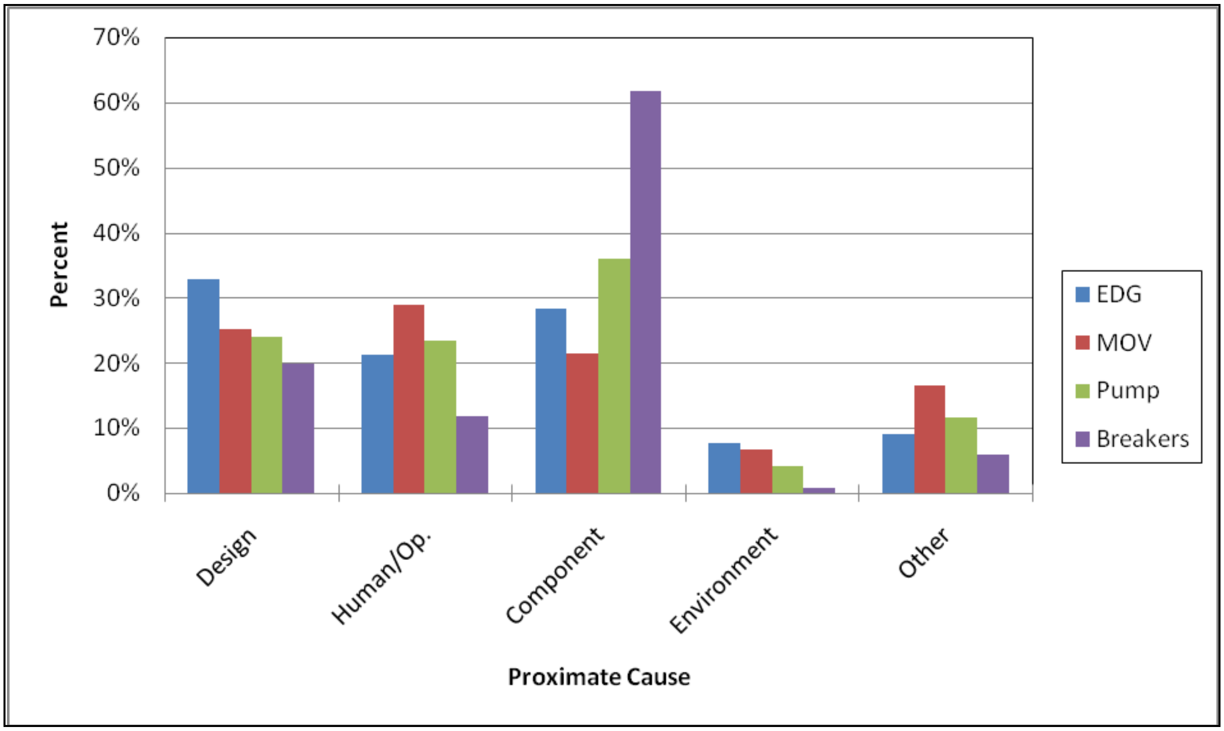

Figure 3. Proximate cause distributions for the four components

4.2 Coupling Factors

NUREG/CR-5460 presents a coupling factor classification system, which is used as a systematic and consistent method for classifying coupling factors of multiple component unavailability. A modified version of this classification system is used in the coding of operational data and in evaluating plant-specific defenses against multiple failures. The coupling factor classification format consists of five major classes:

- Hardware (quality) based,
- Design based
- Maintenance based,
- Operation based, and
- Environment based.

These five classes are divided into subcategories to provide more detail for important parameters and attributes. This is illustrated in Table II. The multi-layered coding approach acknowledges that during classification it is likely that only major categories can be identified because event descriptions used for coding are often not detailed enough to allow fine distinction down to the subcategory level.

Table II Coupling factors and their descriptions

Coupling Factor	Subfactor	Description
Hardware	Manufacturing	Components share the same manufacturing process.
	Installation/Construction (initial or modification)	Components share installation or construction features, from initial installation, construction, or subsequent modifications.
Design	Component parts (internal parts)	Components share the same design and internal parts.
	System configuration (physical appearance)	CCF event is a result of design features within the system in which the components are located.
Maintenance	Schedule	Components share the same maintenance and/or test schedules. For example, the components failed because maintenance was delayed until failure.
	Procedure	Components are affected by the same inadequate maintenance or test procedure. For example, the components failed because the maintenance procedure was incorrect or a calibration setpoint was incorrectly specified.
	Staff	Components are affected by a maintenance staff personnel error.
Operation:	Procedure	Components are affected by an inadequate operations procedure. For example, the components failed because the operational procedure was incorrect and the pumps were operated with the discharge valve closed.
	Staff	Components are affected by the same operations staff personnel error.
Environment	Internal	Components share an internal environment. For example, the process fluid flowing through the components is too hot.
	External	Components share the external environment. For example, the room that houses the components is too hot.

Figure 4 shows the coupling factor distribution for the four components. Maintenance and design are the major coupling factors for the four components.

4.3 Defensive Mechanisms/Strategies

To understand a defense strategy against a CCF event, it is necessary to understand that defending against a CCF event is no different from defending against an independent failure that has a single root cause, except that more than one failure has occurred, and they are related through a coupling mechanism.

There are three methods of defense against a CCF: (1) defend against the failure proximate cause; (2) defend against the CCF coupling factor; or (3) defend against both items 1 and 2. When a defense strategy is developed using protection against a proximate cause as a basis, the number of individual failures may decrease. During a CCF analysis, a defense based on the proximate cause may be difficult to assess particularly when a root cause analysis is not performed on each failure and those that are performed are not complete. However, given that a defense strategy is established based on reducing the number of failures by addressing proximate causes, it is reasonable to postulate that if fewer component failures occur, fewer CCF events would occur.

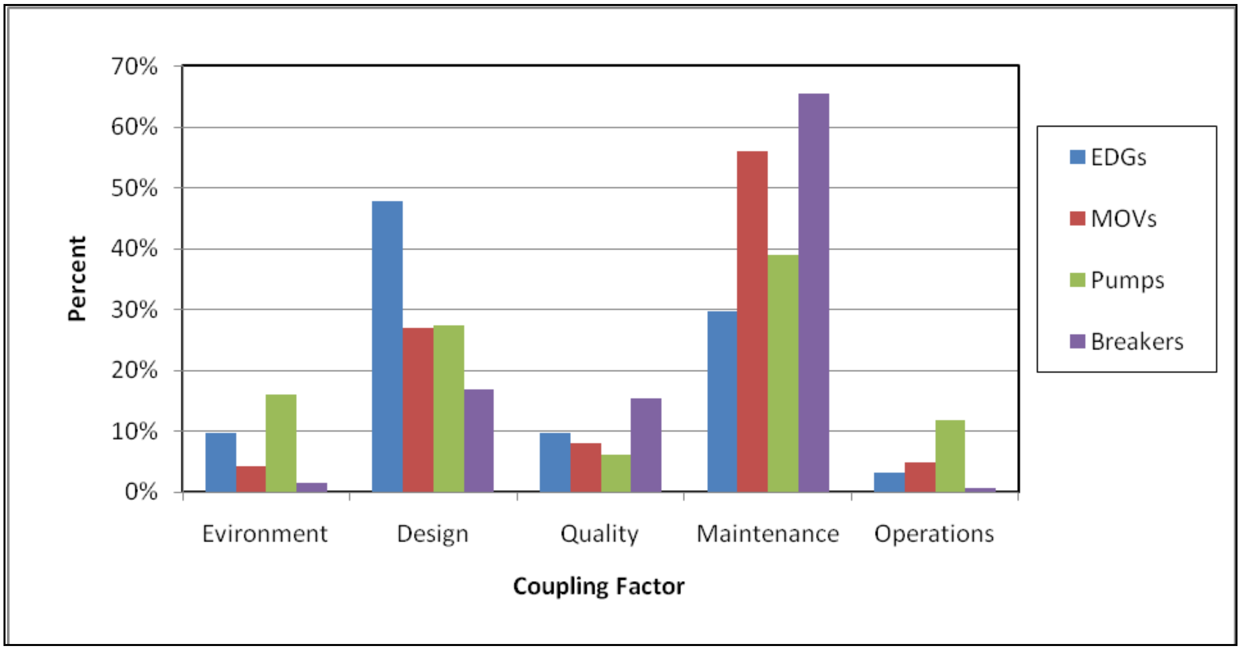

Figure 4. Coupling factor distributions for the four components

The above approach does not address the way that failures are coupled. Therefore, CCF events can still occur, but at a lower frequency. If a defense strategy is developed using protection against a coupling factor as a basis, the relationship between the failures is eliminated. During a CCF analysis, defense based on the coupling factor is easier to assess because the coupling mechanism between failures is more readily apparent and therefore easier to interrupt. Given that a defense strategy is developed with protection against the coupling factor as the basis, component failures may occur that may not be related to any other failures. A defense strategy based on addressing both the proximate cause and coupling factor would be the most comprehensive.

A defense strategy against proximate causes typically includes design control, use of qualified equipment, testing and preventive maintenance programs, procedure review, personnel training, quality control, redundancy, diversity, and barriers. For coupling factors, a defense strategy typically includes diversity (functional, equipment, and staff), barriers, and staggered testing and maintenance. The defense mechanisms for the CCF system are functional barrier, physical barrier, monitoring and awareness, maintenance staffing and scheduling, component identification, diversity, no practical defense, and unknown. These defenses are constructed primarily based on defending against the CCF coupling factors. A summary of the defenses is provided in Table III.

Table III Common-cause failure defensive mechanisms/strategies

Defense Mechanism	Description
Functional Barrier	A CCF event could be prevented by modification of the equipment functional interconnections. Defenses involving system or component design changes would fall under this category.
Physical Barrier	A physical restriction, barrier, or separation could have prevented a CCF. An example would be installation of a watertight door to preclude flooding of an equipment room.
Monitoring/Awareness	Increased monitoring, surveillance, or personnel training could have prevented a CCF.
Maintenance Staffing and Scheduling	A maintenance program modification could have prevented a CCF. This would include modifications such as staggered testing and maintenance/operation staff diversity.
Component Identification	Improvements in component identification, especially between identical trains in a system and similar systems in multi-plant facilities. Examples of this would be more visible equipment identification, bar coding, and color-coding.
Diversity	A modification to diversity could have prevented a CCF. This includes diversity in equipment, types of equipment, procedures, equipment functions, manufacturers, suppliers, personnel, etc.
No Practical Defense	No practical defense could be identified.
Unknown	Adequate detail is not provided on the cause and coupling factor for a CCF event to make an adequate defense mechanism identification.

We show the defensive mechanism distributions for the four components in Figure 5. Surveillance is the most common way of preventing CCFs.

5 CONCLUSIONS

In summary, the authors provide the following general insights:

- The number all CCF events, as well as complete CCF events has decreased over the years. The number of all CCF events has been relatively flat for the last 4 or five years and for about the last 10 years for complete CCF events.
- There is no significant change in the distributions of causes or coupling factors when comparing the distributions for 1980 – 1989 with the corresponding distributions of 1990 – 2005.
- The CCF results show that regulatory and maintenance programs are generally effective at reducing the number of CCF events.
- Maintenance and hardware design are the leading coupling factors for the four component types as well as for all components. Environment is the next most important proximate cause.

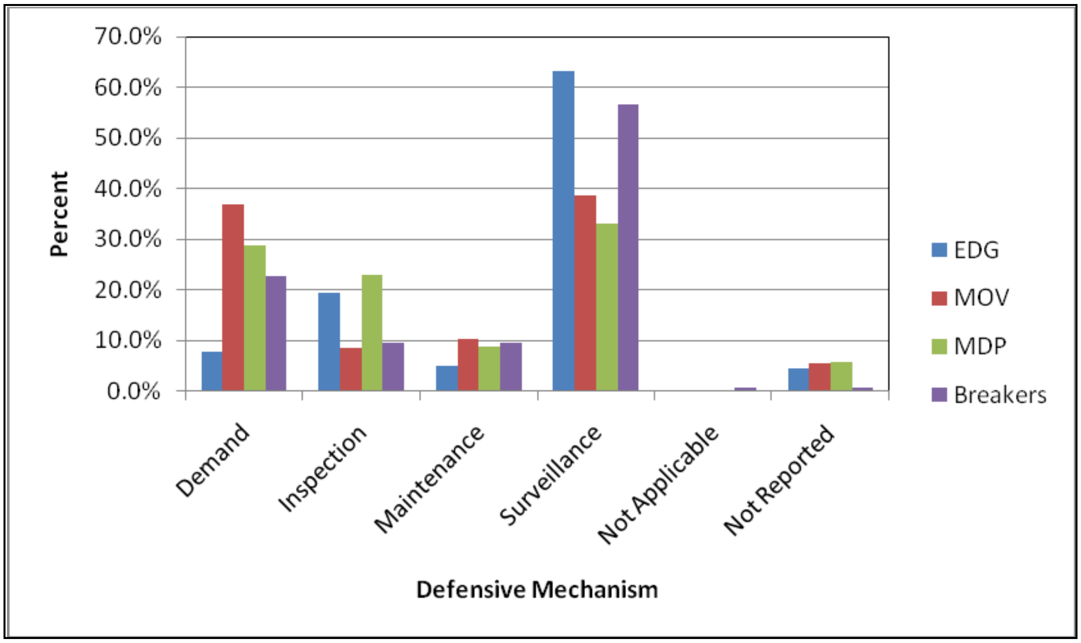

Figure 5. Defesive mechanism distributions for the four components

- The most important causes for EDGs, MOVs, and pumps are Design, Operations/Human, and Internal to Component – all three being about equal. For circuit breakers Environment is the most important proximate cause, followed by Design and Internal to Component.

6 REFERENCES

1 U.S. Nuclear Regulatory Commission, Procedures for Treating Common Cause Failures in Safety and Reliability Studies: Procedural Framework and Examples. NUREG/CR-4780, Volume 1, January 1988.

2 U.S. Nuclear Regulatory Commission, Procedures for Treating Common Cause Failures in Safety and Reliability Studies: Analytical Background and Techniques, NUREG/CR-4780, Volume 2, January 1989.

3 U.S. Nuclear Regulatory Commission, Procedure for Analysis of Common Cause Failures in Probabilistic Safety Analysis, NUREG/CR-5801, April 1993.

4 U.S. Nuclear Regulatory Commission, *Common-Cause Failure Database and Analysis System*, NUREG/CR-6268, Volumes 1-4, June 1998.

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

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

7 U.S. Nuclear Regulatory Commission, Reactor Operational Data Results and Databases, http://nrcoe.inl.gov/results, (2007).

8 U.S. Nuclear Regulatory Commission, *Common-Cause Failure Event Insights – Emergency Diesel Generators*, NUREG/CR-6819, Volume 1, May 2003.

9 U.S. Nuclear Regulatory Commission, *Common-Cause Failure Event Insights – Motor-Operated Valves*, NUREG/CR-6819, Volume 2, May 2003.

10 U.S. Nuclear Regulatory Commission, *Common-Cause Failure Event Insights – Pumps*, NUREG/CR-6819, Volume 3, May 2003.

11 U.S. Nuclear Regulatory Commission, *Common-Cause Failure Event Insights – Breakers*, NUREG/CR-6819, Volume 4, May 2003.

12 Dale M. Rasmuson, Ali Mosleh, and Thomas E. Wierman, "Insights from Analyzing NRC's Common-Cause Failure Database, *Journal of Risk and Reliability*, to be published.