SLAC-TN-09-001
January 2009

Life Cost Based FMEA Manual

A step by step guide to carrying out a cost-based Failure Modes and Effects Analysis

Seung Rhee: previously at Stanford University
Cherrill Spencer: SLAC National Accelerator Laboratory

Based on work carried out from 2001 to 2004

Work supported by the U.S. Department of Energy under contract number
DE-AC02-76SF00515

TABLE OF CONTENTS

1. Introduction

Failure occurs when one or more of the intended functions of a product are no longer fulfilled to the customer's satisfaction. The most critical product failures are those that escape design reviews and in-house quality inspection and are found by the customer. The product may work for a while until its performance degrades to an unacceptable level or it may have not worked even before customer took possession of the product. The end results of failures which may lead to unsafe conditions or major losses of the main function are rated high in severity.

- **Traditional FMEA**

Failure Modes and Effects Analysis (FMEA) is a tool widely used in the automotive, aerospace, and electronics industries to identify, prioritize, and eliminate known potential failures, problems, and errors from systems under design, before the product is released (Stamatis, 1997). Several industrial FMEA standards such as those published by the Society of Automotive Engineers, US Department of Defense, and the Automotive Industry Action Group employ the Risk Priority Number (RPN) to measure risk and severity of failures. The Risk Priority Number (RPN) is a product of 3 indices: Occurrence (O), Severity (S), and Detection (D). In a traditional FMEA process design engineers typically analyze the "root cause" and "end-effects" of potential failures in a sub-system or component and assign penalty points through the O, S, D values to each failure. The analysis is organized around categories called failure modes, which link the causes and effects of failures.

A few actions are taken upon completing the FMEA worksheet. The RPN column generally will identify the high-risk areas. The idea of performing FMEA is to eliminate or reduce known and potential failures before they reach the customers. Thus, a plan of action must be in place for the next task. Not all failures can be resolved during the product development cycle, thus prioritization of actions must be made within the design group.

- **Limitations of traditional FMEA**

One definition of detection difficulty (D) is how well the organization controls the development process. Another definition relates to the detectability of a particular failure in the product when it is in the hands of the customer. The former asks "What is the chance of catching the problem before we give it to the customer?" The latter asks "What is the chance of the customer catching the problem before the problem results in a catastrophic failure?" (Palady, 1995) These differing definitions confuse the FMEA users when one tries to determine detection difficulty. Are we trying to measure how easy it is to detect where a failure has occurred or when it has occurred? Or are we trying to measure how easy or difficult it is to prevent failures?

Ordinal scale variables are used to rank-order industries such as, hotels, restaurants, and movies (Note that a 4 star hotel is not necessarily twice as good as a 2 star hotel). Ordinal values preserve rank in a group of items, but the distance between the values cannot be measured since a distance function does not exist. Thus, the product or sum of ordinal variables loses its rank since each parameter has different scales. The RPN is a product of 3 independent ordinal variables, it can indicate that some failure types are “worse” than others, but give no quantitative indication of their relative effects.

- **Cost as a measure of failure**

To resolve the ambiguity of measuring detection difficulty and the irrational logic of multiplying 3 ordinal indices, a new methodology was created to overcome these shortcomings, Life Cost-Based FMEA. Life Cost-Based FMEA measures failure/risk in terms of monetary cost. Cost is a universal parameter that can be easily related to severity by engineers and others. Thus, failure cost can be estimated using the following simplest form:

$$\text{Expected Failure Cost} = \sum_{i=1}^{n} p_i c_i \qquad (1)$$

p: Probability of a particular failure occurring
c: Monetary cost associated with that particular failure
n: Total number of failure scenarios

- **Formation of team**

FMEA is most effective when there are inputs into it from all concerned disciplines of the product development team. However, FMEA is a long process and can become tedious and won’t be effective if too many people participate. An ideal team should have 3 to 4 people from: design, manufacturing, and service departments if possible. Depending on how complex the system is, the entire process can take anywhere from one to four weeks working full time. Thus, it is important to agree to the time commitment before starting the analysis else, anxious managers might stop the procedure before it is completed.

2. Failure Mode and Effects Analysis (FMEA)

Failure Mode and Effects Analysis (FMEA) is used to assist in identifying potential failure modes early in the process of design. Traditional FMEA measures risk using the Risk Priority Number (RPN). The FMEA worksheet consists of a table that will be filled in by the FMEA team; it lists the causes and effects of potential failure modes which are known by the team of engineers. These failure modes are organized around functions or the “Voice of the Customer” (VOC) (see Table 1). The following section describes the elements of the spreadsheet used for listing identified failure scenarios in a device.

Table 1 Components of a FMEA Worksheet

Function or Requirement	Potential Failure Modes	Causes of Failure	Root Cause	Effect of Failure	Occurrence	Severity	Detection	RPN	Actions Recommended to Reduce RPN	Responsibility and Target Completion Date

2.1. Function

Function is the specific behavior (e.g., hold vacuum) intended by the designers. Use the functional analysis to list major sub-functions or use customer requirements (Voice Of the Customers= VOC) in this column. Discrepancies from the intended function or requirement are the result of a failure in the system. We recommend organizing the FMEA worksheet first by listing the functions of the device in the leftmost column.

2.2. Potential Failure Mode

It describes the departure from the intended function or requirement. For function-based FMEA, interpret *failure modes* as a sub-function occurring improperly or not at all. Potential failure modes can be considered in any of the following four categories:

1. *No Function*: There is a complete absence of the intended function.
2. *Partial/degraded function*: The item does not meet some of the required functions
3. *Intermittent function*: The item performs a function intermittently.
4. *Unintended function*: Another function (behavior) is performed which was unintended in the original design.

It is important to note that even if certain failures have never occurred for a similar device, it should be listed on the FMEA worksheet if the failure is physically possible.

2.3. Cause of Failure

It describes why the desired requirement fails. Consider the needed conditions for each customer requirement. Also, ask yourself “what has to happen for the function to occur properly?” Then, list the possible causes of failure due to components’ behaviors, usage conditions (especially regarding human interaction), operating environment, and interfaces with other systems.

2.4. Root Cause of Failure

To find the root cause of failure may, in many cases require detailed analysis of the failure mode. You may need to identify root causes by using by other techniques such as “Five Why’s” (ask why succeeding failures happen five times until a root cause is determined) or the Ishikawa Fishbone Root Cause Analysis (organize root causes around man, machine, material, method, measurement, environment) (Ishikawa, 1985).

2.5. Effect of Failure

Effect of a failure on product, user, or other systems is the noticeable effect on performance, safety, and perceived quality. As a designer, this is the effect you are trying to prevent in your own design. *The root cause is where you will make changes in your existing designs as will be discussed later in section 2.10.*

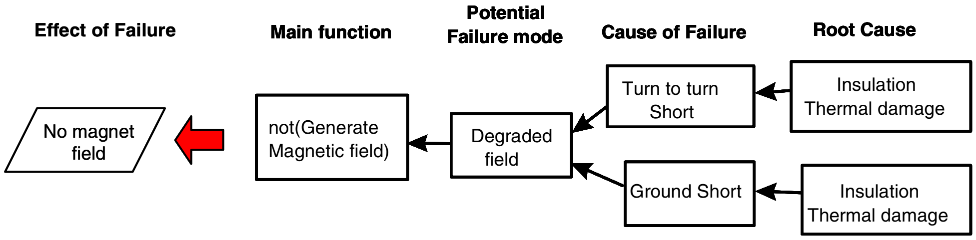

Figure 1 Failure Scenarios

Figure 1 shows an example of a cause-and-effect chain of events. There are many such "failure scenarios" or "event chains" possible in an FMEA and you should list each on a separate row with an associated RPN. It should be noted that failures can have many causes, and each scenario should be listed on a separate line on the FMEA worksheet.

2.6. Probability of Occurrence (O)

Occurrence is defined as how frequently the specific failure cause is projected to occur and result in the "failure mode". The literature prescribes that Occurrence is assigned to the cause (and failure mode) and has nothing to do with the probability of the end effects. However, we recommend associating the Occurrence rating with the entire failure scenario, since some causes could have many different effects. *Occurrence* should refer to the probability of cause → a particular failure mode → a particular effect/event. In mathematical terms:

$$\textit{Probability of failure} = (\textit{Probability of cause}) \times (\textit{Probability of failure given the cause}) \qquad \textbf{(2)}$$

Table 2 Example of Occurrence criteria [AIAG, 1995]

Probability of Failure	Probability of Failure	Occurrence Ranking
Very High: Failure is almost inevitable	≥ 1 in 2	10
	1 in 3	9
High: Repeated failures	1 in 8	8
	1 in 20	7
Moderate: Occasional failures	1 in 80	6
	1 in 400	5
	1 in 2,000	4
Low: Relatively few failures	1 in 15,000	3
	1 in 150,000	2
Remote: Failure is unlikely	1 in 1,500,000	1

Occurrence scores are generated on the basis of an industry- or company-specific mapping from probabilities to a 1-10 scale (see Table 2).

2.7. Severity of effect (S)

Severity is typically defined as an assessment of the seriousness of the potential "end effects," and is assessed independent of the causes. However, we recommend assessing Severity to the entire failure scenario (causes, failure modes effects). Severity is estimated on a 1 to 10 scale (see Table 3).

Table 3 Severity of effect scores [AIAG, 1995]

Effect	Severity of Effect	Severity Ranking
Hazardous without warning	when a failure mode affects safe device operation without warning	10
Hazardous with warning	when a failure mode affects safe device operation with warning	9
very high	device inoperable: loss of primary function	8
High	device operable: at a highly reduced level of performance	7
Moderate	device operable: at a reduced level of performance	6
Low	device operable: at a slightly reduced level of performance	5
very low	device operable: defect noticed by most customers	4
Minor	device operable: defect noticed by average customers	3
very minor	device operable: defect noticed by discriminating customers	2
None	almost no effect	1

2.8. Detection difficulty (D),

Detection, sometimes called detectability, has no standard definition. There is some confusion surrounding this index, since different definitions exist for this term. If the team does not have a good understanding of this index, we recommend using a value of "1" for all fields and the team can fill it in later if time permits. The most common interpretation of detection is an assessment of the ability of the "design controls" to identify a potential cause or design weakness before the component, subsystem or system is released for production. Detection scores are generated on the basis of likelihood of detection by the relevant company design review and testing procedures program (see Table 4). Column A reflects the chance of catching a failure before it goes to the customers. Column *B* reflects the organization's controls, systems and maturity level of its quality and reliability programs.

Table 4. Detection criteria [Palady, 1995]

Detection Difficulty	Criteria	Rating
Impossible to detect	No known techniques available	10
Remote detection	Only unproven or unreliable technique available	9
Very slight detection	Proving durability tests on products with system components installed	8
Slight detection	Tests on product with prototypes with system components installed	7
Low detection	Tests on similar system components	6
Medium detection	Tests on preproduction system components	5
Moderate detection	Tests on early prototype system elements	4
Good detection	Simulation and modeling in early stage	3
High chance of detection	Proven computer analysis available in early design stage	2
Certain to detect	Proven detection methods available in concept stage	1

Occurrence, Severity, and Detection ratings can be customized to the user's needs and type of industry.

2.9. Risk Priority Number (RPN)

We define the ***Risk Priority Number (RPN)*** as follows:

$$RPN \quad = \quad (Occurrence) \times (Severity) \times (Detection) \qquad (3)$$

Larger RPNs indicate the need for corrective action or failure resolution. Give special attention to the effect and its causes when the severity rating is high regardless of the RPN. You should construct a Pareto chart (Crosby, 1969) of RPNs vs. causes or failure modes to clearly summarize the FMEA. Note that each discrete failure scenario (i.e. mode, cause, and effect) should have its own associated Occurrence, Severity and Detection values, and therefore a distinct RPN number.

2.10. Actions

Actions Recommended to Reduce RPN (see Table 1) is a list of corrective actions and failure resolutions. Recommendations could include, in the order of priority:

1) Design solutions to eliminate the failure mode or reduce its likelihood, including: functional redundancies and error proofing the assembly, installation and usage.
2) Actions to reduce the severity of the failure mode in terms of its impact on the user, performance, and other systems
3) Developing means of detecting causes of failure modes during manufacturing including: inspection, testing, and error proofing.
4) Tests to provide more information data to assess *Probability* and *Severity*
5) Providing diagnostics to easily identify the failure mode or cause during manufacturing or operation.

6) Establish periodic maintenance or check-ups to enhance availability and safety.

3. Concept of Life Cost Based FMEA

Lifecycle cost is the total monetary cost of ownership of a product during the lifetime of its use. This includes acquisition cost, marketing, cost of ownership (repair, scheduled maintenance, and usage costs), and sometimes retirement cost of the product. Acquisition cost is relatively well perceived and defined in industry. However, cost of ownership is overlooked most of the time during the design stage. Repair and scheduled maintenance costs are hard to predict and no formal set of tools exist to make predictions. Life Cost Based FMEA is a tool developed to predict unexpected failure costs and ultimately compare lifecycle cost between different designs.

From Equation 1, expected failure cost is the sum of all possible failures with respect to their probability and cost of failure. Probability of failure can be determined from field data, test data, or empirical data. Cost of failure can be measured in terms of time as will be discussed in the following and hardware cost.

3.1. Cost

Failures may occur at any stage of the life cycle and can be detected either during the same stage or during subsequent stages. The failure cost is smallest when the origin and detection occur during the same stage. The failure cost increases as the origin and detection stages become further apart.

The example shown in Figure 2 is where a failure is detected during the operations stage and the initial origin of the failure is a design error. Due to design error, the part has to be redesigned, remanufactured, and reinstalled. There may be some delay between each of these activities also. Recovery time is the whole time the system is inoperable due to the failure. Recovery time is associated with lost opportunity.

Figure 2 shows the four possible failure initiating stages and the failure detection stages.

- Failure **origin** indicates when the failure has been initially introduced. The four possible stages are: **Design, Manufacture, Installation, and Operation**.
- **Detection** phase indicates the stage at which the failure has been realized. The four possible stages are: **Design Review, Inspection, Testing, and Operation.**

Time is the basic unit used to convert failure consequence into cost. Detection time, fixing time, delay time and loss time are the four fundamental time penalties in this analysis.

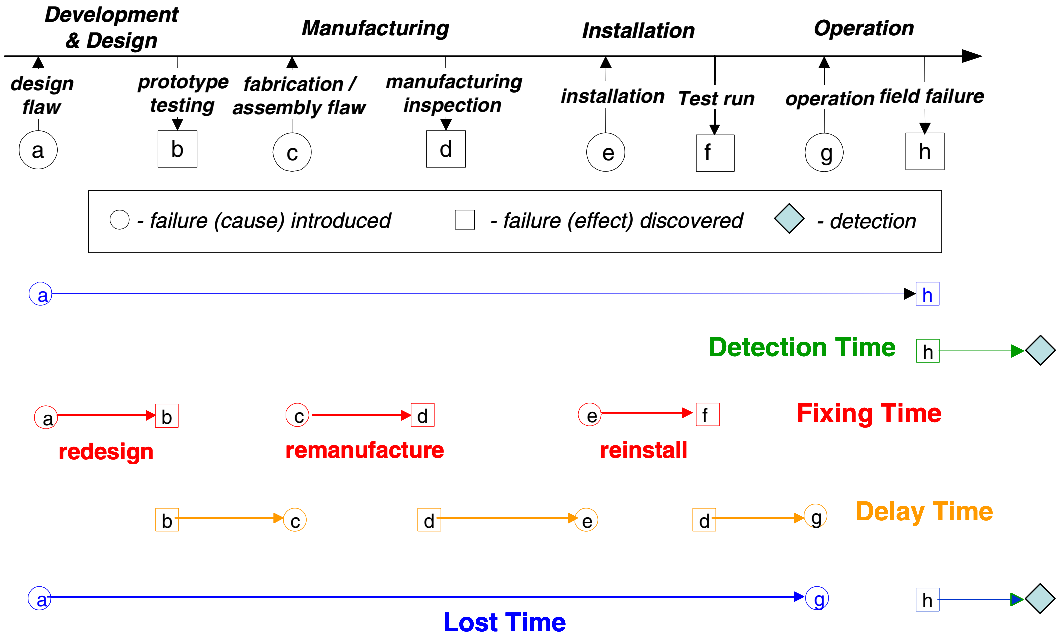

Figure 2. Initial Origin and Detection Stages of Failure

- **Detection Time**: Time to realize and identify a certain type of failure that has occurred and diagnose the exact location and its root cause.

- **Fixing Time:** Time to fix each individual component. Redesign, remanufacturing, and reinstallation are some examples of activities that lead to fixing time.

- **Delay Time**: Time incurred for a non-value activity such as waiting for technicians to respond, set up time, and mailing/shipping time.

- **Loss Time**: Time during which the system has been shut down and has not produced any value. Only applies to failures that happen during the operations stage. Loss time is the sum of Detection time, Fixing time, and Delay time. Loss time is used to calculate the opportunity cost of failure.

Table 5 shows a Life Cost-Based FMEA table that is filled-in for this methodology. The “Outputs” in this table are the 3 main components of Failure cost: labor cost, parts cost, and opportunity cost. Labor and opportunity costs are dependent on time and parts cost is dependent on material cost. Units for time penalties are in hours.

Table 5. Life Cost Based FMEA Table

			Input										Output		
Failure Mode	Root Cause of Failure	Effect of Failure	Origin	Detection Phase	Re-occuring	Frequency	Detection Time	Fixing Time	Delay Time	Loss Time	Quantity	Parts Cost ($)	Labor Cost($)	Material Cost($)	Opportunity Cost($)
Thermal swtich trip due to overheating	Too many loads on circuit	Magnet turned off	Oper	Oper	30	0.001	0.5	4	0	5	1	50	180	15	112,500
	Water passage is blocked	Magnet turned off	Oper	Oper	30	2	1	4	0	5	1	50	38,400	3,000	125,000
	Damaged coil	Magnet turned off	Inst	TR	1	4	0.5	2	0	3	1	1250	1,280	5,000	62,500
	Water sprayed on to coil	Magnet turned off	Oper	Oper	30	3	2	8	0	10	1	50	115,200	4,500	250,000

- **Origin** indicates the stage at which the root cause of the failure lies in Figure 1.

- **Detection** indicates the stage at which the failure has occurred and been identified.

- **Re-occurring** indicates whether the failure is a one time event or could reoccur during the life time of the system. Failures that have root causes in design, manufacturing, or installation stages are usually one time errors and "1" is prescribed in this column. Failures that have root causes in assembly and operation stages are most likely to have random failures throughout the lifetime of the system. This lifetime is 30 years for the magnets in the International Linear Collider (ILC) which we are using as an example. Thus, "30" is prescribed in Table 6 under this column for failures that originate during the operation stage.

- **Frequency** indicates how often the failure occurs. Failures that originate in design, manufacturing, or assembly are assumed to be one time event failures and the probability of occurrence is assigned to the frequency variable. Failures that originate in assembly or operations reoccur during the life time of the system, thus frequency of failure during a one year period is assigned to this variable. Frequency will be discussed in more detail in **Section 3.2**.

- **Quantity** indicates the total number of components/systems affected by the failure. It describes whether a failure affects an individual component, a batch, a sector, or the entire system. "1" is assigned to isolated failures that happen randomly. Manufacturing failures may affect a whole batch of parts that are going through the manufacturing process together, resulting in scrapping the entire batch and re-manufacturing. A manufacturing failure detected during the installation stage would require all of the components to be replaced. An event such as an earthquake may affect magnets in a whole accelerator region or just a couple of sectors, depending on the earthquake magnitude.

- **Parts Cost** is the actual material cost to fix the failure if it is done through parts replacement. If the failure is a water hose leak and the hose needs to be replaced, the actual cost of the hose, $50, is taken as the value of the parts cost.

3.1.1. Labor Costs

Labor cost can be derived with the time information input in the cost-based FMEA table using the following equation:

$$\begin{aligned}\text{Labor Cost} = \text{Occurrence} \times \{&[\text{Detection Time} \times \text{Labor rate} \times \ \#\text{ of Operators}] + \\ &[\text{ Fixing Time} \times \text{Labor rate} \times \#\text{ of Operators} \times \text{Quantity}] + \\ &[\text{Delay Time} \times \text{Labor rate} \times \#\text{ of Operators}]\}\end{aligned}$$

A typical Labor rate used for this analysis is **$75/hour** for the operators.

Assumption: Operators work in pairs when they enter the tunnel to diagnose and to fix the problems.

3.1.2. Material Costs

Component replacement due to failure is considered as material cost. Material cost is obtained using the following equation:

$$\text{Material Cost} = \text{Occurrence} \times \text{Quantity of parts to replace} \times \text{Cost of Part}$$

3.1.2.1. Corrector Magnets

Parts cost to replace corrector magnets and their components are shown in Table 6.

Table 6 Parts Cost for Corrector Magnets

Part	Min	Mean	Max
Solid wire Coil	$250	$400	$1000
Core	$200	$750	$2000
Whole Corrector	$750	$2000	$4000

3.1.2.2. Water cooled Magnets

Parts cost to replace water cooled electromagnets and their components are shown in Table 7. These were typical costs for medium sized magnets in ~2002.

Table 7 Parts Cost for Water Cooled Magnets

Part	Min	Mean	Max
Hollow Cu Coil	$500	$1500	$4000
Core	$1250	$3500	$20,000
Whole Magnet	$4000	$11,000	$30,000

The average cost to replace circuit boards for a magnet power supply is $500. This includes the cost of the manual labor to fix the boards and the cost to replace necessary components on the board.

3.1.3. Opportunity Cost

Opportunity cost is the cost that incurs when a failure inhibits the main function of the system and prevents any value creation. In a particle collider this would be the inability to generate particle collisions and hence no data for the experimental particle physicists. Opportunity cost is calculated using the following equation:

$$\text{Opportunity Cost} = \text{Loss Time} \times \text{Hourly Opportunity Cost} \tag{4}$$

where,

$$\text{Loss Time} = \{\text{Detection Time} + \text{Fixing Time} + \text{Delay Time}\}$$

The setting of the hourly opportunity cost might be easier to understand if one thinks of losing the opportunity to create particle collisions while broken device is repaired. Think about a case where staff is sitting idle while the accelerator has no beam. The power sources will not be turned off for repairs taking a few hours, so the electricity bill will be the same as if the beams were there. A third consideration is the value of the whole facility; some experts argue that the capital cost of the accelerator should be included in the hourly opportunity cost. In which case you amortize the several billion dollar construction cost over the total number of required operating hours in a 30 year operating life.

As you will see from the example costs for the ILC (if it had been built in about 2002) given below there can be large differences between the 3 opportunity costs evaluated in 3 different ways. But note that even the lowest hourly opportunity cost is order of magnitude higher than the hourly labor rate for the repair technicians. Three different numbers are used in this analysis:

$10,000/hour:	Only direct labor is considered (Technicians, Physicists and Staff)
$25,000/hour:	Direct labor + electricity that is consumed by the ILC during shutdown.
$50,000/hour:	Direct labor + Electricity + Depreciation of the ILC ($6B) over 30 year period.

3.2. Frequency and Probability

Frequency is either the number of failure events or the probability for a specific failure to happen during a given period of time. A frequency value of “0.1”, for a design related failure means that there is a 10% chance a mistake will occur during the design process. Thus, it is not possible to have a frequency value greater than “1” for failures that have root causes that trace back to design, manufacturing, and assembly stages. Failures that have root causes in assembly and operations will have values of any real number in the frequency column.

Frequency values can be obtained from observing historical data of failure devices with similar designs used under similar environmental conditions. At SLAC we have 17 years worth of data on component failures in the various beamlines stored in 2 computer databases called CATER and ARTEMIS. Data from the CATER system can be used to predict failures modes and their probability for most component designs for the ILC.

What if data does not exist for a certain design in the current system? Reliability of components/system has to be modeled using different failure distributions or test data. The most common distributions used for failure analysis are Weibull distribution for fatigue related failures and exponential distribution for electronics and probabilistic modeling. A detailed description of predicting failure frequency is given in the next section.

4. Availability/Reliability Predictions

Mission-critical products and complex systems like particle collider require engineers to estimate the reliability of critical components and systems before they are built. In many cases, engineers rely on test data, published data, or field data to predict reliability. Reliability is defined as the probability of a **device** performing its purpose adequately for an intended period of time. The basic parameter to measure reliability is known as the failure rate. General expression for failure rate is expressed as the ratio of total number of failures to the total operating time which can be expressed as follows:

$$Failure\ \ Rate\ \ (\lambda) = \frac{K}{T} \tag{5}$$

where *K* is the number of failures and *T* is the total operating time.

The base model to predict the overall reliability of a single component, taking into account all operating conditions, has the generic form:

$$\lambda_p = \lambda_b \cdot \pi_T \cdot \pi_A \cdot \pi_R \cdot \pi_S \cdot \pi_C \cdot \pi_E \tag{6}$$

where λ_p is the part failure rate, λ_b is the base failure rate at some fixed operating conditions, π_T temperature modification factor, π_A application factor, π_R power modification factor, π_S electrical stress factor, π_C construction factor, and π_E environmental modification factor.

Mean Time Between Failure (MTBF)

MTBF is the average time between maintenances. MTBF value is the ratio of total operating time to the total number of failures. It can be expressed by taking the reciprocal of the failure rate as:

$$MTBF = \frac{T}{K} = \frac{1}{\lambda} \tag{7}$$

Mean Time To Repair (MTTR)

MTTR is the statistical mean or average of the distribution time to repair. MTTR value is calculated by taking the cumulative totals of repair time over a specific period and dividing it by the total number of incidents. Mathematically it is expressed as:

$$MTTR = \sum_{i=1}^{n} \frac{T_i}{n} \tag{8}$$

where, *n*= number of incidents and *T* is the time to repair the *i* th incident.

Availability is the probability that a **system** will operate to satisfactory conditions at any given time. Availability is the ratio between Uptime and Total Scheduled operating hours. It can be expressed as:

$$Availability \quad (A) = \frac{Uptime}{Scheduled \quad Operating \quad Hours} = \frac{MTBF}{MTBF + MTTR} \tag{9}$$

Field failures do not generally occur at a uniform rate, but follow a distribution in time commonly described as a "bathtub curve." The reliability bathtub curve is a conceptual model that is used to describe reliability at a component level over its life cycle. The bathtub consists of three stages as shown in Figure 3. Not all products follow the bath tub curve model but most do.

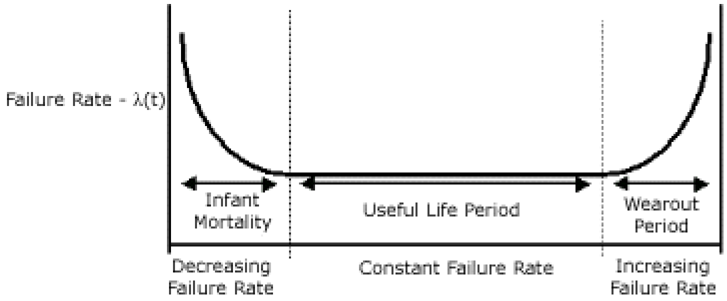

Figure 3. Reliability Bathtub Curve

The three phases are:

1. **Infant Mortality Phase**: The early life period of device operation is characterized by a rapidly declining failure rate. It occurs between 0 and 10,000 hours (~1 year) of device operation. Quality control defects due to poor workmanship, contamination, and other substandard manufacturing practice are liable for failures at this stage. Examples include premature failure due to poor manufacturing or assembly errors, use of poor quality material, etc. This has led to the development of burn-in procedures to

eliminate infant mortality rate. The failure rate during the early life period can be modeled by the Weibull Distribution (Ebeling, 1997).

2. **Useful Life Phase**: Beyond the infant mortality period, in the useful life period, the failure rate is assumed to be following an exponential distribution. The failure rate in this phase is at its lowest and is relatively constant. It begins after 10,000 hours (~1 year) of device operation. Failures during this stage are due to random or normal wear and tear where failures are caused by unexpected or sudden over stress conditions. This is where intelligent engineering can keep the failure rate at a negligible level.

3. **Wearout Phase**: Failures during this phase are due to component aging. Examples of what causes aging include fatigue, corrosion, creep, and other aging phenomena. Failures during this phase do not occur randomly.

Engineering work is done at the design stage to reduce or eliminate failures during the Useful Life and Wearout phases. FMEA allows us to identify failures in these stages for a particular design and to analyze how frequently these failures might occur, this will aid in increasing the reliability of the product. Three different approaches are discussed to predict the frequency of failures: Using empirical data, failure distribution estimation, and a mixture of both.

Step 1 Determine the new component or system that needs to be analyzed
Step 2 Identify if such a component or system exists in the current system (SLC)
If a similar or the same component exists in the current system follow section (4.1) Empirical data. If it is a brand new design then follow section (4.2) Distribution estimate. If some component of the total system is currently in use then follow **(4.3) Mixture of Data.**
Step 3 Categorize the components or systems into different sizes, capacities, and features for the failure rate analysis.

4.1. Empirical Data

Many of the components designed for the ILC are very similar to designs in the SLC and PEP II SLAC used the Computer Aided Trouble Reporting (CATER) system from 1988 to 2003 and now is using Accelerator Remedy Trouble Entry and Maintenance Information System (ARTEMIS) to keep track of all component failures in the all the beamlines. Since we are interested in predicting the availability of the new system, only failures that actually brought down the accelerator will be considered as a failure data point in the analysis. A lot of information is captured in the CATER + ARTEMIS database system and only the following data points are needed to conduct an availability and frequency analysis: assumptions

1. ***Date and Time of report***
The date enables us to ascertain beam lines were running when the failure occurred. Knowing the beamlines that were operational at that moment gives

us how many components were working. This information is used to analyze the type of failures in chronological order. The start time of the failure is required to determine how long it took to detect the failure, how long it took to fix, and to see if there were any delays.

2. ***Beam Time Loss***
   This information tells us how long the accelerator was shutdown due to this failure. This value should be equal to the sum of detection time, fixing time and delay time. We are interested in failures that actually forced the accelerator to shutdown.
3. ***Failure component***
   This information tells us which component has failed. You may have to work out the type of component to put it in the correct category.
4. ***Location of failure***
   This information tells us where the failed component resides along the beam lines. It indicates if the failed component was in the LINAC, North Damping ring, South Damping ring, HER, LER, and etc.
5. ***Observation***
   The technician who gets to the scene of the failure reports what is observed when they arrive. It is entered into the CATER/ARTEMIS by the main control operator.
6. ***Action taken***
   This information describes what the technicians have done to fix the problem. There are no categories in the trouble report systems for entering the root cause of failure. Thus, it is the FMEA team's responsibility to interpret the root cause of failure from *Action taken* and *Observation* descriptions.
7. ***Date and time of finished repair***
   This information helps us interpret how long the repair took and how long the beam line was shut down for.

Once these pieces of information are gathered from the CATER or ARTEMIS system and analyzed a few other pieces of information need to be gathered to carry out the reliability analysis as follows:

1. Determine the time period to investigate in the CATER system
   From a statistical point of view, 30 data points are said to be the minimum number to do any statistical analysis. Obviously we are able to make better predictions if there are more data points. However, analyzing hundreds of data entries may take a long time. We recommend observing a period that contains more than 50 data entries (failures) and several different types of beamlines. A 5 year period is recommended for the initial investigation.

2. Beamline running schedule
   The beam line configuration changes overtime and the number of components change with respect to the configuration. Thus, we need to know which beamlines were running during the investigation period and how many hours it was suppose to run (Runtime).

3. Number of components in each beam line
   In order to count the number of components in each previously specified category, the FMEA team will have to consult with drawings and lattices of the beamlines.

4. Number of components in the ILC
   To predict the frequency of failure for the ILC we need to know how many components of the same categories there will be in the ILC.

Step 4. Fill out the Availability table as shown in Table 8 for each type of component in a separate table. Within the table each row corresponds to a particular beamline's running period.

Beam line, operation hours (Run hours), and number of components in the beam line are all found in the previous steps.

- **Component hours** is the product of *Run Hours* and *# of Components* in the listed beamline. This is a parameter created to calculate the average availability of a single component at SLAC.
- **# of failures** indicates the number of component failures that occurred during that operation period as found by searching the CATER/AREMIS databases.
- **MTBF** is calculated by dividing *Component hours* by the *# of failures* during that period. The unit is in hours.
- **TR** is the total repair time for all of the failures during that period. This is the sum of beam loss time for that period. The unit is in hours.
- **MTTR** is total repair time (TR) divided by the number of failures for that period. The unit is in hours.
- **Availability** is calculated using Equation 6. This calculation yields the empirical availability for one component of certain type at SLAC.

Table 8. Availability Table

Date	Beam Line	Run Hours	# of Components	*Component* Hours	# of Failures	MTBF (hr)	TR (hr)	MTTR (hr)	Availability
5/1/97 ~ 6/8/98	SLC	8828	2300	20,304,400	15	1,353,626	136	9.06	0.999771

Step 5 Calculate Availability for the entire system

The average availability of a single magnet can be calculated by adding the total *Component Hours* and *MTBF* for the entire year period. Most of the components in the ILC are run in series without redundancy. Thus, if one fails, the whole system will shut down. First, we will consider systems that are not redundant and then consider systems that are in redundant.

a. No Redundancy in System

We can estimate the availability of a system that has components in series using the following equation:

$$A_{\text{Sys}} = (A_{\text{single component}})^n \tag{10}$$

Where A is availability and *n* is the total number of components in the system.

b. Redundancy in system

If the component has low reliability but the system requires a high availability, a redundant system is one solution to achieve the requirement. The engineer has to evaluate if it's more cost effective to design and build a high reliability component or to build a redundant system.

<u>Standby Reliability Model</u>
When identical components are in parallel and in a standby mode, only one component is activated at a time. If the active component fails the other component hooked up in parallel is switched on. The overall reliability is calculated as a two-part configuration: the reliability of the first component and the reliability of the second part, after the first part fails. Thus, the calculation becomes the unreliability of the first component multiplied by the reliability of the second part after the first part fails if we assume perfect switching. For components in parallel, we use the following equation to calculate MTBF:

$$\text{MTBF}_{\text{Set}} = \sum_{i=1}^{n} \frac{1}{\lambda_i} \tag{11}$$

where n is the number of identical component in parallel and λ is the failure rate of one component. Thus, for two identical components in parallel redundancy the expected MTBF of the set becomes 2/ λ. For example, if the MTBF of a motor is 50,000 hours, a redundant system with two identical motors will yield a MTBF of 100,000 hours.

<u>Standby Reliability with Repair</u>
For identical components that are in parallel and one is repaired without interrupting the system, the following reliability equation is used to calculate the set.

$k_1 = \lambda_1 + \lambda_2 + r$
$k_2 = \lambda_1 \lambda_2$

$$x_1, x_2 = \frac{-k_1 \pm \sqrt{k_1^2 - 4k_2}}{2}$$

$$\text{R(t)} = \frac{R(t) = (k_1 + x_1)e^{x_1 t} - (k_1 + x_2)e^{x_2 t}}{x_1 - x_2} = e^{-\lambda t} \qquad (12)$$

λ is the failure rate of the component, R is the reliability, t is 6480 hours which is the operation time for a one year period (Eberling, 1997).

Knowing the MTBF for the redundant set of components, availability of the redundant set can be calculated and the overall system availability can be calculated using Equation 10 and paying attention to the number of components in the system.

Step 6 Calculate MTBF and Downtime

Knowing the availability of the entire system, the MTBF for the entire system can be calculated using Equation 7. The expected operating hours for the ILC is 6480 hours/year. Thus, the downtime of the accelerator can be predicted using the following equation:

$$\text{Downtime} = (1\text{-Availability}) \times 6480 \text{ hours}$$

Step 7 Calculate Frequency

Knowing downtime and the MTTR for the system, failure frequency per year can be calculated using the following equation:

$$\text{Frequency (Failure/year)} = \frac{Downtime}{MTTR}$$

To predict specific types of failures as defined in the FMEA table, one can follow steps 4 through 7 for each individual failure modes or root causes. It is critical to find the root cause of each failure from the CATER system to conduct this analysis. This further analysis will result in creating several versions of table 6.

4.2. Reliability Estimation from Distributions

When a new design is being introduced and no field data exists, we have to rely on manufacturer's reliability data or use time-to-failure distributions. The most popular failure distributions are the Weibull, normal, and exponential distributions.

The normal distribution is frequently used to model quality related characteristics and sampling measures. It is widely used for process behaviors for quality control purposes. It is symmetrical and has a single mode. Despite its popularity it is probably the most overused and incorrectly used distribution (Wasserman, 2003). In the real world, processes are noisy and do not conform to a nice bell shape curve. It also has infinite tails at both ends. Since ILC failures are not process oriented failures, we will not use the normal distribution.

4.2.1. Exponential distribution

The exponential distribution is widely used in electronics and probabilistic modeling. It is applicable for modeling constant failure-rate phenomena.

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

The unique property of the exponential distribution is:

$$MTTF = \int_0^\infty R(t) = \frac{1}{\lambda}$$

The exponential distribution is widely used for modeling time-to-failure of electronic components. It is also widely used to model failure at the system level. Component manufacturers usually specify the MTTF for their component and this value can be used to model the overall MTTF of the system.

When multiple components are in series and if one fails the whole system shuts down, the MTBF of the overall system uses the following equation:

$$MTBF = \sum_{i=1}^{n} \frac{1}{\lambda_i} \tag{13}$$

where n is the number of components in the system. Thus, for *n* components of identical failure rate λ, the expected MTBF = n/λ.

4.2.2 Weibull distribution

Weibull is a distribution that can be modeled for a wide range of phenomena. The Weibull distribution is expressed in the form of:

$$\lambda(t) = \frac{\beta}{\theta}(\frac{t}{\theta})^{\beta-1}$$

Where λ is decreasing with time for $\beta<1$; it is increasing with time for $\beta>1$; and $\beta=1$ corresponds to a constant failure-rate. β is the shape factor and θ is the mean time to failure. The three parameter Weibull distribution is used to model phenomena that take a shortest time to evolve, such as failures due to fatigue, corrosion, creep, and other degradation phenomena.

Weibull analysis is extensively used to study mechanical, chemical, electrical, electronic, material, and human failures. The primary advantages of the Weibull analysis are its abilities to:

- Provide moderately accurate failure analysis and failure forecasts with extremely small data samples, making solutions possible at the earliest indications of a problem.
- Provide simple and useful graphical plots for individual failure modes that can be easily interpreted and understood, even when data inadequacies exist.
- Represent a broad range of distribution shapes so that the distribution with the best fit can be selected.
- Provide physics-of-failure clues based on the slope of the Weibull probability plot.

Although the use of the normal or lognormal distribution generally requires at least 20 failures or knowledge from prior experience, Weibull analysis works extremely well when there are as few as 2 or 3 failures, which is critical when the result of a failure involves safety or extreme costs. Parameters for the Weibull distribution for most components can be found in many references (http://www.barringer1.com/wdbase.htm).

Using distribution systems to model the MTBF in Excel will be discussed in the following section, Monte Carlo Simulation.

4.3. Mixture of Data

A system is most likely to be assembled with many components or subsystems. In order to predict an accurate overall MTBF, components operated under similar environmental conditions to the new system whenever possible. This means some subsystem may have empirical data and some may not. Using equation 12, we can predict the MTBF for any given system with data that from a combination of empirical data, manufacturer's test data, and Weibull failure distribution. Modification factors in equation 6 are based upon testing and historical data. If the values are unknown, "1" will be used as the modification variable.

5. Monte Carlo Simulation

Life Cost-Based FMEA as described up till now uses point estimation for its analysis. The danger with using point estimation is the potential for misinterpretation of the average numbers. Strategy based on average conditions can be false since one does not know if the condition has reached the upper or lower thresholds. A sensitivity analysis on the estimates will provide better confidence in the result and make for a better understanding of which variables are the cost drivers.

5.1 Modeling Time

A Monte Carlo simulation is applied to the Life Cost-Based FMEA to perform a sensitivity analysis on the variables associated to failure cost: detection time, fixing time, delay time, quantity, and parts cost. An example of a triangular distribution with minimum fixing time of 1.2 hours, mode of 2.5 hours and max value of 4.5 hours is shown in Figure 4. A triangular distribution using minimum, mode, and maximum value was used. There are many distribution systems one can use for the simulation; however, with limited past history data and using estimated variables, a triangular distribution was selected. There are several commercial software programs for applying a Monte Carlo simulation; we have used **Crystal Ball v2000.2** in our analysis.

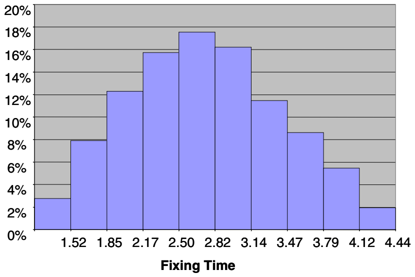

Figure 4. Triangular Distribution (Min: 1.2, Mode: 2.5, Max: 4.5)

For each time category, the users must decide what the minimum, mode, and maximum values will be. These values are acquired using empirical data or expert opinion. The steps to applying Monte Carlo simulation in the Crystal Ball software are as follows:

1. Move the cursor to the cell that requires a distribution analysis
2. Select “Define Assumption” icon on the menu bar
3. From the popup window, select “Triangular Distribution” and click “OK” button.
4. Input the 3 values : Min, Likeliest, Max
5. Repeat steps 1 through 4 for all unknown variables.
6. Move the cursor to the cell that sums up the total cost
7. Select “Define Forecast” button on the main menu
8. Type in Forecast Name (e.g. “Labor Cost”)
9. Go to the menu bar and under “Run” select “Run Preferences”
10. Type “5000” under maximum number of trials and select “OK” button.
11. Select “Run” under the run menu bar.
12. Several popup windows should appear that correspond to the forecast name that was specified in step 8. (Figure 5)

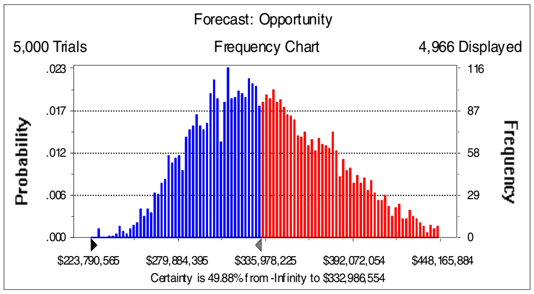

Figure 5. Distribution of Opportunity Cost

13. Sensitivity analysis on each forecast can be made through sliding the triangle icon on underneath the distribution curve and reading the certainty level. More detail on how to interpret these graphs will be given in section 6.

5.2 Modeling MTBF using Weibull distribution

For components or subsystems where empirical data does not exist, MTBF can be modeled using Crystal Ball.

1. Move the cursor to the cell that requires a Weibull distribution analysis and type in the typical MTBF for that particular component
2. Select “Define Assumption” icon from the menu bar
3. From the popup window, select “Weibull Distribution” and click “OK” button.
4. Type in the location, scale, and shape factors from the table
5. Move the cursor to the cell that sums up the total cost
6. Select “Define Forecast” button on the main menu
7. Type in Forecast Name (e.g. “Labor Cost”)
8. Go to the menu bar and under “Run” select “Run Preferences”
9. Type “5000” under maximum number of trials and select “OK” button.
10. Select “Run” under the run menu bar.
11. Several popup windows should appear that correspond to the forecast name that was specified in step 8.

5.3. Modeling Parts Cost

Material cost which is a product of parts cost and quantity affected can be simulated using the steps in 5.1 and 5.2. Triangular distribution for cost of parts and quantity are used.

6. How to Interpret and Use Results

The failure cost for each failure scenario will be calculated on each row of the Lifecycle Cost based FMEA sheet (Table 5). Labor cost and Material cost are the expected direct cost for the failures. Opportunity cost does not incur an extra cost to run the ILC but it is expenses lost due to the collider not operating. The failure cost is also plotted after running the Monte Carlo simulation (Figure 5)
You should consider mitigating the high failure costs (sum of labor and material costs) through 3 different strategic abatements:

6.1 Higher reliability

This approach is taken for failures that have high frequency. If it is a component failure, you should consider using a component with a higher MTBF or making the system redundant to achieve an overall higher reliability. You will need to conduct a lifecycle cost analysis to compare the two different possibilities and conduct trade-off analysis.

6.2 Design for serviceability

This approach tries to reduce the downtime of the collider and reduce the fixing time. You may consider relocating components or sub-systems with higher failure frequency to a location that is more accessible once the cover is opened up. Designing special tools or jigs to make the components more serviceable is another possibility.

6.3 Design diagnostic capability

This approach can be effective for failures that can be predicted with an early detection system. Sensors are quite affordable these days and alerting the user ahead of the actual failure can be quite economical for cases where higher reliability is not feasible. Printers for example alert the user the toner is low 500 pages before it stops printing. Thus, the user has ample time to order a new set of toner and replace it before the printer becomes inoperable.

6.4 Examples of Regular FMEA and Life Cost-Based FMEA

Spencer took part in a regular FMEA process on a water-cooled electromagnet for a particle accelerator (Bellomo, 2000; Rago, 2002). Both authors developed the life cost-based FMEA using systems of electromagnets and permanent magnets (Rhee, 2003; Rhee, 2004).

REFERENCES

AIAG (1995): *Potential Failure Mode and Effect Analysis (FMEA) Reference Manual,* Automotive Industry Action Group. www.aiag.org, 4th edition is latest.

Bellomo, Paul (2000) and Carl E. Rago, Cherrill M. Spencer, Zane J. Wilson, "A Novel Approach to Increasing the Reliability of Acclerator Magnets", IEEE Transactions on Applied Superconductivity, 10 (1), (2000) p. 284,

Crosby, Philip, B., (1969). *Cutting the Cost of Quality: The Defect Prevention Workbook for Managers*, Boston, MA, Industrial Education Institute

Ebeling, Charles, (1997). *An Introduction to Reliability and Maintainability Engineering*, McGraw-Hill Science/Engineering/Math, New York

Ishikawa, Kaora, (1985). *What is Total Quality Control? The Japanese Way*, Prentice Hall, Englewood Cliffs, London, UK, pp. 44-5.

Palady, Paul (1995) *Failure Modes and Effects Analysis: Predicting and Preventing Problems Before They Occur,* Atlantic Books

Rago, Carl E. (2002) and Cherrill M. Spencer, Zachary Wolf, Gerald Yocky, "High Reliability Prototype Quadrupole for the Next Linear Collider", IEEE Transactions on Applied Superconductivity, 12 (1), (2002) p. 270

Rhee, Seung J. (2003) and Cherrill M. Spencer, "Cost based failure modes and effects analysis (FMEA) for systems of accelerator magnets", Proceedings, Particle Accelerator Conference, May 2003.
http://warrior.lbl.gov:7778/PAC_PUBLIC/view_pac.display_abstract?this_id=3327

Rhee, Seung J. (2004) and Cherrill M. Spencer, "Comparison Study of Electromagnet and Permanent Magnet Systems for an Accelerator Using Cost-Based Failure Modes and Effects Analysis ", IEEE Transactions on Applied Superconductivity, 14 (2), (2004) p.413

Stamatis, D.H (1997) *Failure Mode and Effect Analysis: FMEA from Theory to Execution,* ASQC/Quality Press. 2nd edition released in 2003.

Wasserman, Gary S., (2003), *Reliability Verification, Testing, and Analysis in Engineering Design*, Marcel Dekker Inc., NY, NY