AN ABSTRACT OF THE THESIS OF

Gregory M. Mocko for the degree of Master of Science in Mechanical Engineering presented on May 30, 2001. Title: Incorporating Uncertainty into Diagnostic Analysis of Mechanical Systems

Redacted for Privacy

Abstract approved: ______________________________

Robert K. Paasch

Analyzing systems during the conceptual stages of design for characteristics essential to the ease of fault diagnosis is important in today's mechanical systems because consumers and manufacturers are becoming increasingly concerned with cost incurred over the life cycle of the system. The increase in complexity of modern mechanical systems can often lead to systems that are difficult to diagnose, and therefore require a great deal of time and money to return the system to working condition. Mechanical systems optimized in the area of diagnosability can lead to a reduction of life cycle costs for both consumers and manufacturers and increase the useable life of the system.

A methodology for completing diagnostic analysis of mechanical systems is presented. First, a diagnostic model, based on components and system indications, is constructed. Bayes formula is used in conjunction with information extracted from the Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA), component

reliability, and prior system knowledge to construct the diagnostic model. The diagnostic model, when presented in matrix form, is denoted as the *Component-Indication Joint Probability Matrix.* The Component-Indication Joint Probability Matrix presents the joint probabilities of all possible mutually exclusive diagnostic events in the system.

Next, methods are developed to mathematically manipulate the Component-Indication Joint Probability Matrix into two matrices, (1) the Replacement Matrix and (2) the Replacement Probability Matrix. These matrices are used to compute a set of diagnosability metrics. The metrics are useful for comparing alternative designs and addressing diagnostic problems to the system, component and indication level, during the conceptual stages of design. Additionally, the metrics can be used to predict cost associated with fault isolation over the life cycle of the system.

The methodology is applied to a hypothetical example problem for illustration, and applied to a physical system, an icemaker, for validation.

Incorporating Uncertainty into Diagnostic Analysis of Mechanical Systems

by
Gregory M. Mocko

A THESIS

submitted to

Oregon State University

in partial fulfillment of
the requirement for the
degree of
Master of Science

Presented May 30, 2001
Commencement June 2001

Master of Science thesis of Gregory M. Mocko presented on May 30, 2001.

Approved:

Redacted for Privacy

Major Professor, representing Mechanical Engineering

Redacted for Privacy

Chair of Department of Mechanical Engineering

Redacted for Privacy

Dean of Graduate School

I understand that my thesis will become part of the permanent collection of Oregon State University libraries. My signature below authorizes release of my thesis to any reader upon request.

Redacted for Privacy

Gregory M. Mocko, Author

ACKNOWLEDGEMENTS

I would like to thank Dr. Robert Paasch for his help and direction during this research and for introducing me to a very new and exciting field of research in mechanical engineering. I would also like to thank Mr. Scott Henning for providing much of the information needed to complete this research and for the great tours of the Boeing facilities. Additionally, I would like to thank the National Science Foundation and the Boeing Company for the financial contributions to fund this research.

TABLE OF CONTENTS

Page

TABLE OF CONTENTS, CONTINUED

LIST OF FIGURES

LIST OF TABLES

LIST OF TABLES, CONTINUED

LIST OF APPENDICES

LIST OF APPENDIX FIGURES

LIST OF APPENDIX TABLES

LIST OF APPENDIX TABLES, CONTINUED

This thesis is dedicated to Hannah Mocko, my patient and understanding wife, and Jesus Christ, my personal savior who provided me with strength, perseverance, and guidance throughout my studies at Oregon State.

Incorporating Uncertainty in Diagnostic Analysis of Mechanical Systems

1 Introduction

Henry Ford, one of the most famous designers and engineers of all time, had perfected the techniques of *concurrent engineering* and *design for X* long before these terms were officially coined. In his book, *My Life and Work*, his objectives and goals in design and production of the Model T are presented. Ford designed for simplicity in operation, for absolute reliability, and for high quality. In addition, Henry Ford also desired to create an end product that could be easily serviced. Ford states,

> The important feature of the new model… was its simplicity. All [components] were easily accessible so that no skill would be required for their repair or replacement… it ought to be possible to have parts so simple and so inexpensive that the menace of expensive hand repair work would be entirely eliminated… it was up to me, the designer, to make the car so completely simple… the less complex the article, the easier it is to make, the cheaper it may be sold… the simplest designs that modern engineering can devise…. Standardization, then, is the final stage of the process. We start with the consumer, work back through the design, and finally arrive at manufacturing [Bralla 1996].

As described in the previous quotation, characteristics vital to the ease of service and maintenance were designed into the Model T from the conceptual stages. Unfortunately, many of the design philosophies that Henry Ford perfected in his designs have been lost in today's mechanical systems.

Without question, the mechanical systems of today have evolved into complex systems since the Model T. Consumer's desire for a greater number of functions and higher performance can lead to an increase in system complexity. The increase in complexity can often lead to designs that are not easily manufactured, serviced, maintained, or assembled.

Over the past decade an effort has been put forth on many issues pertaining to the concurrent design of products. Extensive research has been devoted to areas of assembly and manufacturing in design. As a result, formal methodologies have been developed to optimize systems in the area of assembly and manufacturing. These design tools provide an efficient and precise technique to optimize the design and design process of mechanical systems. *Design for assembly* (DFA), perhaps the most mature of these formal methodologies, has proven to bring a significant cost savings in production. DFA can, but not always, lead to an increase in reliability, but also may lead to designs that are more difficult to service. Despite the increase in system reliability, costs associated with service over the life cycle may offset the reliability benefit [Gerhenson 1991]. Less effort has been focused on design characteristics associated with the service and maintenance of mechanical systems. As a result, the development of formal methodologies in the areas of service and maintenance has lagged significantly behind.

1.1 Motivation for Diagnosability Analysis

Diagnosis of failures in electromechanical systems is costly in both time and money. Therefore, designing products with diagnosability optimized is becoming increasingly important in today's mechanical systems. Consumers and manufacturers are becoming increasingly concerned with costs associated with the entire life cycle of the product. Products with lower life cycle costs benefit consumers and manufacturers. Customers will incur fewer costs throughout the product life cycle, resulting in increased customer satisfaction, increased customer loyalty, and in turn an increase in revenue to the manufacturer. Additionally, manufacturers will incur fewer costs during warranty periods, resulting in longer warranty periods; a benefit to the customer.

The ability to isolate diagnosability difficulties and recommend areas of improvement during the conceptual stages of mechanical systems design will lead to a more efficient fault isolation process, and thereby reduce the total life cycle costs to the consumers and manufacturers, increase safety, and reduce system downtime. The inefficiency of fault isolation in mechanical systems serves as the primary motivation for exploring diagnosability improvement in mechanical systems.

1.2 Research Goals

Design for diagnosability is the area of design that focuses on decisions made throughout the design process, and how they affect the diagnosability of a system. Systems can be analyzed during the conceptual stages of design, and in turn decisions can be made to optimize the design in the areas of diagnosability. Design for diagnosability can be approached from two different perspectives. The first method, known as *achieved diagnosability*, improves diagnosis and maintenance procedures and incorporates electronic diagnostics into systems all ready in use. Achieved diagnosability, as defined by Simpson and Sheppard [1994] is the ability to observe system behavior under the observation of testing stimuli. This is a passive approach to the diagnosability optimization, requiring engineers to manage the errors designed into the system.

The second approach is to optimize the *inherent diagnosability* of a system from the conceptual stages of design. Inherent diagnosability is based on changes in the architecture, and their affect on the overall diagnosability of the system. Our efforts, in this research, are focused on the inherent diagnosability of mechanical systems.

This research investigates the effect of indication uncertainty on accurate failure diagnosis. The goal of this research is the development and refinement of methodologies for measuring and predicting inherent diagnosability. Specifically, methodologies are developed to analyze the *distinguishability* (observation phase) of mechanical systems during the conceptual stages of design and to systems all ready in use. The diagnostic methodologies developed will ultimately predict the probability of correctly diagnosing failures in mechanical systems. These methodologies will enable designers to predict life cycle costs, areas that cause problems in the diagnostic process, and possible improvements to be made to the system.

1.3 Overview of Research

In section 2 of this paper, we will briefly present the fault diagnostic process of mechanical systems. An overview of the observation phase is presented to develop a better understanding of the analysis methods developed.

Figure 1.1 is an overview of the diagnostic analysis methodology developed in this research. Three matrices are developed to complete diagnostic analysis of mechanical systems.

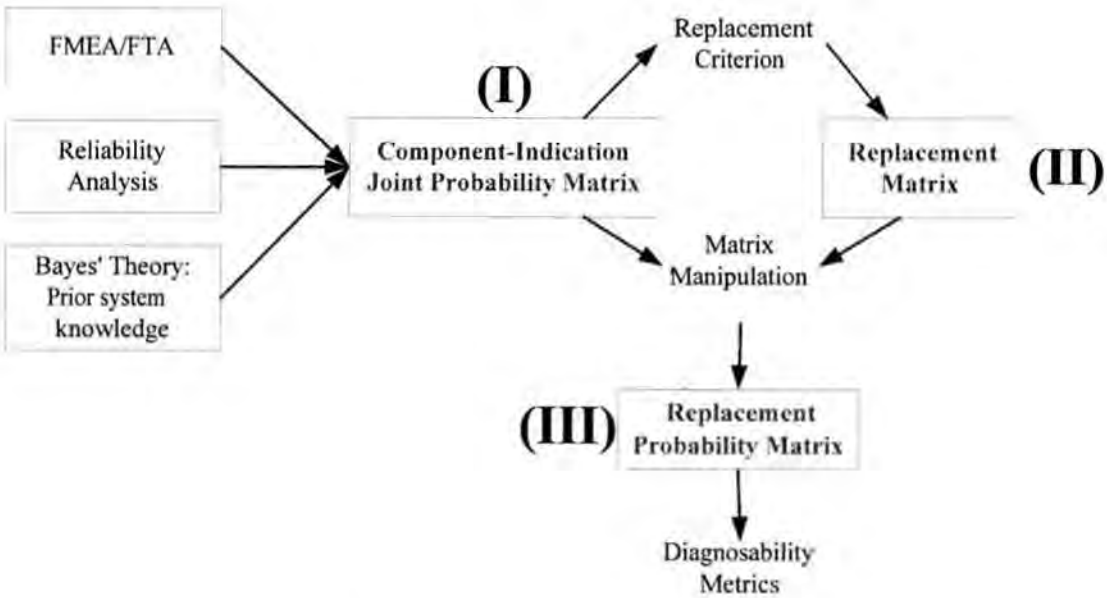


Figure 1.1. Overview of Diagnostic Analysis Methodology.

The first matrix that is formed is the *Component-Indication Joint Probability Matrix* (I). The matrix represents a diagnostic model of the system. In section 3 the information used for constructing the diagnostic model is presented. The Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA), component reliability, and indications certainty are used to construct the Component-Indication Joint Probability Matrix. The modeling and underlying mathematics for incorporating uncertainty into the diagnostic model are developed. Bayes' theory and truth tables are presented to incorporate uncertainty into the diagnostic model of a physically embodied system. The diagnostic modeling methodology is applied to a hypothetical illustrative example.

Next, the *Replacement Matrix* (II) is constructed by applying replacement criterion to the Component-Indication Joint Probability Matrix. The Replacement Matrix represents the component that will be replaced during the diagnostic process (see section 4.1).

Finally, the *Replacement Probability Matrix* (III) is computed by matrix multiplication of the *Component-Indication Joint Probability Matrix* and the *Replacement Matrix.* The diagnosability metrics are extracted directly from this matrix. Diagnosability metrics are introduced in section 4. The illustrative example is again utilized to verify the analysis method and the diagnosability metrics. The diagnosability analysis results of the illustration example and a discussion of those results are provided in section 5.

In section 6, the diagnosability methodologies and metrics are applied to the icemaker validation example. The analysis is completed for varying indication certainties. The diagnosability results for the icemaker validation example are discussed (see section 6.2).

This research builds upon previous research conducted in the area of system diagnosability. Methodologies are refined and new research topics are introduced and explored to benefit the areas of predicting system diagnosability.

1.4 Background Research

[Gerhenson 1991] presents a systematic methodology to balance serviceability, reliability, and modularity during the conceptual stages of design. Serviceability design is used in conjunction with DFA to create a design that has enhanced life-cycle qualities and production benefits. A methodology is developed to analyze mechanical system serviceability in both quantitative and qualitative ways. Finally, Gerhenson examines the tradeoffs between service costs and other life-cycle costs.

Ruff [1995] presents the method of mapping a system's *performance measurements* to system *parameters.* Performance measurements are the visible indications that monitor whether the intended function of the component is or is not being performed. Performance measures can be indications from lights, gauges, human observations, etc. Parameters refer to the system components that are measured. The parameters can be valves, controllers, ducting, or actuators. The diagnosability of the system is directly related to the interdependencies between measurements and parameters.

Clark [1996] extends Ruff's distinguishability metric to evaluate competing design alternatives. Clark presents metrics to compute the probability of failure for the components. This, in turn, is used to predict how difficult the system is to diagnose. The total diagnosability is computed using the average number of candidates for a given failure and the diagnosability of each component. The diagnosability of the system is a function of the total number of failure indications, the number of components, and the number of component candidates for each indication set. Clark develops *Weighted Distinguishability (WD)* to represent the interdependencies between components and indication sets. Clark extends the example of the BACS to determine how diagnosability varies in competing designs.

Wong [1994] presents a diagnosability analysis method that minimizes both time and cost during the conceptual stages of design. The analysis emphasizes the expected time to diagnose an indication and the expected time to diagnose a system. The method is used to select competing designs in order to optimize the design. The results from Wong's method show that the system diagnosability can be improved by changing the LRU-function relationships. Wong develops a checking order index to determine the order of checking of each system component. The index is calculated by dividing the probability of failure by the average time to check that specific component. Wong applies the method to an existing and redesigned bleed air control system (BACS).

Murphy [1997] developed prediction methods for a system's *Mean Time Between Unscheduled Removals (Unjustified)* ($MTBUR_{unj}$). The $MTBUR_{unj}$ metric is a significant component attribute in doing diagnosability analysis. This present research will broaden the methodology that Murphy began in predicting $MTBUR_{unj}$. The methods developed emphasize the ambiguity associated with system components and indications. The metrics are applied to the BACS using historical data. Multiple design changes are made to the BACS to determine the effect on system diagnosability.

Fitzpatrick [1999] develops an analytical model to determine the reliability and maintainability costs over the life cycle of the product. The goal of the research is to determine the effects that design changes may have on the total life-cycle cost of competing designs. Fitzpatrick develops methods for predicting *Mean Time Between Failures (MTBF)* and *Mean Time Between Maintenance Actions (MTBMA)* in addition to $MTBUR_{unj}$. The metrics can be used to determine cost for each component and the total expected cost of the system. The metrics are applied to the BACS to verify the metrics.

Henning [2000] develops matrix methods with which the probability of justified and unjustified removals is computed. A diagnosability model is constructed using the information gained from the FMEA. Matrix notation is used to describe the diagnosability model mathematically. Failure rate and replacement matrices are formed from component-indication mapping and replacement criterion, and mathematically manipulated to form the replacement rate matrix. The diagnosability metrics are computed from the replacement rate matrix. Diagnostic fault isolation is based solely on observation, not on diagnostic testing.

Simpson and Sheppard [1994] devote *System Test and Diagnosis* to the study of diagnosis and test in electronic systems. They introduce background and motivation to the development of the discipline. A historical perspective is provided about the formal methods all ready developed and research areas to come. Strategies for analyzing diagnosability are presented. They introduce bottoms up and top down strategies for system modeling. Advanced topic in the area of diagnosis where inexact diagnosis, fuzzy logic, and neural networks are presented. Case studies are provided throughout the book to present the topics, tools, and methods introduced. Simpson and Sheppard introduce highly mathematical and theoretical analysis of diagnosis to electronic applications.

Simpson and Sheppard [1998] organize a collection of technical papers written by researchers and scientists in the area of diagnosability and testability. The papers discuss subjects in the area of theoretical diagnosability from many different perspectives.

In both Simpson and Sheppard books the area of diagnosis is applied to complex electronic systems. Although much of the same terminology can be interchanged between mechanical and software diagnostic analysis, they are very different processes. Simpson presents a series of tests to be conducted on an electronic system. The tests have a known input signature and a known output signature for components that are good. However, when a component is faulty, the signature changes. A set of comprehensive tests is conducted on the electronics to verify their condition. These tests require little time to complete, thereby resulting in a large number of tests. However, the observation phase is of little help to fault isolation in electronic systems.

In mechanical systems, however, observations provide a great deal of information on the status of the system. Components are larger and the observations of indications and components allow conclusions to be drawn about the state of a mechanical system. For this reason, new methodologies of fault diagnosis in mechanical systems are presented focusing on the observation phase.

1.5 Conventions

In this research the conventions for analysis are the following:

- Use the single failure assumption; one and only one component is assumed to be the cause of the system failure.
- Indications are binary events; the indication is either pass or fail.

2 Diagnosis of Failures in Mechanical Systems

The underlying goal of mechanical system diagnosis is to identify possible causes of failure, narrow down the possible causes of failure to one component, replace the particular component that causes failure, and return the system to normal operating condition. However, because of system architecture, indication uncertainty, time constraints, or cost constraints it is not always possible to isolate the cause of failure to one particular component. Once the fault is isolated to the fewest possible causes of failure, the maintenance technician must decide whether to replace a component or not.

In this research, we will focus on the observation phase associated with failure diagnosis. The *observation* phase involves noting failure indications and conducting maintenance tasks based on the observed indications. The indications can be in the form of lights and gages or observable abnormalities noticeable to the performance of the system (i.e. lower performance of engine, loud noise) [Henning 2000].

We are led to conclusions and possible causes of failure based on the observations. An example of this is the warning lights and gages located on the dashboards of modern automobiles. Operators can monitor the state of the vehicle and diagnose a problem without conducting diagnostic tests on the vehicle. A check engine light on a car infers a specific set of components that may cause the indication light to appear. All possible causes of failure in the system for each failure indication are defined as an ambiguity group [Simpson 1994].

Modern airplane systems have many sensors and Built-In Test Equipment (BITE) to locate and isolate system failures to a smaller subset of components in the system. Upon initial analysis of a Boeing air supply system it was determined that there is an average of one component failure mode per indication. In the fault diagnosis process of the Boeing system, the observation phase provides information needed to isolate the faults to only a few components with a high level of accuracy [Boeing 2000].

We will discuss the idea of justified and unjustified maintenance actions as it relates to diagnosis of failures in mechanical systems. The maintenance actions are presented for a simplified example when indications are perfect and for an example when there is some error associated with each indication. If a system indication infers *fail,* the maintenance technician may decide to replace or leave a component that could have caused the failure indication. Perfect indications infer *good* when all components mapped to the particular indication are *good* and infer *fail* when at least one component is *bad.* If the technician replaces the component that caused the indication to infer *fail*, it is defined as a *justified removal.* If the component that is replaced is *good*, and therefore did not cause system indication to infer *fail*, then it is an *unjustified removal. Unjustified removals*, for perfect indications, are a result of the ambiguity associated with each indication.

However, the assumption that indications are perfect is not realistic. The fact is that indications are not 100 percent perfect, resulting in indications that infer *fail* when all components mapped to the indication are *good.* Therefore, *unjustified removals* of *good* components can be attributed to both ambiguity for each indications and indication certainty. Indication error can result from a variety of sources, including human error, experience of the technician, faulty equipment, environmental abnormalities, and ambiguous readings [Bukowski 1993]. The method for computing and predicting the uncertainty of indications is beyond the scope of this research.

For example, if an imperfect indication infers *fail* the technician may decide to replace a component. However, since the indications are imperfect there is a chance that one component in the ambiguity group is *bad* or all components in the ambiguity group are *good.* Therefore, the probability of completing an unjustified removal is related to the ambiguity and the uncertainty of each indication. Most indications have a high degree of certainty. However, as small as the error may be, the probability of completing an *unjustified removal* increases with an increase in indication uncertainty.

Conversely, imperfect indications can infer *pass* when one component in the ambiguity group is *bad.* Misdiagnosis of this type results in leaving *bad* components in the system. If all system indications infer *pass*, the technician will probably decide not to replace any components. However, *unjustified leaves* result if no component is replaced, when in actuality a *bad* component is present in the system. Additionally, the normal operation of the system is when all indications infer *pass* and when all components in the system are actually *good. Justified leaves* correspond to normal system operation, and are defined as leaving good components in the system when indications infer pass. Therefore, *justified* and *unjustified leaves* of components are a result of indication certainty.

3 Constructing the Diagnostic Model

The first step in diagnostic analysis is to construct a diagnostic model of the system. The diagnostic model is constructed based on information extracted from the FMEA and FTA, component reliability analysis, indication certainty, and prior knowledge about the component-indication relationship. The methodology for constructing the diagnostic model based on the system information is shown in Figure 3.1.

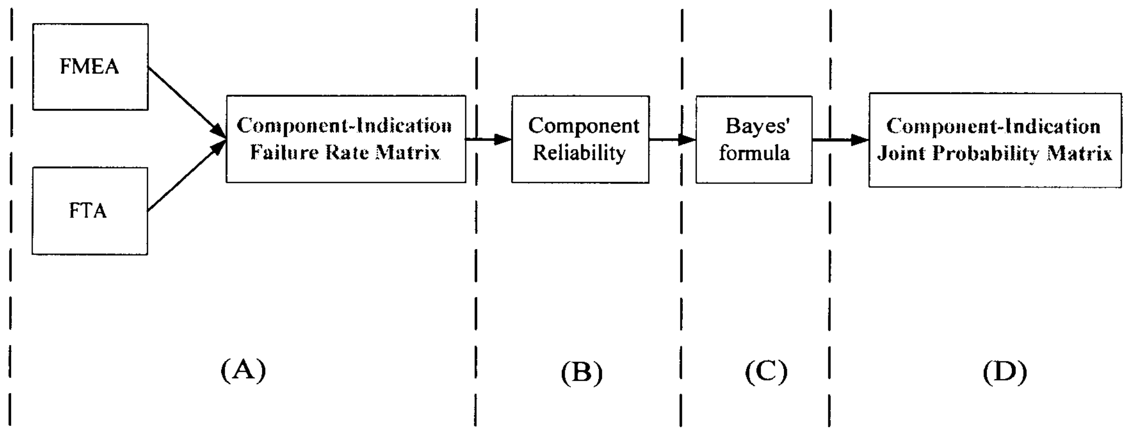


Figure 3.1. Procedure for constructing a diagnostic model.

The diagnostic model is constructed by first extracting failure rate and indication information from the FMEA and FTA (Figure 3.1A). The information is arranged in graphical and matrix form (see Figure 3.2 and Figure 3.3). The *Component-Indication Failure Rate Matrix* is constructed based on the information extracted from the FMEA and FTA. Next, the component reliability model and exposure times are used to compute the probability that each component is *good* or *bad* for each failure mode (Figure 3.1B). Finally, using Bayes' formula the joint probabilities of each of the mutually exclusive events are computed (Figure 3.1C). The diagnostic model, when presented in matrix form, is denoted as the *Component-Indication Joint Probability Matrix* (Figure 3.1D).

This section describes the use of the component reliability model, prior knowledge about component-indication relationships, Bayes' theory, and truth tables to incorporate indication uncertainty into the diagnostic model. To explain the method for constructing the diagnostic model, we will use a simple illustrative example. The illustrative example does not represent an actual system; the failure rates, exposure times, and component-indication relationships are hypothetical. The illustrative example is used throughout the construction of the diagnostic model, and again presented in the diagnostic analysis methodology and diagnosability metrics sections.

3.1 Extracting data from the FMEA and FTA

First, the diagnostic model is constructed utilizing information obtained from the failure modes and effects analysis (FMEA) and fault tree analysis (FTA). The FMEA contains the functions of the components, the failure modes and failure rates for each component, the effects of the failures, and the failure indications associated with each component failure. Additional information about component failures and failure indications is obtained from the FTA. The FTA focuses on particular failures and failure indication, whereas the FMEA focuses on specific components. The information extracted from the FMEA and the FTA is combined to embody all failure rates and indications associated with the system [Henning 2000].

Based on the relationship between failure rates and failure indications, the component-indication mapping is constructed. The system components are placed along the top of the figure, and failure indications to which they are mapped are placed along the bottom. The lines connecting the components to the indications represent the hypothetical rates of indication occurrences to component failures. The component-indication mapping is presented in graphical format (see Figure 3.2).

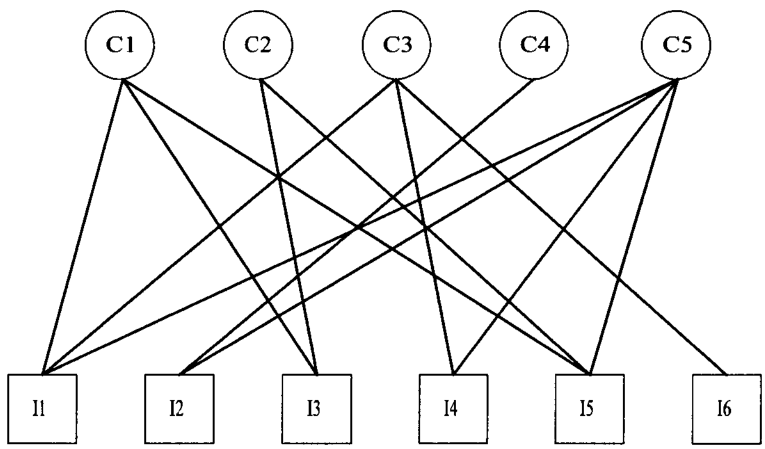


Figure 3.2. Construction of diagnostic model.

The component failure rate-indication mapping is reorganized into matrix format. The components are placed along the top of the matrix and the indications along the side of the matrix. The failure rates of the components are entered into the appropriated cells for each component (see Figure 3.3).

1.0×10^{-7}	**C1**	**C2**	**C3**	**C4**	**C5**
I1	2	0	4	0	3
I2	0	0	0	2	15
I3	3	2	0	0	0
I4	0	0	17	0	25
I5	10	12	0	0	3
I6	0	0	8	0	0

Figure 3.3. Component Indication failure rate matrix.

In the next section we will discuss the computation of component reliability based on the failure rates in Figure 3.3.

3.2 Component Reliability Computation

Next, a reliability prediction model is utilized in conjunction with the failure rates to determine the probability that each component is *good* and the probability that each component is *bad*. Reliability is defined as the probability that a system or component will perform properly for a specified period of time under a given set of operating conditions [Bentley 1993]. The reliability of a component gives rise to the important correlation of failure rate. A bathtub curve is used to describe the failure rates of components in the system. The failure rate is dependent on the time that the component is in use. The initial portion of the bathtub curve is referred to as *infant mortality*. The failure rates of the components in the infant mortality portion are caused by defective equipment and do not accurately represent the actual failure rate of the component. Large failure rates at the beginning of the component use can be minimized by a wearin period or strict quality control of the components. The middle section of the bathtub curve contains a nearly constant failure rate. This section is referred to as the *normal life* of the component. The failure rates in the normal life portion are generally caused by random failures. The right hand portion of the bathtub curve indicates an increasing failure rate. This period is referred to as the *end-of-life* period. The rapid increase in failure rates is used to determine the life of the component. The *end-of-life* failure period can be avoided by specifying the components expected life (see Figure 3.4).

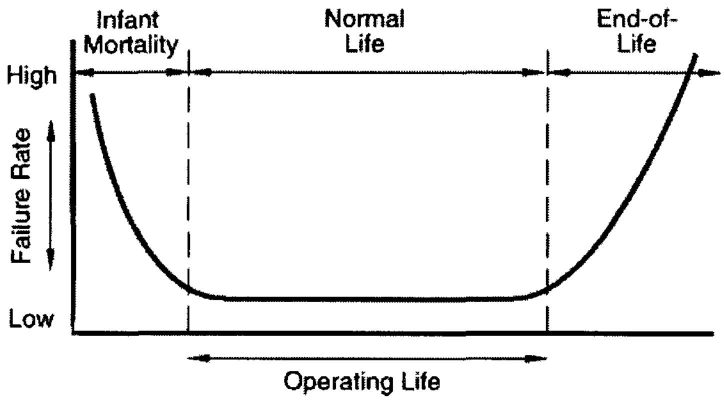
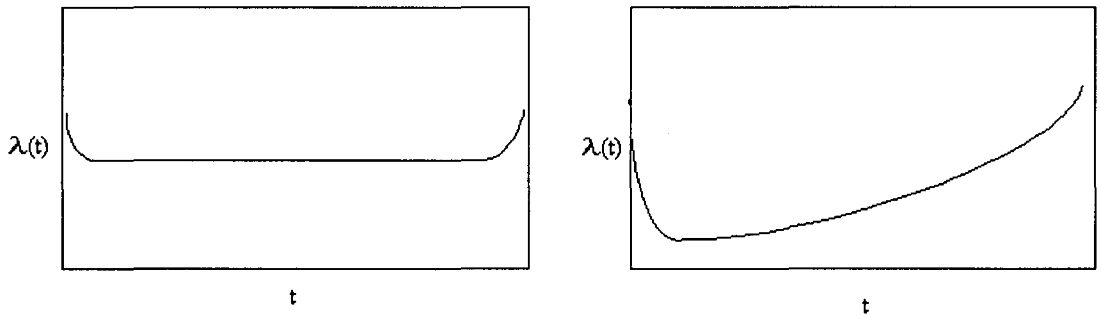


Figure 3.4. Bathtub reliability curve.

Figure 3.4 represents the general form of failure rates for many different types of components and systems. However, the failure rate curve is substantially different for electronic and mechanical equipment. Failure rate curves for electronic and mechanical equipment are presented in Figure 3.5.



(a) Electronic hardware (b) Mechanical equipment

Figure 3.5. Failure rates for different types of systems [Lewis 1996].

In this research we will assume a constant failure rate for mechanical components. A constant failure rate assumption is often used to describe the reliability of the component, with the *operating life* of the component the period of interest. The constant failure rate assumption is valid because infant mortality can be eliminated through strict quality control and a wearin period. In addition, if mechanical components are replaced as they fail, the failure rate of the components is approximately constant. Finally, the time domain of interest can be limited to the normal life period, so that it only envelops the constant failure rate portion of the operating life.

The constant failure rate model for continuously operating systems results in an exponential probability density function distribution. The derivation of the probability density function (PDF) and the cumulative density function (CDF) for a constant failure rate assumption are presented in [Lewis 1996]. Additionally, the component reliability is presented in equation 3.1.

$$R(t) = e^{-\lambda t} \qquad \textbf{(3.1)}$$

Where λ is failure rate and *t* is exposure time.

Plots of reliability and failure rates as functions of time are shown in figure (see Figure 3.6).

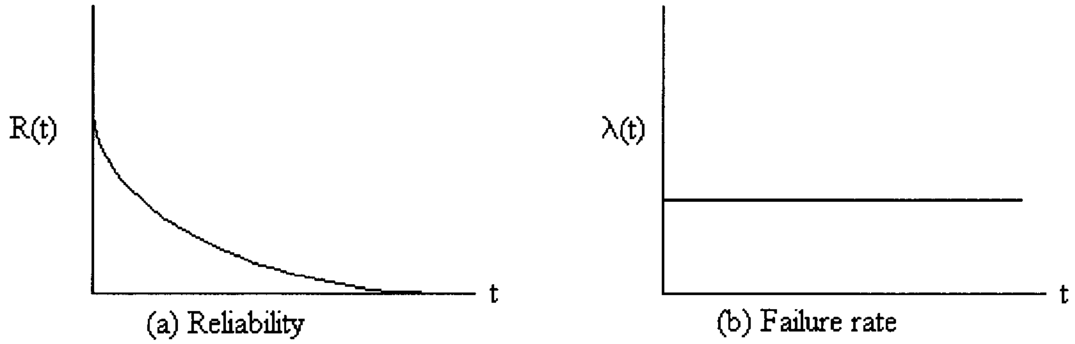


Figure 3.6. Exponential Distribution [Lewis 1996].

The reliability for every failure mode of each component is computed based on the failure rate extracted from the FMEA and FTA and the exposure time of each component. *Exposure time* is defined as the length of time the component has been in use. For example, if a component is operated continuously for the entire system life, the exposure time is the expected life of the system. If a component is operated intermittently over the life of the component, the exposure time is the total length of time the component is operated. For the illustrative example, hypothetical exposure times, for an expected life of 10,000 hours, are given in Table 3.1.

Table 3.1. Exposure times of illustrative example.

Component	Exposure time (hr)
C1	5000
C2	3700
C3	1750
C4	7200
C5	10000

The probabilities that each component is either *good* or *bad* are computed for the illustrative example based on the failure rates in Figure 3.3 and the exposure times from Table 3.1 (see Table 3.2).

Table 3.2. Reliability computation values.

Component-Indication	Exposure Time (hr)	$Pr(C_i$=good)	$Pr(C_i$ = bad)
C1, I1	5000	0.999	0.001
C1, I3	-	0.999	0.001
C1, I5	-	0.995	0.005
C2, I3	3700	0.999	0.001
C2, I5	-	0.996	0.004
C3, I1	1750	0.999	0.001
C3, I4	-	0.997	0.003
C3, I6	-	0.999	0.001
C4, I2	7200	0.999	0.001
C5, I1	10000	0.997	0.003
C5, I2	-	0.985	0.015
C5, I4	-	0.975	0.025
C5, I5	-	0.997	0.003

In the next section we will discuss how the component reliabilities are utilized in conjunction with Bayes formula and known indication certainties to compute the joint probabilities of all mutually exclusive events in the system and further develop the diagnostic model.

3.3 Incorporating Bayes' Formula into Diagnostic Analysis

Bayes' theorem is used to determine the truth of an event based on prior knowledge and current observation [D'Ambrosio 1999]. If an event becomes more or less likely to occur based on the occurrence of another event, then the first event is said to be a condition of the second event. The conditional probability of event A given that event B has occurred is written as $Pr(A|B)$. If events A and B are independent of each other, then the conditional probability is simply the same as the probability of the individual events, that is $Pr(B|A) = Pr(B)$.

Bayes' theorem is concerned with deducing the probability of B given A from the knowledge of $Pr(A)$, $Pr(B)$, and $Pr(A|B)$. $Pr(A)$ is called the prior probability. $Pr(A|B)$ is the posterior probability. Bayes' theorem is used in diagnostic modeling based on inference drawn from prior probabilities of component failure and conditional probabilities of component-indication relationships. Based on the current observation of system indications, the joint probabilities are computed.

Mechanical systems most often are composed of many components and indications and their associated interdependencies. The diagnostic model must incorporate each mutually exclusive event for all components and indications in mechanicals systems. For example, more than one component can be mapped to a particular indication. The joint probability of an exclusive event must take into account all relevant components and indications.

Four mutually exclusive events are developed based on the single failure assumptions during the fault diagnosis process. Any one component in the system can be *bad* while all other components are *good* or all components in the system can be *good.* Additionally, system indications can either infer *pass* or *fail* (see Table 3.3).

Table 3.3. Definition of events in the diagnostic truth table.

Event	Joint Occurrence
HIT	One Indication=fail, ONE Component=bad
False Alarm	One Indication=fail, ALL Component = good
Miss	All Indication=pass, ONE Component=bad
OK	All Indication=pass, ALL Component=good

In our system, the *HIT* event occurs when one component is *bad* and one indication infers *fail. False Alarm*s occur when one indication infers *fail* but all components are *good. Miss*'s occur when all indications infer *pass* but one component is *bad.* The *False Alarm* and the *Miss* events are referred to as Type I and Type II errors, and are undesirable in any diagnosis. Finally, *OK*'s occur when all indications infer *pass* and all components are *good* (see Figure 3.7).

<table>
<tr><th></th><th>C1=bad</th><th>C2=bad</th><th>C3=bad</th><th>C4=bad</th><th>C5=bad</th><th>C1=good</th><th>C2=good</th><th>C3=good</th><th>C4=good</th><th>C5=good</th></tr>
<tr><td>I1=fail</td><td colspan="5" rowspan="6">HIT
Pr (One Indication=fail, ONE Component=bad)</td><td colspan="5" rowspan="6">False Alarm
Pr (One Indication=fail, ALL Component = good)</td></tr>
<tr><td>I2=fail</td></tr>
<tr><td>I3=fail</td></tr>
<tr><td>I4=fail</td></tr>
<tr><td>I5=fail</td></tr>
<tr><td>I6=fail</td></tr>
<tr><td>I1=pass</td><td colspan="5" rowspan="6">Miss
Pr (All Indication=pass, ONE Component=bad)</td><td colspan="5" rowspan="6">OK
Pr (All Indication=pass, ALL Component=good)</td></tr>
<tr><td>I2=pass</td></tr>
<tr><td>I3=pass</td></tr>
<tr><td>I4=pass</td></tr>
<tr><td>I5=pass</td></tr>
<tr><td>I6=pass</td></tr>
</table>

Figure 3.7. Diagnostic truth table for fault diagnosis.

The truth table presented in Figure 3.7, is further simplified according to each event defined in Table 3.3. The False Alarm columns are combined together to symbolize the event that one indication infers *fail* and all components are *good.* Similarly, the Miss rows are combined together to symbolize the event that all indications infer *pass* and any component in the system is *bad.* The OK events are combined into one cell to symbolize the event that all indications infer *pass* and all components are *good* (see Figure 3.8).

<table>
<tr><th></th><th>C1=bad</th><th>C2=bad</th><th>C3=bad</th><th>C4=bad</th><th>C5=bad</th><th>All Components=good</th></tr>
<tr><td>I1=fail</td><td colspan="5" rowspan="6">HIT</td><td rowspan="6">False Alarm</td></tr>
<tr><td>I2=fail</td></tr>
<tr><td>I3=fail</td></tr>
<tr><td>I4=fail</td></tr>
<tr><td>I5=fail</td></tr>
<tr><td>I6=fail</td></tr>
<tr><td>All Indications=pass</td><td colspan="5">Miss</td><td>OK</td></tr>
</table>

Figure 3.8. Combined diagnostic truth table.

The equations used to compute the joint probabilities of all mutually exclusive events are derived from Bayes' formula. The general form of Bayes formula is presented for greater than two possible conditions (see Eq. 3.4).

$$\Pr(A \mid B, C, D\ldots) = \frac{\Pr(A, B, C, D\ldots)}{\Pr(B, C, D\ldots)} \tag{3.4}$$

Equation 3.4 is rearranged to compute the joint probability of an event based on prior and conditional probabilities (see Eq. 3.5).

$$\Pr(A, B, C, D\ldots) = \Pr(A \mid B, C, D\ldots) \times \Pr(B, C, D\ldots) \tag{3.5}$$

The joint probabilities of each event are computed based on *prior probabilities* and *posterior probabilities*. The prior probabilities for the diagnostic process are computed from the component reliability model (see section 3.2). The prior probabilities are the probability that the component is either *good* or *bad*. *Posterior probability* is also needed to compute the joint probabilities. The posterior probability is referred to as indication certainty. Indication certainty is the probability that the indications will infer *fail* when one component mapped to it is *bad* or the probability that the indication will infer *pass* when all components mapped to it are *good* (see Table 3.4).

Table 3.4. Indication certainty, Posterior Probability.

Pr(Indication =*fail*| One Component=*bad*)
Pr(Indication =*fail*| All Components=*good*)

Indication certainty must be known to compute the joint probability of events in the diagnostic process to ultimately construct the diagnostic model. However, during the conceptual stages of design, these values may not always be known. The uncertainty of the indications can be estimated for conceptual designs based on similar systems or can be approximated based prior design experience. As more knowledge is gained about the system, the indication uncertainty values can be refined.

The equations used for computing the joint probabilities of all mutually exclusive events in the system are presented. The nomenclature presented in Table 3.5 is used in the joint probability equations.

Table 3.5. Nomenclature used in joint probability equations.

Nomenclature	Definition
B	Bad
C	Component
F	Fail
G	Good
I	Indication
i	*i*th Component
j	*j*th Indication
P	Pass

HIT Joint Probability:

The HIT joint probability is computed for all component-indication events. Each time a component is *bad* and an indication infers *fail* is a mutually exclusive event for all indications and components. The joint probability of each of these mutually exclusive events cannot be combined. Equation 3.6 computes the HIT joint probabilities.

$$\Pr(I_j = F, C_l = B, \cdots, C_i = G) = \Pr(I_j = F \mid C_l = B, \cdots, C_i = G) \times \Pr(C_l = B, \cdots, C_i = G) \qquad \textbf{(3.6)}$$

The $\Pr(C_l{=}B,\ldots, C_i{=}G)$ is the probability of independent events occurring at the same time, and can therefore be modified into the product of the probabilities of each event occurring. The joint probability for each hit event is computed using the appropriate component reliability data. For example, only those components that are mapped to the indication are used in the computation of the joint probability.

$$\Pr(I_j = F, C_l = B, \cdots, C_i = G) = \Pr(I_j = F \mid \text{One}\,C = B) \times \Pr(C_l = B) \times \cdots \times \Pr(C_i = G) \qquad \textbf{(3.7)}$$

False Alarm Joint Probability:

The False Alarm joint probability is computed for each system indication separately. For example, in the illustrative example problem, six false alarm joint probabilities are computed corresponding to the six independent system indications. The False Alarm assumes every component mapped to a single indication is *good.* Equation 3.8 computes the False Alarm joint probabilities for all indications.

$$\Pr(I_j = F, C_1 = G, \cdots, C_i = G) = \Pr(I_j = F \mid C_1 = G, \cdots, C_i = G) \times \Pr(C_1 = G, \cdots, C_i = G) \quad \textbf{(3.8)}$$

The conditional probabilities in equation 3.8 are replaced with the known indication uncertainties to yield equation 3.9.

$$\Pr(I_j = F, C_1 = G, \cdots, C_i = G) = \Pr(I_j = F \mid \text{All C's} = G) \times \Pr(C_1 = G) \times \cdots \times \Pr(C_i = G) \quad \textbf{(3.9)}$$

Miss Joint Probability:

The Miss joint probability is computed for each component in the system. The Miss event occurs when one component is *bad* and all indications mapped to the component infer *pass*. The Miss joint probability is computed assuming that only one component has failed in any of the failure modes and that all indications mapped to the component, regardless of failure mode infer pass. In the illustrative example, five Miss joint probability values are computed, corresponding to the five components in the system. Equation 3.10 computes the Miss joint probability values.

$$\begin{aligned} \Pr(I_1 = P, \cdots, I_j = P, C_1 = B) = \Pr(I_1 = P \mid C_{11} = B) \times \Pr(C_{11} = B) \ldots \text{OR} \\ \cdots \Pr(I_j = P \mid C_{1j} = B) \times \Pr(C_{1j} = B) \end{aligned} \quad \textbf{(3.10)}$$

Since the indications are collectively exhaustive, the probabilities in Eq. 3.10 can be summed for each component:

$$\Pr(I_1 = P, \cdots, I_j = P, C_1 = B) = \Pr(I_1 = P \mid C_{11} = B) \times \Pr(C_{11} = B) \ldots + \\ \ldots \Pr(I_j = P \mid C_{1j} = B) \times \Pr(C_{1j} = B) \tag{3.11}$$

The certainties for all indications in the system are substituted into Eq. 3.11 to yield Eq. 3.12.

$$\Pr(I_1 = P, \cdots, I_j = P, C_1 = B) = \Pr(I_1 = P \mid \text{One}\, C = B) \times \Pr(C_{11} = B) \ldots + \\ \ldots \Pr(I_j = P \mid \text{One}\, C = B) \times \Pr(C_{1j} = B) \tag{3.12}$$

<u>OK Joint Probability:</u>

The OK joint probability is computed based on the previously computed joint probabilities. The total probability of all mutually exclusive events must sum to 1.0 to represent a collectively exhaustive system analysis. The joint probability of the OK event is computed by subtracting the total sum of the HIT, False Alarm, and Miss probabilities from unity. The OK event assumes all components are *good* and all indications infer *pass,* thereby resulting in a single value for the system. Equation 3.13 computes the OK joint probability for the system.

$$\Pr(\text{All I's} = P, \text{All C's} = G) = 1.0 - \sum_{i,j=1}^{n,m} [\text{HIT } C_i, I_j] - \sum_{j=1}^{m} [\text{False Alarm } I_j] - \sum_{i=1}^{n} [\text{Miss } C_i] \tag{3.13}$$

Equations 3.7, 3.9, 3.12, and 3.13 are used to compute the joint probability of all mutually exclusive events associated with mechanical fault diagnosis. The equations are used in conjunction with the component reliability and indication uncertainty (see Table 3.2 and Table 3.6).

Table 3.6. Indication uncertainty for illustrative example.

Pr (I1=fail I Any one Component = fail)	99.99%
Pr (I1=fail I All Component = good)	0.01%
Pr (I2=fail I Any one Component = fail)	99.99%
Pr (I2=fail I All Component = good)	0.01%
Pr (I3=fail I Any one Component = fail)	99.99%
Pr (I3=fail I All Component = good)	0.01%
Pr (I4=fail I Any one Component = fail)	99.99%
Pr (I4=fail I All Component = good)	0.01%
Pr (I5=fail I Any one Component = fail)	99.99%
Pr (I5=fail I All Component = good)	0.01%
Pr (I6=fail I Any one Component = fail)	99.99%
Pr (I6=fail I All Component = good)	0.01%

3.4 Formation of Component-Indication Joint Probability Matrix, PR

The *Component-Indication Joint Probability Matrix*, denoted by **PR**, is composed of the joint probabilities for all events in the system. Based on the data and equations presented in the previous section, the joint probabilities are computed are arranged in matrix form. The cells in the *Component-Indication Joint Probability Matrix* that have a value of zero indicate that the particular indication is not directly related to the state of the corresponding component. For example, the failure of component one (C1) is not mapped directly to indication two (I2). Therefore the probability that C1 is *bad* and I2 infers *fail* is negligible or never occurs. Additionally, the probabilities of the indications are computed by summing each of the rows in the matrix. The probabilities of the components are computed by summing each of the columns in the matrix (see Figure 3.9).

	C1	C2	C3	C4	C5	All Good	Indication Prob
I1	0.000996	0.000000	0.000697	0.000000	0.002990	0.000100	0.0048
I2	0.000000	0.000000	0.000000	0.001417	0.014865	0.000098	0.0164
I3	0.001498	0.000739	0.000000	0.000000	0.000000	0.000100	0.0023
I4	0.000000	0.000000	0.002897	0.000000	0.024614	0.000097	0.0276
I5	0.004950	0.004394	0.000000	0.000000	0.002967	0.000099	0.0124
I6	0.000000	0.000000	0.001399	0.000000	0.000000	0.000100	0.0015
All Pass	0.000001	0.000001	0.000001	0.000000	0.000005	0.934977	0.9350
Comp Prob	0.0074	0.0051	0.0050	0.0014	0.0454	0.9356	

Figure 3.9. Component-Indication Joint Probability Matrix.

In the next section, we will discuss how the *Component-Indication Joint Probability Matrix* is utilized to complete diagnostic analysis.

4 Diagnosability Analysis

In order to complete diagnostic analysis, as illustrated in Figure 1.1, two additional matrices are formed based on the Component-Indication Joint Probability Matrix. First, the Replacement Matrix is constructed by applying replacement criterion to the Component-Indication Joint Probability Matrix. Next, the Replacement Probability Matrix is computed by multiplying the transpose of the Replacement Matrix by the Component-Indication Joint Probability Matrix. Finally, diagnosability metrics are extracted from the Replacement Probability Matrix.

The hypothetical example problem is again utilized to illustrate and verify the diagnostic analysis methodologies. An indication certainty of 99.99 percent is used for the analysis.

4.1 Replacement Matrix, R

The replacement matrix, denoted by **R**, is a binary matrix. The replacement criterion determines which component is replaced for each indication in the system. The replacement criterion is determined before the diagnostic analysis begins. The criterion could be component cost, replacement time, probability of occurrence, or a combination of these factors. For the illustrative example, the chosen replacement criterion is probability of occurrence.

To form the replacement matrix, each row (indication) of the *Component-Indication Joint Probability Matrix* is examined individually. For the illustrative example, a one is entered in the cell of the component with the largest probability of occurrence for each indication. Zeroes are entered into the remaining cells of each row. This process is repeated for all indications. Figure 4.1 is the replacement matrix for the illustration example.

	C1	**C2**	**C3**	**C4**	**C5**	**All Good**
I1	0	0	0	0	1	0
I2	0	0	0	0	1	0
I3	1	0	0	0	0	0
I4	0	0	0	0	1	0
I5	1	0	0	0	0	0
I6	0	0	1	0	0	0
All Pass	0	0	0	0	0	1

Figure 4.1. Replacement Matrix, R.

The newly formed Replacement Matrix is used in conjunction with the Component-Indication Joint Probability Matrix in the next section to construct the Replacement Probability Matrix.

4.2 Computation of the Replacement Probability Matrix, $\mathbf{R_{PR}}$

The Replacement Probability Matrix, denoted by $\mathbf{R_{PR}}$, is computed by multiplying the transpose of the Replacement Matrix by the Component-Indication Joint Probability Matrix (see Eq. 4.1).

$$R_{PR} = [R]^T \cdot [PR] \qquad \textbf{(4.1)}$$

The Replacement Probability Matrix for the illustrative example is presented in Figure 4.2.

Replaced ↓ / Failed →	C1	C2	C3	C4	C5	All Good	
C1	**0.00645**	0.00513	0.00000	0.00000	0.00297	0.00020	
C2	0.00000	**0.00000**	0.00000	0.00000	0.00000	0.00000	
C3	0.00000	0.00000	**0.00140**	0.00000	0.00000	0.00010	
C4	0.00000	0.00000	0.00000	**0.00000**	0.00000	0.00000	
C5	0.00100	0.00000	0.00359	0.00142	**0.04247**	0.00030	
None replaced	0.00000	0.00000	0.00000	0.00000	0.00000	**0.93498**	
Pr (Just removal)	0.00645	0.00000	0.00140	0.00000	0.04247		**0.05032**
Pr(Unjust removal)	0.00100	0.00513	0.00359	0.00142	0.00297	0.00059	**0.01470**
Pr(Just leave)						0.93498	**0.93498**
Pr(Unjust leave)	0.00000	0.00000	0.00000	0.00000	0.00000		**0.00001**
Pr(Just Action)	0.00645	0.00000	0.00140	0.00000	0.04247	0.93498	**0.98529**

Figure 4.2. Replacement Probability Matrix, R_{PR}.

The Replacement Probability Matrix is a square matrix. The columns represent the actual condition of each component in the system and the rows represent the action completed on each component in the system. An action is defined as either *replacing* or *leaving* a component in the system. The values along the diagonal represent the *justified action* probabilities. The values in the off-diagonals represent the *unjustified action* probabilities. For example, the justified probability that all components are *good* and none are replaced is 0.93498.

The diagnosability metrics are computed based on the unjustified and justified probabilities extracted from the Replacement Probability Matrix. The metrics are developed and discussed in the next section.

4.3 Distinguishability Metrics

Distinguishability (D) is the metric that measures the efficiency of fault isolation after completion of the observation phase. As presented in Henning [2000], distinguishability is defined as the probability of correctly replacing a bad component given an indication infers *fail.* In this research the definition of distinguishability is expanded to include all possible courses of action during the diagnostic process. It is possible for components to either be replaced or left in the system during the fault diagnosis process. As previously defined, a justified action is replacing those components that are bad and leaving those components that are good in the system. As the distinguishability of the system increases, the probability of completing a justified action is maximized. By maximizing the chance of completing justified actions, and thereby minimizing the completion of unjustified actions during the diagnostic process, cost and time are minimized. The distinguishability metric is presented in several forms. Distinguishability metrics are computed to the system, indication, and component level (D_{SYS}, D_{IND}, D_{LRU}). Additionally, the system level distinguishability value comes in many forms. System distinguishability is computed for all actions and for replacements completed during the diagnostic process. Table 4.1 presents the distinguishability metrics definitions.

Table 4.1. Definitions of distinguishability metrics.

Metric	Probability of:
$D_{IND,j}$	Justified removal, given *jth* failure indication
$D_{LRU,i}$	Justified removal, given *ith* component failed
D_{SYS}	Justified removal, given *some* failure indication (or some component failed). Computed as: $\sum_{i=1}^{n} \Pr(\text{Just.removal} C_i)$ or $\sum_{j=1}^{m} \Pr(\text{Just removal} I_j)$ The metric value is just for the replaced components
$D_{SYS,\,TOTAL}$	Computed as: $\sum_{i=1}^{n} \Pr(\text{Just.removal} C_i) + \Pr(\text{Just.leave} C_i)$ or $\sum_{j=1}^{m} \Pr(\text{Just.removal} I_j) + \Pr(\text{Just.leave} I_j)$ Computed for both justified removals and justified "leaves"
$D_{SYS,\,JUST\,REMOVAL}$	Computed as: $\dfrac{\sum_{i=1}^{n} \Pr(\text{Just.Removal} C_i)}{\sum_{i=1}^{n} \Pr(\text{Just.Removal} C_i) + \sum_{i=1}^{n} \Pr(\text{Unjust.Removal} C_i)}$

The system distinguishability [D_{SYS}], defined as probability of completing justified removals, is computed by summing the probability of completing a justified removal for all components in the system. The total distinguishability of the system [$D_{SYS,\,TOTAL}$], defined as probability of completing all justified actions during the diagnostic process, is computed by summing the probability of all justified actions from the Replacement Probability Matrix. The distinguishability of the system normalized for justified removals [$D_{SYS,\,JUST\,REMOVAL}$] is computed for justified removals of system components (see Figure 4.2).

In addition to diagnostic analysis of entire systems, it is important to isolate problems associated with specific components or indications in the architecture of the system. In order to locate and alleviate diagnosability problems with the overall mechanical system, the system must be analyzed to an indication and/or component level. The component distinguishability is extracted from each column in the Replacement Probability Matrix. For example, the probability of completing a justified removal of component one (C1) is 0.00645.

The indication distinguishability is computed by multiplying the *Component-Indication Joint Probability* [PR] by the *Replacement Matrix* [R]. The indication distinguishability [D_{IND}] is extracted from each row of the matrix (see Figure 4.3).

$$\begin{array}{r} \text{I1} \\ \text{I2} \\ \text{I3} \\ \text{I4} \\ \text{I5} \\ \text{I6} \\ \text{All Good} \end{array} \begin{bmatrix} 0.000996 & 0.0 & 0.000697 & 0.0 & 0.002990 & 0.000100 \\ 0.0 & 0.0 & 0.0 & 0.001417 & 0.014865 & 0.000098 \\ 0.001498 & 0.000739 & 0.0 & 0.0 & 0.0 & 0.000100 \\ 0.0 & 0.0 & 0.002897 & 0.0 & 0.024614 & 0.000097 \\ 0.004950 & 0.004394 & 0.0 & 0.0 & 0.002967 & 0.000099 \\ 0.0 & 0.0 & 0.001399 & 0.0 & 0.0 & 0.000100 \\ 0.000001 & 0.000001 & 0.000001 & 0.0 & 0.000005 & 0.934977 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0.00299 \\ 0.01487 \\ 0.00150 \\ 0.02461 \\ 0.00495 \\ 0.00140 \\ 0.93498 \end{bmatrix}$$

Figure 4.3. Computation of indication distinguishability metrics.

In the next section, the diagnosability analysis is completed for varied indication certainty and for hypothetical design changes of the system architecture of the illustration example.

5 Results

The distinguishability analysis results for the illustrative example problem are presented. The distinguishability of the system, $D_{SYS,\ JUST\ REMOVAL}$, decreases from 0.781 when the indications are perfect (100% certain), to a minimum value of 0.6212 when the all indications are 99 percent certain. Additionally, the probability of completing a justified action after the observation phase, $D_{SYS,TOTAL}$, decreases from 0.98589 for perfect indications to 0.95509 for indications that have a certainty of 99 percent (see Table 5.1).

Table 5.1. Distinguishability analysis for various indication certainties.

Pr (I=fail I One C=fail)	Pr (I=fail I All C=good)	$D_{SYS,\ TOTAL}$	$D_{SYS,\ JUST\ REMOVAL}$
100.00%	0.00%	0.98589	0.78103
99.999%	0.001%	0.98583	0.78031
99.99%	0.01%	0.98529	0.77390
99.00%	1.00%	0.95509	0.62123

The component distinguishability [D_{LRU}] values are summarized in Table 5.2.

Table 5.2. Component distinguishability for illustrative example.

Component	D_{LRU}
C1	0.00645
C2	0.00000
C3	0.00140
C4	0.00000
C5	0.04247
All Good	0.93498

The indication distinguishability [D_{IND}] values are summarized in Table 5.3.

Table 5.3. Indication Distinguishability metrics.

Indication	D_{IND}
I1	0.00299
I2	0.01487
I3	0.00150
I4	0.02461
I5	0.00495
I6	0.00140
All pass	0.93498

In addition to completing diagnostic analysis on the illustrative example for varied indication certainties, hypothetical design changes were implemented to analyze how distinguishability is affected for changes in system architecture. The illustrative system is modified into three hypothetical alternative designs and diagnostic analysis is completed. The first alternative system, maps all component failure rates to one indication. The second alternative system maps the failure rates of all components to separate indications, resulting in 13 indications. Finally, the third alternative design uses the same number of indications, as in the original system. However, the component-indication mapping is altered (see Table 5.4).

Table 5.4. Alternative designs of illustrative example.

Alternative Designs	Description
-	Original system, illustrative example system
1	All component failures mapped to one indication
2	All component failures mapped to different indications, 13 indications
3	System is modified from System 1, 6 failure indications

The distinguishability results of the original illustrative example and the three alternative designs are summarized in Table 5.5. A uniform indication uncertainty of 99.99 percent is assumed. The worksheets for completing the diagnostic analysis are included in Appendix A.

Table 5.5. Distinguishability results for alternative designs.

Alternative Design #	Pr (I=fail | C = bad)	Pr (I=fail | C = good)	$D_{SYS,\ JUST\ REMOVAL}$	$D_{SYS,\ TOTAL}$
-	99.99%	0.01%	0.98529	0.77390
1	99.99%	0.01%	0.98138	0.70869
2	99.99%	0.01%	0.99870	0.98041
3	99.99%	0.01%	0.99059	0.85581

The architecture of the system clearly affects the distinguishability of the system. For example, the maximum distinguishability ($D_{SYS,\ JUST\ REMOVALS}$) results when each component failure is mapped to a separate indication. Conversely, the minimum distinguishability results when all component failures are mapped to one indication.

System three uses the same number of indications as in the original system. However, the component failures are mapped to different indications, essentially reducing the average ambiguity group size for each indication. A decrease in the average ambiguity group size results in an increase in system distinguishability (see Table 5.6).

Table 5.6. Average size of ambiguity group for hypothetical design alternatives.

Alternative Design #	Average size of ambiguity group
-	2.16
1	5
2	1
3	1.83

The diagnostic analysis is applied to an icemaker validation system in the next section.

6 Validation Example: Icemaker

A common home icemaker is used for validation of the diagnostic modeling methods and distinguishability metrics. The icemaker example was originally used by [Eubanks 1997] to illustrate an advance FMEA method for use during conceptual design. This same example was used by [Henning 2000] for development of diagnostic analysis methodologies. The icemaker provides an example of a physically embodied system of moderate complexity.

6.1 Icemaker Diagnostic Model

The information needed to complete the diagnostic model of the icemaker example is presented. Indication certainty and exposure times for each component are estimated for constructing the diagnostic model. Additionally, the indications are assumed to have a uniform certainty of 99 percent (see Table 6.1).

Table 6.1. Icemaker indication certainty.

Pr (Any indication=fail I Any one Component = fail)	99%
Pr (Any Indication=fail I All Components = good)	1%

Examples of the exposure times for icemaker components are given in Table 6.2.

Table 6.2. Component exposure times.

Expected life of icemaker	15 years	
Icemaker cycles/day	3	
Component	**Exposure Time (hrs)**	**Exposure Time Assumptions**
C1: Feeler arm	5475	(20 min/cycle)
C2: Switch Linkage	2737.5	(10 min/cycle)
C3: Switch	2737.5	(10 min/cycle)
C4: Mold	32850	(2 hours/cycle
C5: Freezer	131400	(Life of freezer)
C6: Water Delivery	4106.25	(15 min/cycle)
C7: Mold Heater	1095	(4 min/cycle)
C8: Ice Harvester	547.5	(2 min/cycle)
C9: Ice Timer	32850	(25% of life of refrigerator)
E: External Factor	657	(Intermittent, happen .5% over lifetime)

Failure indications for the icemaker example originally derived in [Henning 2000] are given in Table 6.4.

Table 6.3. Failure indications [Henning 2000].

i1	No ice in the bucket
i2	Ice overflowing
i3	Low ice level in the bucket
i4	Ice layer in bucket and/or fused ice cubes
i5	No water in the mold (not observable)
i6	Small or irregular ice cubes
i7	Ice stuck in the mold (not observable)
i8	Icemaker not running
i9	Feeler arm in the bucket
i10	Large or partially liquid ice cubes

Indication sets are formed from the individual indications. The indication sets are used to develop the component-indication mapping (see Table 6.4).

Table 6.4. Indication sets [Henning 2000].

I1	No ice + ice layer	(i1 + i4)
I2	No ice	(i1)
I3	Ice overflow	(i2)
I4	Low ice level	(i3)
I5	Small ice size + ice layer	(i6 + i4)
I6	No ice + feeler arm in bucket	(i1 + i9)
I7	Small ice size	(i6)

The relationship between components and indication in the icemaker system are shown in Table 6.5.

Table 6.5. Component-indication set relationships [Henning 2000].

Component	Indication Sets
C1: Feeler Arm	I2 I6
C2: Switch Linkage	I2 I3 I4
C3: Switch	I2 I3
C4: Mold	I1 I5
C5: Freezer	I1 I2
C6: Water Delivery	I2 I5
C7: Mold Heater	I1 I2
C8: Ice Harvest	I1 I2
C9: Ice Timer	I2 I5
E: External Factor	I5 I7

Using Table 6.1, Table 6.2, Table 6.3, Table 6.4, Table 6.5, and the FMEA, a diagnostic model for the icemaker is constructed (see Figure 6.1).

	C1	C2	C3	C4	C5	C6	C7	C8	C9	E	All Good
I1	0.000	0.000	0.000	0.003	0.120	0.000	0.007	0.001	0.000	0.000	0.009
I2	0.000	0.014	0.009	0.000	0.191	0.007	0.001	0.000	0.089	0.000	0.006
I3	0.000	0.029	0.013	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.010
I4	0.000	0.019	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.010
I5	0.000	0.000	0.000	0.024	0.000	0.017	0.000	0.000	0.045	0.002	0.009
I6	0.001	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.010
I7	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.010	0.010
All Pass	0.000	0.001	0.000	0.000	0.004	0.000	0.000	0.000	0.002	0.000	0.327

Figure 6.1. Icemaker Component-Indication Joint Probability Matrix.

In the next section we will complete the diagnosability analysis based on the model constructed of the icemaker system.

6.2 Icemaker Diagnostic Analysis

Table 6.6 summarizes the distinguishability values of the icemaker. The worksheets for calculating the icemaker distinguishability metrics are presented in Appendix D.

Table 6.6. Icemaker diagnosability analysis for imperfect indications.

Pr (I=fail | One C=fail)	Pr (I=fail | All C=good)	$D_{SYS, TOTAL}$	$D_{SYS, JUST REMOVAL}$
100.00 %	0.00 %	0.8109	0.6893
99.999 %	0.001 %	0.8108	0.6892
99.99 %	0.01 %	0.8102	0.6886
99.00 %	1.00 %	0.7514	0.6368

The distinguishability of the icemaker system decreases as indication uncertainty is increased. For example, the probability of correctly replacing a bad component in the system decreases from a probability of 0.6893 for perfect indication to 0.6368 for indications that are 99 percent certain.

Table 6.7 and Table 6.9 summarize the distinguishability results for individual indications and components in the icemaker system. Component and indication results are computed based on 99 percent indication certainty.

Table 6.7. Icemaker indication distinguishability.

Indication	D_{IND} Pr (Just)	Pr (Unjust)
I1	0.1204	0.0190
I2	0.1910	0.1271
I3	0.0290	0.0226
I4	0.0188	0.0098
I5	0.0454	0.0521
I6	0.0100	0.0011
I7	0.0099	0.0097
All pass	0.3269	0.0071

Indication two (I2), indication three (I3), and indication seven (I7) contain values of unjustified removals close to the probability of completing a justified removal. For Indication five (I5), the probability of completing an unjustified removal is greater than completing a justified removal. In order to increase the distinguishability of the system, these indications should be examined. Upon further investigation of the Component-Indication mapping it is determined the indications with large ambiguity groups are the main areas of concern with distinguishability of the system (see Table

6.8). For example, indication two (I2) has an ambiguity group of eight components and a high probability of completing an unjustified removal.

Table 6.8. Number of components in ambiguity group.

Indication	No. of components in ambiguity group
I1	4
I2	8
I3	2
I4	1
I5	4
I6	1
I7	1

In order to improve the distinguishability of the system, the architecture should be changed to decrease the size of the ambiguity groups for each indication. This can be achieved by either increasing the number of indications in the system or by altering the component-indication mapping of the current system.

The distinguishability results of icemaker components enable specific diagnostic problems to be located (see Table 6.9).

Table 6.9. Icemaker component distinguishability.

Component	D_{LRU} Pr (Just removal)	Pr (Unjust removal)	Pr (Unjust leave)
C1: Feeler Arm	0.0000	0.0000	0.0436
C2: Switch Linkage	0.0478	0.0141	0.0007
C3: Switch	0.0000	0.0218	0.0003
C4: Mold	0.0000	0.0268	0.0003
C5: Freezer	0.3114	0.0000	0.0035
C6: Water Delivery	0.0000	0.0233	0.0003
C7: Mold Heater	0.0000	0.0080	0.0001
C8: Ice harvesting	0.0000	0.0013	0.0000
C9: Ice timer	0.0454	0.0892	0.0017
E: External factors	0.0000	0.0024	0.0098

The probability of completing an unjustified removal can be significantly increased based on problems associated with only a few components in the system. Conversely, if these problems are alleviated, the system distinguishability can be greatly improved. For example, component three (C3), component four (C4) and component six (C6) are subject to a relatively high probability of unjustified removals. Additionally, component nine (C9) has the greatest chance of being removed unjustly. To increase the distinguishability of the system, the problems with these specific components should be addressed. To alleviate the diagnostic problems, the exposure time of the components can be reduced, the reliability of the components can be increased, or the architecture of the system can be altered.

7 Summary and Conclusions

The objective in this research was to create a diagnostic model that incorporated uncertainty caused from imperfect indications. Bayes' formula is used to construct an accurate diagnostic model of a physically embodied system based on information extracted from the FMEA, FTA, component reliability, and known indication uncertainty.

A new method for computing the diagnosability of systems is presented. The method uses a series of matrices that are mathematically manipulated to form the Replacement Probability Matrix. This matrix represents the joint probabilities of mutually exclusive diagnostic events. The distinguishability metrics are extracted from the Replacement Probability Matrix. Distinguishability metrics are developed for analysis to the system, component, and indication levels. The methodologies have been applied to an illustrative example problem and the icemaker system initially described in Eubanks [1997]. The methodology can be used to analyze systems at the conceptual stages of design or to improve systems already in use. Areas of concern in the architecture of the system can be identified and addressed to eliminate problems with fault isolation that may be encountered. The metrics have a mathematical foundation and produce an objective evaluation, thereby minimizing subjective analysis of conceptual designs.

Additionally, the methodologies are evolutionary. During the initial stages of design, concise and comprehensive information may not be readily available to completely analyze the system. However, as the design evolves and abstractness is reduced, the diagnostic analysis is based on more refined information, thereby resulting in greater accuracy.

Diagnostic analysis results of the illustrative example and the icemaker show that an increase in indication uncertainty has a detrimental effect on the completion of justified actions during the diagnostic process. As indication uncertainty is increased, the probability of completing an *unjustified removal* or *unjustified leave* also increases. In addition, the architecture of the system also affects the system diagnosability. As the architecture of the system is altered to decrease the average size of the ambiguity group, the diagnosability of the system increases.

8 Future Work

There is opportunity for future work in several areas. Utility theory and Bayesian networks should be utilized to further research the optimal replacement criterion to maximize the knowledge gained about the state of the components in the system and minimize the costs associated with the fault diagnosis. In addition to the observation phase, an additional phase of the diagnostic process involving the completion of diagnostic tests must be further researched. Diagnostic testing provides additional knowledge about the state of the components in the system, and thereby increases the probability of replacing a component that has caused the failure indication to occur. Similar methodologies and metrics related to the test phase should be further researched and developed. With the inclusion of the diagnostic testing phases, utility theory and Bayesian networks should be utilized to predict the optimal testing order of components. The allocation of maintenance time is another area of research in the diagnosis of mechanical systems that should be studied. Decision networks and utility theory should be applied to allocate maintenance time between the diagnostic testing tasks, component access tasks, and component replace/repair tasks.

Additionally, the use of the methodologies, not only as a design prediction tool, but also as a maintenance and service tool that can aid technicians during fault isolation procedures should be explored. Finally, the long-term goal is the creation of a computer program for diagnostic analysis using the developed methodologies as the underlying mathematics.

References

Bentley, John P., 1993, *An Introduction to Reliability & Quality Engineering*, New York: John Wiley & Sons Inc.

Boeing Company, 2000, Air Supply Control System, *System Description and Safety Analysis*, D926T0271

Bralla, James G, 1996, *Design For Excellence*, New York: McGraw-Hill, Inc.

Breese, J.S., and David Heckerman, 1996, Topics in Decision-Theoretic Troubleshooting: Repair and Experiment. Technical Report MSR-TR-96-06, Microsoft Research.

Bukowski, R.W., and B.A. Kelley, 1993, "A Bayesian Approach to Confidence in System Testing," *IEEE Autotestcon*, pp. 481-487.

Clark, G.E., Paasch, R.K., 1996, "Diagnostic Modeling and Diagnosability Evaluation of Mechanical Systems, " *Journal of Mechanical Design*, Vol. 118, No. 3, pp. 425-431.

D'Ambrosio, Bruce, 1999, "Inference in Bayesian Networks," AI Magazine, Summer 1999, pp. 21-36.

Eubanks, Charles F., Steven Kmenta, and Kosuke Ishii, 1996, "System Behavior Modeling as a Basis for Advanced Failure Modes and Effects Analysis," *Proceedings of the 1996 ASME Computers in Engineering Conference.*

Eubanks, Charles F., Steven Kmenta, and Kosuke Ishii, 1997, "Advanced Failure Modes and Effects Analysis Using Behavior Modeling," *Proceedings of the 1997 ASME Design Theory and Methodology Conference.*

Fitzpatrick, M., Paasch, R., 1999, "Analytical Method for the Prediction of Reliability and Maintainability Based Life-Cycle Labor Costs," *Journal of Mechanical Design*, Vol. 121, No. 4, pp. 606-613.

Gershenson, J., and Kosuke Ishii, 1991, "Life-Cycle Serviceability Design," *Design Theory and Methodology*, Vol. 31, pp. 127-134.

Henning, S., and R. Paasch, 2000, "Diagnostic Analysis for Mechanical Systems," *Proceedings of the 2000 ASME Design Theory and Methodology Conference.*

Kmenta, Steven and Kosuke Ishii, 1998, "Advanced FMEA Using Meta Behavior Modeling for Concurrent Design of Products and Controls," *Proceedings of the 1998 ASME Design Engineering Technical Conferences.*

Lewis, E.E., 1996, *Introduction to Reliability Engineering*, New York: John Wiley & Sons, Inc. pp 138-147.

Murphy, M. D., Paasch, R. K., 1997, "Reliability Centered Prediction Technique for Diagnostic Modeling and Improvement," *Research in Engineering Design*, Vol. 9, No. 1, pp. 35-45.

Ruff, D. N., Paasch, R. K., 1997, "Evaluation of Failure Diagnosis in Conceptual Design of Mechanical Systems," *Journal of Mechanical Design*, Vol. 119, No. 1, pp. 57-64.

Simpson, W.R. and J.W. Sheppard, 1992, "Fault Isolation in an Integrated Diagnostic Environment," *IEEE Design and Test of Computers*, Vol. 9, No. 4.

Simpson, William R., and John W. Sheppard, 1994, *System Test and Diagnosis*, Boston: Kluwer Academic Press.

Simpson, William R., and John W. Sheppard, 1998, *Research Perspectives and Case Studies in System Test and Diagnosis*, Boston: Kluwer Academic Press.

Appendices

Appendix A. Distinguishability Analysis of Alternative System Designs

The worksheets for completing the diagnostic analysis of the illustrative example are presented. The included analysis assumes a uniform indication certainty of 99.99 percent. Additionally, the exposure times of the components remain the same for all of the alternative designs (see Table A.1).

Table A.1. Component exposure times.

Component	Exposure time (hr)
C1	5000
C2	3700
C3	1750
C4	7200
C5	10000

Alternative Design 1, One Failure Indication:

Table A.2. Failure rate matrix, Alternative Design 1.

1.0×10^{-7}	C1	C2	C3	C4	C5
I1	15	14	29	2	46

Table A.3. Component reliability computation, Alternative Design 1.

Component-Indication	Exposure Time (hr)	Pr(C_i=good)	Pr (C_i = bad)
C1, I1	5000	0.993	0.007
C2, I1	3700	0.995	0.005
C3, I1	1750	0.995	0.005
C4, I1	7200	0.999	0.001
C5, I1	10000	0.955	0.045

Table A.4. Component-indication joint probability matrix, Alternative Design 1.

	C1	C2	C3	C4	C5	All Good	Indication Prob.
I1	0.0071	0.0049	0.0048	0.0013	0.0441	0.0001	0.0622
All Pass	0.0001	0.0001	0.0001	0.0001	0.0001	0.9373	0.9378
Comp Prob	0.0072	0.0050	0.0049	0.0014	0.0442	0.9374	1.0000

Table A.5. Replacement matrix, Alternative Design 1.

	C1	C2	C3	C4	C5	All Good
I1	0	0	0	0	1	0
All Pass	0	0	0	0	0	1

Table A.6. Replacement probability matrix, Alternative Design 1.

Replaced ↓ / Failed →	C1	C2	C3	C4	C5	All Good	
C1	**0.00000**	0.00000	0.00000	0.00000	0.00000	0.00000	
C2	0.00000	**0.00000**	0.00000	0.00000	0.00000	0.00000	
C3	0.00000	0.00000	**0.00000**	0.00000	0.00000	0.00000	
C4	0.00000	0.00000	0.00000	**0.00000**	0.00000	0.00000	
C5	0.00705	0.00487	0.00477	0.00135	**0.04410**	0.00009	
None replaced	0.00010	0.00010	0.00010	0.00010	0.00010	**0.93728**	
Pr(Just removal)	0.00000	0.00000	0.00000	0.00000	0.04410		**0.04410**
Pr(Unjust removal)	0.00705	0.00487	0.00477	0.00135	0.00000	0.00009	**0.01813**
Pr(Just leave)						0.93728	**0.93728**
Pr(Unjust leave)	0.00010	0.00010	0.00010	0.00010	0.00010		**0.00049**
Pr(Just Action)	0.00000	0.00000	0.00000	0.00000	0.04410	0.93728	**0.98138**

Alternative Design 2, 13 Failure Indications:

Table A.7. Failure rate matrix, Alternative Design 2.

10^{-7} hour^{-1}	C1	C2	C3	C4	C5
I1	2	0	0	0	0
I2	0	0	4	0	0
I3	0	0	0	0	3
I4	0	0	0	2	0
I5	0	0	0	0	15
I6	3	0	0	0	0
I7	0	2	0	0	0
I8	0	0	17	0	0
I9	0	0	0	0	25
I10	10	0	0	0	0
I11	0	12	0	0	0
I12	0	0	0	0	3
I13	0	0	8	0	0

Table A.8. Component reliability computation, Alternative Design 2.

Component-Indication	Exposure Time (hr)	Pr(C_i=good)	Pr (C_i = bad)
C1, I1	5000	0.999	0.001
C1, I6	-	0.999	0.001
C1, I10	-	0.995	0.005
C2, I7	3700	0.999	0.001
C2, I11	-	0.996	0.004
C3, I2	1750	0.999	0.001
C3, I8	-	0.997	0.003
C3, I13	-	0.999	0.001
C4, I4	7200	0.999	0.001
C5, I3	10000	0.997	0.003
C5, I5	-	0.985	0.015
C5, I9	-	0.975	0.025
C5, I12	-	0.997	0.003

Table A.9. Component-indication joint probability matrix, Alternative Design 2.

	C1	C2	C3	C4	C5	All Good	Indication Prob
I1	0.0010	0.0000	0.0000	0.0000	0.0000	0.0001	0.0011
I2	0.0000	0.0000	0.0007	0.0000	0.0000	0.0001	0.0008
I3	0.0000	0.0000	0.0000	0.0000	0.0030	0.0001	0.0031
I4	0.0000	0.0000	0.0000	0.0014	0.0000	0.0001	0.0015
I5	0.0000	0.0000	0.0000	0.0000	0.0149	0.0001	0.0150
I6	0.0015	0.0000	0.0000	0.0000	0.0000	0.0001	0.0016
I7	0.0000	0.0007	0.0000	0.0000	0.0000	0.0001	0.0008
I8	0.0000	0.0000	0.0030	0.0000	0.0000	0.0001	0.0031
I9	0.0000	0.0000	0.0000	0.0000	0.0247	0.0001	0.0248
I10	0.0050	0.0000	0.0000	0.0000	0.0000	0.0001	0.0051
I11	0.0000	0.0044	0.0000	0.0000	0.0000	0.0001	0.0045
I12	0.0000	0.0000	0.0000	0.0000	0.0030	0.0001	0.0031
I13	0.0000	0.0000	0.0014	0.0000	0.0000	0.0001	0.0015
All Pass	0.0000	0.0000	0.0000	0.0000	0.0000	0.9340	0.9340
Comp Prob	0.0075	0.0052	0.0051	0.0014	0.0456	0.9353	1.0000

Table A.10. Replacement matrix, Alternative Design 2.

	C1	C2	C3	C4	C5	All Good
I1	1	0	0	0	0	0
I2	0	0	1	0	0	0
I3	0	0	0	0	1	0
I4	0	0	0	1	0	0
I5	0	0	0	0	1	0
I6	1	0	0	0	0	0
I7	0	1	0	0	0	0
I8	0	0	1	0	0	0
I9	0	0	0	0	1	0
I10	1	0	0	0	0	0
I11	0	1	0	0	0	0
I12	0	0	0	0	1	0
I13	0	0	1	0	0	0
All Pass	0	0	0	0	0	1

Table A.11. Replacement probability matrix, Alternative Design 2.

Replaced ↓ / Failed →	C1	C2	C3	C4	C5	All Good	
C1	**0.00749**	0.00000	0.00000	0.00000	0.00000	0.00030	
C2	0.00000	**0.00517**	0.00000	0.00000	0.00000	0.00020	
C3	0.00000	0.00000	**0.00507**	0.00000	0.00000	0.00030	
C4	0.00000	0.00000	0.00000	**0.00144**	0.00000	0.00010	
C5	0.00000	0.00000	0.00000	0.00000	**0.04556**	0.00040	
None replaced	0.00000	0.00000	0.00000	0.00000	0.00000	**0.93397**	
Pr(Just removal)	0.00749	0.00517	0.00507	0.00144	0.04556		**0.06473**
Pr(Unjust removal)	0.00000	0.00000	0.00000	0.00000	0.00000	0.00129	**0.00129**
Pr(Just leave)						0.93397	**0.93397**
Pr(Unjust leave)	0.00000	0.00000	0.00000	0.00000	0.00000		**0.00001**
Pr(Just Action)	0.00749	0.00517	0.00507	0.00144	0.04556	0.93397	**0.99870**

Alternative Design 3, Original system failure rate-indication mapping modified:

Table A.12. Failure rate matrix, Alternative Design 4.

1.0×10^{-7}	**C1**	**C2**	**C3**	**C4**	**C5**
I1	12	0	4	0	3
I2	0	0	0	2	15
I3	3	2	0	0	0
I4	0	0	0	0	25
I5	0	12	0	0	3
I6	0	0	25	0	0

Table A.13. Component reliability computation, Alternative Design 4.

Component-Indication	**Exposure Time (hr)**	**Pr(C_i=good)**	**Pr (C_i = bad)**
C1, I1	5000	0.994	0.006
C1, I3	5000	0.999	0.001
C2, I3	3700	0.999	0.001
C2, I5	3700	0.996	0.004
C3, I1	1750	0.999	0.001
C3, I6	1750	0.996	0.004
C4, I2	7200	0.999	0.001
C5, I1	10000	0.997	0.003
C5, I2	10000	0.985	0.015
C5, I4	10000	0.975	0.025
C5, I5	10000	0.997	0.003

Table A.14. Component-indication joint probability matrix, Alternative Design 4.

	C1	C2	C3	C4	C5	All Good	Indication Prob
I1	0.0060	0.0000	0.0007	0.0000	0.0030	0.0001	0.0097
I2	0.0000	0.0000	0.0000	0.0014	0.0149	0.0001	0.0164
I3	0.0015	0.0007	0.0000	0.0000	0.0000	0.0001	0.0023
I4	0.0000	0.0000	0.0000	0.0000	0.0247	0.0001	0.0248
I5	0.0000	0.0044	0.0000	0.0000	0.0030	0.0001	0.0075
I6	0.0000	0.0000	0.0044	0.0000	0.0000	0.0001	0.0045
All Pass	0.0000	0.0000	0.0000	0.0000	0.0000	0.9348	0.9348
Comp Prob	0.0075	0.0052	0.0051	0.0014	0.0455	0.9354	1.0000

Table A.15. Replacement matrix, Alternative Design 4.

	C1	C2	C3	C4	C5	All Good
I1	1	0	0	0	0	0
I2	0	0	0	0	1	0
I3	1	0	0	0	0	0
I4	0	0	0	0	1	0
I5	0	1	0	0	0	0
I6	0	0	1	0	0	0
All Pass	0	0	0	0	0	1

Table A.16. Replacement probability matrix, Alternative Design 4.

Replaced ↓ / Failed →	C1	C2	C3	C4	C5	All Good	
C1	**0.00746**	0.00074	0.00069	0.00000	0.00298	0.00020	
C2	0.00000	**0.00442**	0.00000	0.00000	0.00298	0.00010	
C3	0.00000	0.00000	**0.00437**	0.00000	0.00000	0.00010	
C4	0.00000	0.00000	0.00000	**0.00000**	0.00000	0.00000	
C5	0.00000	0.00000	0.00000	0.00142	**0.03955**	0.00020	
None replaced	0.00000	0.00000	0.00000	0.00000	0.00000	**0.93480**	
Pr (Just removal)	0.00746	0.00442	0.00437	0.00000	0.03955		**0.05579**
Pr (Unjust removal)	0.00000	0.00074	0.00069	0.00142	0.00596	0.00059	**0.00940**
Pr (Just leave)						0.93480	**0.93480**
Pr (Unjust leave)	0.00000	0.00000	0.00000	0.00000	0.00000		**0.00001**
Pr (Just Action)	0.00746	0.00442	0.00437	0.00000	0.03955	0.93480	**0.99059**

Appendix B. Schematics of icemaker example

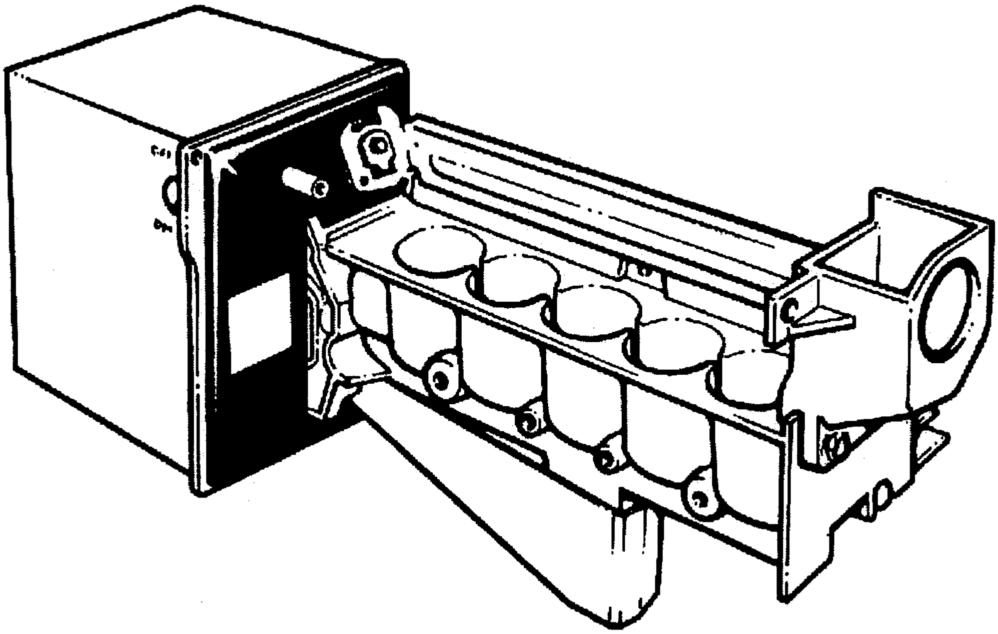


Figure B.1. Schematic of assembled icemaker.

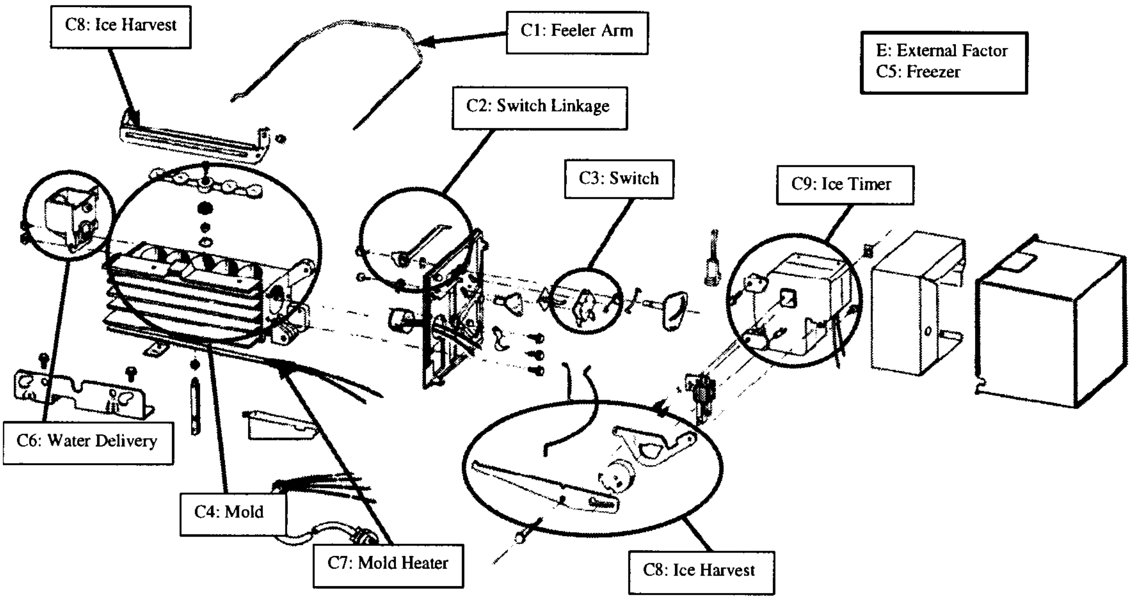


Figure B.2. Exploded view of icemaker.

Appendix C. Icemaker FMEA Document

Table C.1. Icemaker FMEA Document [Henning 2000].

Component	Function	Failure Mode	Failure Type	Failure Rate [per million cycles]	Effect	Sys Effect (observable)	Indication Code ( ) = sometimes	Indication Set
1. Feeler arm	Sense ice level in bucket	Broken off	Full	3		No ice, feeler arm in bucket at times	1, (9)	[2], (6)
2. Switch linkage	Feeler arm – Switch connection	Stuck closed	Full	60		Ice overflow	2	[3]
		Stuck closed	Intermittent	50		Ice overflow	(2)	[3]
		Stuck open	Full	80		No ice	1	[2]
		Stuck open	Intermittent	70		Low ice in bucket at times	-3	[4]
3. Switch	Activate/deactivate ice maker	Stuck closed	Full	50		Ice overflow	2	[2]
		Stuck open	Full	50		No ice	1	[3]
4. Mold	Hold water, form ice geometry and size	Crack	Partial	8	Water leak	Small ice, ice layer in bucket	6, (4)	[5]
		Hole	Full	1	Water leak, mold empty	No ice, ice layer in bucket	1, 4	[1]
5. Freezer	Freeze water	Not functioning	Full	30	High temp	No ice, water in bucket at times	1, (4)	[2], (1)
6. Water Delivery System	Fill mold w/ water	Not functioning	Full	25	No water in mold	No ice	1	[2]
		Slow water	Partial	45		Small ice	6, (3)	[5]
7. Mold heating system	Loosen ice	No heat	Full	90	Ice stuck in mold	No ice	1, (4)	[2], (1)
8. Ice harvesting system	Remove ice from mold	Not functioning	Full	30	Ice stuck in mold	No ice	1, (4)	[2], (1)
9. Ice timer	Allow proper freezing time	Not functioning	Full	40	Ice stuck in mold	No ice	1	[2]
		Too fast	Partial	15	Water leak	Small ice	6, (4)	[5]
EXTERNAL: Refrigerator Alignment	Create a consistent water level in the ice mold	Small misalignment	Mild severity	150		Small ice	6	[7]
		Large misalignment	Severe	40	Water leak	Small ice, ice layer in bucket	6, 4	[5]

Appendix D. Distinguishability analysis of icemaker validation example

Table D.1. Icemaker failure rate matrix.

1.0×10^{-7}	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**	**E**
I1	0.00	0.00	0.00	0.99	9.90	0.00	69.30	19.80	0.00	0.00
I2	0.99	79.20	49.50	0.00	19.80	24.75	19.80	9.90	39.60	0.00
I3	0.00	108.90	49.50	0.00	0.00	0.00	0.00	0.00	0.00	0.00
I4	0.00	69.30	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
I5	0.00	0.00	0.00	7.92	0.00	44.55	0.00	0.00	14.85	39.60
I6	1.98	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
I7	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	148.50
All good	0.03	2.60	1.00	0.09	0.30	0.70	0.90	0.30	0.55	1.90

Table D.2. Exposure times for icemaker components.

Ice maker cycles/day	3	
Ice maker expected life	15 years	
Component	**Exposure time (hrs)**	**Exposure time approximations**
C1: Feeler arm	5475	20 min/cycle
C2: Switch Linkage	2737.5	10 min/cycle
C3: Switch	2737.5	10 min/cycle
C4: Mold	32850	2 hours/cycle
C5: Freezer	131400	Life of freezer
C6: Water Delivery	4106.25	15 min/cycle
C7: Mold Heater	1095	4 min/cycle
C8: Ice Harvester	547.5	2 min/cycle
C9: Ice Timer	32850	25% of life of refrigerator, continuous operation
E: External Factor	657	Intermittent, happen .5% over lifetime

Table D.3. Component reliability computation.

Component-Indication	Exposure Time (hr)	Pr(Ci=good)	Pr (C_i = bad)
C1,I2	5475	0.999	0.001
C1,I6	5475	0.999	0.001
C2,I2	2737.5	0.978	0.022
C2,I3	2737.5	0.970	0.030
C2,I4	2737.5	0.981	0.019
C3,I2	2737.5	0.986	0.014
C3,I3	2737.5	0.986	0.014
C4,I1	32850	0.997	0.003
C4,I5	32850	0.974	0.026
C5,I1	131400	0.877	0.123
C5,I2	131400	0.769	0.231
C6,I2	4106.25	0.990	0.010
C6,I5	4106.25	0.982	0.018
C7,I1	1095	0.992	0.008
C7,I2	1095	0.998	0.002
C8,I1	547.5	0.999	0.001
C8,I2	547.5	0.999	0.001
C9,I2	32850	0.877	0.123
C9,I5	32850	0.952	0.048
E,I5	657	0.997	0.003
E,I7	657	0.990	0.010

Table D.4. Prior knowledge about component-indication relationship.

Pr(I1=fail $\mid$ Any one Component = fail)	99%
Pr(I1=fail $\mid$ All Component = good)	1%
Pr(I2=fail $\mid$ Any one Component = fail)	99%
Pr(I2=fail $\mid$ All Component = good)	1%
Pr(I3=fail $\mid$ Any one Component = fail)	99%
Pr(I3=fail $\mid$ All Component = good)	1%
Pr(I4=fail $\mid$ Any one Component = fail)	99%
Pr(I4=fail $\mid$ All Component = good)	1%
Pr(I5=fail $\mid$ Any one Component = fail)	99%
Pr(I5=fail $\mid$ All Component = good)	1%
Pr(I6=fail $\mid$ Any one Component = fail)	99%
Pr(I6=fail $\mid$ All Component = good)	1%
Pr(I7=fail $\mid$ Any one Component = fail)	99%
Pr(I7=fail $\mid$ All Component = good)	1%

Table D.5. Component-indication joint probability matrix.

	C1	C2	C3	C4	C5	C6	C7	C8	C9	E	All good	Indication Prob
I1	0.00	0.00	0.00	0.00	0.12	0.00	0.01	0.00	0.00	0.00	0.01	0.14
I2	0.00	0.01	0.01	0.00	0.19	0.01	0.00	0.00	0.09	0.00	0.01	0.32
I3	0.00	0.03	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.05
I4	0.00	0.02	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.03
I5	0.00	0.00	0.00	0.02	0.00	0.02	0.00	0.00	0.05	0.00	0.01	0.10
I6	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.01
I7	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.01	0.02
All good	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.33	0.33
Comp Prob	0.00	0.06	0.02	0.03	0.31	0.02	0.01	0.00	0.14	0.01	0.39	**1.00**

Table D.6. Icemaker replacement matrix.

	C1	C2	C3	C4	C5	C6	C7	C8	C9	E	All good
I1	0	0	0	0	1	0	0	0	0	0	0
I2	0	0	0	0	1	0	0	0	0	0	0
I3	0	1	0	0	0	0	0	0	0	0	0
I4	0	1	0	0	0	0	0	0	0	0	0
I5	0	0	0	0	0	0	0	0	1	0	0
I6	0	0	0	0	0	0	0	0	0	0	1
I7	0	0	0	0	0	0	0	0	0	0	1
All pass	0	0	0	0	0	0	0	0	0	0	1

Table D.7. Icemaker replacement probability matrix.

Replaced ↓ / Failed →	C1	C2	C3	C4	C5	C6	C7	C8	C9	E	All good	
C1	**0.00**	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	
C2	0.00	**0.05**	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.02	
C3	0.00	0.00	**0.00**	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	
C4	0.00	0.00	0.00	**0.00**	0.00	0.00	0.00	0.00	0.00	0.00	0.00	
C5	0.00	0.01	0.01	0.00	**0.31**	0.01	0.01	0.00	0.09	0.00	0.02	
C6	0.00	0.00	0.00	0.00	0.00	**0.00**	0.00	0.00	0.00	0.00	0.00	
C7	0.00	0.00	0.00	0.00	0.00	0.00	**0.00**	0.00	0.00	0.00	0.00	
C8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	**0.00**	0.00	0.00	0.00	
C9	0.00	0.00	0.00	0.02	0.00	0.02	0.00	0.00	**0.05**	0.00	0.01	
E	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	**0.00**	0.00	
None replaced	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.01	**0.35**	
Pr (Just removal)	0.000	0.048	0.000	0.000	0.311	0.000	0.00	0.00	0.05	0.00		**0.405**
Pr (Unjust removal)	0.000	0.014	0.022	0.027	0.000	0.023	0.008	0.001	0.089	0.002	0.044	**0.231**
Pr (Just leave)											0.347	**0.347**
Pr (Unjust leave)	0.001	0.001	0.000	0.000	0.004	0.000	0.000	0.000	0.002	0.010		**0.018**
Pr (Just Action)	0.000	0.048	0.000	0.000	0.311	0.000	0.000	0.000	0.045	0.000	0.347	**0.751**