PRODUCT DESIGN FOR RELIABILITY

LebenTech ®

Innovative Solutions Inc.

BY: LENNOX BENNETT

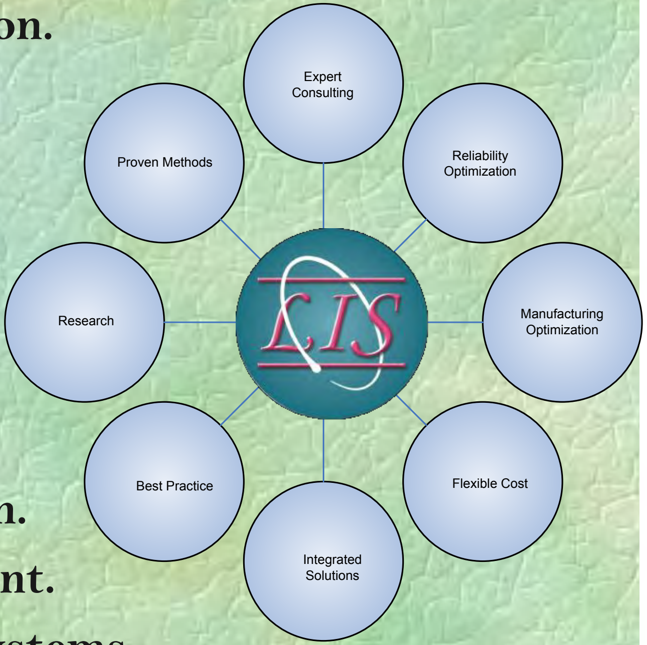
TRAINING PROGRAM FLOW CHART

DAY	DURATION		MODULES	DESCRIPTION
1	1^{15}	9:15 – 10:30 AM	1	Design for Reliability Fundamentals
	2^{45}	10:30 – 1:15 PM	2	Process for Developing Reliable Systems
	2^{25}	1:50 – 4:15 PM	3	Design and Analysis of Experiments
	1^{15}	4:30 – 5:45 PM	4	Human Factors in Reliable Design
2	8^{15}	1 - 9:15 – 10:30 AM 2 - 10:35 – 12:30 PM 3 - 1:20 – 2:00 PM 4 - 2:05 – 4:05 PM 5 - 4:15 – 5:45 PM	5	Design Verification and Validation Testing
3	2^{30}	9:15 – 11:45 AM	6	Product Risk and Safety Evaluation
	1^{25}	12:35 – 2:00 PM	7	Models for Product Warranties
	3	2:05 – 5:20 PM	8	Software Reliability Design Analysis and Testing

WHAT LebenTech DO

Demonstrated Capabilities Includes:

- Reliability, Availability, and Maintainability [RAM] Analysis.
- Equipment failure and repair data acquisition and analysis.
- Productive system case study and evaluation.
- Customize training for personnel.
- Equipment life cycle cost analysis.
- Asset improvement optimization.
- Operation research.
- Reliability testing and analysis.
- Production reliability model development.
- Reliability and manufacturing optimization.
- Productivity measurement and improvement.
- Modeling and analysis of manufacturing systems.
- FRACAS Implementation and management.
- Reliability program development and implementation.



– Proactive Innovative Solutions for Success and Competitive Advantages

CORPORATE HEADQUARTERS

Presenter: Lennox Bennett

Sample Road Coral Springs | FL 33067 | 954 – 796 – 7107 | info@lebentech.com | www.lebentech.com

THE THREE DAYS PROGRAM

Based on Key Principles

This seminar integrates strategies, applications and results. You will not only learn how to implement a design for reliability program and methods for enhancing product design, but also be informed of cost implications, emphasizing how they can influence you to develop a reliable design.

- ❑ For sustained growth and to thrive in a competitive market your company must manage the product design process more effectively and efficiently than your competitors.
- ❑ Acquiring the benefits of product design for reliability requires a significant change that begins with creating a reliability culture. This requires dedicated support from top management throughout the organization.
- ❑ Your participation in this seminar will enable you to avoid the trap of piecemeal reliability. You will walk away with a true vision and perspective of a structured approach to designing reliability into product.
- ❑ It is difficult to be profitable if you cannot achieve reliability at a reasonable price. Reliability begins with robust design, procurement and installation then there is transfer to operations and maintenance. A common reliability vision that represents the company's interest should be established.

FOCUS OF EACH DAY PRESENTATION

Day 1

- Provides the value proposition for a cohesive, business driven product design reliability strategies and creates foundation of understanding of the principal tools required to manage or determine product reliability and the impact of human factors in reliable design.
- Participants will be exposed to various concepts and reliability methods that can be utilized to develop a reliable system. They will also be provided with the opportunity of learning how to incorporate statistical thinking to optimize product design parameters.

Day 2

- Addresses how various testing strategies are utilized to characterized, verify, validate product reliability requirements and improve product reliability during development. We will also discuss how reliability engineering data analysis will enable you to make more effective decisions and manage risk.
- On this day we will discuss how to instill performance metrics that are proactive and is focused on verification of design adequacy. We will illustrate how these technique are used for quantifying and improve product reliability in the development phase.

FOCUS OF EACH DAY PRESENTATION

Day 3

- Focuses on emphasizing methods of evaluating product design risks, integrating DFR with Safety, and serves to quantify the contribution of reliability and risk to safe performance of the product.
- A comprehensive analysis is provided regarding designing products for warranty cost reductions. Participants will be presented with opportunities to solve various problems associated with product warranty claims. We will also discuss methods of optimizing warranty period.
- On this day we extend the discussion to incorporate various approaches utilized in the process of testing software based on different objectives. A limited segment of the time is devoted to software verification techniques and software system safety.
- We also present various methods that are used to develop reliable software. A special emphasis is given to software testing strategies and elements of the testing process.
- Last but not least the discussion will culminate with validating software for reliability.

BENEFITS FOR ATTENDING SEMINAR

Participants shall leave the seminar with the following specific information and concepts:

- Knowledge for the implementation and application of reliability concepts and techniques learned that will create value in business operations.
- Information necessary for developing and designing products to function for reliability.
- Understanding of how reliability engineering data analysis will enable them to make more effective decisions and manage risk.
- Knowledge of how to apply RCFA to get out of the cycle of recurring failures caused by doing the same thing but expect different results.
- Methods of how to approach reliability as a collaborative process between management, design, procurement, operations and maintenance.
- Top management perspective of the strategic importance of product reliability management for business success.
- General competence and understanding of the best tools and methods needed to implement and sustain a successful product reliability program.

BENEFITS FOR ATTENDING SEMINAR

Strategic and Competitive Benefits of Attending and Implementing What you Learn

Table 1-1: Impact of implementing what is learned

Strategic Advantages	Competitive Advantages
Achieve and sustain Profitability.	Better product development strategy.
Teams walk away with a common vision and understanding of DFR.	Increased availability – more time operating and output per hour.
Increase customer satisfaction.	Reduction in cost of unreliability.
Helps develop a reliability leader.	Proactive reliability driven maintenance.
Improved safety.	Low system maintenance cost – company's with the highest product reliability have the lowest maintenance cost.
Confidence in design and reliability process.	Better managed and controlled process.
Helps reduce product vulnerability.	Survival in a competitive market.

M1 - LEARNING OBJECTIVES

Participant Shall be able to:

- ♦ Determine the cost consequences of poor product reliability.
- ♦ Recognize and develop reliability specification for their products.
- ♦ Develop and implement a generic DFR process for their company's product | system design.
- ♦ Develop general understanding of how reliability techniques are applied to design robust products.
- ♦ Gain understanding of concepts, metrics, and methods used in reliability, when to apply a specific tool during the product development life cycle.
- ♦ Adapt and effective reliability culture within their organization and helps determine what needs to be added or improved in their DFR initiative.

Adapt | Implement | Improve

INTRODUCTION

- Design for Reliability is a technical seminar designed to equip participants of varying backgrounds and from various industries with sufficient understanding regarding reliability assessment, methods used to ensure their company's products are reliably designed and parts are applied in a robust manner.

- This seminar presents an overview of the analytical tools utilized to ensure a robust design, minimal variations and discusses several considerations for ensuring a manufacturable product.

- To maximize return on net asset, company's must create a synergy between the affecting functions of a system and product design, procurement, product maintenance, product risk, product vulnerabilities, and product availability. This is the scope of integrating engineering design and reliability methods in product development.

- Selective application of hardware and software reliability methods will provide you with a better understanding of the strategic and engineering components of a successful reliability modeling and reliability program, and the analytical tools available to more effectively managed business risk relating to product development.

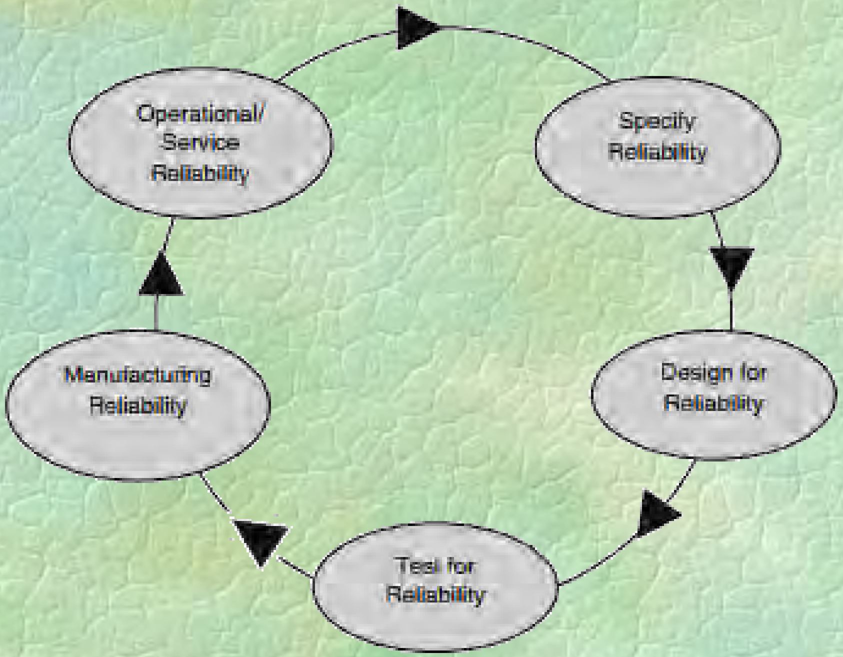
- This inaugural seminar will not only inform, but challenge every aspect about how you currently design your products.

ELEMENTS OF THE RELIABILITY CIRCLE

Specify Reliability

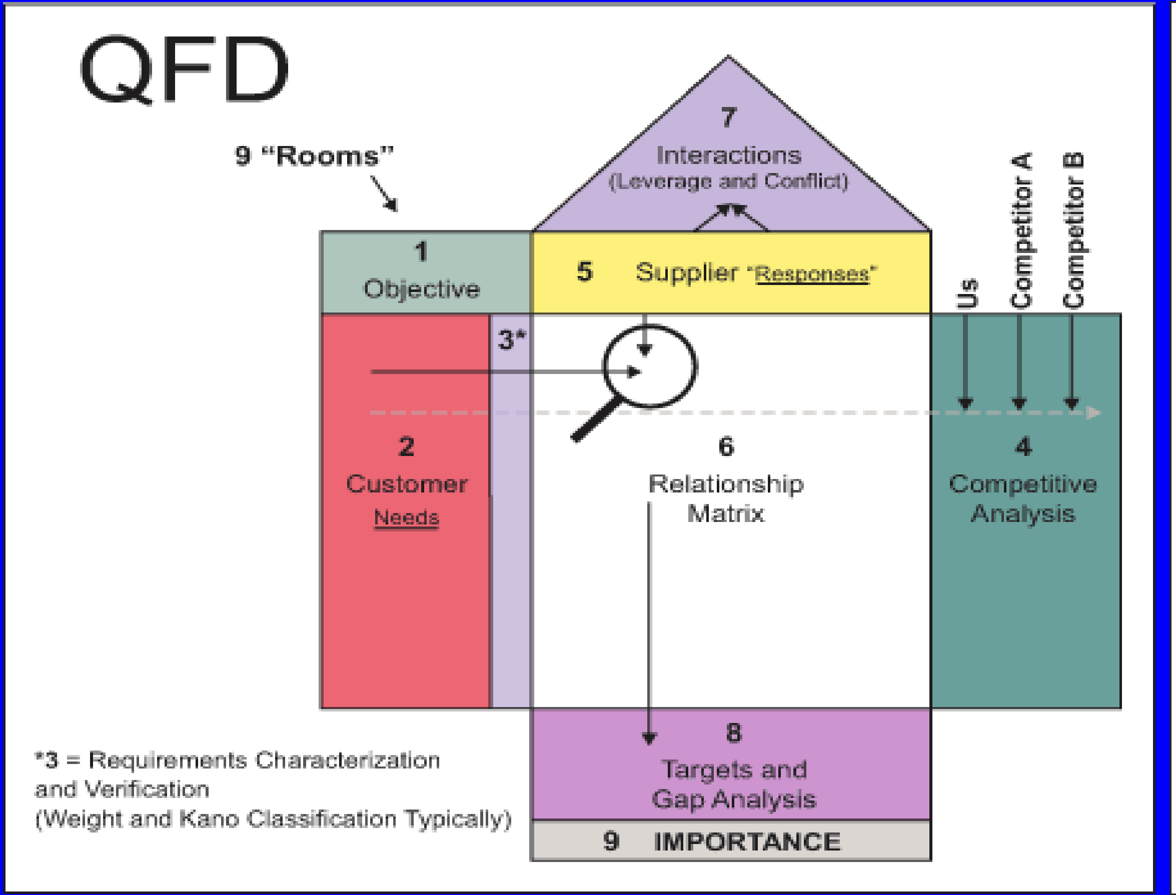
- ❑ The first step in the reliability circle is to establish the reliability specifications/targets.
- ❑ It is essential that the requirements come from customer needs and wants and program objectives.
- ❑ The following are the different methods to collect the reliability information: House of Quality (Customer needs and wants), customer surveys, benchmarking, customer duty cycles and environment, experience from similar existing products such as warranty data, etc.
- ❑ Gather the data from above sources and prioritize them to set the targets.
- ❑ Reliability requirements are statements that detail functional, mission oriented requirements with minimum Life Cycle cost, resources and maximum probability of success.

Figure 1-18: The Reliability Circle



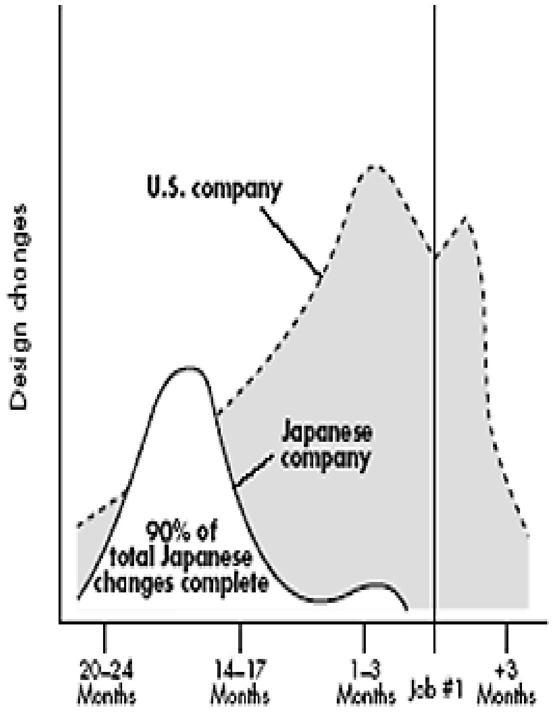
ELEMENTS OF THE RELIABILITY CIRCLE

Figure 1-1: Elements of Quality Function Deployment



*3 = Requirements Characterization and Verification (Weight and Kano Classification Typically)

Japanese automaker with QFD made fewer changes than U.S. company without QFD



ELEMENTS OF THE RELIABILITY CIRCLE

Overview of Design for Reliability

❑ Design for reliability objectives includes the identification of failure modes and means for preventing them or minimize the effects of these failure modes.

❑ It is possible by successful implementation of the techniques such as Failure mode and effects analysis, Fault tree analysis, stress analysis, reliability modeling, design of experiments, root cause analysis techniques and by implementing redundancy in the design. The reliability will be built into product by providing safety factors to the design.

❑ Other objective is reduction of variability in presence of the noise. It is achieved by applying design of experiments, parameter design and tolerance design during product design.

❑ The first major tool to be used is Failure Modes and Effects Analysis (FMEA). This is an important tool to ensure that reliability is integrated with product design.

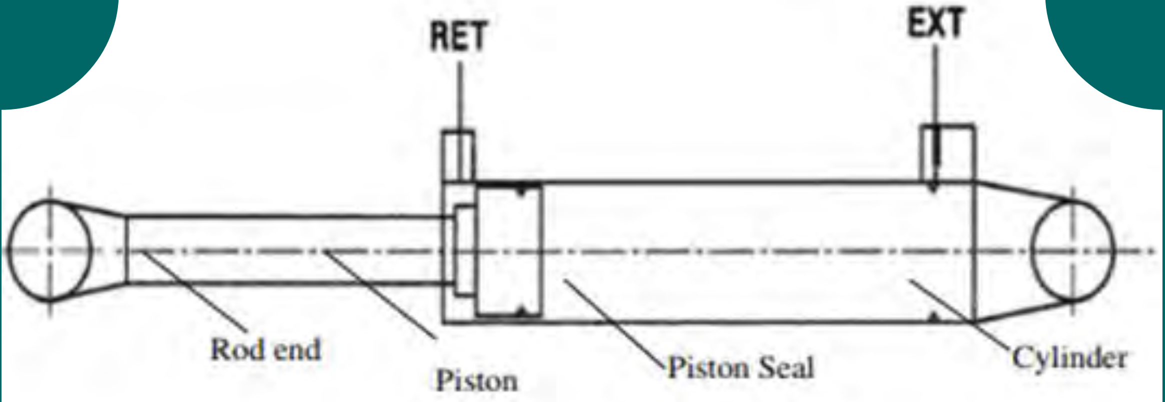
ELEMENTS OF THE RELIABILITY CIRCLE

Overview of Design for Reliability

- ❑ Reliability modeling is used to make initial product Reliability or failure rate estimates.
- ❑ These estimates are important in understanding the feasibility of a design’s capability of meeting the reliability goals needed to satisfy customer requirements.
- ❑ Also, such calculations direct and assist in the determination of design tradeoffs to ensure that the best design approach is taken.
- ❑ Example Application: Let’s calculate the reliability of an actuator (Figure 1-19)? Reliabilities of cylinder, piston, Rod end, and piston seal at 50,000 flight cycles are 0.992, 0.99, 0.995, and 0.97.
- ❑ Solution: Since all the components are essential for the successful extension and retraction of the actuator, all the components fit in a series reliability model.

ELEMENTS OF THE RELIABILITY CIRCLE

Figure 1-19: **Simplified Actuator**

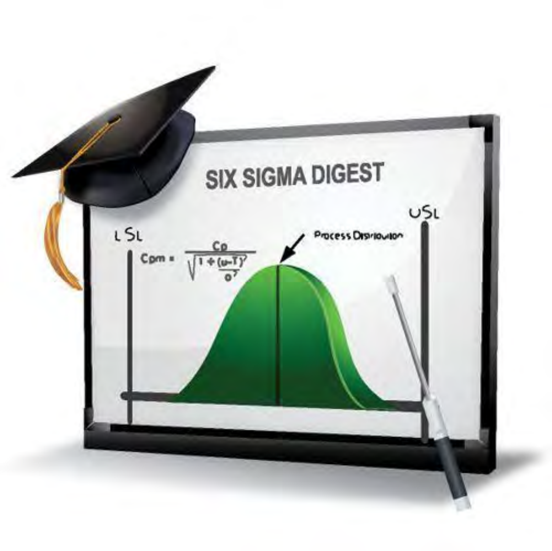


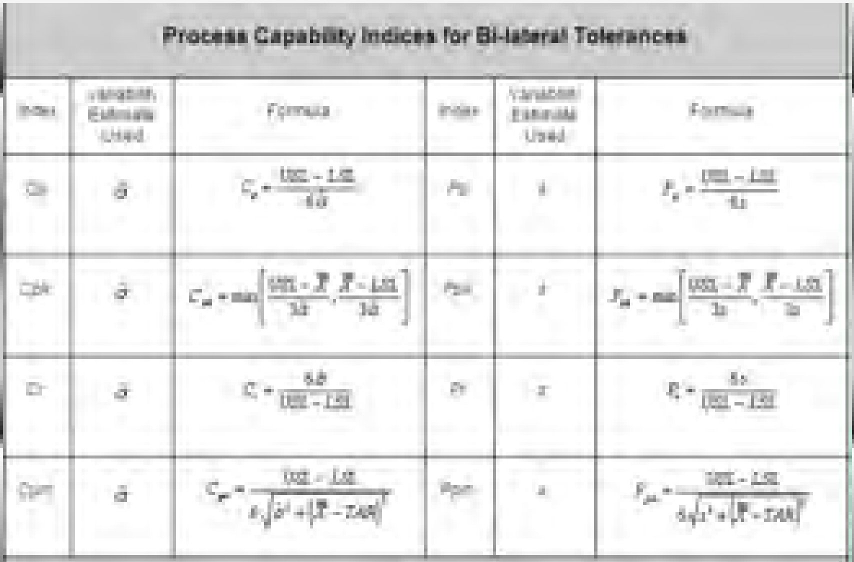
$$R_{\text{Actuator}} = R_{\text{Cylinder}} \times R_{\text{piston}} \times R_{\text{Rod end}} \times R_{\text{piston seal}}$$
$$= 0.992 \times 0.99 \times 0.995 \times 0.97$$
$$R_{\text{actuator}} = 0.9479 \text{ @50,000 flight cycles}$$

ELEMENTS OF THE RELIABILITY CIRCLE

Maintain the Manufacturing Reliability – Process Control Methods

- ❑ The manufacturing engineer is then responsible for ensuring that the manufacturing process does not deviate from the specifications.
- ❑ Here more aspects of reliability engineering discipline merge with quality engineering. Statistical Process Control (SPC) methods can be useful in this regard.
- ❑ HALT, Burn-in and Screening (HASS) are designed to prevent infant mortality failures, which are typically caused by manufacturing-related problems, from happening in the field.





Process Capability Indices for Bi-lateral Tolerances

Index	Variation Estimate Used	Formula	Index	Variation Estimate Used	Formula
Cp	$\hat{\sigma}$	$C_p = \frac{USL - LSL}{6\hat{\sigma}}$	Pp	s	$P_p = \frac{USL - LSL}{6s}$
Cpk	$\hat{\sigma}$	$C_{pk} = \min\left[\frac{USL - \bar{X}}{3\hat{\sigma}}, \frac{\bar{X} - LSL}{3\hat{\sigma}}\right]$	Ppk	s	$P_{pk} = \min\left[\frac{USL - \bar{X}}{3s}, \frac{\bar{X} - LSL}{3s}\right]$
Cr	$\hat{\sigma}$	$C_r = \frac{6\hat{\sigma}}{USL - LSL}$	Pr	s	$P_r = \frac{6s}{USL - LSL}$
Cpm	$\hat{\sigma}$	$C_{pm} = \frac{USL - LSL}{6\sqrt{\hat{\sigma}^2 + (\bar{X} - TAR)^2}}$	Ppm	s	$P_{pm} = \frac{USL - LSL}{6\sqrt{s^2 + (\bar{X} - TAR)^2}}$

WHAT CUSTOMERS CARES ABOUT

Motivation for DFR

- Product Life……….... i.e. useful life before product begins to wear-out
- Minimum Downtime……….. i.e. System Mean Time to Failure
- Stable Performance…………. i.e. number of operations, robust performance in various environment
- Operation at Test………. i.e. product performs at incoming test, diagnostics checks
- On Time Startup…………….. i.e. ease of device or system start ups, not dead on arrivals.

Old Measures [Internal]:

1. RMA rates.
2. Warranty Cost

New Measured Metrics (External)

1. Product Life-Cycle Costs.
2. Service Contract Metrics.
3. Consumer Operational Impact.

Key Considerations

Reliability in Product Designs

- ♦ Effective and reliable performance of equipment/system is imperative:

  1 – In world of reliability optimization.
  2 – In world of robust product design.

- ♦ Plan and execution of efficient and safe product operation.

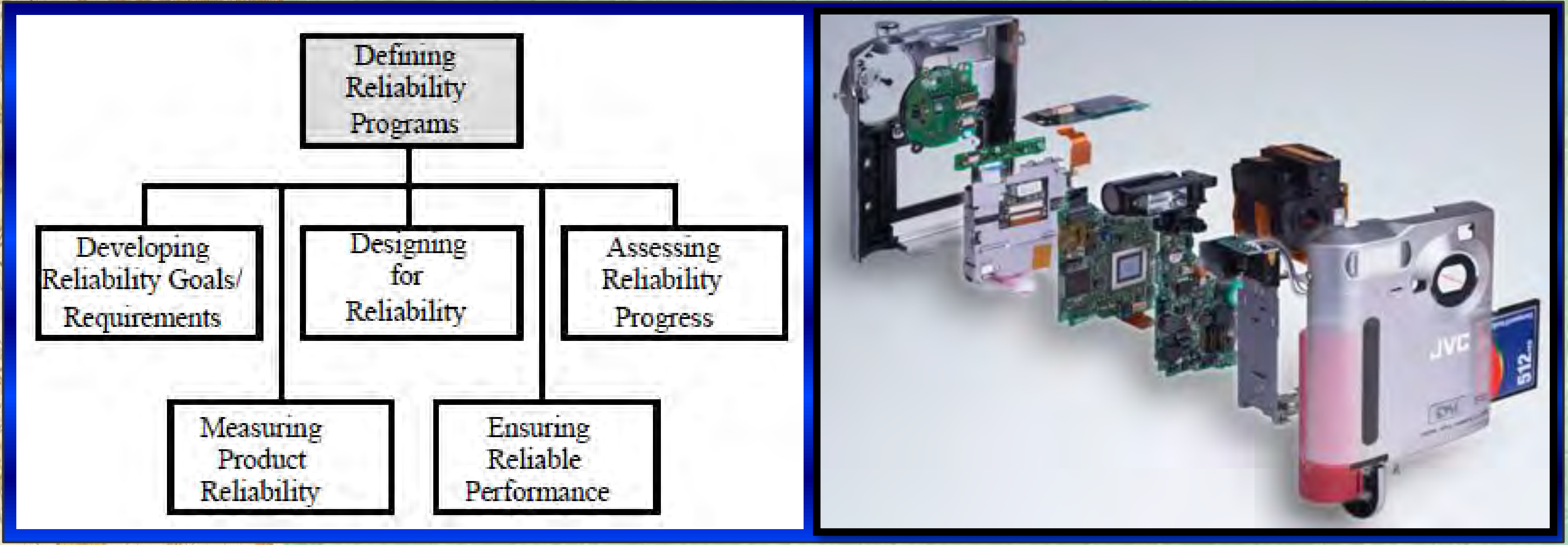
  1. Inherently requires effective risk reduction.
  2. Reliability analysis of critical components and subsystems.
  3. Evidence of equipment quantification through risk analysis.
  4. Regulation for risk assignment apply to all equipment critical to operation success.
  5. Operate to minimize risk associated with equipment.
  6. Risk analysis becomes safety issue.
  7. FDA requires risk analysis as portion of design control.

Associated risk render application of reliability engineering techniques imperative.

RELIABILITY APPLICATION IN NEW PRODUCT DESIGN

How is Reliability Designed into The Product?

Figure 1-4: RiAC Blue Print for Product Reliability



Defining Reliability Programs

Developing Reliability Goals/ Requirements

Designing for Reliability

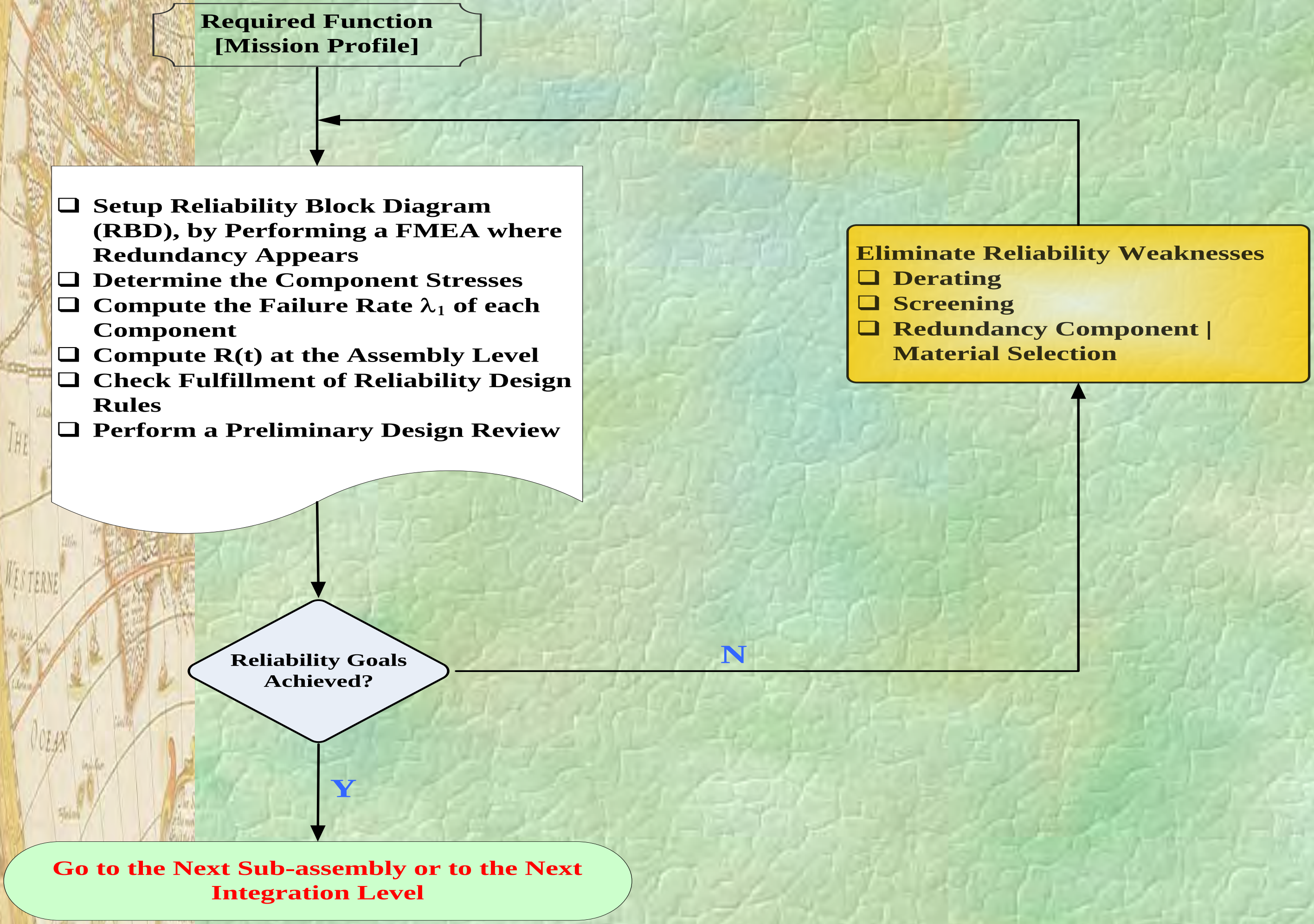
Assessing Reliability Progress

Measuring Product Reliability

Ensuring Reliable Performance

RELIABILITY APPLICATION IN NEW PRODUCT DESIGN

Figure 1-6: Reliability Analysis Procedure at the Assembly Level



Required Function
[Mission Profile]

- ❑ Setup Reliability Block Diagram (RBD), by Performing a FMEA where Redundancy Appears
- ❑ Determine the Component Stresses
- ❑ Compute the Failure Rate λ_1 of each Component
- ❑ Compute R(t) at the Assembly Level
- ❑ Check Fulfillment of Reliability Design Rules
- ❑ Perform a Preliminary Design Review

Reliability Goals Achieved?

N

Eliminate Reliability Weaknesses

- ❑ Derating
- ❑ Screening
- ❑ Redundancy Component | Material Selection

Y

Go to the Next Sub-assembly or to the Next Integration Level

RELIABILITY ENGINEERING CONCEPTS

What is Reliability?

- **For the Customer:**

A reliable medical device does what the customer wants to do, when the customer wants to do it.

Translation

- **For the Designer**

The reliability of the medical device is the probability, at a desired confidence level, that the medical device will perform its function, without failure, under pre-established conditions, during a specified period of time.

COMMON USEFUL FUNCTIONS IN DFR

Five Common Functions in Reliability

Reliability Function

- The reliability function can be derived using definition of the cumulative distribution function, $F(x) = \int_0^x f(s)ds$. From our definition of the *cdf*, the probability of an event occurring by time t is given by:

$$F(t) = \int_0^t f(s)ds$$

- Or one could equate this event to the probability of a unit failing by time t. Since this function defines the probability of failure by a certain time, we could consider this the unreliability function.
- Subtracting this probability from 1 will give us the reliability function, one of the most important functions in life data analysis. The reliability function gives the probability of success of a unit undertaking a mission of a given time duration. Figure 1-14 illustrates this.

RELIABILITY FUNCTION AND ITS APPLICATION

Reliability Function R(t)

The reliability of a product is the probability that it does not fail before time t. It is therefore the complement of the CDF:

$$\mathbf{R}(\mathbf{t}) = \mathbf{1} - \mathbf{F}(\mathbf{t}) = \mathbf{1} - \int_0^t \mathbf{f}(\mathbf{t})\,\mathbf{dt}$$

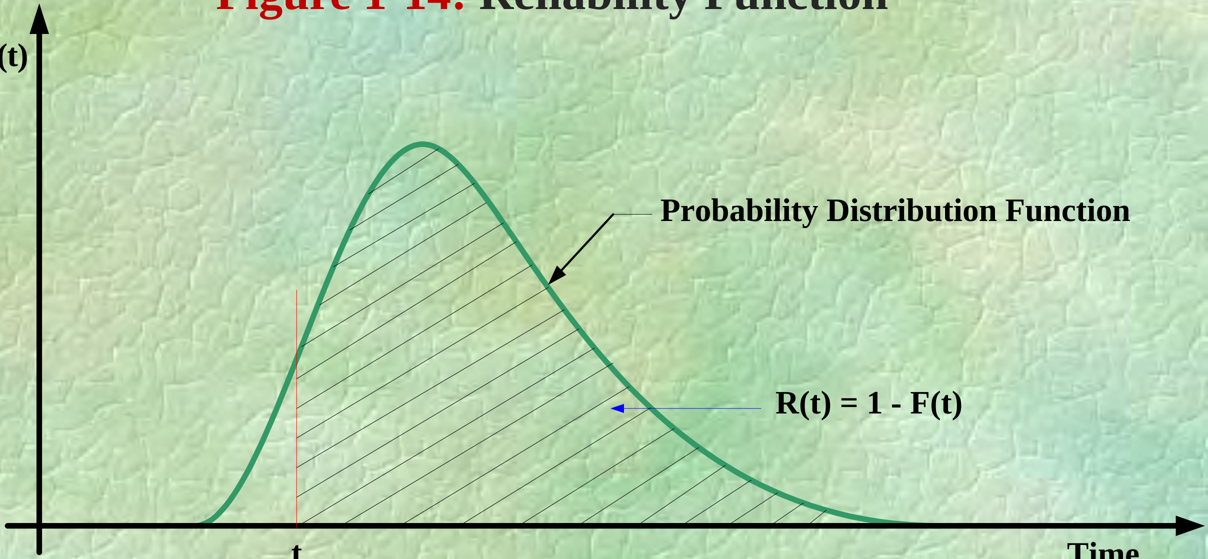
Typical Characteristics:

- ❑ When t = 0, R(t) = 1
- ❑ When t $\longrightarrow$ ∞, R(t) $\longrightarrow$ 0

or

$$\mathbf{R}(\mathbf{t}) = \int_t^\infty \mathbf{f}(\mathbf{t})\,\mathbf{dt}$$

Figure 1-14: Reliability Function



RELIABILITY FUNCTION AND ITS APPLICATION

Example Application

Time to failure distribution of a computer memory chip follows normal distribution with mean 9000 hours and standard deviation 2000 hours. Find the reliability of this chip for a mission of 8000 hours.

SOLUTION

Using Table 1-6, the reliability for a mission of 8000 hours is given by:

$$\mathbf{R}(\mathbf{t}) = \Phi\left(\frac{\boldsymbol{\mu}-\mathbf{t}}{\boldsymbol{\sigma}}\right) = \Phi\left(\frac{9000-8000}{2000}\right) = \Phi(0.5) = 0.6915$$

Reliability function, R(t), is defined as the probability that the system will not fail during the stated period of time, t, under stated operating conditions. If TTF represents the time-to-failure random variable with failure function (cumulative distribution function) F(t), then the reliability function R(t) is given by: R(t) = P{the system doesn't fail during (0 , t)} = 1 - F(t)

UNDERSTANDING RELIABILITY SPECIFICATIONS

Common Reliability Specifications

- At a minimum, a reliability specification (Quantitative) should consist of three basic components.
  1. A specified reliability.
  2. Time associated with specified reliability.
  3. A desired confidence level.

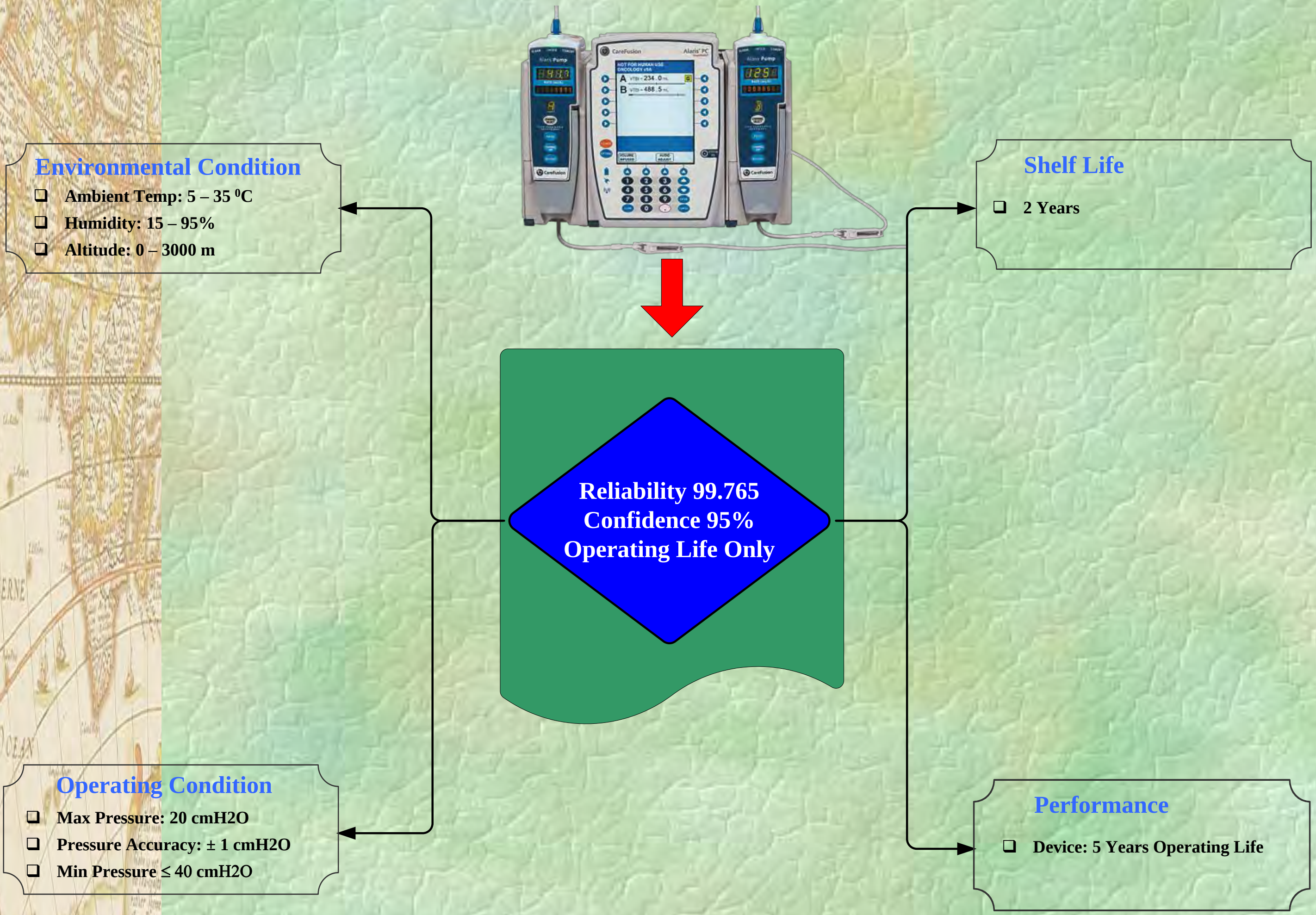
- Consideration is also given to:
  1. Normal environmental condition.
  2. What constitute a failure.
  3. Measurement of time.
  4. Frequency and type of preventive maintenance.

- MTBF (after a specific time)
  1. 99% reliability after 2 years of operation with 95% confidence level.
  2. A scale of measurement of time must be set (Hours, cycles, shelf life, etc.).
  3. The meaning of failure must be absolutely clear (Written definition).

- Mean Time to Fail (MTTF): Not appropriate for use as a sole reliability metrics.

UNDERSTANDING RELIABILITY SPECIFICATIONS

Figure 1-17: What Reliability Goals are Appropriate for the Insulin Pump



Environmental Condition

- ❑ Ambient Temp: 5 – 35 ^{0}C
- ❑ Humidity: 15 – 95%
- ❑ Altitude: 0 – 3000 m

Shelf Life

- ❑ 2 Years

Reliability 99.765
Confidence 95%
Operating Life Only

Operating Condition

- ❑ Max Pressure: 20 cmH2O
- ❑ Pressure Accuracy: ± 1 cmH2O
- ❑ Min Pressure ≤ 40 cmH2O

Performance

- ❑ Device: 5 Years Operating Life

ELEMENTS OF RELIABILITY REQUIREMENTS

Fundamental Elements for Consideration

- **Measurable**

  Reliability specification are best represented as probability statements that are measured by analysis or test during product development.

- **Customer usage and operating environment**

  In developing specifications consideration must be given to the use and conditions for application.

- **Confidence**

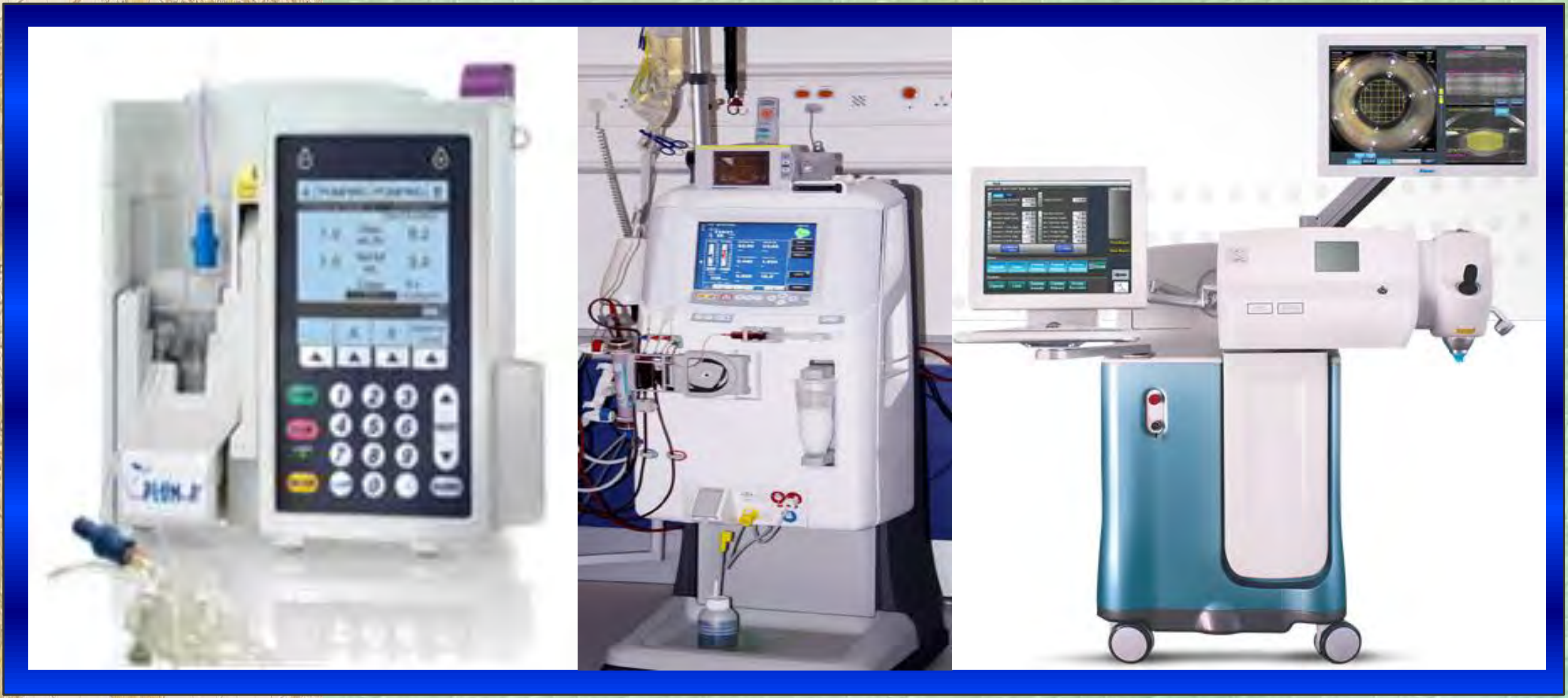
  A confidence level should be specified for a reliability requirement. This allows for variation in data when compared with specification.

- **Time | Age**

  Could mean hours, years, cycles, mileage, actuations (Whatever is associated with age of the equipment). For example 90% reliability at 10,000 actuations.

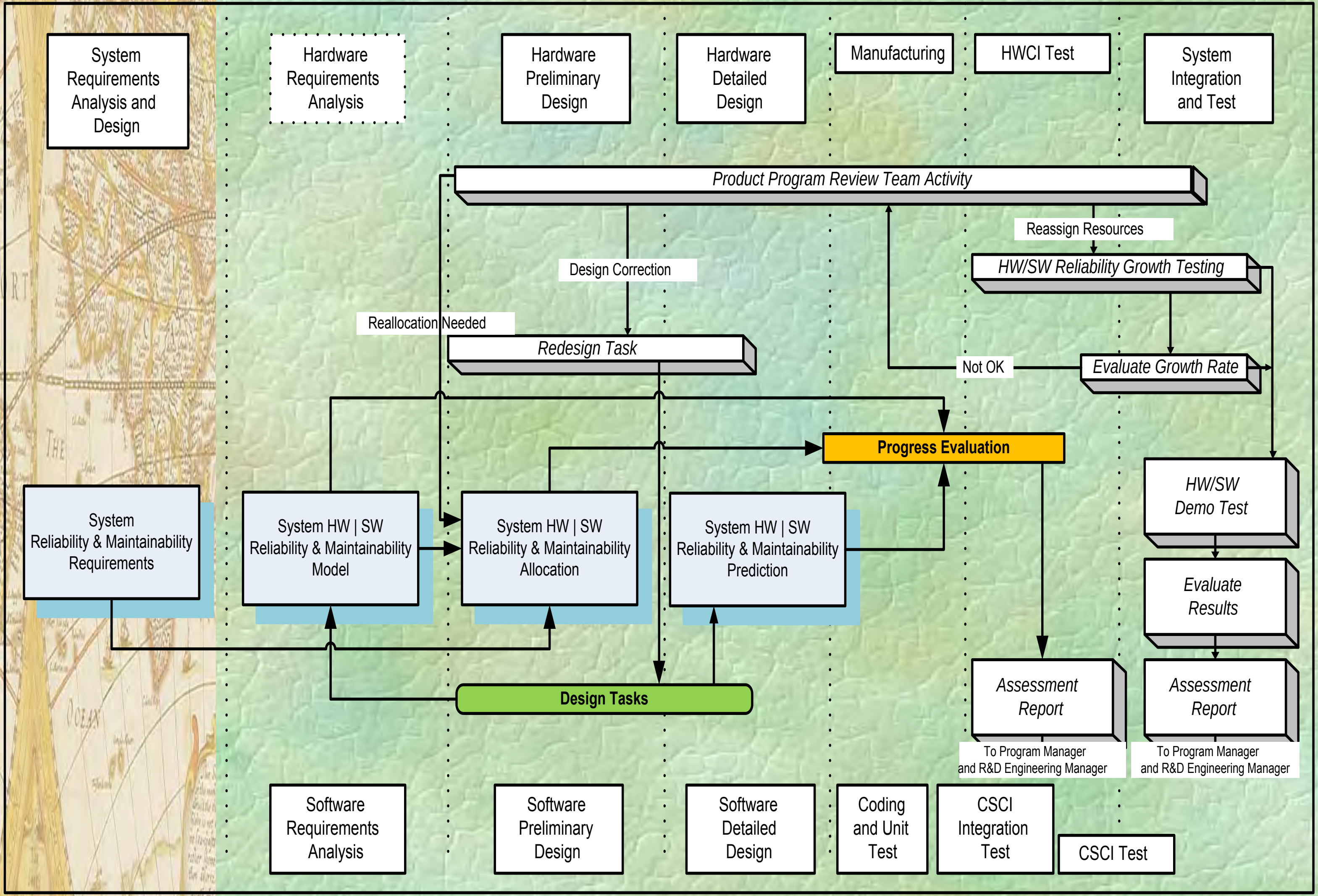
HW AND SW RELIABILITY APPLICATION

Figure 1-23: Clinical Medical Devices – Infusion Pump | Dialysis Machine | LexSx® Laser



SYSTEM RELIABILITY APPLICATION

Figure 1-27: System Reliability And Maintainability Tasks


System Requirements Analysis and Design
Hardware Requirements Analysis
Hardware Preliminary Design
Hardware Detailed Design
Manufacturing
HWCI Test
System Integration and Test
Product Program Review Team Activity
Reassign Resources
HW/SW Reliability Growth Testing
Design Correction
Reallocation Needed
Redesign Task
Not OK
Evaluate Growth Rate
Progress Evaluation
System Reliability & Maintainability Requirements
System HW | SW Reliability & Maintainability Model
System HW | SW Reliability & Maintainability Allocation
System HW | SW Reliability & Maintainability Prediction
HW/SW Demo Test
Evaluate Results
Design Tasks
Assessment Report
To Program Manager and R&D Engineering Manager
Assessment Report
To Program Manager and R&D Engineering Manager
Software Requirements Analysis
Software Preliminary Design
Software Detailed Design
Coding and Unit Test
CSCI Integration Test
CSCI Test

– Proactive Innovative Solutions for Success and Competitive Advantages

DESIGN PHASE RELIABILITY TOOLS

Table 1-10: Techniques that can be Applied to Improve Reliability

Item No.	Reliability Tools	Comments
1	Reliability Growth Tests	A test that identifies problems and solves them as the design progresses. Thus, is essentially, a “test, analyze, and fix” method that is used in a closed-loop corrective action manner
2	Durability Tests	Typically, Accelerated Tests that determine the failure rate for the entire expected life. Duplicates field failures by providing a harsher but representative environment. Performed instead of testing under normal conditions in order to eliminate testing that would otherwise take months or years.
3	Qualification Tests	Consist of stressing the product for all expected failure mechanisms. The test can be stopped if there are no failures during the expected life—thus, are performed to measure the achievement of the reliability requirement.
4	Demonstration Tests	Design Approval Tests are similar and usually require stressing during only a portion of the useful life.
5	Compliance Test	Test executed to ensure product performance complies with specific standards such as: IEC – 60601-1-2, UL , DOE 160E, AND MIL-STD-810

USE APPLICABLE ENGINEERING TEST

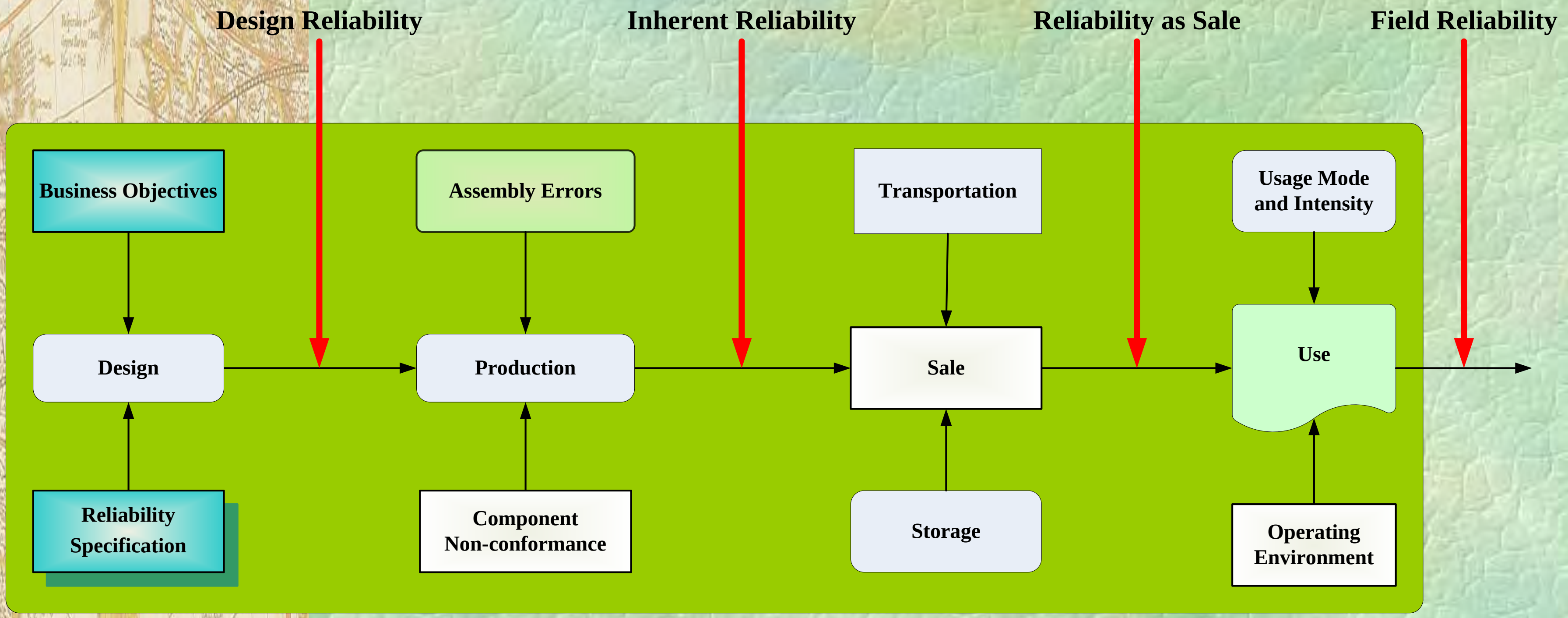
MANUFACTURING PHASE RELIABILITY TOOLS

Table 1-12: Analytical Tools that Can be Applied to Prevent Failures and Prove Reliability

Item No.	Reliability Tools	Comments
	To Prevent or Reduce failures	
1	**Process Failure Mode, Effects, And Criticality Analysis:**	Used on the manufacturing process before it is installed. Similar to Design FMECA.
2	**Statistical Process Control**	Designed to ensure that the manufacturing process continues to produce products with no more than expected variation in the critical parameters. Often considered a test for determining the control of quality instead of reliability
	Analytical Tools to Prove Reliability	
1	**Environmental Stress Screening Tests:**	Also, known as **Burn-in and Screening Tests**. Tests to catch "infant mortality" failures. If the product is manufactured properly, these tests are not required. Note: These tests are also performed in the Design Phase such that early failures do not mask the true reliability. Unfortunately, these tests are sometimes used as the "final word." As a result, the screening may not be long enough and weak products may be provided to the customer.
2	**Production Reliability Acceptance Tests**	Also, known as **Failure Rate (MTBF) Tests.** Used to detect any degradation in the inherent reliability of a product over the course of production and to assure products being delivered meet the customer's reliability requirements and/or expectations (by testing a production lot and accepting or not accepting based on a sampling plan). Also, used to qualify new products.
3	**High Accelerated Stress Screening**	Is a quality control activity used to maintain reliability during the production process
4	**On-Going Reliability testing (ORT)**	**Provides assurance that the product design reliability shall be sustained over time.**

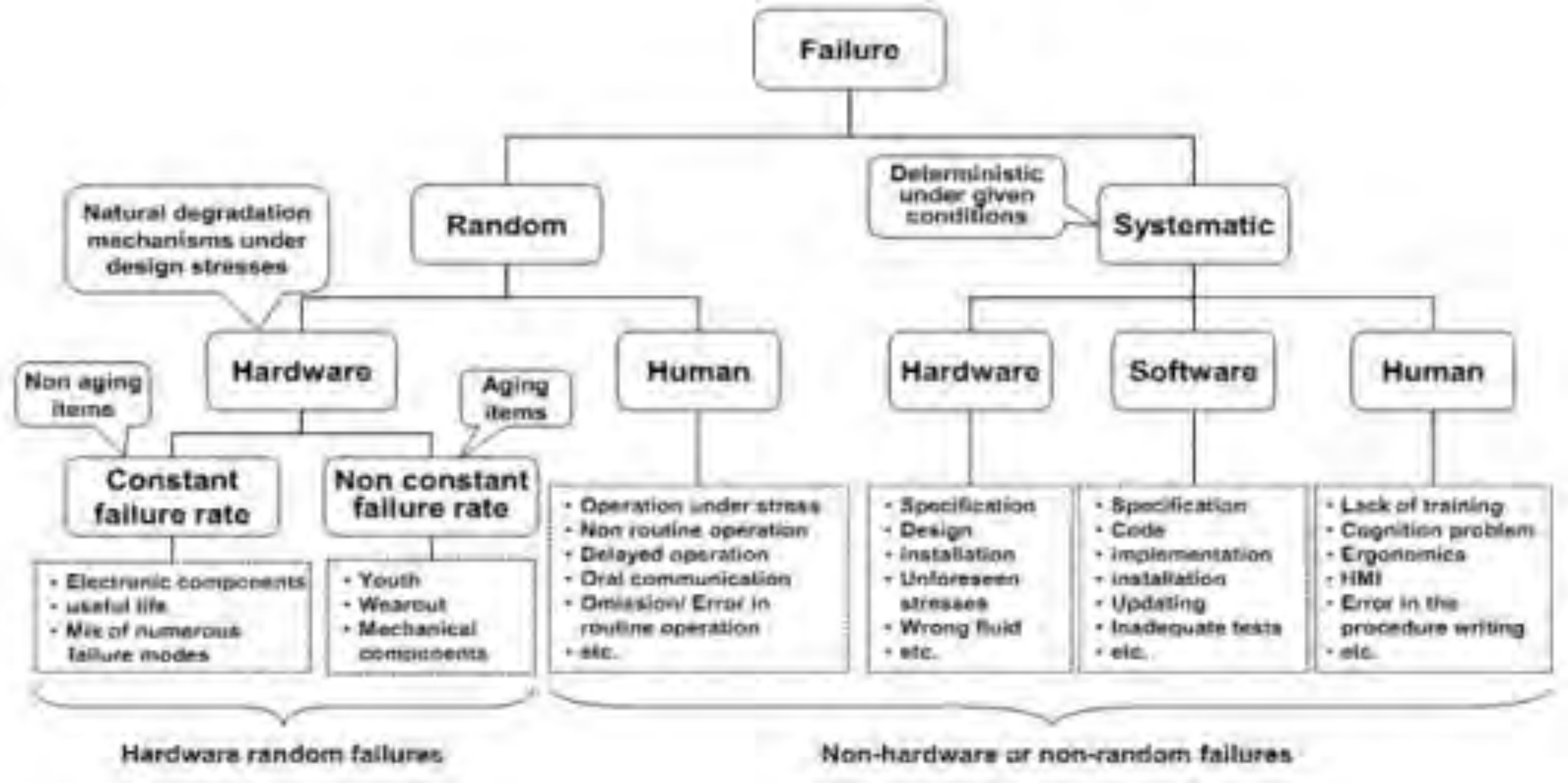
PRODUCT FIELD RELIABILITY PERFORMANCE

Figure 1-30: Factors Influencing Field Reliability



FAILURE DETAILS AND CATEGORIZATION

Figure 1-31: Failure Classification by Cause [ISO/TR 12489, 2013]



REPRESENTATION OF UNRELIABILITY

Figure 1-33: Selected Tasks for Improving Unreliability

Indicators and Constraints

- Improving environment knowledge
- Establish process CTQ checkpoint
- Design for manufacturing capabilities
- Reliability metrics and balance scorecards
- Analyzing short term warranty | RMA data

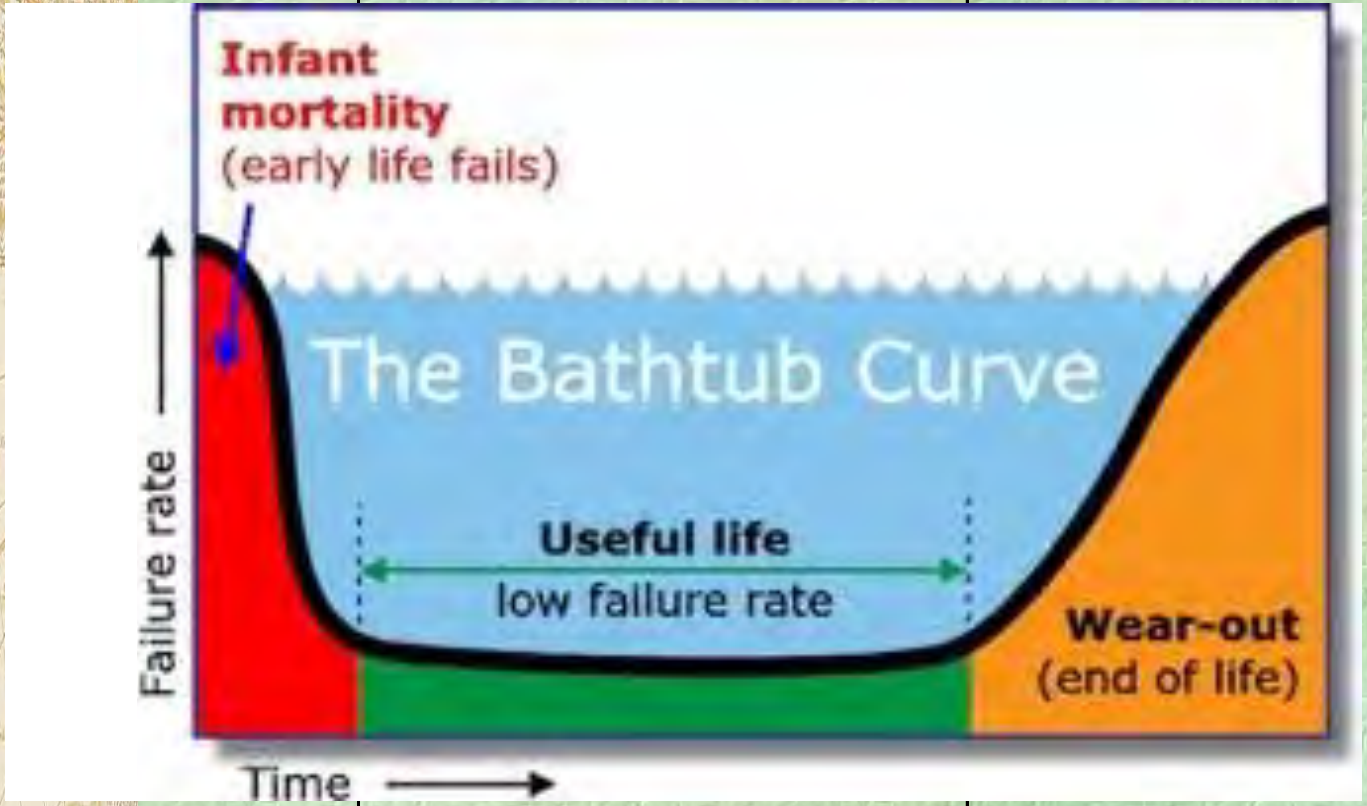
Verification & Reliability Prediction

Begin to utilize:

- Industry and field data
- Accelerated Life Testing
- Reliability Prediction tools

Analysis of Wear-out Mechanism

- ALT [Test to failure]
- System modeling
- Long term data analysis
- Materials characterization



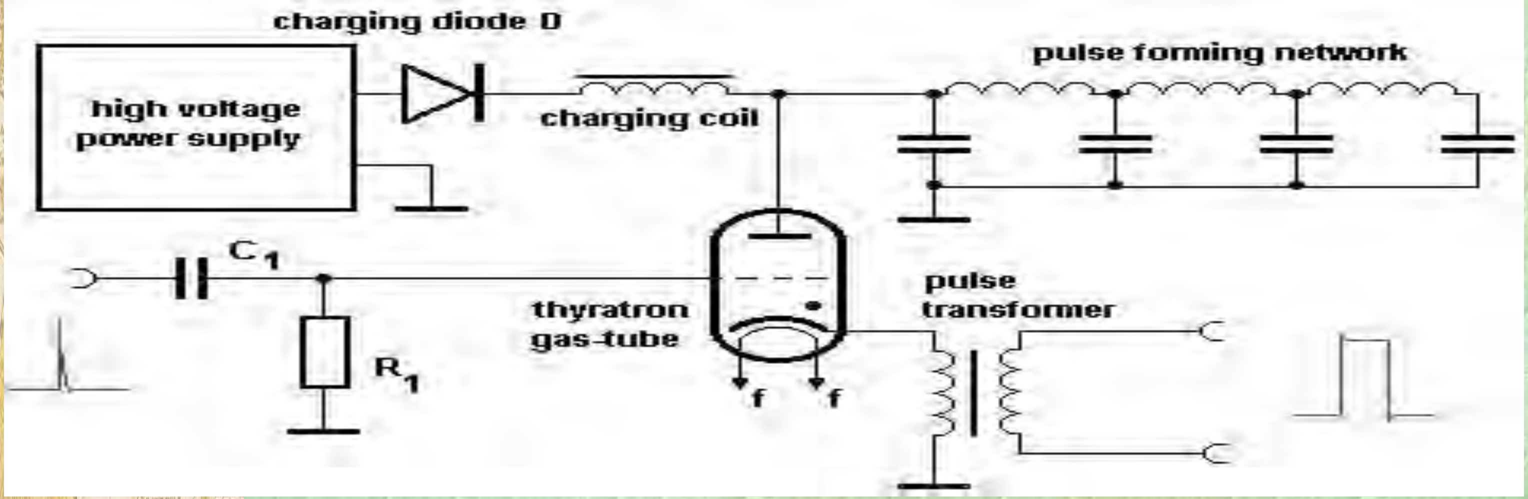
Source: Guest-internet.com/blog/improving-the-reliability-of-Wi-Fi-hotspots

AN APPROACH TO EVALUATE COST ASSOCIATED WITH UNRELIABILITY

Hypothetical Example Application

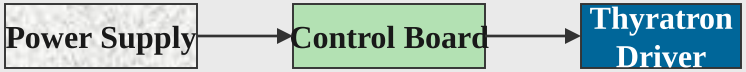
- ❑ Figure 1-37 illustrates three critical components of medical device used for performing laser surgery.
- ❑ The components are connected in series and failure of anyone of these will lead to a single point failure of the system.
- ❑ When a single point failure occurs the device will not be available to treat patients until repaired.
- ❑ Use the information provided in Table 1-17 to determine the cost associate with the unreliability of these components.

Figure 1-37: Partial Schematic of How Components are Related



AN APPROACH TO EVALUATE COST ASSOCIATED WITH UNRELIABILITY

Table 1-17: Product MTBF and Failure Rate

	Reliability Block Diagram of Components			
Medical Device	 Power Supply → Control Board → Thyratron Driver			**Summary**
Study Interval	35,040	43,800	52,560	8,760 Hrs / year
Number of Failures	1	2	3	1.15 Failure / Yr
MTBF	35,040	21,900	17,520	7,617 Hrs / Failure
Failure Rate	28.5 E-06	45.7 E-06	57.1 E-04	131.3 E-06 Failure / Hr

MTBF_{TD} = 52,560 Hrs ÷ 3 Failures = 17,520 Hrs / Failure and the failure rate is the reciprocal of the MTBF.

Hours / Failure = 8760 Hrs ÷ 1.15 Failures per year = 7,617.

COST CATEGORIES IMPACT 0F UNRELIABILITY

Table 1-20: Breakdown of Cost of Unreliability

Cost Categories	Cost Impact of Unreliability
Direct Cost	Warranty Costs
	Field Repair Costs
Indirect Replacement	Inventory Costs for Spares
	Product Service Indirect Costs
Problem Solving Costs	Concession Costs
	Product Recall Costs
	Engineering Support costs
	Root Cause Investigation Costs
	Customer Visit Travel and Leisure Expenses
Opportunity Costs	Lower Margins on New Jobs
	Impact of failures on Customers
	Lost Sales with Impacted to Customers
Long Term Business Costs	Liability | Legal Cost
	Lost of Potential Customers
Aggregate Costs to Company	Impact to reputation

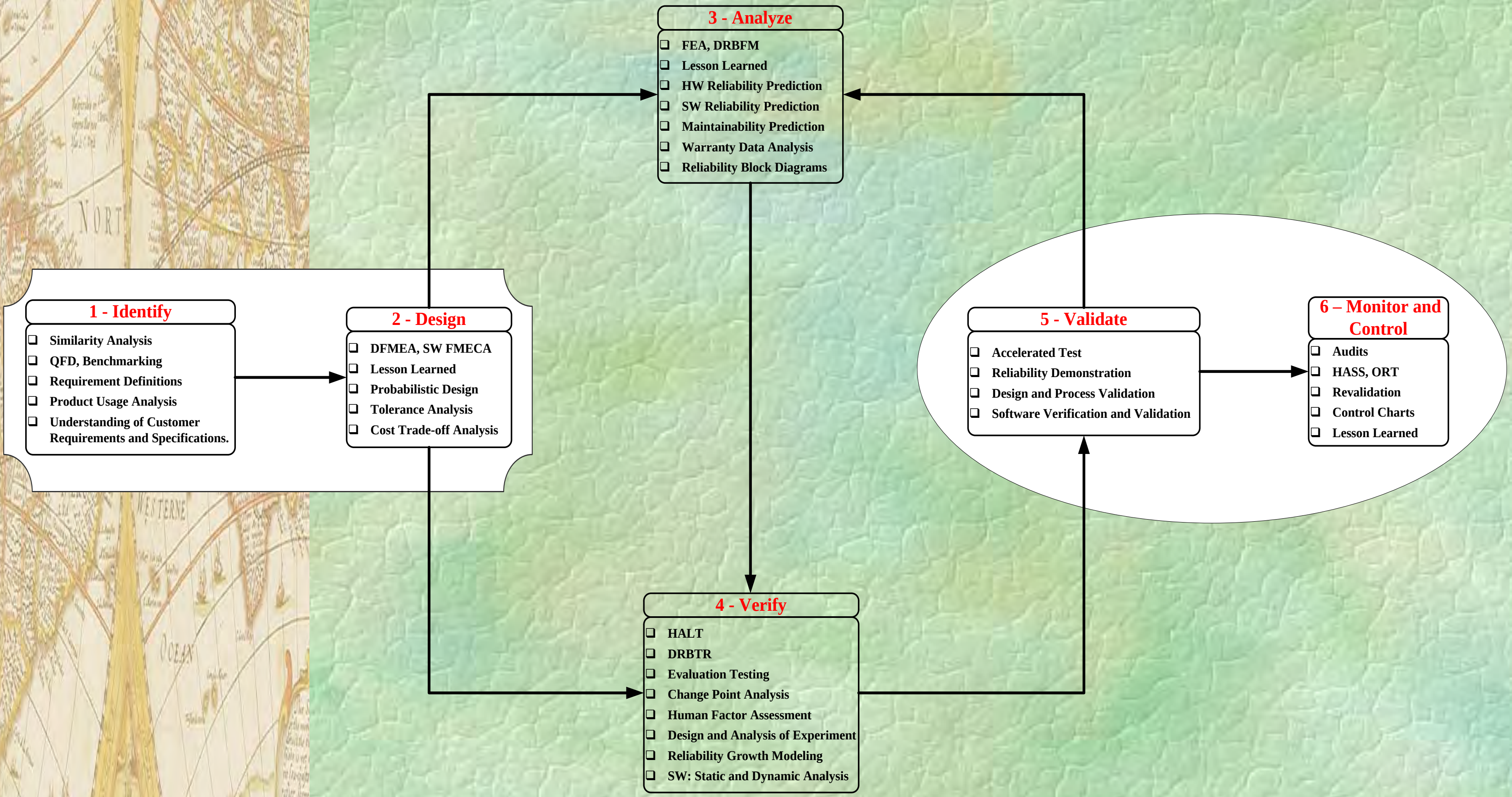
Visible::

Smaller but significant costs

Hidden

Large Business Risks and Exposure

PRODUCT DESIGN FOR RELIABILITY APPROACH



1 - Identify

- ❑ Similarity Analysis
- ❑ QFD, Benchmarking
- ❑ Requirement Definitions
- ❑ Product Usage Analysis
- ❑ Understanding of Customer Requirements and Specifications.

2 - Design

- ❑ DFMEA, SW FMECA
- ❑ Lesson Learned
- ❑ Probabilistic Design
- ❑ Tolerance Analysis
- ❑ Cost Trade-off Analysis

3 - Analyze

- ❑ FEA, DRBFM
- ❑ Lesson Learned
- ❑ HW Reliability Prediction
- ❑ SW Reliability Prediction
- ❑ Maintainability Prediction
- ❑ Warranty Data Analysis
- ❑ Reliability Block Diagrams

4 - Verify

- ❑ HALT
- ❑ DRBTR
- ❑ Evaluation Testing
- ❑ Change Point Analysis
- ❑ Human Factor Assessment
- ❑ Design and Analysis of Experiment
- ❑ Reliability Growth Modeling
- ❑ SW: Static and Dynamic Analysis

5 - Validate

- ❑ Accelerated Test
- ❑ Reliability Demonstration
- ❑ Design and Process Validation
- ❑ Software Verification and Validation

6 – Monitor and Control

- ❑ Audits
- ❑ HASS, ORT
- ❑ Revalidation
- ❑ Control Charts
- ❑ Lesson Learned

Figure 1-44: DFR Key Activities

PRODUCT DFR IMPLEMENTATION CHALLENGES

Table 1-23: Potential Challenges RE May Encounter Implementing DFR

Challenges with Implementing DFR	Overcoming the Challenge	Key Points for Implementing DFR Activities
We are already good enough. Why do we need it?	Cost Justification	**Start DFR activities Early in the process**
Being early enough. Time to market/Rush to demonstrate so they skip steps	Management Buy-in	**Reliability engineer's job is to lead | coach the design team**
Reliability engineers are tied up on current projects and new projects are starting without them	Voice of the Customer	**Integration or Reliability and Quality Engineers with design teams**
Getting the designers to understand so that they can drive the program	Education to Designers	**Warranty | Field data analysis [Both statistical and root cause analysis] needs to be fed back to both design and reliability teams**
Culture – will it accept? How do you get management buy-in? Requires patience. Requires addressing concerns of management.	Ability to Measure Success [Metrics]	**Reduce the number of tools in the toolbox, but use the remaining well. Neither all steps nor tools are necessary for all programs.**
	Case Study | Successful Demonstration.	

M2 - LEARNING OBJECTIVES

Participant Shall be able to:

- Distinguish between the different methods that can be used to predict reliability of their product.
- Gain understanding of how to develop a reliability allocation model for their company products.
- Utilize FMECA and FTA to identify critical components and sub-systems within their company's product.
- Acquire knowledge that enable participants to utilize PFMEA to establish process control, identify critical process and potential test areas where human performance deficiencies could damage or impact device performance.
- Utilize DFMEA to prevent potential failures, improve design weaknesses and develop product testing strategies.
- Gain knowledge of how to develop system model for company's product and analyze system for reliability
- Gain knowledge of how to develop and implement a FRACAS system and integrate with CAPA process within their organization.

Adapt | Implement | Improve

RELIABILITY REQUIREMENTS IN DESIGN

Determine Customer's Product Needs

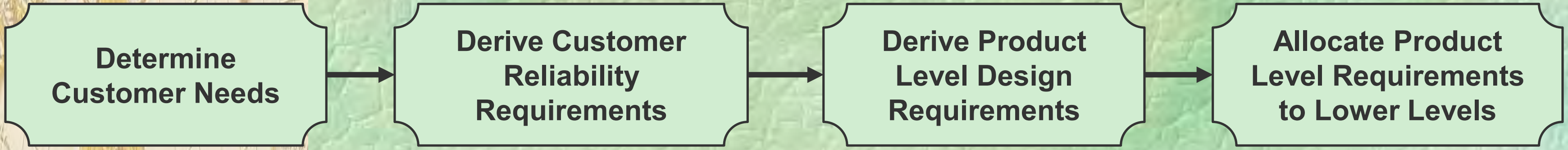
- ❑ The concept/planning phase is the time to establish reliability goals and requirements that addresses the different exposures and characteristics during the product's life cycle.
- ❑ Determining customer needs is the basis for deriving operational performance reliability requirement and subsequent design requirements.
- ❑ Customer's needs are prerequisite to deriving performance reliability requirements.
- ❑ These needs should be determined early in the C/P phase of the product development program, before large investment of time and resources are made.
- ❑ Performance reliability requirements, in turn are the basis for design requirements, which should be defined before starting any design and development.
- ❑ Approach used to determine customer's need include: market surveys, benchmarking, life cycle planning and environmental characterization.

RELIABILITY REQUIREMENTS IN DESIGN

Developing Reliability Requirements:

- ❑ Requirement stated should be realistic and achievable and then translate into design specifications.
- ❑ Developing reliability requirements for products and systems is a multi-step process as shown in figure 2-2.
- ❑ The process includes a number of common tasks as summarized in table 2-1.
- ❑ Each step in the process is pertinent in selecting the level of reliability that drives the scope of the design oriented tasks necessary to meet customer's needs and expectations.

Figure 2-2: Reliability Requirements Development Process


Determine Customer Needs
Derive Customer Reliability Requirements
Derive Product Level Design Requirements
Allocate Product Level Requirements to Lower Levels

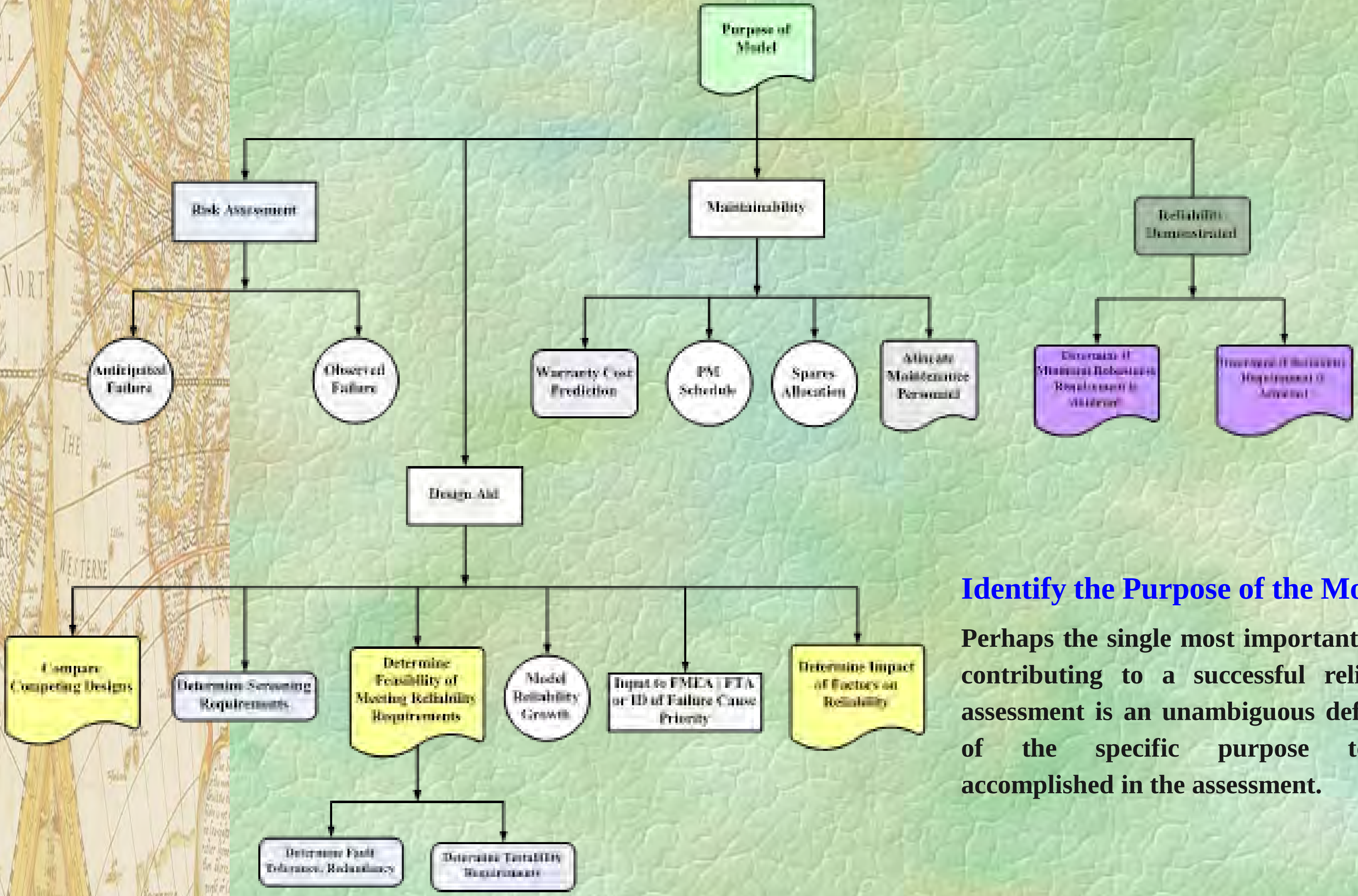
RELIABILITY REQUIREMENTS IN DESIGN

Customer’s Performance Reliability Requirements:

- Customer’s need for a product are typically used to identify or derive the customer’s performance requirements.
- Performance reliability requirements can be derived in one or two ways, depending on what customer needs are stated.
- If the customer’s need is already stated as a recognized reliability requirement [e.g., MTBF] no further action is required, given that the need and the requirement are synonymous.
- On the other hand when the performance requirement is hidden, the basic definition of the need must be analyzed to derive any reliability requirements.
- Let’s take for example a need stated as availability [function of both reliability and maintainability], or as a safety concern \no safety critical failure].
- Modeling and simulation is an effective techniques that can be used to determine a level of reliability, or a range of reliability, necessary to meet more general customer need or requirement.

SELECTED PURPOSES - RELIABILITY MODELING

Figure 2-3: Breakdown of Potential Reliability Modeling Purposes


Purpose of Model
Risk Assessment
Maintainability
Reliability Demonstrated
Anticipated Failure
Observed Failure
Warranty Cost Prediction
PM Schedule
Spares Allocation
Allocate Maintenance Personnel
Determine if Minimum Reliability Requirement is Attained
Determine if Reliability Requirement is Attained
Design Aid
Compare Competing Designs
Determine Screening Requirements
Determine Feasibility of Meeting Reliability Requirements
Model Reliability Growth
Input to FMEA / FTA or ID of Failure Cause Priority
Determine Impact of Factors on Reliability
Determine Fault Tolerance, Redundancy
Determine Testability Requirements

Identify the Purpose of the Model

Perhaps the single most important factor contributing to a successful reliability assessment is an unambiguous definition of the specific purpose to be accomplished in the assessment.

SYSTEM LEVEL | SUB-SYSTEM DESIGN ANALYSIS

FMEA

A failure modes and effects analysis [FMEA] is an inductive bottom-up method for analyzing a system design or manufacturing process in order to evaluate the potential for failures.

- Can be described as a reliability planning tool that consist of a systematic group of activities intended to:

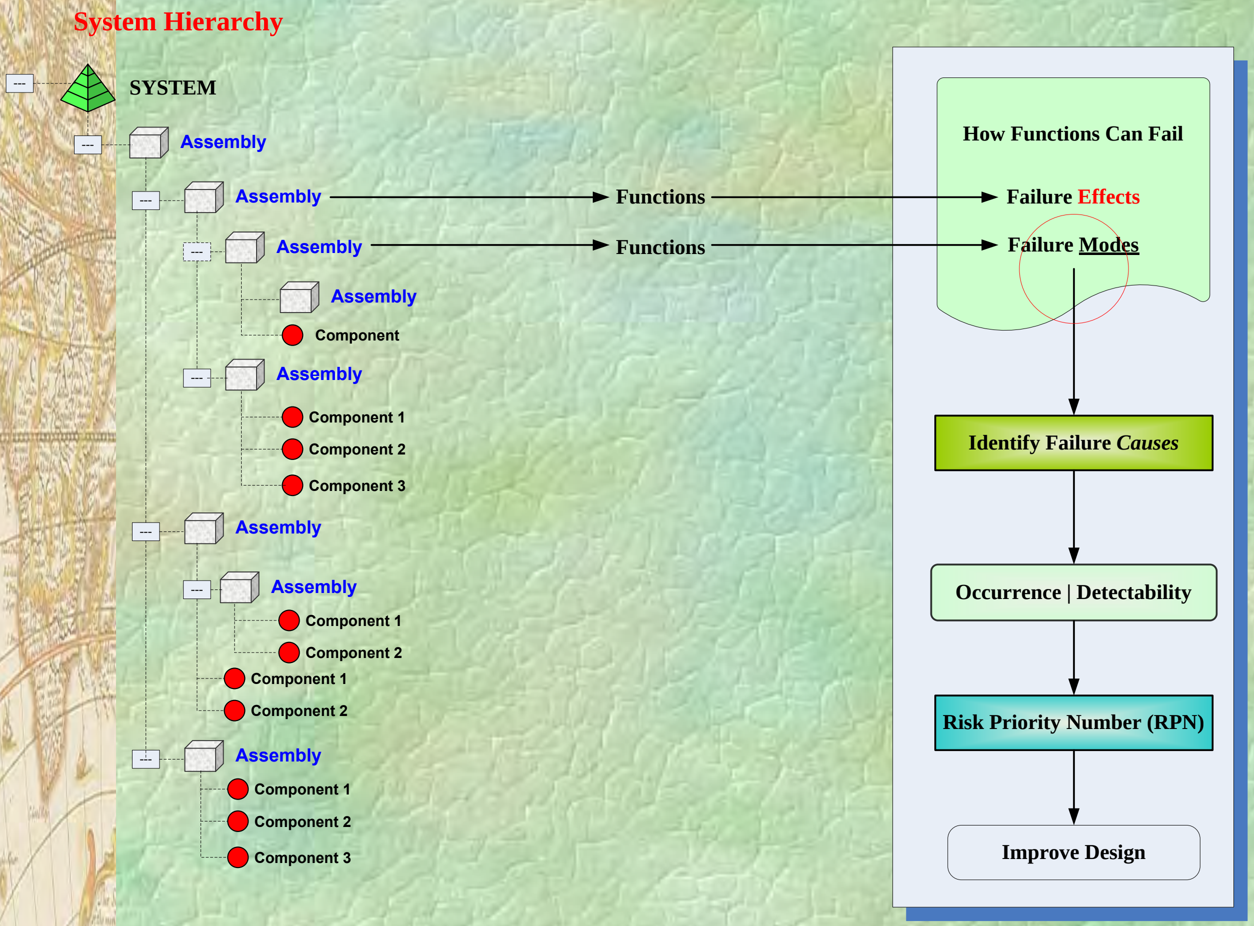
  1. Recognize and evaluate the potential failure of a product / process and its effect.
  2. Identify root cause of potential failure mode at a very fundamental level that is related to the underlying failure.
  3. Prioritize potential failures according to their risk.
  4. Provides actions that could eliminate or reduce the chance of the potential failure occurring.
  5. Providing a living document for use and for continuous reliability improvements.

Basic Types of FMEA

- ❑ Concept.
- ❑ Design [DFMEA].
- ❑ Process [PFMEA].
- ❑ Service.
- ❑ Functional.

USING FMEA AS THE BASIS FOR A RELIABILITY MODEL

Figure 2-4: The Basic FMEA Approach

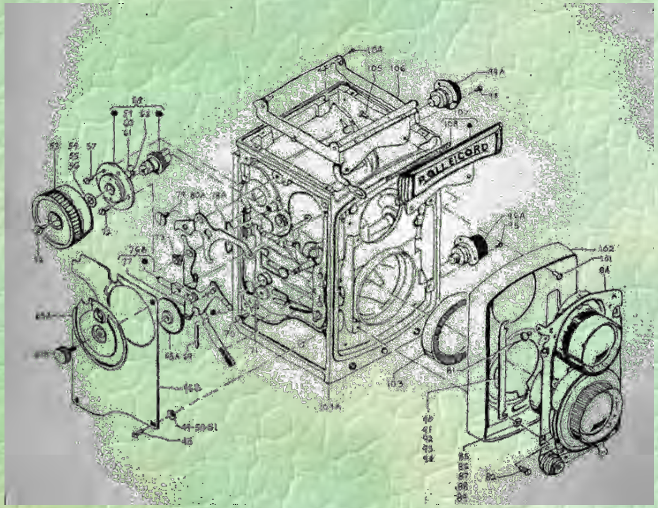


A FMEA can be an effective tool in identifying specific failure causes that needs to be quantified in a reliability model. Figure 2-4 illustrates a generic approach.

PRODUCT DESIGN DEFICIENCY 1

The Product is Manufactured Properly but Poorly Designed.

- ❑ Product not design for robust performance
- ❑ Excessive heat, vibration, noise
- ❑ Inadequate design life assumption
- ❑ Specified energy level is too low, too high.
- ❑ Actual stresses higher than design loads
- ❑ Material specification unsuitable for application



PRODUCT DESIGN DEFICIENCY 2

The Product Design Leads to Poor Manufacturing

❑ Is orientation, alignment important to function?

❑ Can the components be assembled upside-down or backwards?

❑ Are the engineering tolerances compatible with manufacturing capabilities?

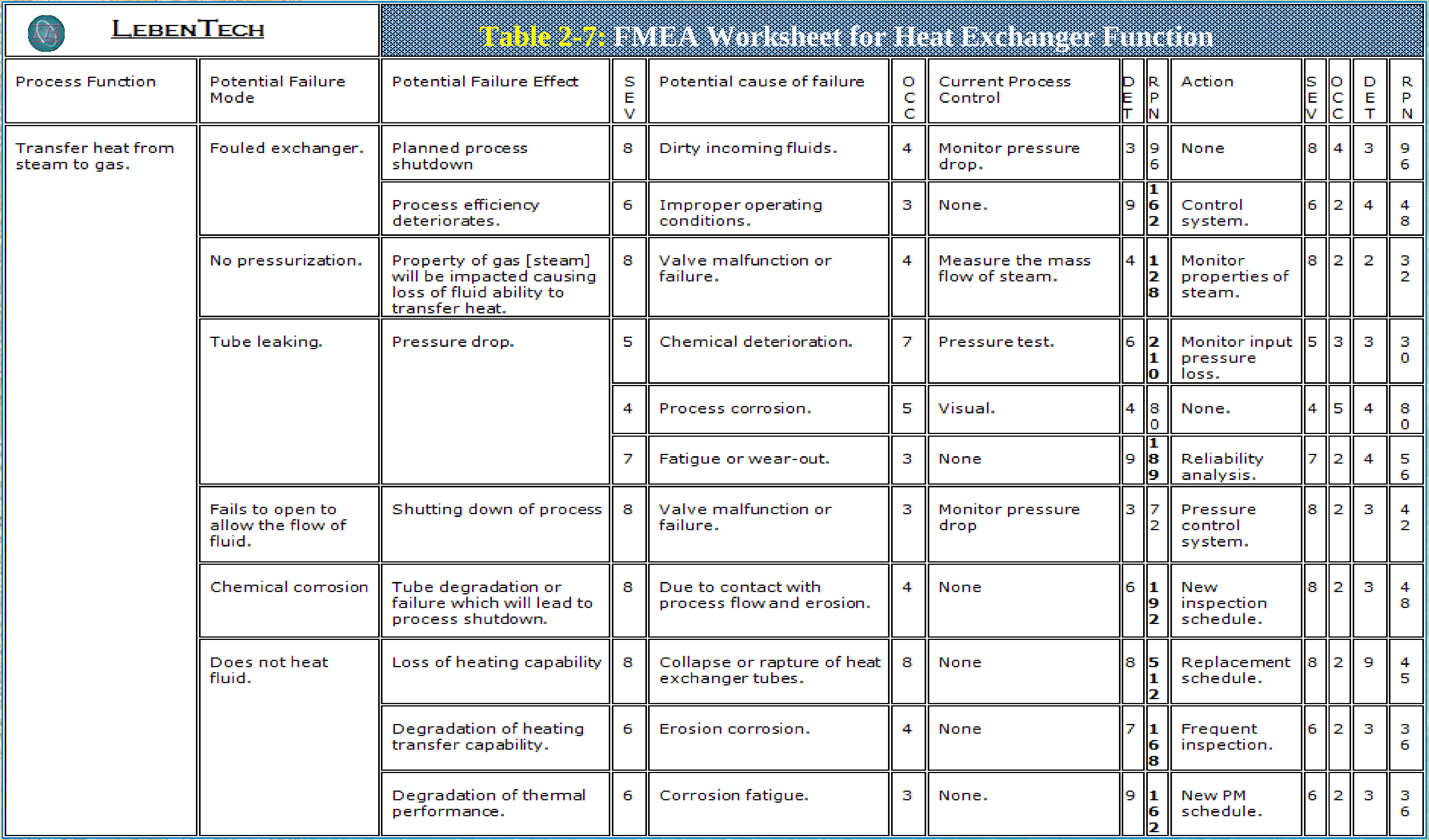
Incorporate!

❑ DESIGN FOR Assembly [DFA]

❑ Design for Manufacturing [DFM]

AS Part of Development Process

EQUIPMENT FMEA APPLICATION



LebenTech

Table 2-7: FMEA Worksheet for Heat Exchanger Function

Process Function	Potential Failure Mode	Potential Failure Effect	SEV	Potential cause of failure	OCC	Current Process Control	DET	RPN	Action	SEV	OCC	DET	RPN
Transfer heat from steam to gas.	Fouled exchanger.	Planned process shutdown	8	Dirty incoming fluids.	4	Monitor pressure drop.	3	96	None	8	4	3	96
		Process efficiency deteriorates.	6	Improper operating conditions.	3	None.	9	162	Control system.	6	2	4	48
	No pressurization.	Property of gas [steam] will be impacted causing loss of fluid ability to transfer heat.	8	Valve malfunction or failure.	4	Measure the mass flow of steam.	4	128	Monitor properties of steam.	8	2	2	32
	Tube leaking.	Pressure drop.	5	Chemical deterioration.	7	Pressure test.	6	210	Monitor input pressure loss.	5	3	3	30
			4	Process corrosion.	5	Visual.	4	80	None.	4	5	4	80
			7	Fatigue or wear-out.	3	None	9	189	Reliability analysis.	7	2	4	56
	Fails to open to allow the flow of fluid.	Shutting down of process	8	Valve malfunction or failure.	3	Monitor pressure drop	3	72	Pressure control system.	8	2	3	42
	Chemical corrosion	Tube degradation or failure which will lead to process shutdown.	8	Due to contact with process flow and erosion.	4	None	6	192	New inspection schedule.	8	2	3	48
	Does not heat fluid.	Loss of heating capability	8	Collapse or rapture of heat exchanger tubes.	8	None	8	512	Replacement schedule.	8	2	9	45
		Degradation of heating transfer capability.	6	Erosion corrosion.	4	None	7	168	Frequent inspection.	6	2	3	36
		Degradation of thermal performance.	6	Corrosion fatigue.	3	None.	9	162	New PM schedule.	6	2	3	36

FMEA APPLICATION IN HEALTHCARE SYSTEM

Table 2-8: Failure Mode and Effect Analysis (FMEA) of Dialysis Operation

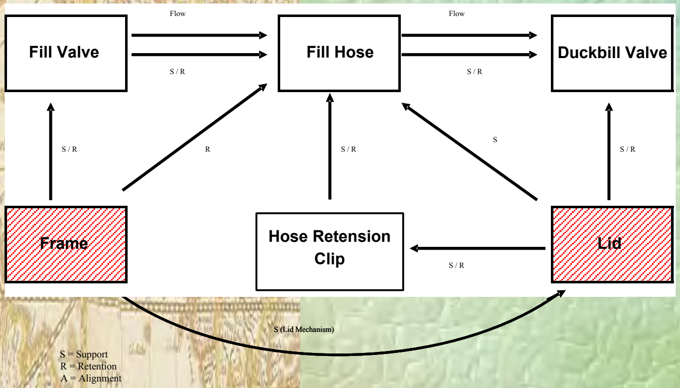
System Function Specification	Potential Failure Mode | Error	Potential Effects of Failure | Error	SEV	Potential Causes of Failure | Error	OCC	Current Design Control / Mitigation		DET	RPN
						Method of Prevention	Detection Means		
Removes harmful waste and extra fluids from blood.	Patient loss of blood	Clotting of the hemodialysis circuit | blood lines		Air in blood lines		Monitored by determine activated clotting times			
	Sub-optimal treatment from hemodialysis			Low blood flow rate		Low dose | minimum heparin			
				Inadequate anticoagulation		Standard Anticoaglation			
						Heparin modeling			
	Equipment failure	Treatment disruption | Delays | Possible harm		Disruption of electricity due to power failure					
				Improper treatment setup (Technician)					
		Hemorrhaging – leads to fatal error		Reversal of dialysis lines (Attention not paid to alarm)					
	Contaminated Blood	Haemolytic Anaemia		Chloramines		Water Purification			
		HIV		Dialysis membrane improperly reused			Monitoring level of blood lines		
				Use of disposable disk filters		Use of external transducer protector			
				Lack of monitoring		Disinfection after treatment			
		Cardiovascular morbidity		Contaminants in water | dialysate		Properly designed and maintained water treatment system	AAMI Standard for quality assurance		
				Air in blood					
				Flow of dialysate into blood due to fiber leak					
		Vomiting | Nausea		**Heparin not rinse with 100 cc saline**		Patient safety intervention			

DFMEA INTERFACE WITH VERIFICATION PLAN

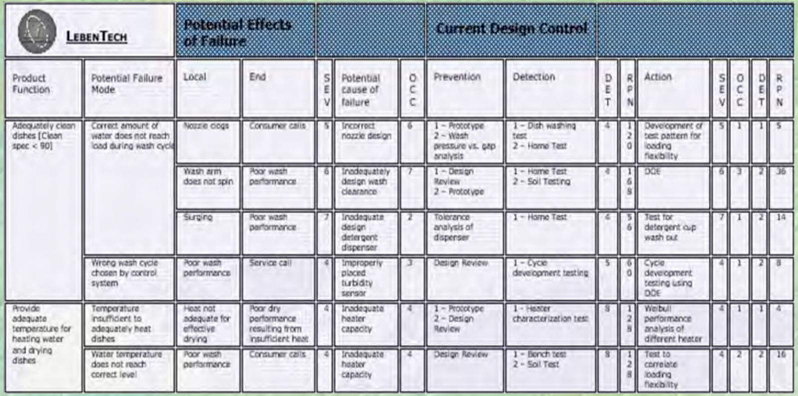
Figure 2-10: Design Improvement Plan

Functional Block Diagram

Fill System

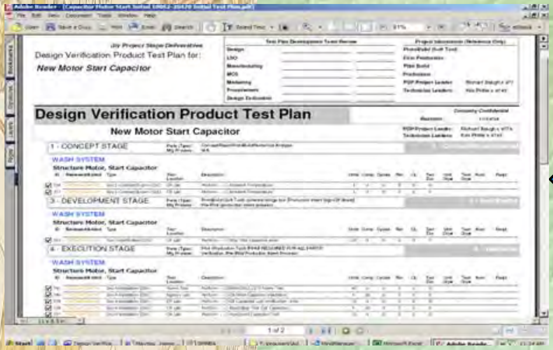


DFMEA



LebenTech		Potential Effects of Failure					Current Design Control								
Product Function	Potential Failure Mode	Local	End	SEV	Potential cause of failure	OCC	Prevention	Detection	DET	RPN	Action	SEV	OCC	DET	RPN
Adequately clean dishes [Clean spec < 90]	Correct amount of water does not reach load during wash cycle	Nozzle clogs	Consumer calls	5	Incorrect nozzle design	6	1 – Prototype 2 – Wash pressure vs. gap analysis	1 – Dish washing test 2 – Home Test	4	120	Development of test pattern for loading flexibility	5	1	1	5
		Wash arm does not spin	Poor wash performance	6	Inadequately design wash clearance	7	1 – Design Review 2 – Prototype	1 – Home Test 2 – Soil Testing	4	168	DOE	6	3	2	36
		Surging	Poor wash performance	7	Inadequate design detergent dispenser	2	Tolerance analysis of dispenser	1 – Home Test	4	56	Test for detergent cup wash out	7	1	2	14
	Wrong wash cycle chosen by control system	Poor wash performance	Service call	4	Improperly placed turbidity sensor	3	Design Review	1 – Cycle development testing	5	60	Cycle development testing using DOE	4	1	2	8
Provide adequate temperature for heating water and drying dishes	Temperature insufficient to adequately heat dishes	Heat not adequate for effective drying	Poor dry performance resulting from insufficient heat	4	Inadequate heater capacity	4	1 – Prototype 2 – Design Review	1 – Heater characterization test	8	128	Weibull performance analysis of different heater	4	1	1	4
	Water temperature does not reach correct level	Poor wash performance	Consumer calls	4	Inadequate heater capacity	4	Design Review	1 – Bench test 2 – Soil Test	8	128	Test to correlate loading flexibility	4	2	2	16

Design Verification Plan



Design Verification Product Test Plan for:

New Motor Start Capacitor

Design Verification Product Test Plan

New Motor Start Capacitor

1 - CONCEPT STAGE

WASH SYSTEM

Structure Motor, Start Capacitor

3 - DEVELOPMENT STAGE

WASH SYSTEM

Structure Motor, Start Capacitor

4 - EXECUTION STAGE

WASH SYSTEM

Structure Motor, Start Capacitor

1 of 2

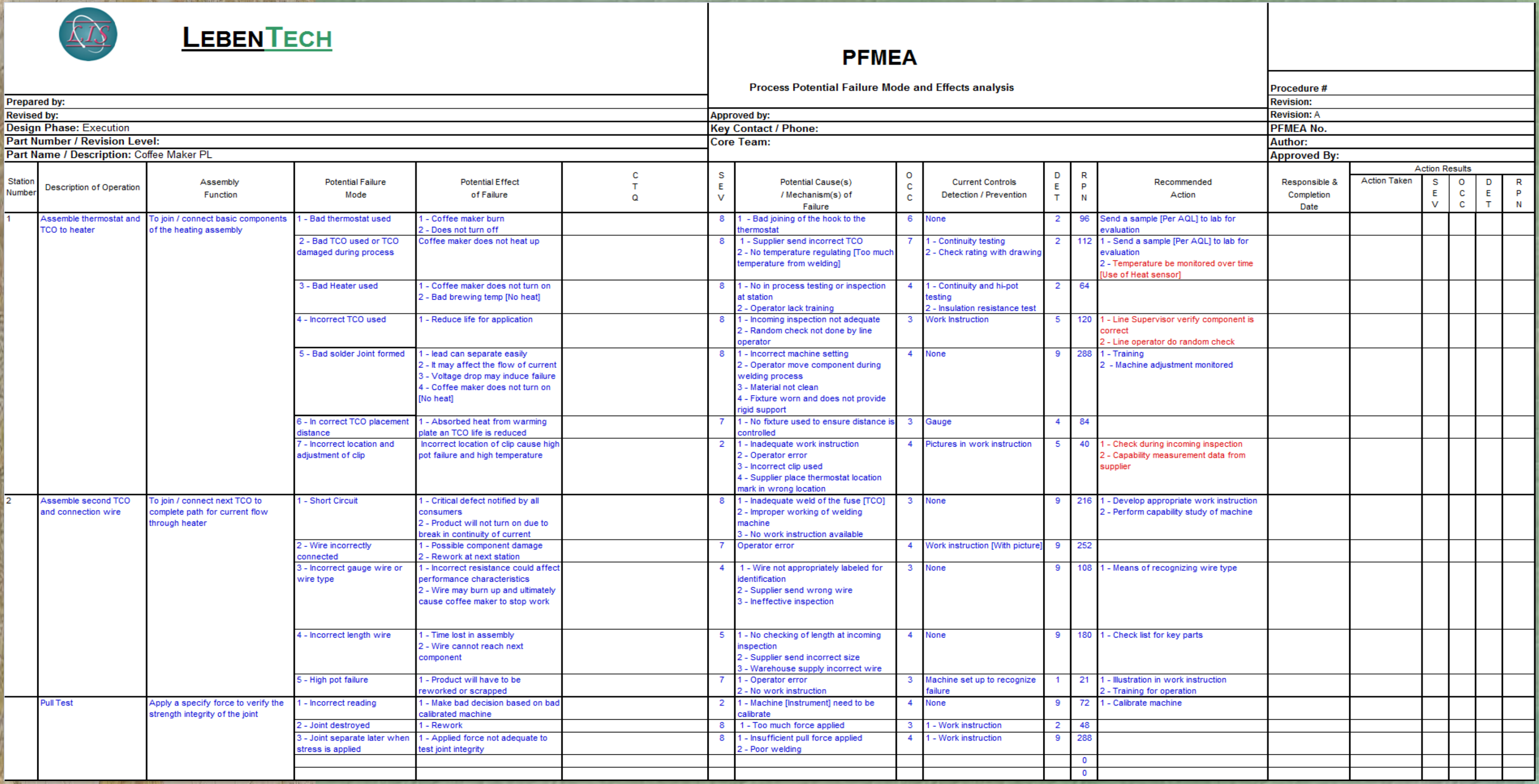
To assure that a complete analysis has been performed, each component failure mode and/or output function should be examined for the following conditions:

- ❑ Failure to operate at the proper time
- ❑ Intermittent operation
- ❑ Failure to stop operating at the proper time
- ❑ Loss of output
- ❑ Degraded output or reduced operational capability

– Proactive Innovative Solutions for Success and Competitive Advantages

COFFEE MAKER PFMEA APPLICATION

Table 2-11: Failure Mode and Effect Analysis (PFMEA) of Coffee Maker Manf. Process



LEBENTECH

PFMEA

Process Potential Failure Mode and Effects analysis

Procedure #
Revision:
Prepared by:
Revised by:
Approved by:
Revision: A
Design Phase: Execution
Key Contact / Phone:
PFMEA No.
Part Number / Revision Level:
Core Team:
Author:
Part Name / Description: Coffee Maker PL
Approved By:

														Action Results				
Station Number	Description of Operation	Assembly Function	Potential Failure Mode	Potential Effect of Failure	CTQ	SEV	Potential Cause(s) / Mechanism(s) of Failure	OCC	Current Controls Detection / Prevention	DET	RPN	Recommended Action	Responsible & Completion Date	Action Taken	SEV	OCC	DET	RPN
1	Assemble thermostat and TCO to heater	To join / connect basic components of the heating assembly	1 - Bad thermostat used	1 - Coffee maker burn 2 - Does not turn off		8	1 - Bad joining of the hook to the thermostat	6	None	2	96	Send a sample [Per AQL] to lab for evaluation						
			2 - Bad TCO used or TCO damaged during process	Coffee maker does not heat up		8	1 - Supplier send incorrect TCO 2 - No temperature regulating [Too much temperature from welding]	7	1 - Continuity testing 2 - Check rating with drawing	2	112	1 - Send a sample [Per AQL] to lab for evaluation 2 - Temperature be monitored over time [Use of Heat sensor]						
			3 - Bad Heater used	1 - Coffee maker does not turn on 2 - Bad brewing temp [No heat]		8	1 - No in process testing or inspection at station 2 - Operator lack training	4	1 - Continuity and hi-pot testing 2 - Insulation resistance test	2	64							
			4 - Incorrect TCO used	1 - Reduce life for application		8	1 - Incoming inspection not adequate 2 - Random check not done by line operator	3	Work Instruction	5	120	1 - Line Supervisor verify component is correct 2 - Line operator do random check						
			5 - Bad solder Joint formed	1 - lead can separate easily 2 - It may affect the flow of current 3 - Voltage drop may induce failure 4 - Coffee maker does not turn on [No heat]		8	1 - Incorrect machine setting 2 - Operator move component during welding process 3 - Material not clean 4 - Fixture worn and does not provide rigid support	4	None	9	288	1 - Training 2 - Machine adjustment monitored						
			6 - In correct TCO placement distance	1 - Absorbed heat from warming plate an TCO life is reduced		7	1 - No fixture used to ensure distance is controlled	3	Gauge	4	84							
			7 - Incorrect location and adjustment of clip	Incorrect location of clip cause high pot failure and high temperature		2	1 - Inadequate work instruction 2 - Operator error 3 - Incorrect clip used 4 - Supplier place thermostat location mark in wrong location	4	Pictures in work instruction	5	40	1 - Check during incoming inspection 2 - Capability measurement data from supplier						
2	Assemble second TCO and connection wire	To join / connect next TCO to complete path for current flow through heater	1 - Short Circuit	1 - Critical defect notified by all consumers 2 - Product will not turn on due to break in continuity of current		8	1 - Inadequate weld of the fuse [TCO] 2 - Improper working of welding machine 3 - No work instruction available	3	None	9	216	1 - Develop appropriate work instruction 2 - Perform capability study of machine						
			2 - Wire incorrectly connected	1 - Possible component damage 2 - Rework at next station		7	Operator error	4	Work instruction [With picture]	9	252							
			3 - Incorrect gauge wire or wire type	1 - Incorrect resistance could affect performance characteristics 2 - Wire may burn up and ultimately cause coffee maker to stop work		4	1 - Wire not appropriately labeled for identification 2 - Supplier send wrong wire 3 - Ineffective inspection	3	None	9	108	1 - Means of recognizing wire type						
			4 - Incorrect length wire	1 - Time lost in assembly 2 - Wire cannot reach next component		5	1 - No checking of length at incoming inspection 2 - Supplier send incorrect size 3 - Warehouse supply incorrect wire	4	None	9	180	1 - Check list for key parts						
			5 - High pot failure	1 - Product will have to be reworked or scrapped		7	1 - Operator error 2 - No work instruction	3	Machine set up to recognize failure	1	21	1 - Illustration in work instruction 2 - Training for operation						
	Pull Test	Apply a specify force to verify the strength integrity of the joint	1 - Incorrect reading	1 - Make bad decision based on bad calibrated machine		2	1 - Machine [Instrument] need to be calibrate	4	None	9	72	1 - Calibrate machine						
			2 - Joint destroyed	1 - Rework		8	1 - Too much force applied	3	1 - Work instruction	2	48							
			3 - Joint separate later when stress is applied	1 - Applied force not adequate to test joint integrity		8	1 - Insufficient pull force applied 2 - Poor welding	4	1 - Work instruction	9	288							
											0							
											0							

SYSTEM LEVEL DESIGN ANALYSIS - FMECA

FMECA Analytical Model Continued

- ❑ Most of the failure rates applied is taken from the NPRD-95 Manual or taken from other data source.
- ❑ Some of the values associated with the failure mode ratios are taken from the FMD-97 database developed by The Reliability Information Analysis Center [RIAC].
- ❑ Company R&D engineers will also provide some of these values.
- ❑ This approach also utilizes the following formula for Item Criticality within a particular severity level:

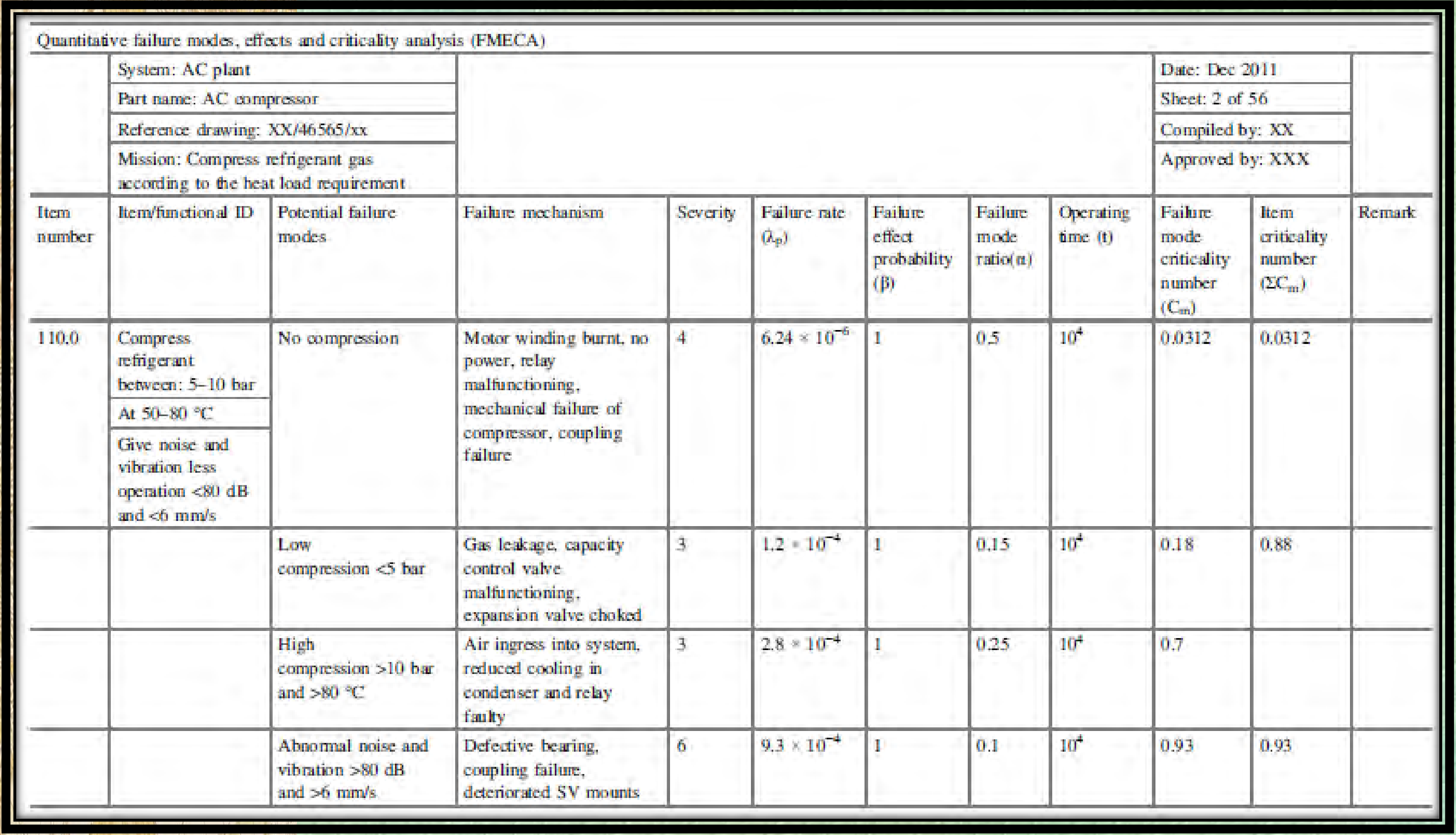
$$C_r = \sum_{n=1}^{j} \left[\beta \alpha \lambda_p t \right]_n$$

Where:

C_r = Item Criticality.
n = Represents the current failure mode of the item being analyzed.
j = Represents the number of failure modes for the item being analyzed.

FMECA APPLICATION IN PRODUCT DESIGN

Table 2-17: Example of DA Form 7612, FMECA Worksheet Using Qualitative Rankings



Quantitative failure modes, effects and criticality analysis (FMECA)

	System: AC plant		Date: Dec 2011	
	Part name: AC compressor		Sheet: 2 of 56	
	Reference drawing: XX/46565/xx		Compiled by: XX	
	Mission: Compress refrigerant gas according to the heat load requirement		Approved by: XXX	

Item number	Item/functional ID	Potential failure modes	Failure mechanism	Severity	Failure rate (λ_p)	Failure effect probability (β)	Failure mode ratio(α)	Operating time (t)	Failure mode criticality number (C_m)	Item criticality number (ΣC_m)	Remark
110.0	Compress refrigerant between: 5–10 bar At 50–80 °C Give noise and vibration less operation <80 dB and <6 mm/s	No compression	Motor winding burnt, no power, relay malfunctioning, mechanical failure of compressor, coupling failure	4	6.24×10^{-6}	1	0.5	10^4	0.0312	0.0312	
		Low compression <5 bar	Gas leakage, capacity control valve malfunctioning, expansion valve choked	3	1.2×10^{-4}	1	0.15	10^4	0.18	0.88	
		High compression >10 bar and >80 °C	Air ingress into system, reduced cooling in condenser and relay faulty	3	2.8×10^{-4}	1	0.25	10^4	0.7		
		Abnormal noise and vibration >80 dB and >6 mm/s	Defective bearing, coupling failure, deteriorated SV mounts	6	9.3×10^{-4}	1	0.1	10^4	0.93	0.93	

Source: Reference 7

SIMILAR ITEM ANALYSIS

Example Application of a Similar Item Analysis

- A new computer product is composed of a processor, a display, a modem and a keyboard. The new product is expected to operate in a 40 ^{0}C environment.
- Data on similar components was located and is shown in the second column of table 2-19.
- The similar item data is for a unit operating in a 20 ^{0}C environment. What MTBF can be expected for a new system if a 30% technology improvement is expected?
- Each component MTBF is corrected for the change in temperature of 20 ^{0}C to 40 ^{0}C.
- Technology improvements were also included and the product MTBF is calculated using the expression:
- $MTBF_P = \Sigma 1/\lambda_i$

Where,

- $MTBF_P$ = Mean Time Between failure of the product
- λ_i = Failure rate of the i component.

WORKED EXAMPLE APPLICATION

Table 2-19: Reliability Analysis of Similar Item

Item	Similar Data MTBF (Hrs)	Temperature * Factor	Improvement Factor	New Product MTBF (Hrs)
Processor	5,000	0.8	1.3	5,200
Display	15,000	0.8	1.3	15,600
Modem	30,000	0.8	1.3	31,200
Keyboard	60,000	0.8	1.3	62,400
System	3,158			3,284

* Temperature conversion factor source "Reliability Toolkit: Commercial Practices Edition", page 176

❑ 5000 * [0.8 * 1.3] = 5200 | 3158 * [0.8 * 1.3] = 3284

$$\mathrm{MTBF}_P = \sum \frac{1}{\lambda_i} = \frac{1}{5,000} + \frac{1}{15,000} + \frac{1}{30,000} + \frac{1}{60,000} = \frac{1}{0.00031666} = 3158$$

WHAT IS RELIABILITY PREDICTION

Overview

- Purpose: The general purpose of reliability prediction is to provide guidance relative to the expected reliability for a product as compared with the customer's need, expressed or implied, for the product.
- The utilization of prediction is a means of developing information for design analysis without actually testing and measuring the product capabilities.
- Prediction provide an array of benefits to product development, including:
  1. Determining the feasibility of a proposed product's design reliability.
  2. Comparison of predicted reliability to the product reliability goals/objectives.
  3. A means of ranking or identifying potential reliability design problem areas.
  4. Evaluation of alternative design, parts, materials and processes.
  5. A quantitative basis for design trade studies without resorting to testing.
- Timing: It is strongly recommended that early prediction be done in the product planning/concept phase.
- The process should be continue throughout the design process and, being updated as more detailed design information becomes available.

WHAT IS RELIABILITY PREDICTION

Table 2-20: Reliability Hierarchy Prediction Listing

Item No.	Level	Example	Phase	Suggested Technique
1	▪ System or Product	▪ Computer Product	▪ Conceptual Design	▪ Similar Item ▪ Part Count
2	▪ Assembly or Component	▪ Processor Assembly	▪ Early Design	▪ Similar Item ▪ Part Count ▪ Reliability Physics
3	▪ Circuit or Part	▪ Microprocessor Part	▪ Detailed Design	▪ Stress Analysis ▪ Reliability Physics ▪ Test Data

RELIABILITY PREDICTION APPLICATION

Reliability Prediction of Electronic Systems

Many reliability models are available for different electronic components in different handbooks and guides like MIL-HDBK [2], PRISM [3, 4] and others. There are two methods for the estimation of the reliability of electronic systems namely Parts Count Method and Parts stress Method

Parts Counts Methods

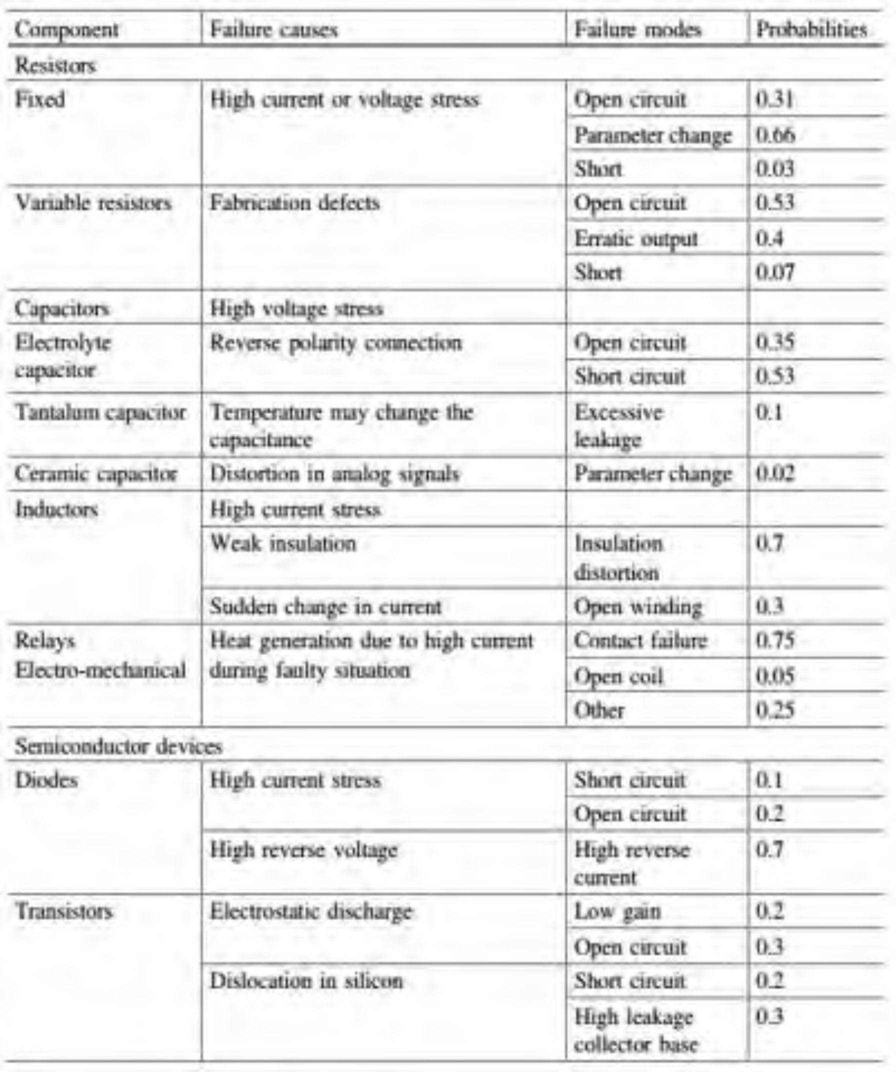
Mathematically the total failure rate for a system based upon the Parts Count method can be expressed as (as given in MIL-HDBK-217F).

$$\lambda_E = \sum_{i=1}^{n} N_i \left(\lambda_g \pi_Q\right) i$$

Where:

λ_E – Total equipment failure rate per 10^6 h
λ_g – Generic failure rate for the ith generic part
π_Q – Quality factor for the ith generic part
N_i – Quantity of the ith generic part
n – Number of different generic part categories in the equipment.

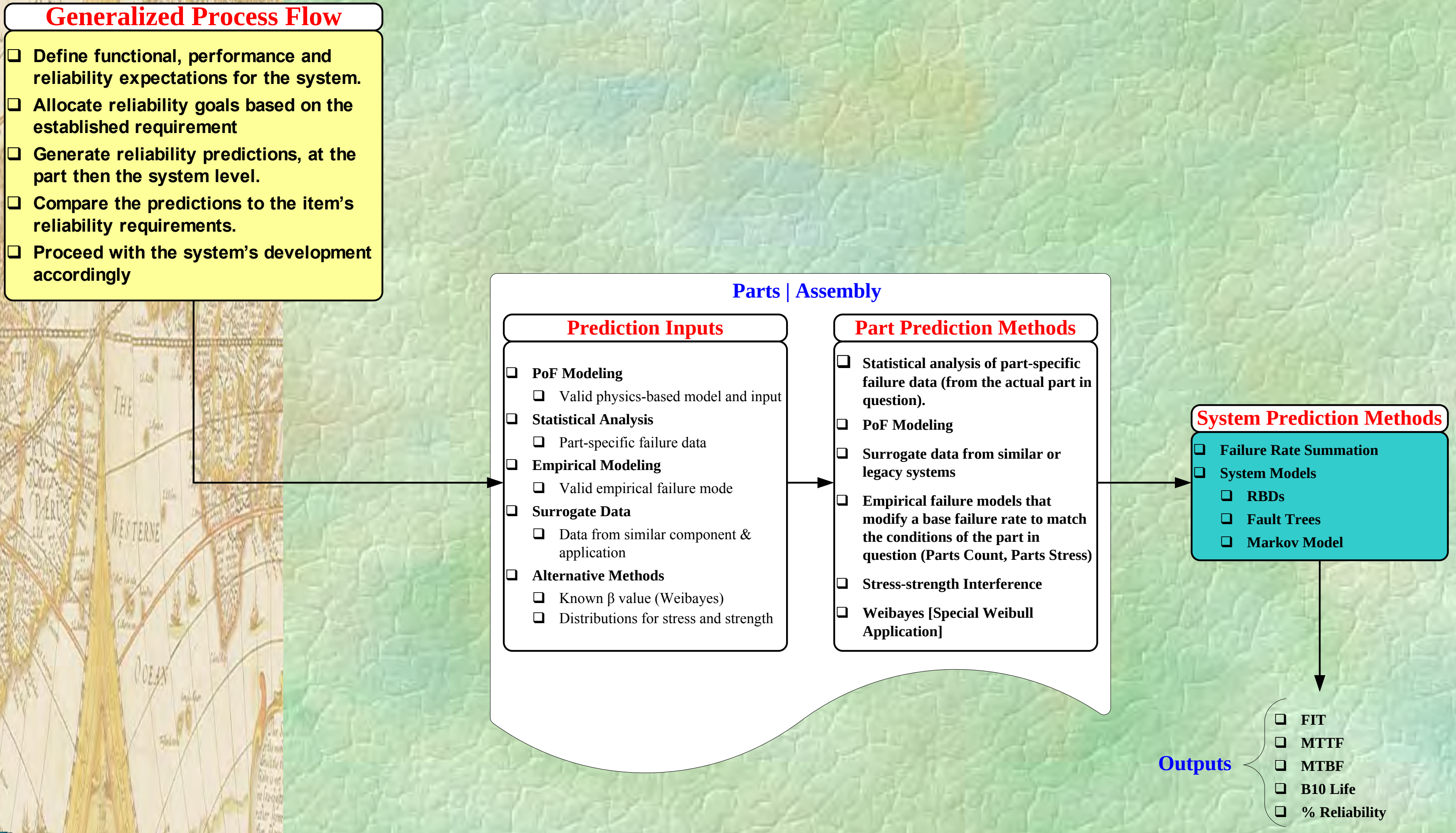
Table 2-22: Failure Modes of Different Electronic Components



Component	Failure causes	Failure modes	Probabilities
Resistors			
Fixed	High current or voltage stress	Open circuit	0.31
		Parameter change	0.66
		Short	0.03
Variable resistors	Fabrication defects	Open circuit	0.53
		Erratic output	0.4
		Short	0.07
Capacitors	High voltage stress		
Electrolyte capacitor	Reverse polarity connection	Open circuit	0.35
		Short circuit	0.53
Tantalum capacitor	Temperature may change the capacitance	Excessive leakage	0.1
Ceramic capacitor	Distortion in analog signals	Parameter change	0.02
Inductors	High current stress		
	Weak insulation	Insulation distortion	0.7
	Sudden change in current	Open winding	0.3
Relays Electro-mechanical	Heat generation due to high current during faulty situation	Contact failure	0.75
		Open coil	0.05
		Other	0.25
Semiconductor devices			
Diodes	High current stress	Short circuit	0.1
		Open circuit	0.2
	High reverse voltage	High reverse current	0.7
Transistors	Electrostatic discharge	Low gain	0.2
		Open circuit	0.3
	Dislocation in silicon	Short circuit	0.2
		High leakage collector base	0.3

RELIABILITY PREDICTION TECHNIQUES

Figure 2-13: Graphical Representation of Reliability Prediction Process



Generalized Process Flow

- ❑ Define functional, performance and reliability expectations for the system.
- ❑ Allocate reliability goals based on the established requirement
- ❑ Generate reliability predictions, at the part then the system level.
- ❑ Compare the predictions to the item's reliability requirements.
- ❑ Proceed with the system's development accordingly

Parts | Assembly

Prediction Inputs

- ❑ PoF Modeling
  - ❑ Valid physics-based model and input
- ❑ Statistical Analysis
  - ❑ Part-specific failure data
- ❑ Empirical Modeling
  - ❑ Valid empirical failure mode
- ❑ Surrogate Data
  - ❑ Data from similar component & application
- ❑ Alternative Methods
  - ❑ Known β value (Weibayes)
  - ❑ Distributions for stress and strength

Part Prediction Methods

- ❑ Statistical analysis of part-specific failure data (from the actual part in question).
- ❑ PoF Modeling
- ❑ Surrogate data from similar or legacy systems
- ❑ Empirical failure models that modify a base failure rate to match the conditions of the part in question (Parts Count, Parts Stress)
- ❑ Stress-strength Interference
- ❑ Weibayes [Special Weibull Application]

System Prediction Methods

- ❑ Failure Rate Summation
- ❑ System Models
  - ❑ RBDs
  - ❑ Fault Trees
  - ❑ Markov Model

Outputs

- ❑ FIT
- ❑ MTTF
- ❑ MTBF
- ❑ B10 Life
- ❑ % Reliability

PARTS COUNT RELIABILITY PREDICTION

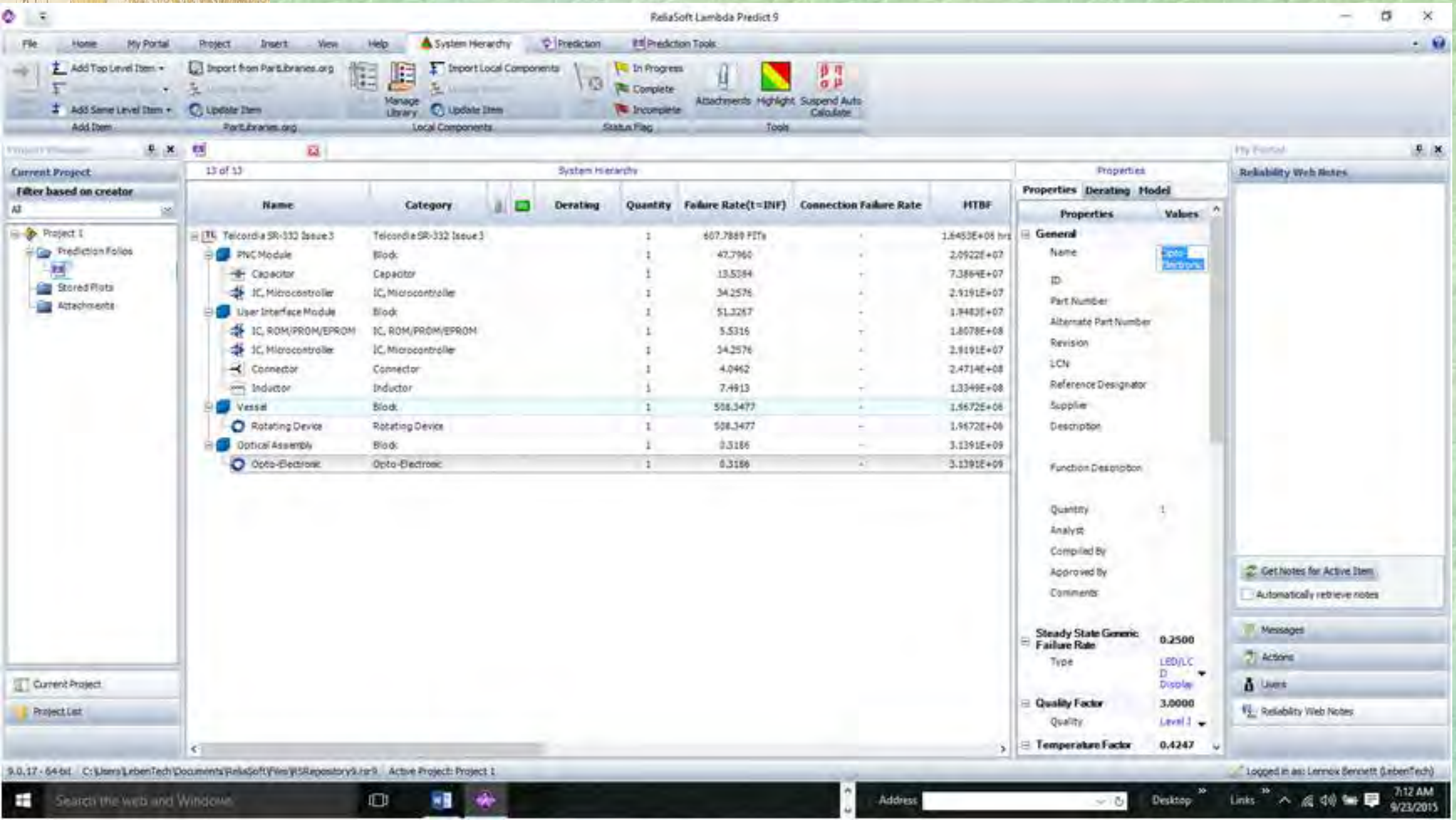
Table 2-25: Communication Product Summary Failure Rate Data

Part Number	Subsystems	Failure Rate (FPMH)	MTBF (Hrs.)	Unreliability
RP0752-562	Miscellaneous Hardware	11.0158	9.08E+04	0.6152
RP1070-562	Battery Board ASM	5.219	1.92E+05	0..364
WZ0059-562	Lithium Battery	0.0023	4.27E+08	0.0002
RP1550-562	Controller Board ASM	135.8726	7359.8355	1.0
RP0224-562	GPS Board ASM	43.74673	2.29E+04	0.9775
RP2551-562	Transmitter Board ASM	158.5077	6308.8418	1.0
RP0250-562	Battery Board ASM	3.8968	2.57E+05	0.2867
RP5005-562	Enclosure Assembly	4.87091	2.05E+05	0.3445
RP2010-562	UI Board ASM	42.1241	2.37E+04	0.9741
RP5008-562	Internal Tx Antenna	7.4207	1.35E+05	0.4745
Total		2.34 E-09	4.28 E+08	

Calculate Reliability for 10 Years Service Life: $R = e^{-\lambda (t)} = = e^{-2.34(10)} = 0.9999 = 99.9\%$

PERFORMING PREDICTION USING SOFTWARE

Figure 2-16: **Electronics Reliability Prediction Using Software Application**



13 of 13 — System Hierarchy

Name	Category	Derating	Quantity	Failure Rate(t=INF)	Connection Failure Rate	MTBF
Telcordia SR-332 Issue 3	Telcordia SR-332 Issue 3		1	607.7869 FITs	-	1.6453E+06 hrs
PNC Module	Block		1	47.7960	-	2.0922E+07
Capacitor	Capacitor		1	13.5384	-	7.3864E+07
IC, Microcontroller	IC, Microcontroller		1	34.2576	-	2.9191E+07
User Interface Module	Block		1	51.3267	-	1.9483E+07
IC, ROM/PROM/EPROM	IC, ROM/PROM/EPROM		1	5.5316	-	1.8078E+08
IC, Microcontroller	IC, Microcontroller		1	34.2576	-	2.9191E+07
Connector	Connector		1	4.0462	-	2.4714E+08
Inductor	Inductor		1	7.4913	-	1.3349E+08
Vessel	Block		1	508.3477	-	1.9672E+06
Rotating Device	Rotating Device		1	508.3477	-	1.9672E+06
Optical Assembly	Block		1	0.3186	-	3.1391E+09
Opto-Electronic	Opto-Electronic		1	0.3186	-	3.1391E+09

Properties — Properties | Derating | Model

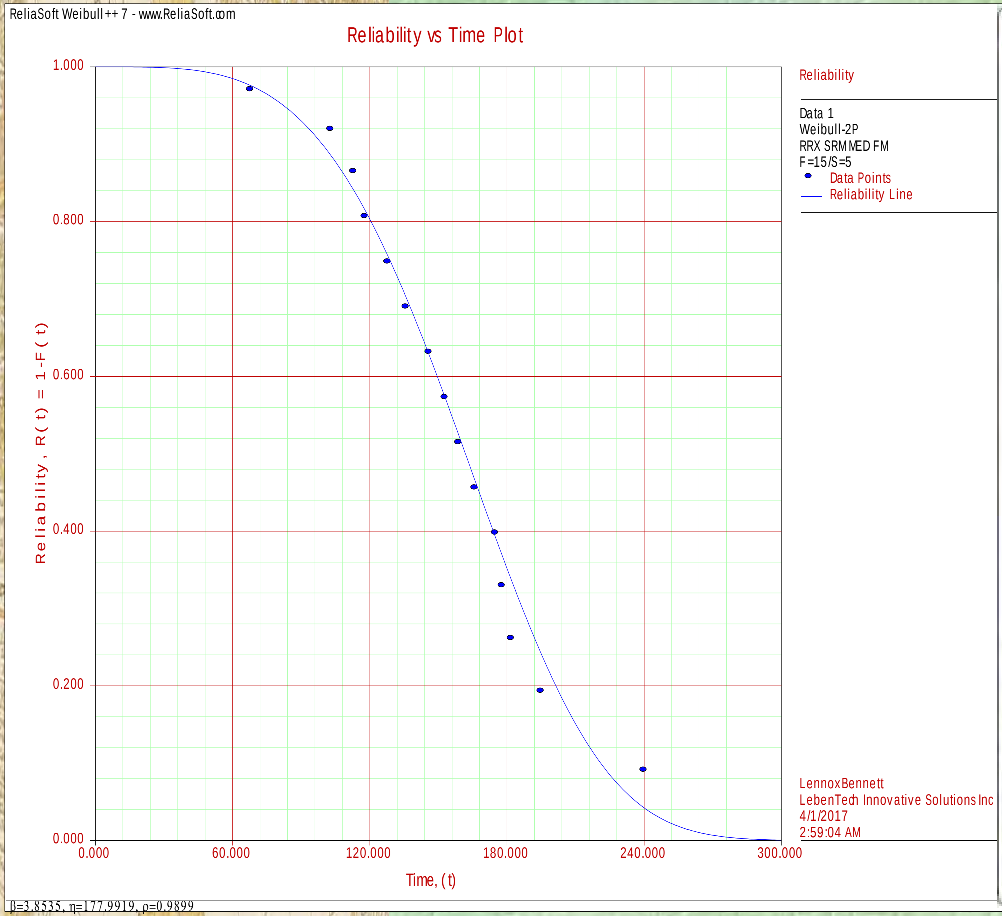
Properties	Values
General	
Name	Opto-Electronic
ID	
Part Number	
Alternate Part Number	
Revision	
LCN	
Reference Designator	
Supplier	
Description	
Function Description	
Quantity	1
Analyst	
Compiled By	
Approved By	
Comments	
Steady State Generic Failure Rate	0.2500
Type	LED/LCD Display
Quality Factor	3.0000
Quality	Level 1
Temperature Factor	0.4247

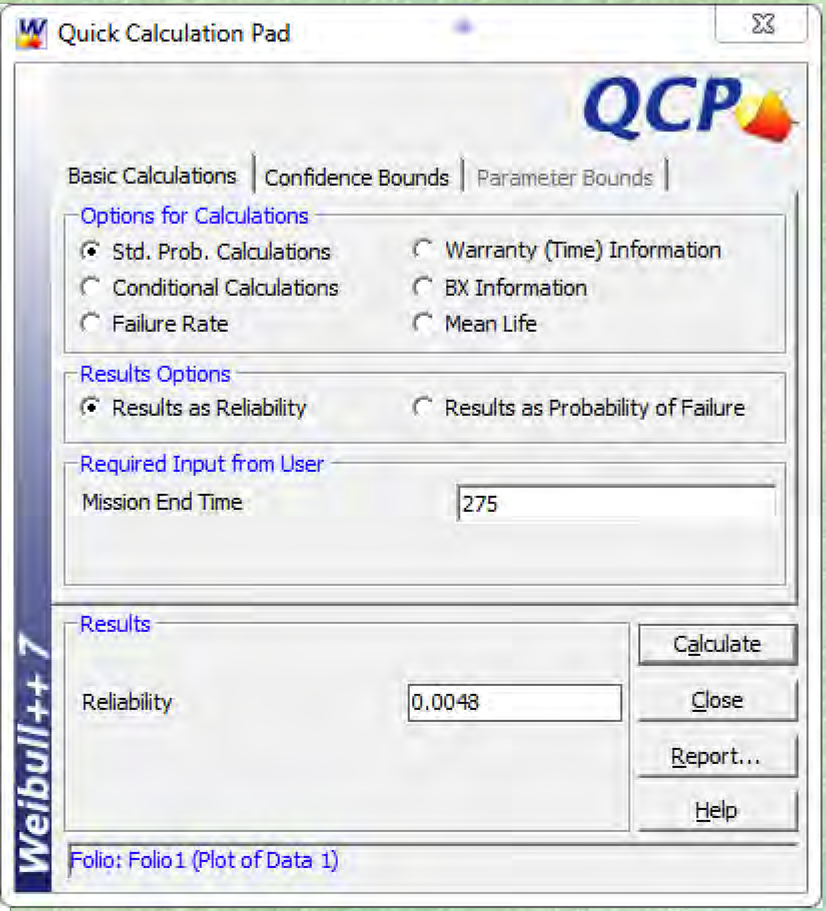
9.0.17 - 64-bit C:\Users\LebenTech\Documents\ReliaSoft\Files\RSRepository9.rsr9 Active Project: Project 1

Logged in as: Lennox Bennett (LebenTech)

STATISTICAL ANALYSIS EXAMPLE

Figure 2-18: Predicting the Reliability at a Specific Time





Options for Calculations

● Std. Prob. Calculations
○ Conditional Calculations
○ Failure Rate
○ Warranty (Time) Information
○ BX Information
○ Mean Life

Results Options

● Results as Reliability
○ Results as Probability of Failure

Required Input from User

Mission End Time: 275

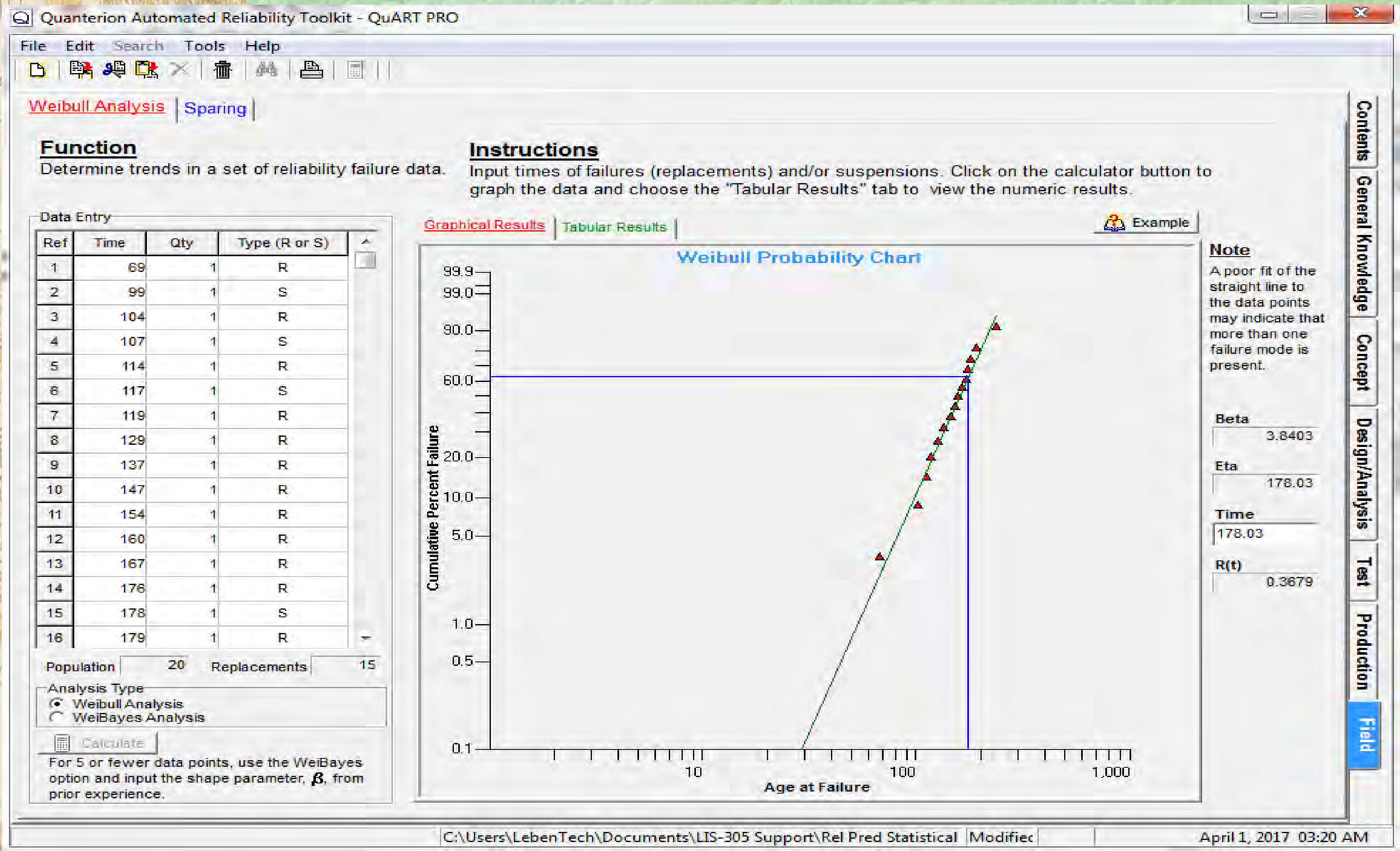
Results

Reliability: 0.0048

Folio: Folio1 (Plot of Data 1)

STATISTICAL ANALYSIS EXAMPLE

Figure 2-20: Weibull Probability Plot of Failure Data – QuART PRO Software



Function

Determine trends in a set of reliability failure data.

Instructions

Input times of failures (replacements) and/or suspensions. Click on the calculator button to graph the data and choose the "Tabular Results" tab to view the numeric results.

Data Entry

Ref	Time	Qty	Type (R or S)
1	69	1	R
2	99	1	S
3	104	1	R
4	107	1	S
5	114	1	R
6	117	1	S
7	119	1	R
8	129	1	R
9	137	1	R
10	147	1	R
11	154	1	R
12	160	1	R
13	167	1	R
14	176	1	R
15	178	1	S
16	179	1	R

Population 20 Replacements 15

Analysis Type
● Weibull Analysis
○ WeiBayes Analysis

For 5 or fewer data points, use the WeiBayes option and input the shape parameter, β, from prior experience.

Note

A poor fit of the straight line to the data points may indicate that more than one failure mode is present.

Beta 3.8403

Eta 178.03

Time 178.03

R(t) 0.3679

C:\Users\LebenTech\Documents\LIS-305 Support\Rel Pred Statistical Modifiec April 1, 2017 03:20 AM

MAINTAINABILITY EVALUATION OF PRODUCT DESIGN

Maintainability Consideration in System Design

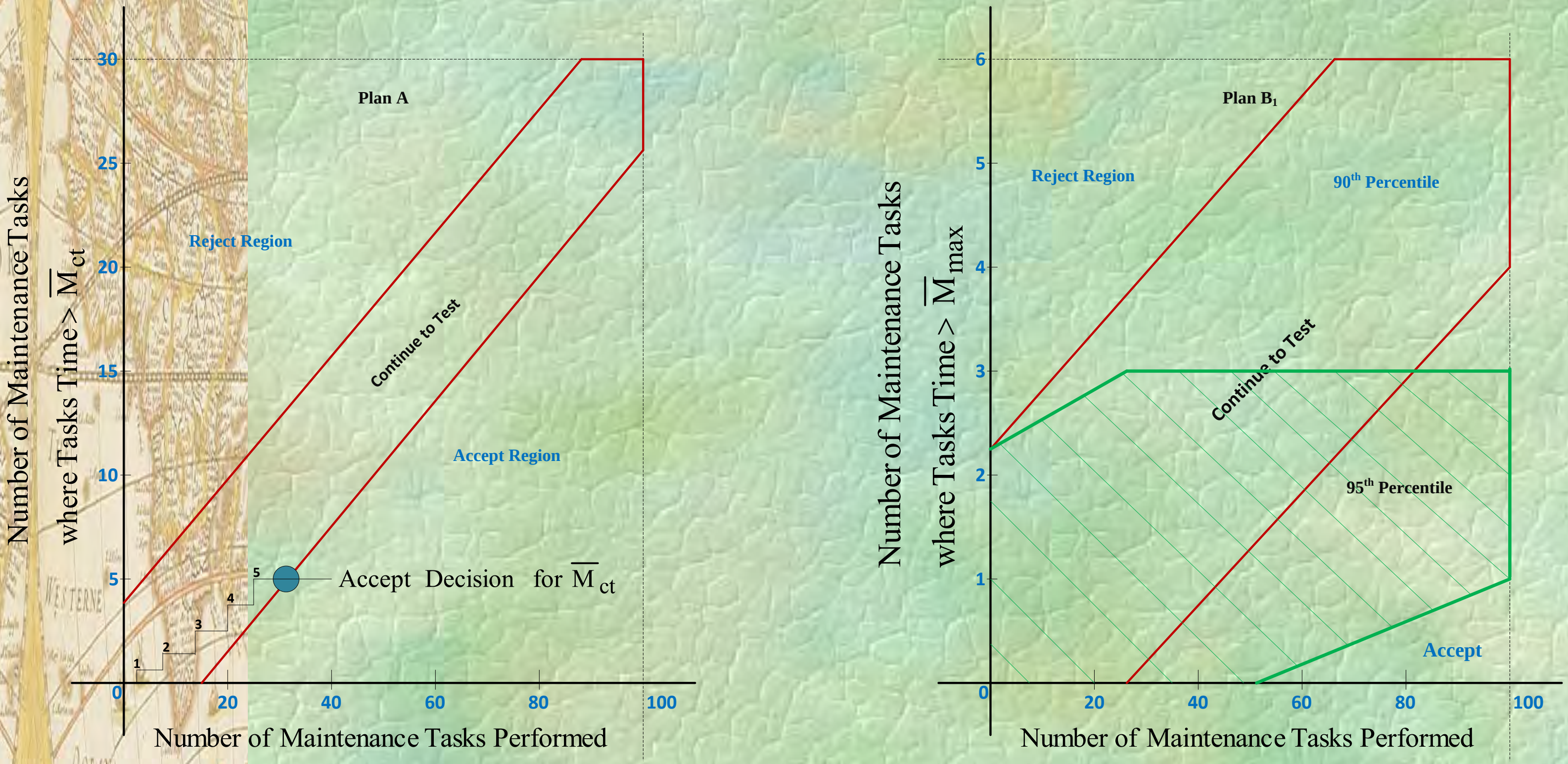
- ❑ **Maintainability Design Evaluation** is concerned with analyzing the maintenance implications of a proposed design and providing timely feedback to the design engineer.
- ❑ When this approach is applied to evaluate the design for maintainability; the applicable design criteria established in Appendix C of MIL-STD-470A will be used as the basis for evaluating the design for maintainability.

Table 2-32: Considerations in Design for Maintainability

Human Factors	Replacement Capability	Simplification
Design for Reliability	Mating and Connection	Good Visual Indicator
Accessibility - Easy Access to Serviceable items	Automate Fault Detection and Isolation (BIT)	Use of Tools and Test Equipment
System Testability	Reduce Number of Components in Final Assembly	Modularization
Standardization	Interchangeability	Mistake Proofing

MAINTAINABILITY EVALUATION OF PRODUCT DESIGN

Figure 2-23: Graphical Representation of M Demonstration Plans



Two sequential test plans were used and are identified herein. An “Accept” decision is reached when the test data indicates that the Mct/MTTR requirement of < 30 minutes is achieved. The graphical representations of the plans are provided in Figure 2-23.

SOFTWARE RELIABILITY PREDICTION

Software Reliability Growth

- ❑ A software reliability growth model mathematically summarizes a set of assumptions about the phenomenon of software failure.

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

- ❑ Where:

$\lambda(t)$ = Software failure rate at time t (failures per CPU second)

λ_o = Initial Software Failure Rate

t = CPU execution Time (seconds)

$$\beta = B\frac{\lambda_o}{W_o}\left(\text{decrease in failure rate per failure occurrence}\right)$$

Where:

B = Fault reduction factor (default = 0.955)

W_o = Initial number of faults in software program per 1,000 lines of code

SOFTWARE RELIABILITY PREDICTION

Example Application: Estimate C Software Reliability

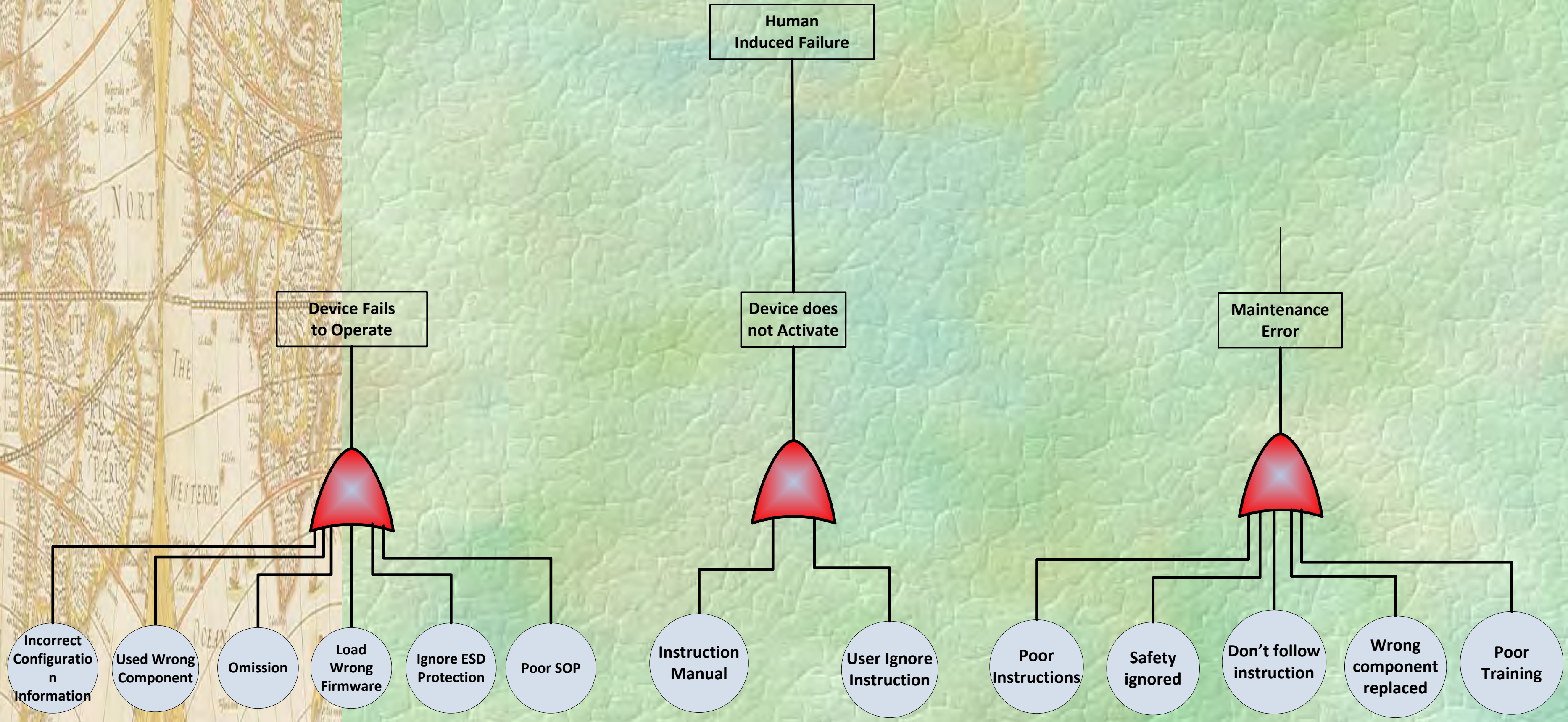
- ❑ Estimate the initial software failure rate and the failure rate after growth testing for 40,000 seconds of CPU execution from time at 3 MIPS. The software is a 25,000 line C program.

Solution

- ❑ R_i = 3 MIPS = 3,000,000 instructions/sec
- ❑ K = 4.2 x 10^{-7}
- ❑ W_o = (6 faults/1000 lines of code) (25,000 lines of code) = 150 faults
- ❑ I = (25,000 source lines of code) (4.5) = 62,500 instructions
- ❑ $\lambda_o = \dfrac{(3{,}000{,}000 \text{ inst./sec}) * (4.2 \times 10^{-7}) * (150 \text{ faults})}{62{,}500} = 0.003024 \text{ failuresper CPU second}$
- ❑ $\beta = B \dfrac{\lambda_o}{W_o} = (0.955)\left(\dfrac{0.003024}{150\text{faults}}\right) = 1.92528\text{x}10^{-5}$
- ❑ λ(40,000) = 0.003024 $e^{-\text{ (1.92528 x 10-5 failures/sec) (40,000 sec})}$ = 0.0013999 failures/CPU second.

HUMAN RELIABILITY PREDICTION

Figure 2-25: Fault Tree of Human Induced Failure of Communication System



ALLOCATING RELIABILITY TO A SYSTEM

Table 2-35: Reliability Allocation Calculation

AGREE APPORTIONMENT

System Reliability Requirement = 0.95%

	Beacon	Subsystem Name	No. Modules | Complexity k_i	Importance Factor w_i	Operating Time [T_i Hrs]	Allocated MTBF [θ_i Hrs]	Allocated Reliability
1	Subsystem 1	X	1	0.5	87600	69166935.8	0.998734301
		X	1	0.5	87600	69166935.8	0.998734301
		X	10	1	87600	13833387.16	0.993687503
		X	3	1	87600	46111290.53	0.998102052
		X	1	1	87600	138333871.6	0.99936695
		X	5	0.2	87600	5533354.864	0.984293392
2	Subsystem 2	X	1	1	87600	138333871.6	0.99936695
		X	12	0.33	87600	3804181.469	0.977235812
		X	3	1	87600	46111290.53	0.998102052
		X	1	1	87600	138333871.6	0.99936695
		X	5	0.2	87600	5533354.864	0.984293392
3	Subsystem 3	X	1	1	87600	138333871.6	0.99936695
		X	1	0.65	87600	89917016.54	0.999026243
4	Subsystem 4						
5	Subsystem 5	X	36	0.2	87600	768521.5089	0.892271252
N =			81				

Importance factor for a subsystem is defined as the probability of system failure if this subsystem fails. If equals 1 the subsyem must operate successfully for the Nexcimer system to operate success fully. If equals 0 then failure of the unit has no effect on system operation.

Looking at coverage the probability of failure for Safery Modume is 1/5 = 0.2 | Probability of failure for Firing Control = 1/5 = 0.2. Loking at dependent events P(A and B) = P(A) * P(B?A) = 0.2 * (0.2/0.02) = 0.20

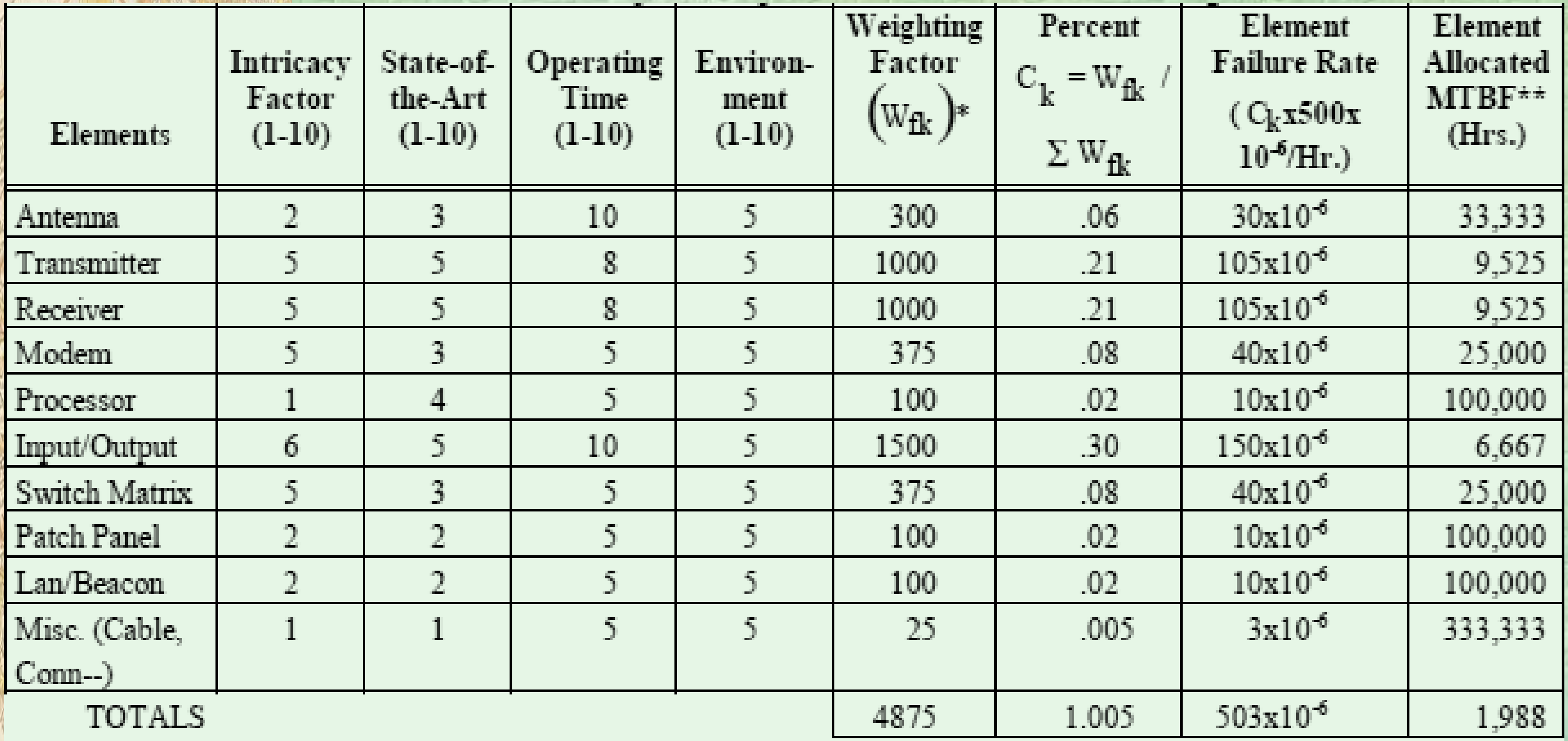
$$\mathrm{MTBF\,for Subsystem}_i = \theta_1 = \frac{N w_i T_i}{k_i\{-\mathrm{In}\,R(T)\}}$$

$$R_i(T_i) = e^{-(T_i / \theta_i)}$$

Copyright © 2016 LEBENTECH ® – Proactive Innovative Solutions for Success and Competitive Advantages

ALLOCATING RELIABILITY TO A SYSTEM

Figure 2-36: Feasibility of Objective Allocation Technique



Elements	Intricacy Factor (1-10)	State-of-the-Art (1-10)	Operating Time (1-10)	Environment (1-10)	Weighting Factor (W_{fk})*	Percent $C_k = W_{fk} / \Sigma W_{fk}$	Element Failure Rate $(C_k x500x 10^{-6}/Hr.)$	Element Allocated MTBF** (Hrs.)
Antenna	2	3	10	5	300	.06	$30x10^{-6}$	33,333
Transmitter	5	5	8	5	1000	.21	$105x10^{-6}$	9,525
Receiver	5	5	8	5	1000	.21	$105x10^{-6}$	9,525
Modem	5	3	5	5	375	.08	$40x10^{-6}$	25,000
Processor	1	4	5	5	100	.02	$10x10^{-6}$	100,000
Input/Output	6	5	10	5	1500	.30	$150x10^{-6}$	6,667
Switch Matrix	5	3	5	5	375	.08	$40x10^{-6}$	25,000
Patch Panel	2	2	5	5	100	.02	$10x10^{-6}$	100,000
Lan/Beacon	2	2	5	5	100	.02	$10x10^{-6}$	100,000
Misc. (Cable, Conn--)	1	1	5	5	25	.005	$3x10^{-6}$	333,333
TOTALS					4875	1.005	$503x10^{-6}$	1,988

Note: *W_{fk} = Intricacy x State-of-the-Art x Operating Time x Environment | ** MTBF = 1/ element failure rate

Source: RiAC Blueprint of Reliability

PRODUCT THERMAL DESIGN ANALYSIS

Thermal Analysis

- ❑ Temperature is one of the most important influences on reliability. Although temperature effects are usually associated with electronics, the reliability of mechanical components is also affected by temperature.

- ❑ By conducting thermal analysis, the designer can determine heat transfer path and modes, temperature extremes experienced by individual components and parts, and the impact of thermal shock caused by rapid change in temperature.

- ❑ In performing the analysis, the designer may find that even with reasonable cooling provisions and optimum placement of components and parts, the temperature encountered by the product and its constituent part make the reliability requirement technically or economically infeasible.

PRODUCT THERMAL DESIGN ANALYSIS

The figures below illustrate the thermal image for the Controller board and RF board respectively from a communication device. The maximum temperature for the controller board is 26.8^{0}C and 33.3^{0}C for the RF Board

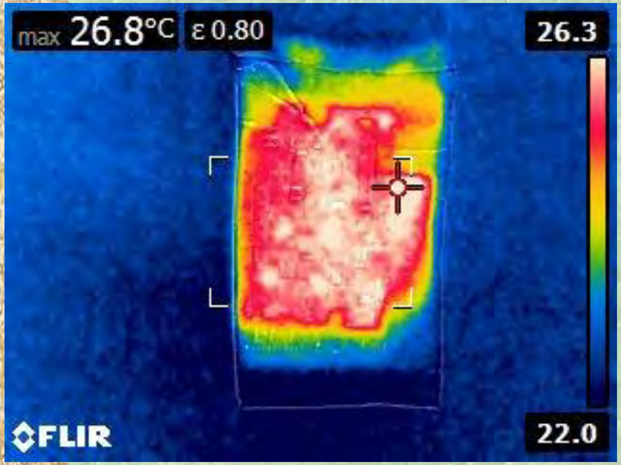


Figure 2-29: Controller Board

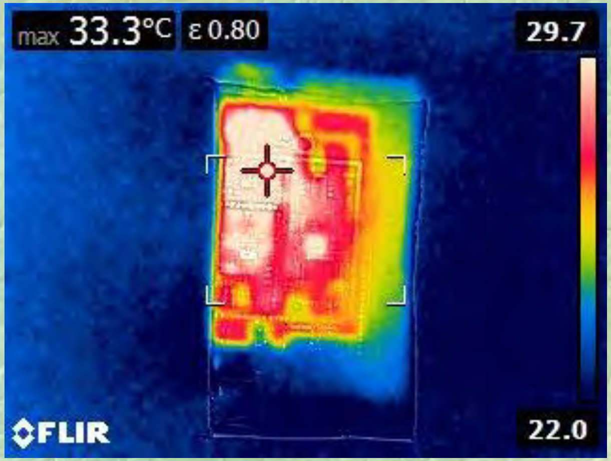


Figure 2-30: RF Board

A FLIR-E63900 was used for the measurement. Ambient temperature condition was 23 – 25^{0}C with power supply set to 7.5 VDC and the device was operating for four days. Communication frequencies of 121.5 MHz and 243 MHz were active for this operation, and the GPS activity was also active but no signal was applied to GPS. As can be seen in the illustration the maximum operating temperatures are below the ambient temperature of 55^{0}C.

APPLICATION OF WORSE CASE ANALYSIS

Table 2-42: Data for Worse Case Analysis Calculations

Parameters: Capacitance	Bias (%)		Random (%)
	Negative	Positive	
Initial Tolerance at 25 ^{0}C	- -	- -	20
Initial Tolerance at (-20 ^{0}C)	28	- -	- -
Initial Tolerance at (+80 ^{0}C)	- -	17	- -
Other-Environments (Hard Vacuum)	20	- -	- -
Radiation (10KR, 10^{13} N/cm^2)	- -	12	- -
Aging	- -	- -	10
Total Variation	48	29	

Where:

Worse Case Minimum = - 48 – 22.4 = -70.4%

Worse Case Maximum = + 29 + 22.4 = +51.4%

Worse Case Minimum Capacitance = 1200 μF – 1200 μF [| -.0.48 | + 0.224] = 355.2 μF

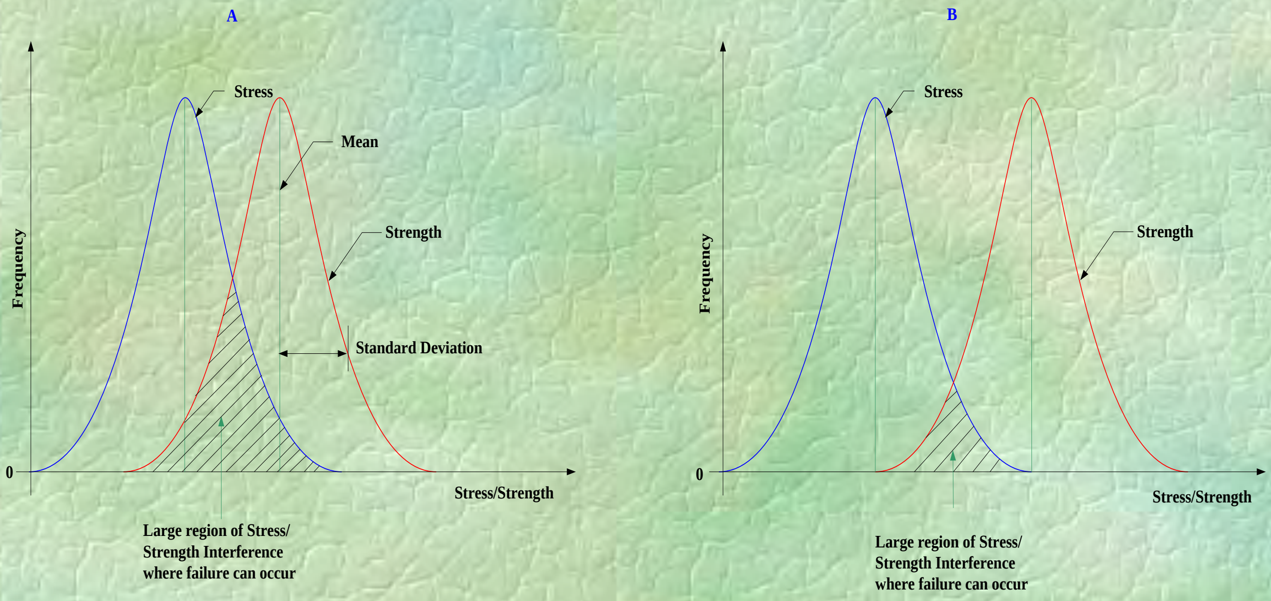
Worse Case Maximum Capacitance = 1200 μF + 1200 μF [| + 0.29 | + 0.224] = 1816.8 μF

It should be noted that quantifying the contribution of environment effects on component variability is a critical step in the development of a Worse Case Analysis. Reference 5 provides additional details.

APPLYING STRESS/STRENGTH TO PRODUCT DESIGN

- An example of a strength as a function of time is the fatigue properties of the material. The fatigue properties pertain to the strength degradation over time.
- At time = 0, the probability of failure is the interaction of the stress and the strength distributions, as illustrated in figure 2-38.
- The calculation of the normally-Distributed Stress and Strength Distribution is:
- $$\frac{\mu_x - \mu_y}{\sqrt{\sigma_x^2 + \sigma_y^2}}$$
- Z = Standard Normal variant (i.e., the number of standard deviations from the normal standardized distribution).

Figure 2-38: Stress-Strength Interference



STRESS-STRENGTH DESIGN CONCEPTS

High Strength for Increased Reliability and Safety

- In general maintaining an inherently low product failure rate is essential to a product’s ability to provide high reliability and high safety.
- To achieve low failure rate a product must provide “high strength”. The product’s ability to withstand the stresses such as heat, chemicals, and vibration that cause failure, can be defined as its strength.
- The design concept of strength and its relationship to failure rate is as follows:
  - When stress exceeds strength a failure occur
  - The lower the strength, the higher the failure rate
  - The higher the strength, the lower the failure rate.
- The chance of stress exceeding strength, thus resulting in a failure is related to the “interference area” between the curves.
- Figure 2-31 illustrates the concept that a failure occurs when some stressor or combination of stressors exceeds the associated strength of the product

APPLYING STRESS/STRENGTH TO PRODUCT DESIGN

Example Application

❑ Several machine tool drives were tested experimentally under identical operating (cutting) conditions. The stress induced in ten belts were found to be 22,300, 11,600, 15,850, 19,900, 13,650, 16950, 26,750, 12,700, 18,400 and 15,100 lb/in^2.

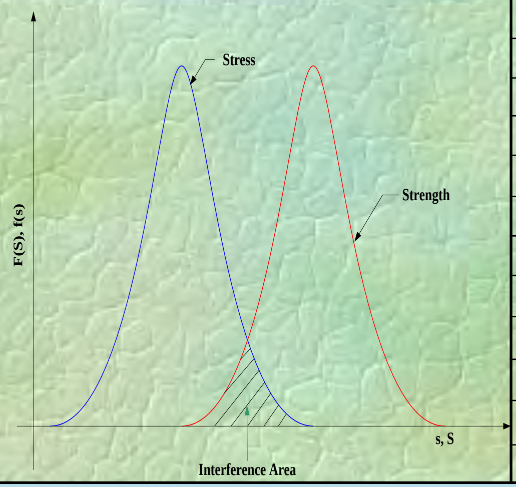
❑ The value of strength found by testing twelve of the belts used in the machine tool drives were: 21,100, 26,950, 19200, 30150, 22050, 24350, 18250, 25700, 23400, 19950, 21600, and 20500 lb/in^2.

❑ Find the reliability of the belt drives.

APPLYING STRESS/STRENGTH TO PRODUCT DESIGN

Example Application

Table 2-46: Stress- Strength Data

	Strength Data		Representation of Stress-Strength	Stress Data	
No	Strength (lb/in^2)	Cumulative Probability	Stress Strength Diagram	Strength (lb/in^2)	Cumulative Probability
1	18250	0.083		11600	0.1
2	19200	0.167		12700	0.2
3	19950	0.250		13650	0.3
4	20500	0.333		15100	0.4
5	21100	0.417		15850	0.5
6	21600	0.500		16950	0.6
7	22050	0.583		18400	0.7
8	23400	0.667		19900	0.8
9	24350	0.750		22300	0.9
10	25700	0.833		26750	1.0
11	26950	0.917			
12	30150	1.000			

APPLYING STRESS/STRENGTH TO PRODUCT DESIGN

Table 2-42: Approximate Distribution for Strength

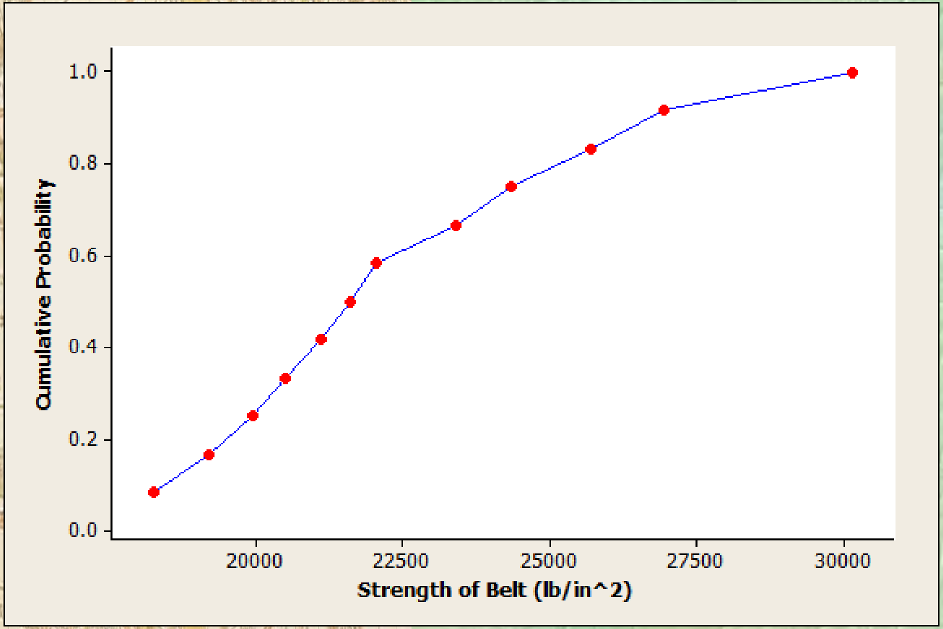
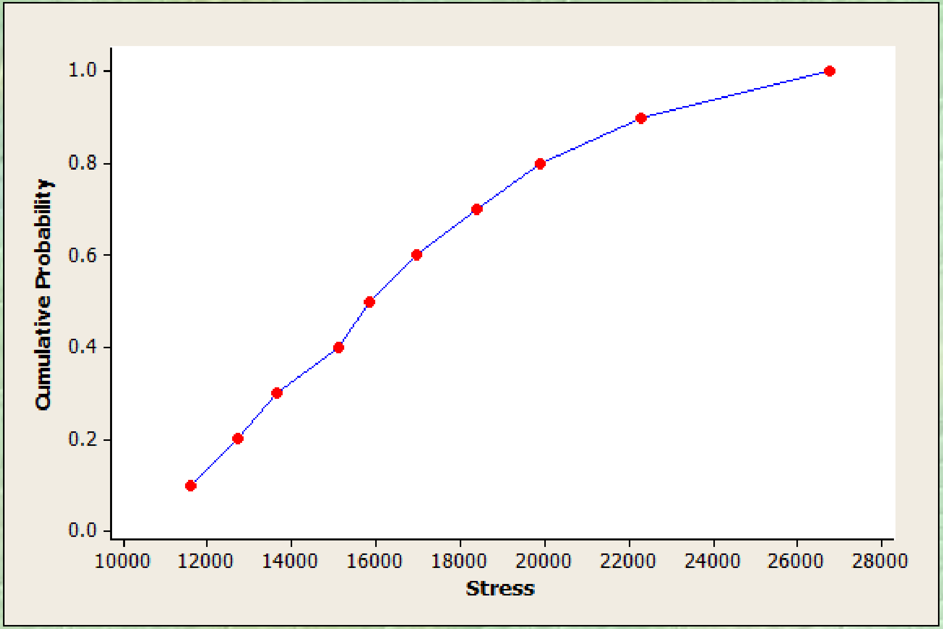
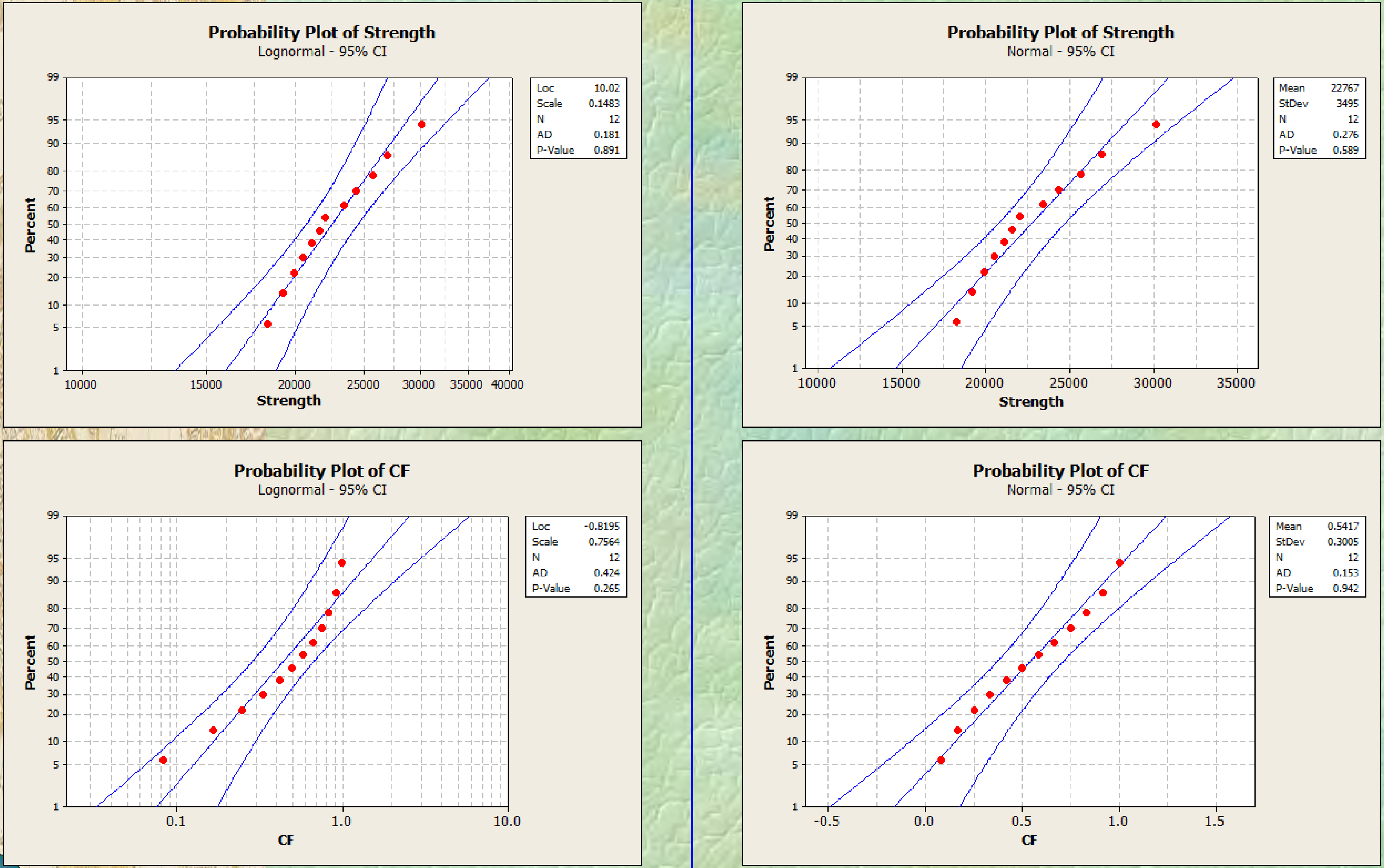


Table 2-43: Approximate Distribution for Stress



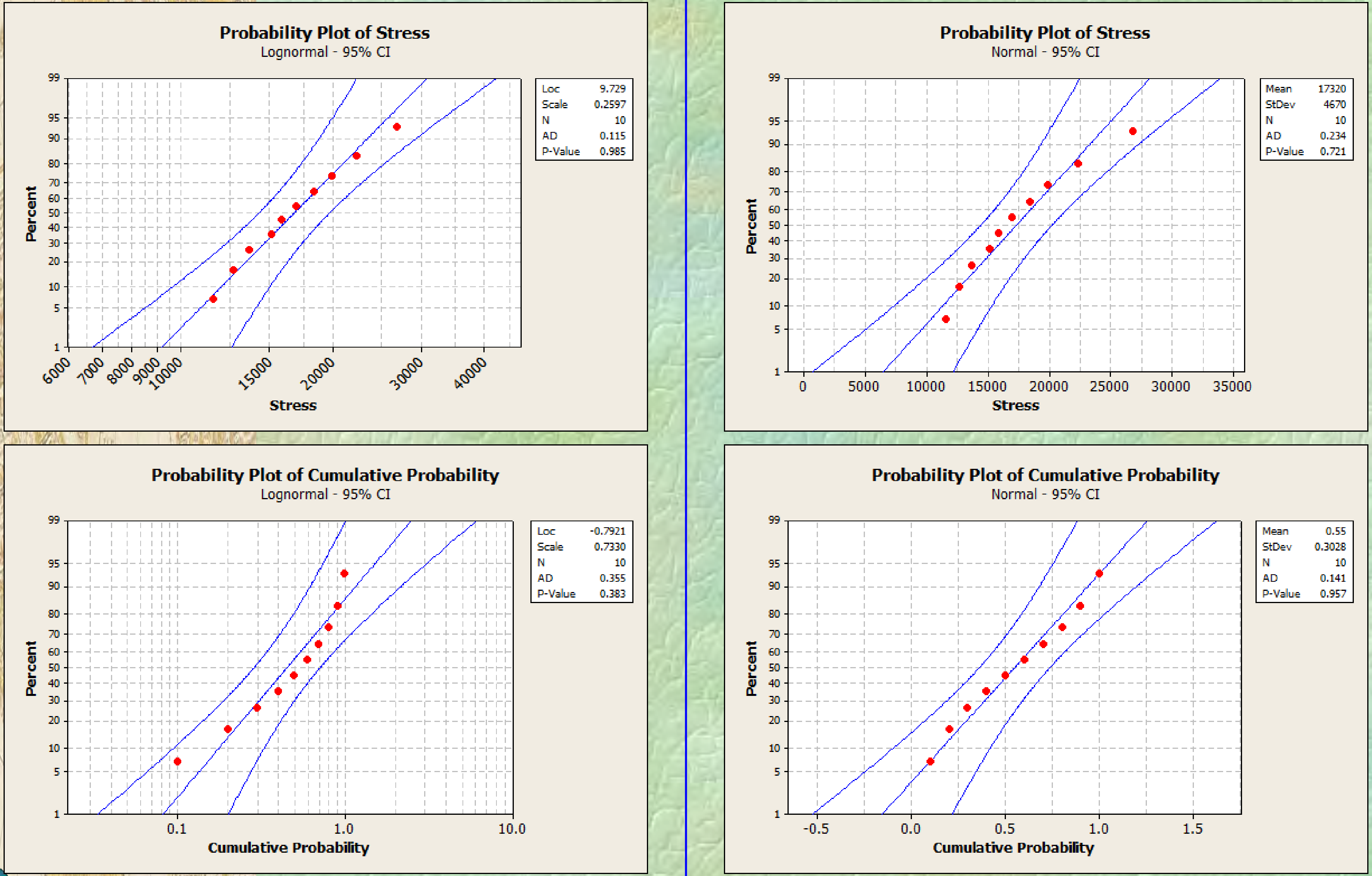
APPLYING STRESS/STRENGTH TO PRODUCT DESIGN

Table 2-44: Comparing Probability Pots of Strength for Normal and Lognormal Distribution



APPLYING STRESS/STRENGTH TO PRODUCT DESIGN

Table 2-45: Comparing Probability Pots of Stress for Normal and Lognormal Distribution



Probability Plot of Stress
Lognormal - 95% CI

Loc	9.729
Scale	0.2597
N	10
AD	0.115
P-Value	0.985

Probability Plot of Stress
Normal - 95% CI

Mean	17320
StDev	4670
N	10
AD	0.234
P-Value	0.721

Probability Plot of Cumulative Probability
Lognormal - 95% CI

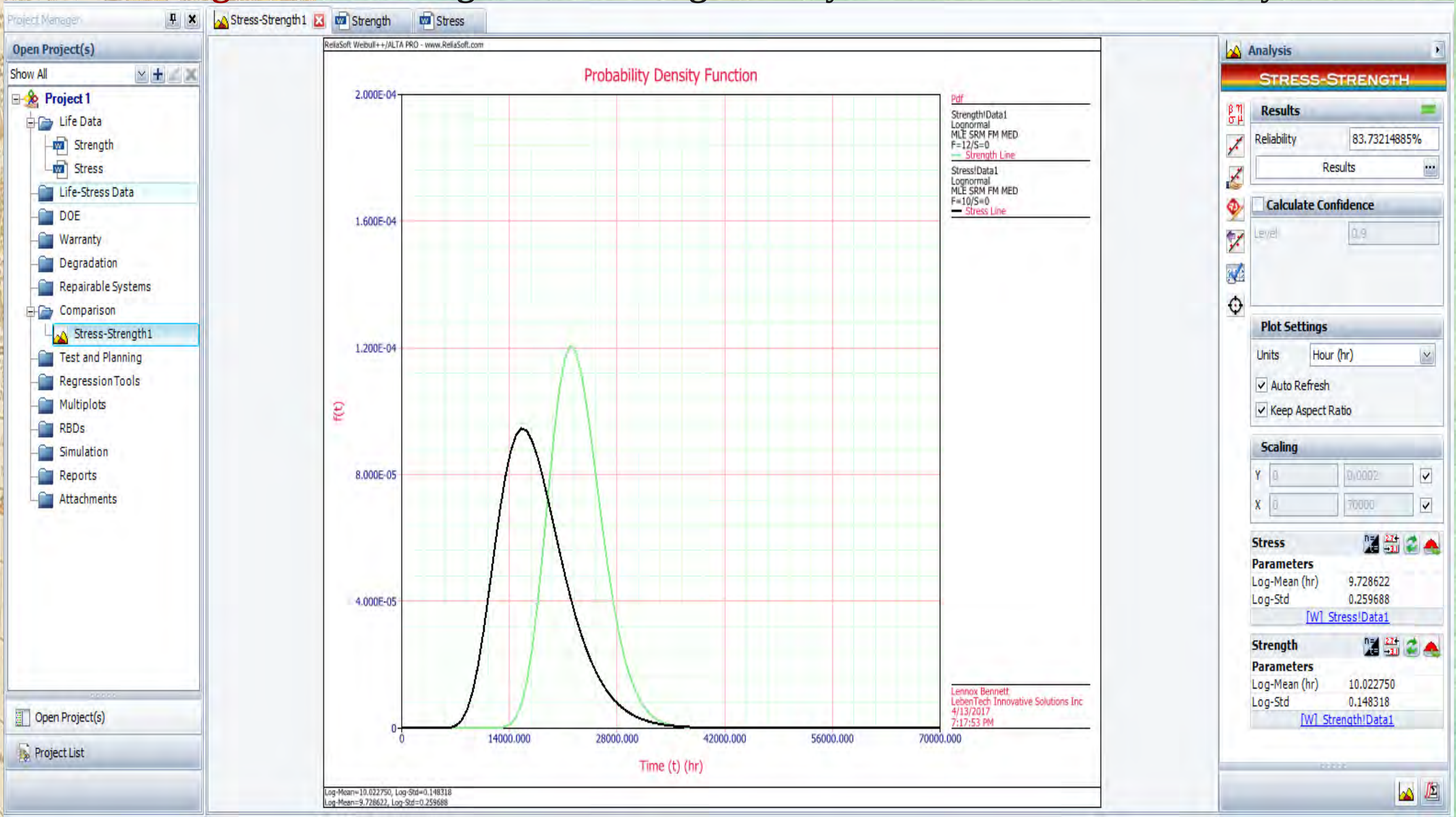
Loc	-0.7921
Scale	0.7330
N	10
AD	0.355
P-Value	0.383

Probability Plot of Cumulative Probability
Normal - 95% CI

Mean	0.55
StDev	0.3028
N	10
AD	0.141
P-Value	0.957

SOFTWARE APPLICATION STRESS-STRENGTH ANALYSIS

Figure 2-46: Using Stress- Strength Analysis to Determine Reliability



Strength!Data1
Lognormal
MLE SRM FM MED
F=12/S=0

Stress!Data1
Lognormal
MLE SRM FM MED
F=10/S=0

Lennox Bennett
LebenTech Innovative Solutions Inc
4/13/2017
7:17:53 PM

Log-Mean=10.022750, Log-Std=0.148318
Log-Mean=9.728622, Log-Std=0.259688

Reliability 83.73214885%

□ Calculate Confidence

Level 0.9

Units Hour (hr)

☑ Auto Refresh

☑ Keep Aspect Ratio

Y 0 0.0002 ☑

X 0 70000 ☑

Stress

Parameters

Log-Mean (hr)	9.728622
Log-Std	0.259688

[W] Stress!Data1

Strength

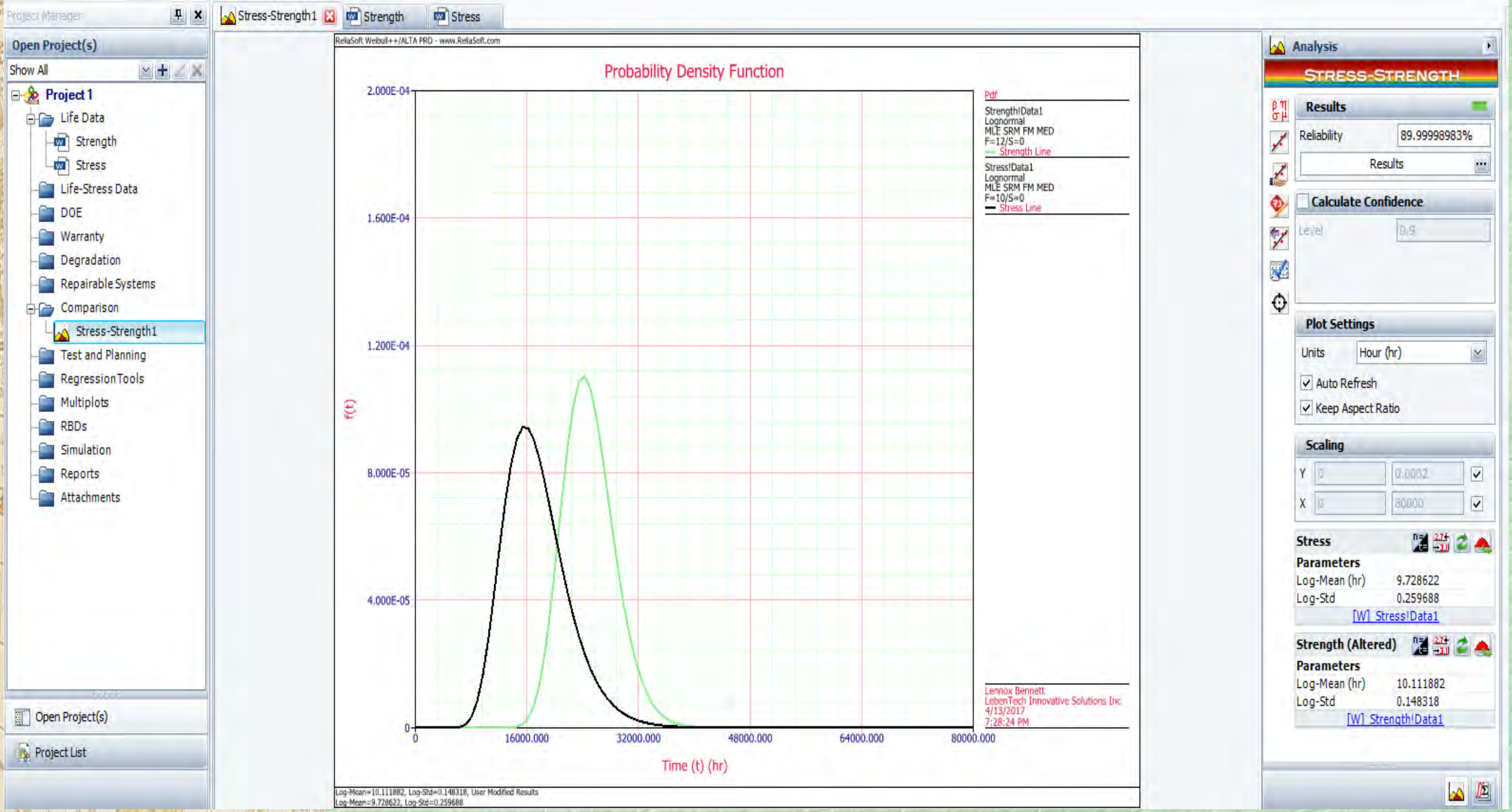
Parameters

Log-Mean (hr)	10.022750
Log-Std	0.148318

[W] Strength!Data1

SOFTWARE APPLICATION STRESS-STRENGTH ANALYSIS

Figure 2-47: Determine Stress- Strength Given Target Reliability



Pdf

Strength!Data1
Lognormal
MLE SRM FM MED
F=12/S=0
— Strength Line

Stress!Data1
Lognormal
MLE SRM FM MED
F=10/S=0
— Stress Line

Lennox Bennett
LebenTech Innovative Solutions Inc
4/13/2017
7:28:24 PM

Log-Mean=10.111882, Log-Std=0.148318, User Modified Results
Log-Mean=9.728622, Log-Std=0.259688

Reliability 89.99998983%

Results

□ Calculate Confidence

Level 0.9

Units Hour (hr)

☑ Auto Refresh

☑ Keep Aspect Ratio

Y 0 0.0002 ☑

X 0 80000 ☑

Stress

Parameters

Log-Mean (hr)	9.728622
Log-Std	0.259688

[W] Stress!Data1

Strength (Altered)

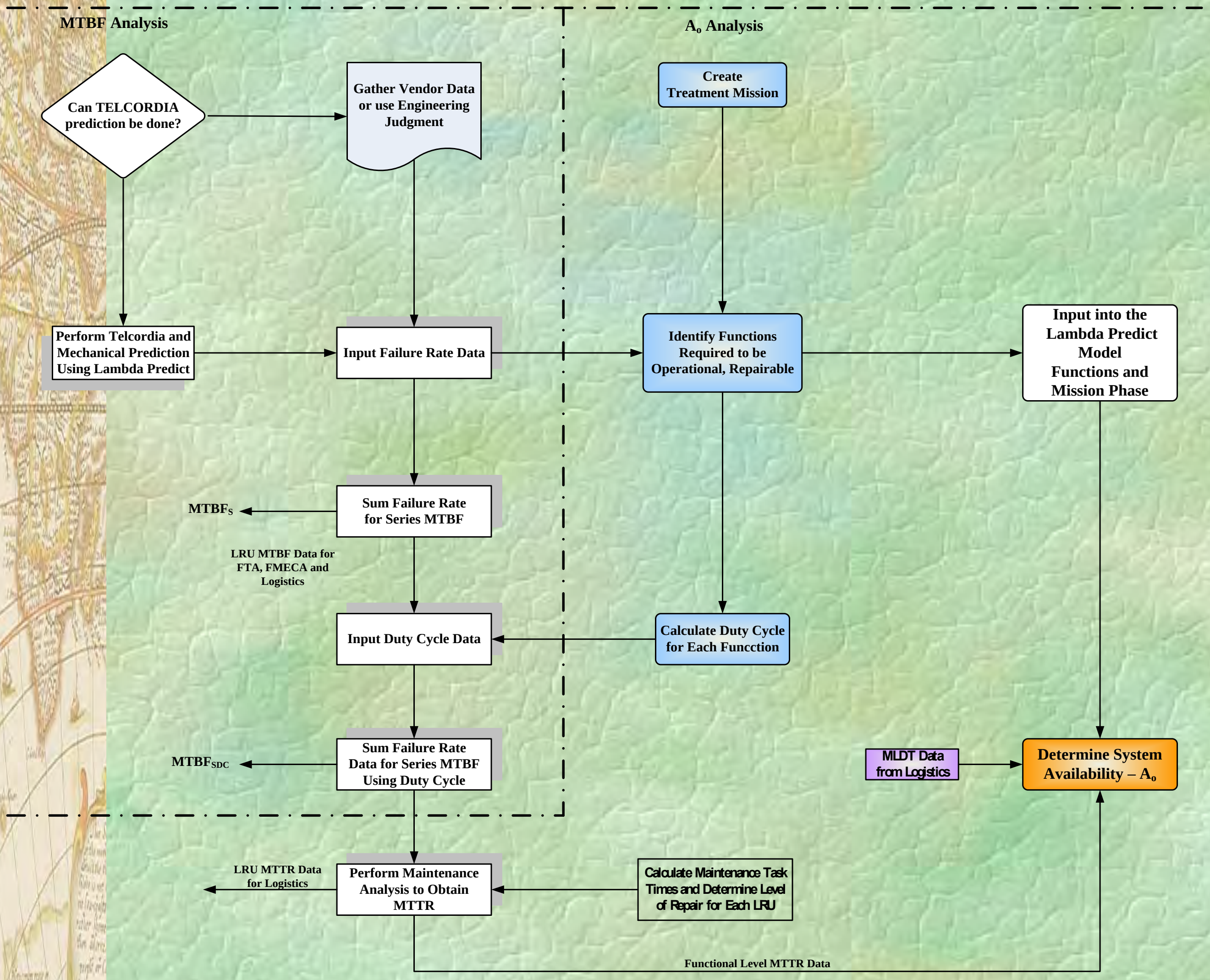
Parameters

Log-Mean (hr)	10.111882
Log-Std	0.148318

[W] Strength!Data1

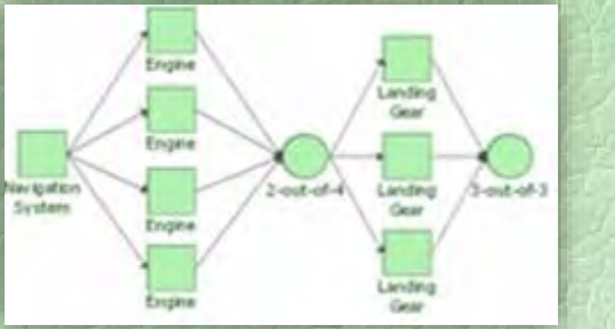
RELIABILITY MODELING APPLICATION

Figure 2-48: Flow Diagram for Reliability, Maintainability, and Availability Predictions


MTBF Analysis
A_o Analysis
Can TELCORDIA prediction be done?
Gather Vendor Data or use Engineering Judgment
Create Treatment Mission
Perform Telcordia and Mechanical Prediction Using Lambda Predict
Input Failure Rate Data
Identify Functions Required to be Operational, Repairable
Input into the Lambda Predict Model Functions and Mission Phase
$MTBF_S$
Sum Failure Rate for Series MTBF
LRU MTBF Data for FTA, FMECA and Logistics
Input Duty Cycle Data
Calculate Duty Cycle for Each Funcction
$MTBF_{SDC}$
Sum Failure Rate Data for Series MTBF Using Duty Cycle
MLDT Data from Logistics
Determine System Availability – A_o
LRU MTTR Data for Logistics
Perform Maintenance Analysis to Obtain MTTR
Calculate Maintenance Task Times and Determine Level of Repair for Each LRU
Functional Level MTTR Data

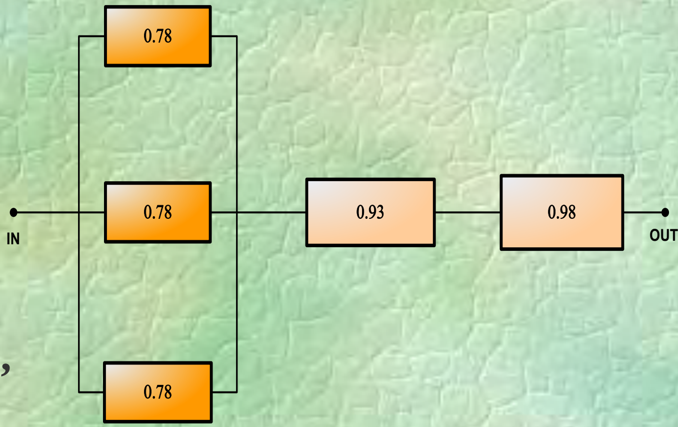
QUANTIFYING SYSTEM RELIABILITY

Reliability Block Diagrams (RBDS)



- ❑ A reliability block diagram is a graphical representation of how the components/subsystems of a system are “ reliability-wise” connected.
- ❑ Blocks represents components of the system:
  - ▪ Each block has a failure and a repair characteristics
- ❑ Lines connect the blocks
  - ▪ The structure of these connections affects the reliability of the system
- ❑ RDB Applications

1. Establishing specification boundaries
2. Vendor appraisal and design selection
3. Design optimization [architecture and components]
4. Establishing subsystem and components requirements
5. Scenario modeling [failure modes, loads, duty cycle, procurement/running costs].



– Proactive Innovative Solutions for Success and Competitive Advantages

SYSTEM AVAILABILITY APPLICATION

- ❑ For series availability, consider the system represented by the block diagram shown in Fig. 2-55.
- ❑ Since the components are in series, the availability can be found by multiplying the availabilities of the two components as shown in equation below:

Series Availability = $A_A * A_B$ = 0.99943 * 0.91254

= 0.91202

- ❑ For parallel availability, consider the system represented by the block diagram in figure 2-56.
- ❑ Since the components are parallel, the system availability can be found as shown in equation below:

Parallel Availability = 1 – $(1 - A_T) * (1 - A_B)$

= 1 – (0.0.08798) * (0.0.08798)

= 0.99226

Where:

A_T - is the availability of the top path

Table 2-55: Example Availability Block Diagram

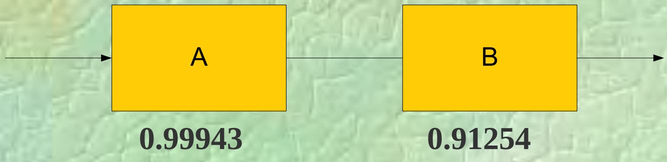
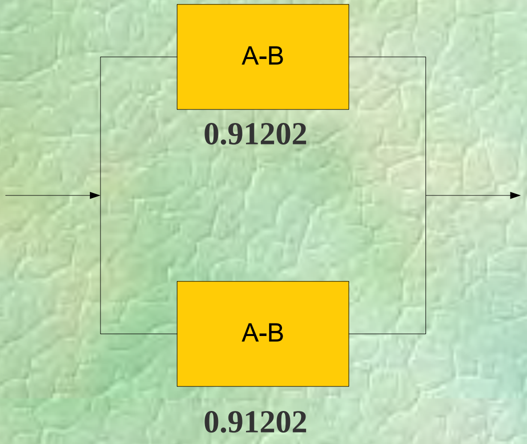


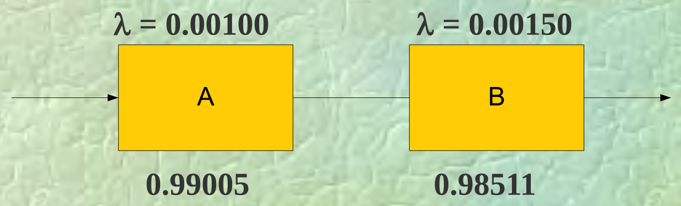
Table 2-56: Availability Block Diagram of System with Redundant Component



SYSTEM RELIABILITY APPLICATION

- ❑ If the underlying distribution for each element is exponential and the failure rate (λ_i) for each element are known, then the reliability of the system can be calculated using equation below:
- ❑ Series Reliability: Consider the system represented by the block diagram shown in Fig. 2-54.

Table 2-57: Example Reliability Block Diagram



- ❑ Components A and B in figure 2-57 are said to be in series, which means must operate for the system to operate.
- ❑ Since the system can be more reliable than the least reliable component, the configuration is often referred to as the weakest link configuration.
- ❑ Since the components are in series, the system reliability can be found by adding together the failure rates of the components and substituting the results in equation below:

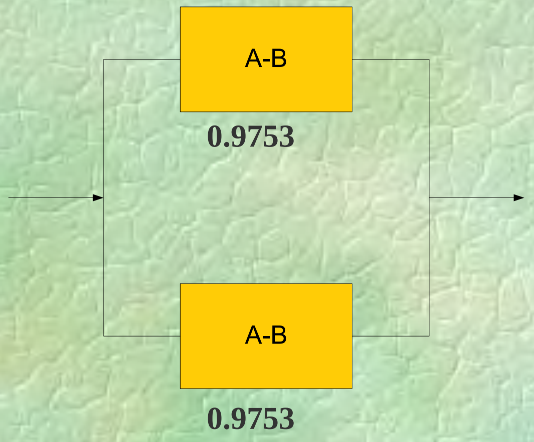
$$R(t) = e^{-(\lambda_A + \lambda_B)t} = e^{-0.0025*10} = 0.9753$$

- ❑ Furthermore, if the individual reliabilities are calculated [the bottom values] we could find that the system reliability by multiplying the reliabilities of the two component as shown in equation below:
- ❑ R(t) = RA(t) * RB(t) = 0.99000 * 0.98510 = 0.9753

SYSTEM AVAILABILITY APPLICATION

- ❑ Reliability with Redundancy: Now consider the system represented by the block diagram shown in Fig. 2-X.
- ❑ The system represented by the RBD in figure 2-58 has the same components (A and B in series denoted by one block labeled: A-B) used in figure 2-57, but two of each components are used in a configuration referred to as redundant or parallel.
- ❑ Two paths of operation are possible. The paths are top A-B and Bottom A-B. If either of two paths is intact, the system can operate.
- ❑ The reliability of the system is most easily calculated [equation below] by finding the probability of failure [1 – R(t)] for each path, multiplying the probabilities of failure, and then subtracting the result from 1.
- ❑ The reliability of each path was determined from the previous example.

Table 2-58: RBD of System with Redundant Components



RELIABILITY BLOCK DIAGRAM SYSTEM MODELING

- **Next, the probability of a path failing is found by subtracting its reliability from 1. Thus, the probability of either path failing is: 1 – 0.9753 = 0.0247.**
- **The probability that both paths will fails is: 0.0247 * 0.0247 = 0.0006.**
- **Finally, the reliability of the system is 1 – 0.0006 = 0.9994, about 2.5% improvement over the series configuration system.**
- **$R(t) = 1 – [1 – R_T(t)] * [1 – R_B(t)] = 1 – (0.0274) * 0.0274) = 0.9994$**
- **Where:**

  R_T is the reliability of the top path

  R_B is the reliability of the bottom path
- **A_i is defined by the following equation and reflects the percent of time a system would be available if delays due to maintenance, parts are ignored.**

$$A_i = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} \times 100\%$$

RELIABILITY BLOCK DIAGRAM SYSTEM MODELING

Figure 2-59: Analyzing the Contribution to System Reliability

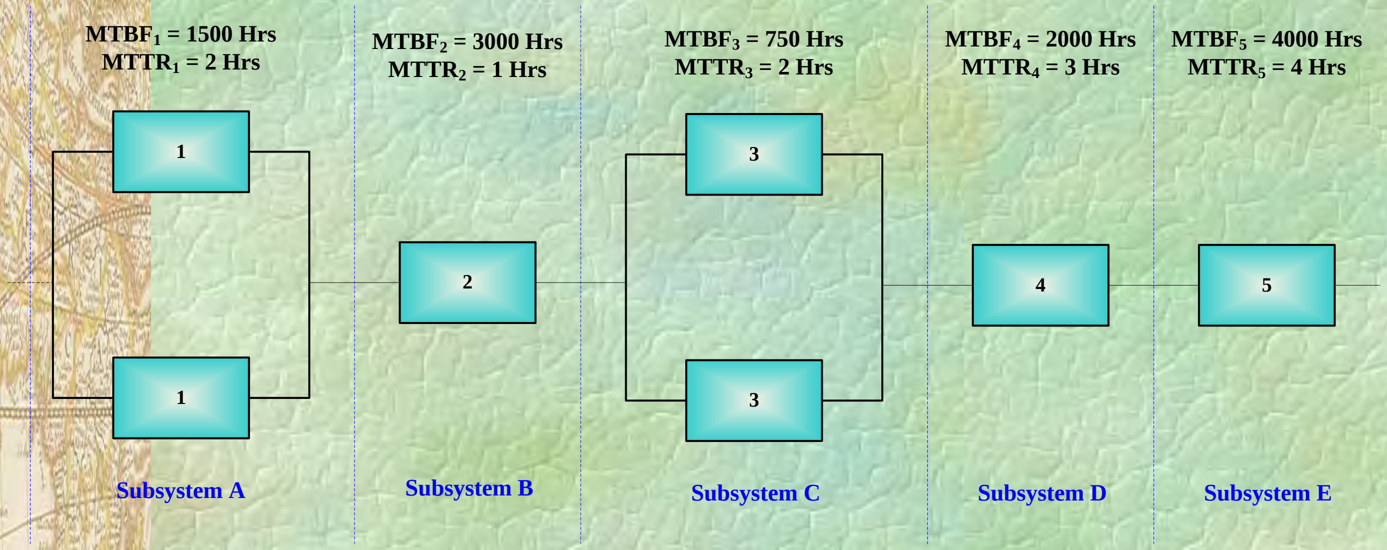


Table 2-47: Availability of System in Figure 2-59

MTBM	Mean System Failures	MTTR	Availability
258.77	1.0658	2.5695	99.7236

1. For ease of calculation, the times to failure and the times to repair were assumed to be distributed exponentially
2. 10,000 simulations trials were run using and operating time of 1,000 hours.

RELIABILITY BLOCK DIAGRAM SYSTEM MODELING

Table 2-48: Relative Unreliability of Subsystems [Repairs ignored]

Subsystem.	Reliability in 1000 Hours	Expected Failures per 1000 Hours	% Contribution to System Unreliability	Contribution to System Unreliability Ranking
A	0.7632	0.2368	14.12	4
B	0.7165	0.2835	16.90	3
C	0.4577	0.5423	32.33	1
D	0.6065	0.3935	23.46	2
E	0.7788	0.2212	13.19	5
System	0.1182	1.6773	-	-

STANDBY REDUNDANCY

- The system reliability of (n + 1) unit, in which one unit is operating and n units on the standby mission until the operating unit fails, is given by:

$$R_{sd}(t)=\sum_{i=0}^{m}\left[\int_{0}^{t}\lambda(t)\,dt\right]^{i} e^{-\int_{0}^{t}\lambda(t)dt}/i!$$

Where:

R_{sd} (t) is the standby system reliability.

m is the number of standby units..

- When modeling a system with standby redundancy the reliability of the standby and the primary unit is needed as well as the reliability of the sensing and switching system that controls the system’s operation.

- The above equation is true if the following are true.

1. The switching arrangement is perfect.
2. The units are identical.
3. The unit failure rates are constant.
4. The standby units are as good as new.
5. The unit failure are statistically dependent.

STANDBY REDUNDANCY

- For constant unit failure rate, the equation becomes:

$$R_{sd}(t) = \sum_{i=0}^{m} (\lambda t)^i e^{-\lambda t} / i!$$

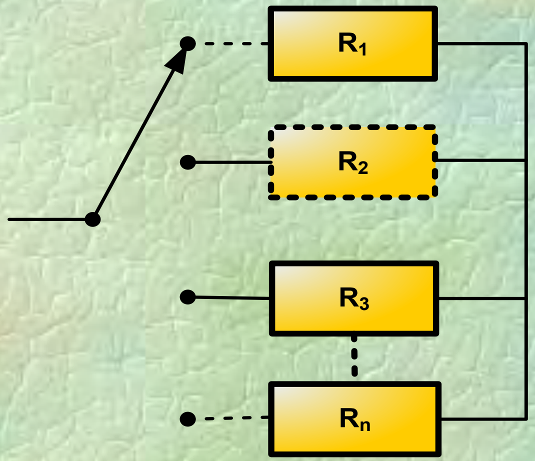


Figure 2-61: Standby Redundancy Model

- The standby system mean time to failure.

$$MTTF_{sd} = \int_0^{\infty} \left[\sum_{i=0}^{m} (\lambda t)^i e^{-\lambda t} / i! \right] dt = (m+1)/\lambda$$

EXAMPLE APPLICATION

- Assume that a standby system has two independent and identical units: one operating and another on standby. The unit failure rate is 0.005 failures per hour.
- Calculate the system reliability for a 100 hour operation and mean time to failure, if the switching mechanism never fails, and the standby unit remains as good as new in its standby mode.

$$R_{sd}(t)=\sum_{i=0}^{m}(\lambda t)^{i}\, e^{-\lambda t}/i!$$

$$R_{sd}(100)=\sum_{i=0}^{1}[(0.005)(100)]^{0}\, e^{-(0.005\times 100)}/0! + [(0.005)(100)]^{1}\, e^{-(0.005\times 100)}/1!$$

$$R_{sd}(100)=[0.5]^{0}\, e^{-(0.5)}/0! + [0.5]^{1}\, e^{-(0.5)}/1! = [0.5]^{0}\times 0.6065 + [0.5]^{1}\times 0.6065$$

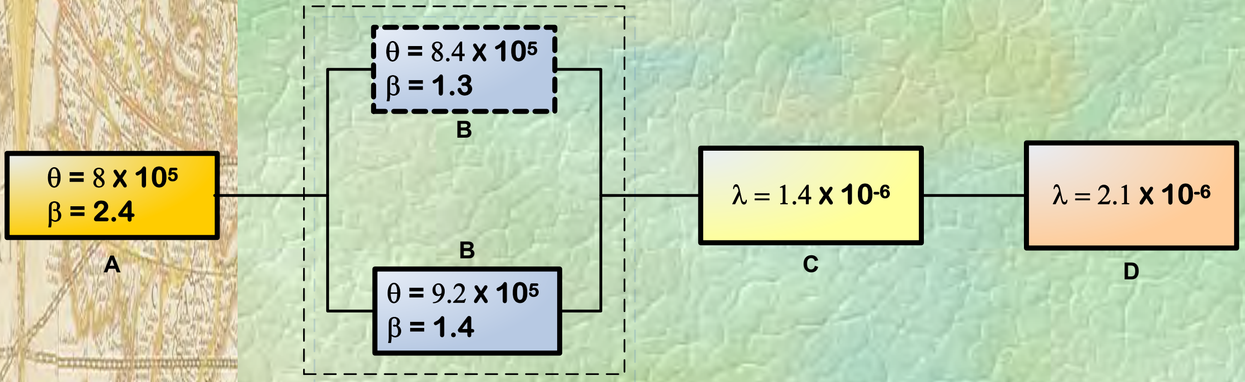
$$R_{sd}(100)= 1\times 0.6065 + 0.5\times 0.6065 = 0.90975$$

- Similarly, using the given data in the following equation MTTF we get:

$$MTTF_{sd} = \int_{0}^{\infty}\left[\sum_{i=0}^{m}(\lambda t)^{i}\, e^{-\lambda t}/i!\right] dt = (m+1)/\lambda = (1+1)/0.005 = 400\text{Hours}$$

RELIABILITY MODELING EXAMPLE APPLICATION

Figure 2-62: RBD for Reliability Modeling



Compound Models

- Determine the system reliability R(t) for t = 15,000 Hrs.

The following are different component failure distributions:

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

$R(t) = e^{-\left(\frac{t}{\theta}\right)^{\beta}}$ Weibull

EXAMPLE APPLICATION

- A product for use in fuel power production plant consist of four sub-systems. Table 2-52 identifies critical subsystems and calculations for operational availability using hypothetical data. A_o is calculated using the equation below:

$$\mathbf{A_o = \frac{Uptime}{Uptime + MCT + MLDT} = \frac{MTBF}{MTBF + MTTR + MLDT}}$$

Table 2-52: Output of A_o Calculations

Equipment	MTBF [Hrs]	MTTR [Hrs]	MLDT	A_o
Compressor	5632	1.00	1.95	0.99948
Compressor Turbine	6233	0.83	5.00	0.99906
Power Turbine	13531	1.11	2.08	0.99976
Generator	10427	0.91	2.13	0.99970

FTA APPLICATION IN PRODUCT DESIGN

Fault Tree Analysis

- ❑ A logical, structured process that can help identify potential causes of system failure before the failures actually occur.
- ❑ Benefits

  1. Identify possible system reliability or safety problems at design time,
  2. Assess system reliability or safety during operation
  3. Identify components that may need testing or more rigorous quality assurance scrutiny,
  4. Identify root causes of system failures.

- ❑ When to Apply FTA

  a. Applied any time during the life of a product, system, subsystem, or equipment item
  b. Primarily used to examine incidents or accidents whose consequences would be classified as catastrophic
  c. Often initiated after a major hazard has been recognized for the first time

APPLICATION INVOLVING TTF DISTRIBUTION

Steps for Performing Quantitative Evaluation

1. Determine the component failure rate [λ_c] of each component using FRACAS, MIL-HDBK-217, NPRD-85, field data, etc.

2. Determine the model failure rate [λ_m] for each component.

   $\lambda_m = \alpha \times \lambda_c$.

   α = The probability that the component will fail in that failure mode [FMD-97].

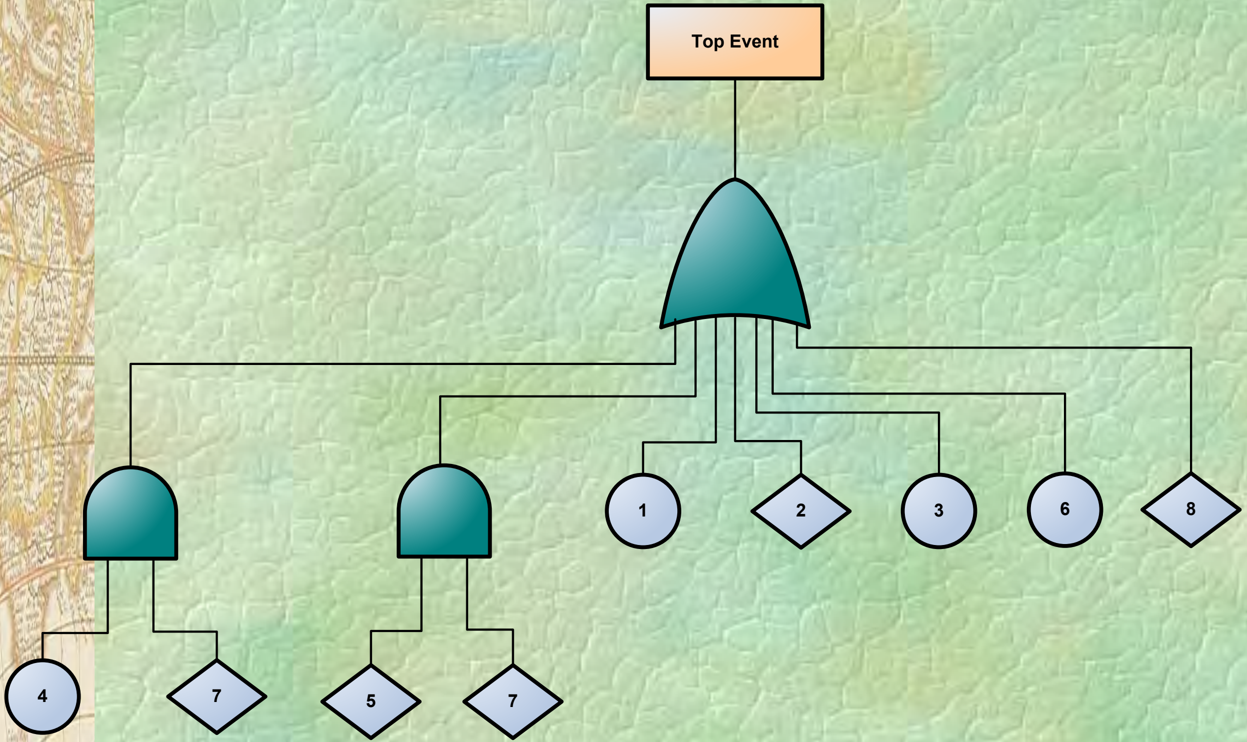
3. Calculate the probability of failure F(t) of each failure mode.

   $$F(t) = 1 - e^{-\lambda_m t}$$

4. Calculate the cut-set probabilities.

APPLICATION INVOLVING TTF DISTRIBUTION

Figure 2-79: Example Fault Tree for Quantitative Evaluation



EXAMPLE APPLICATION CRITICALITY CALCULATION

Table 2-59: Time to Failure [TTF] Data

Fault	λ_c	α	λ_m	λ_m * t	F[t]
1	0.020×10^{-6}	0.80	0.0160×10^{-6}	0.0016	0.001598
2	0.040×10^{-6}	0.12	0.0048×10^{-6}	0.00048	0.000479
3	0.002×10^{-6}	0.25	0.0005×10^{-6}	0.00005	0.000049
4	0.035×10^{-6}	0.60	0.0210×10^{-6}	0.00210	0.002097
5	0.200×10^{-6}	0.30	0.0600×10^{-6}	0.00600	0.005982
6	0.008×10^{-6}	0.20	0.0016×10^{-6}	0.00016	0.000159
7	0.140×10^{-6}	0.75	0.1050×10^{-6}	0.01050	0.010445
8	0.010×10^{-6}	0.40	0.0040×10^{-6}	0.00040	0.000399

Given λ_c , α and the Time (t) = 100,000 hours determine the failure probability of each basic fault.

$\lambda_m = \alpha \times \lambda_c$

$F(t) = 1 - {}^{e-\lambda m\ t}$

CRITICALITY CALCULATION

Table 2-60: Failure Data Reliability

Cut Set Components	F_{cs} (t)	R_{cs} (t)
1 only	0.001598	0.99840
2 only	0.000479	0.99952
3 only	0.000049	0.99995
4 only	0.002097	0.99790
5 only	0.005982	0.99402
6 only	0.000159	0.99984
4 and 7	0.000022	0.99997
5 and 7	0.000062	0.99994

Determine the failure probability of each Cut Set.

$F_{cs}(t) = F_{C1}(t) * F_{C2}(t) * F_{C3}(t) * \ldots\ldots\ldots\ldots\ldots F_{cn}(t)$

$R_{cs}(t) = 1 - F_{cs}(t)$

CRITICALITY CALCULATION

SOLUTION CONTINUED

Determine the top-event Failure Probability:

$R_{OVERALL} = R_{CS1}(t) * R_{CS2}(t) * R_{CS3}(t) * \ldots\ldots\ldots\ldots\ldots R_{CSN}(t)$

$F_{OVERALL} = 1 - R_{OVERALL}$

$R_{OVERALL} = 0.99840 \times 0.99952 \times 0.99995 \times 0.99790 \times 0.99402 \times 0.99984 \times 0.99997 \times 0.99994.$

$R_{OVERALL} = 0.989573$

$F_{OVERALL} = 1 – R_{OVERALL} = 1 – 0.989573 = 0.010427$

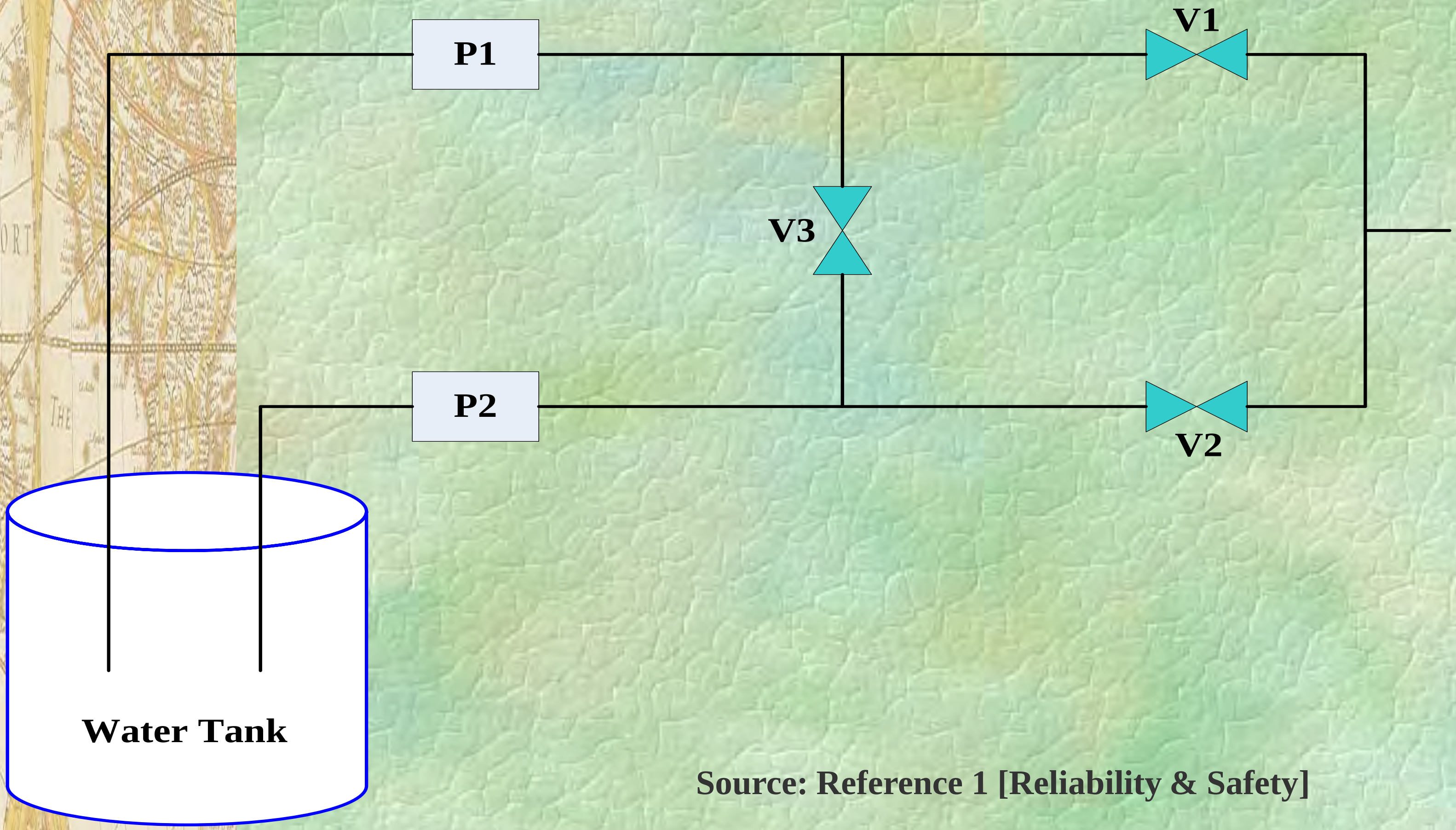
FTA APPLICATION IN PRODUCT DESIGN

Case Study

- The basic aspects of fault tree analysis can be explained through an example of containment spray system which is used to scrub and cool the atmosphere around a nuclear reactor during an accident.
- It is shown in Fig. 2-82. Any one of the pump and one of two discharges valves (V1 and V2) is sufficient for its successful operation. To improve the reliability, an interconnecting valve (V3) is there which is normally closed.
- The system is simplified and the actual system will contain more number of valves.
- Step 1: The undesired top event is defined as 'No water for cooling containment'.
- Step 2: The fault tree is developed deductively to identify possible events leading to the top event. These may be
  A. No water from 'V1 branch and V2 branch'.
  B. No supply to V1 or V1 itself failed. Since V1 failure is basic event, it doesn't need further analysis.
  C. The lack of supply to V1 is due to simultaneous failure of P1 branch and V3 branch.
  D. Supply from V3 branch is due to either failure of V3 or P2.
  E. Similarly V2 branch is also developed. The resulting fault tree is shown in Fig. 2-83.
- Step 3: Qualitative evaluation of fault tree. The qualitative evaluation of fault tree determines minimal cut sets of fault tree. One can write the logical relationship between various events of fault tree as follows: T = A · B

FTA APPLICATION IN PRODUCT DESIGN

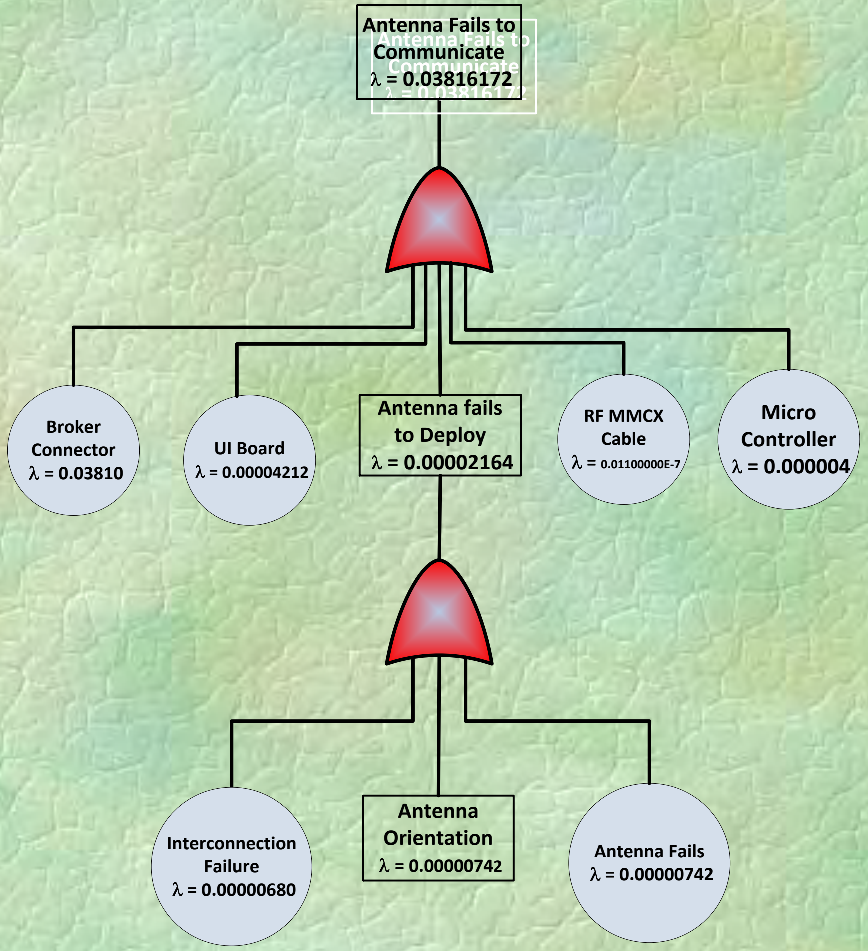
Figure 2-82: Contain Spray System of NPP



Source: Reference 1 [Reliability & Safety]

FTA WORKED EXAMPLE

Figure 2-84: Fault Tree Analysis of Antenna Failure



– Proactive Innovative Solutions for Success and Competitive Advantages

M3 - LEARNING OBJECTIVES

Participant Shall be able to:

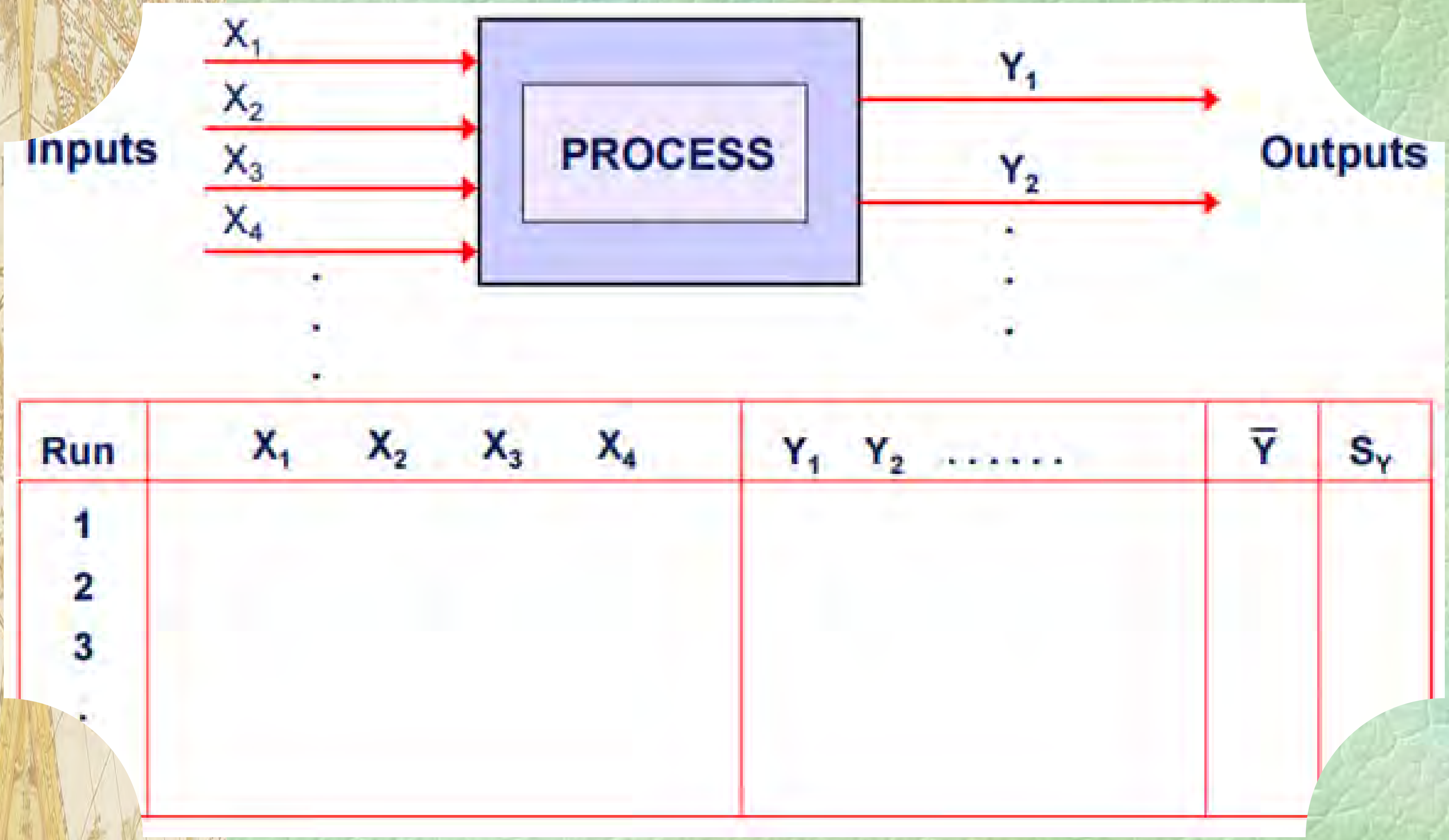
- Acquire knowledge of how to determine the conditions that optimize product parameters.
- Gain understanding of how to improve product reliability using design of experiment.
- Identify important factors and determine the best value of them in order to optimize the performance of the product.
- Gain understanding of how to determine the number of factors, desired level, and number of runs?
- Gain understanding of how to utilize Design of Experiments to support Life Data Analysis.
- Utilized DOE to characterized performance and estimate reliability.

Adapt | Implement | Improve

WHAT IS DESIGN OF EXPERIMENT?

Purposeful changes of the inputs [factors] in order to observe corresponding changes in the output [response].

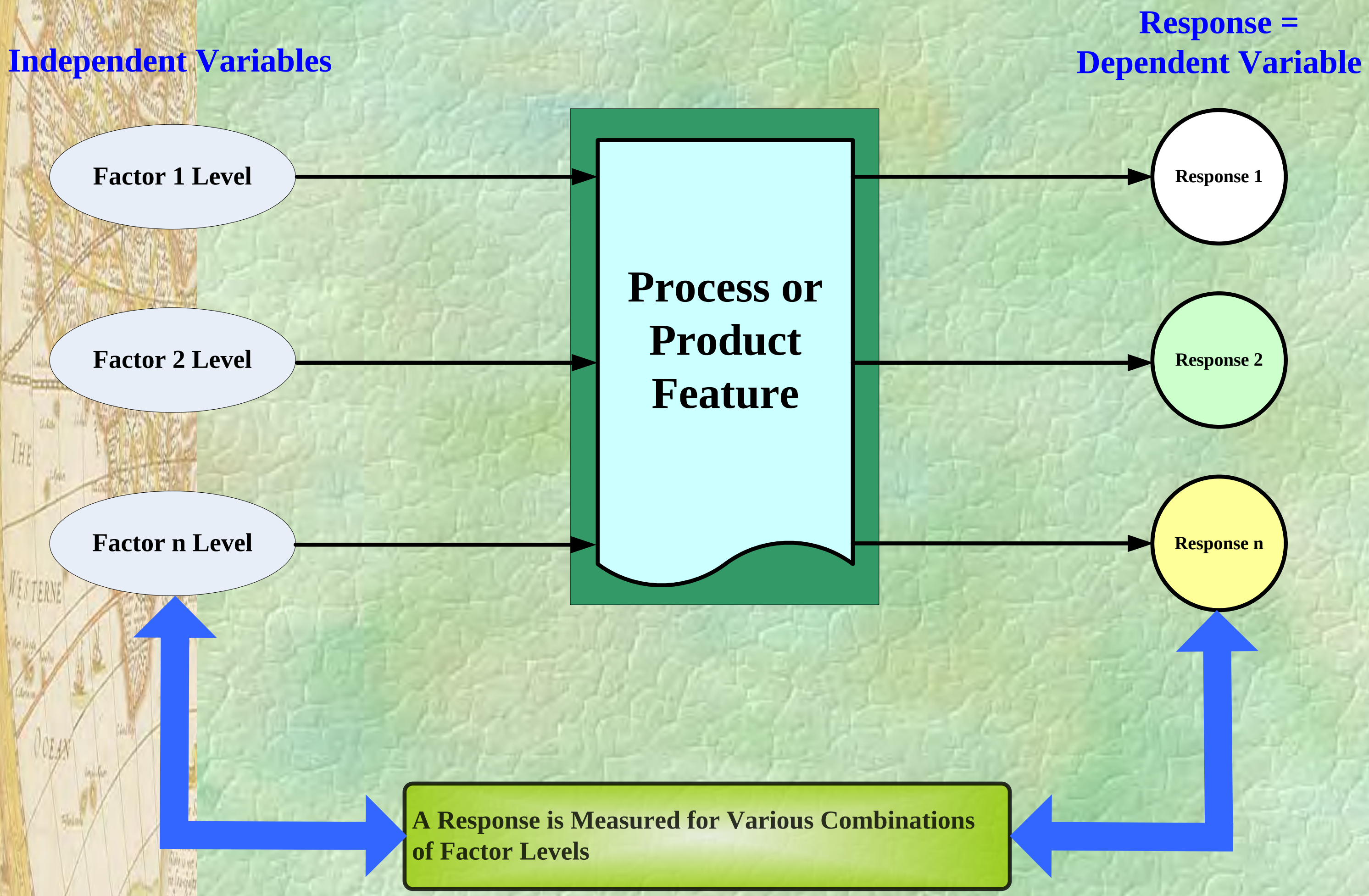
Figure 1: Structure of DOE Engineering Process



Run	X_1	X_2	X_3	X_4	Y_1	Y_2	......	$\bar{Y}$	S_Y
1									
2									
3									
.									

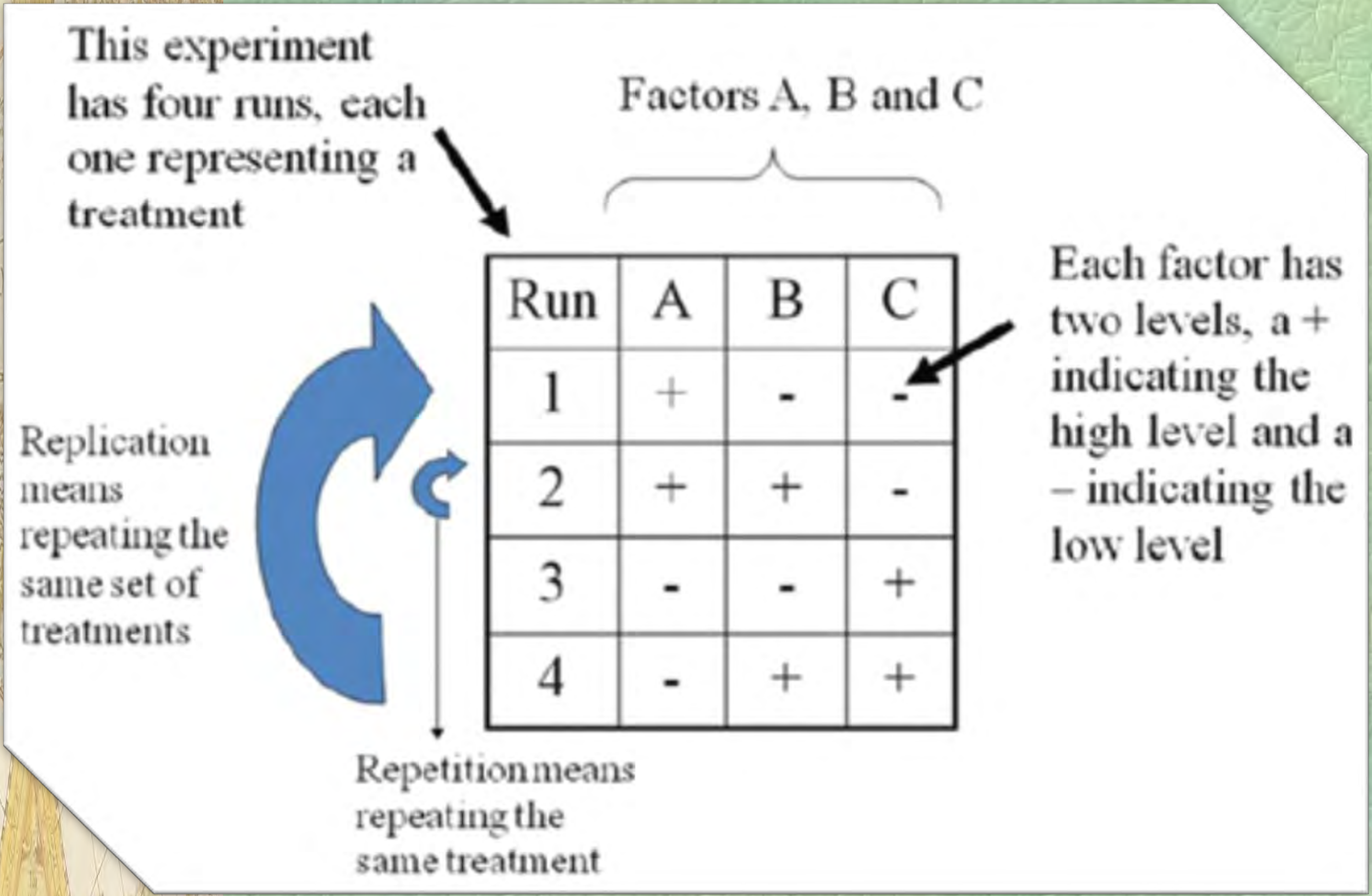
METHODS FOR PERFORMING EXPERIMENT

Figure 2: The DOE Concept



COMPONENTS OF EXPERIMENTAL DESIGN

Figure 3: DOE Terminology



This experiment has four runs, each one representing a treatment

Factors A, B and C

Run	A	B	C
1	+	-	-
2	+	+	-
3	-	-	+
4	-	+	+

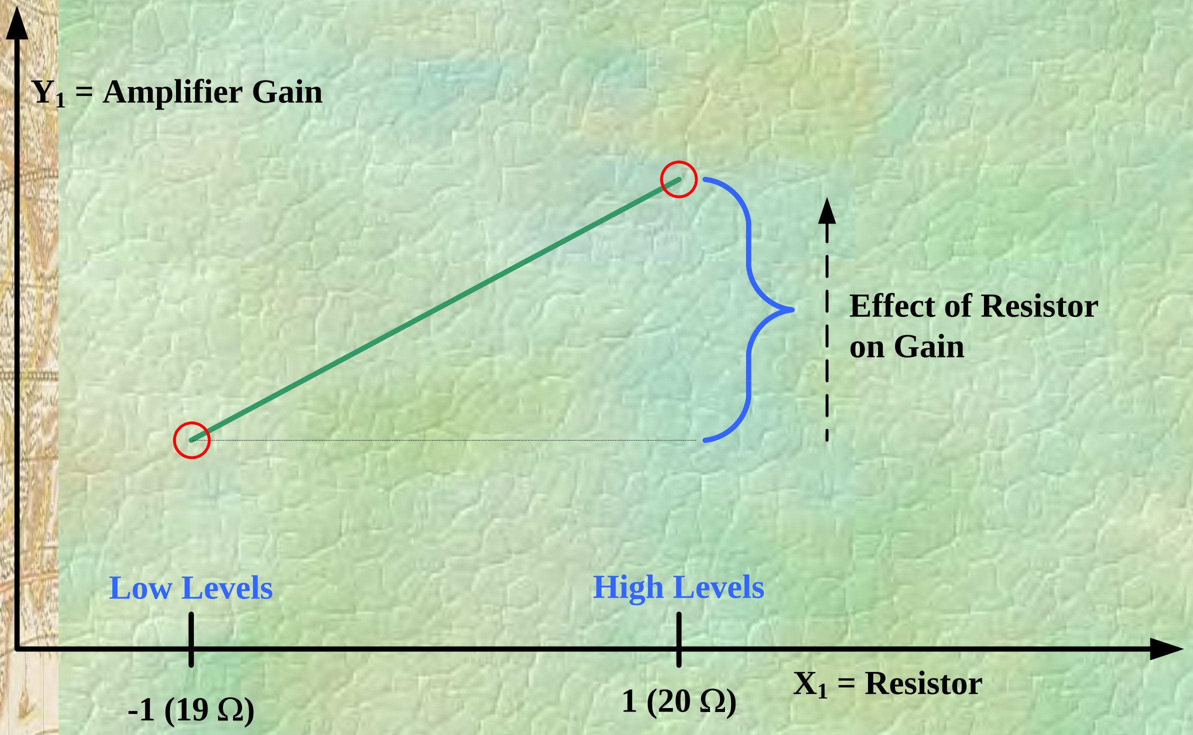
Each factor has two levels, a + indicating the high level and a – indicating the low level

Replication means repeating the same set of treatments

Repetition means repeating the same treatment

COMPONENTS OF EXPERIMENTAL DESIGN

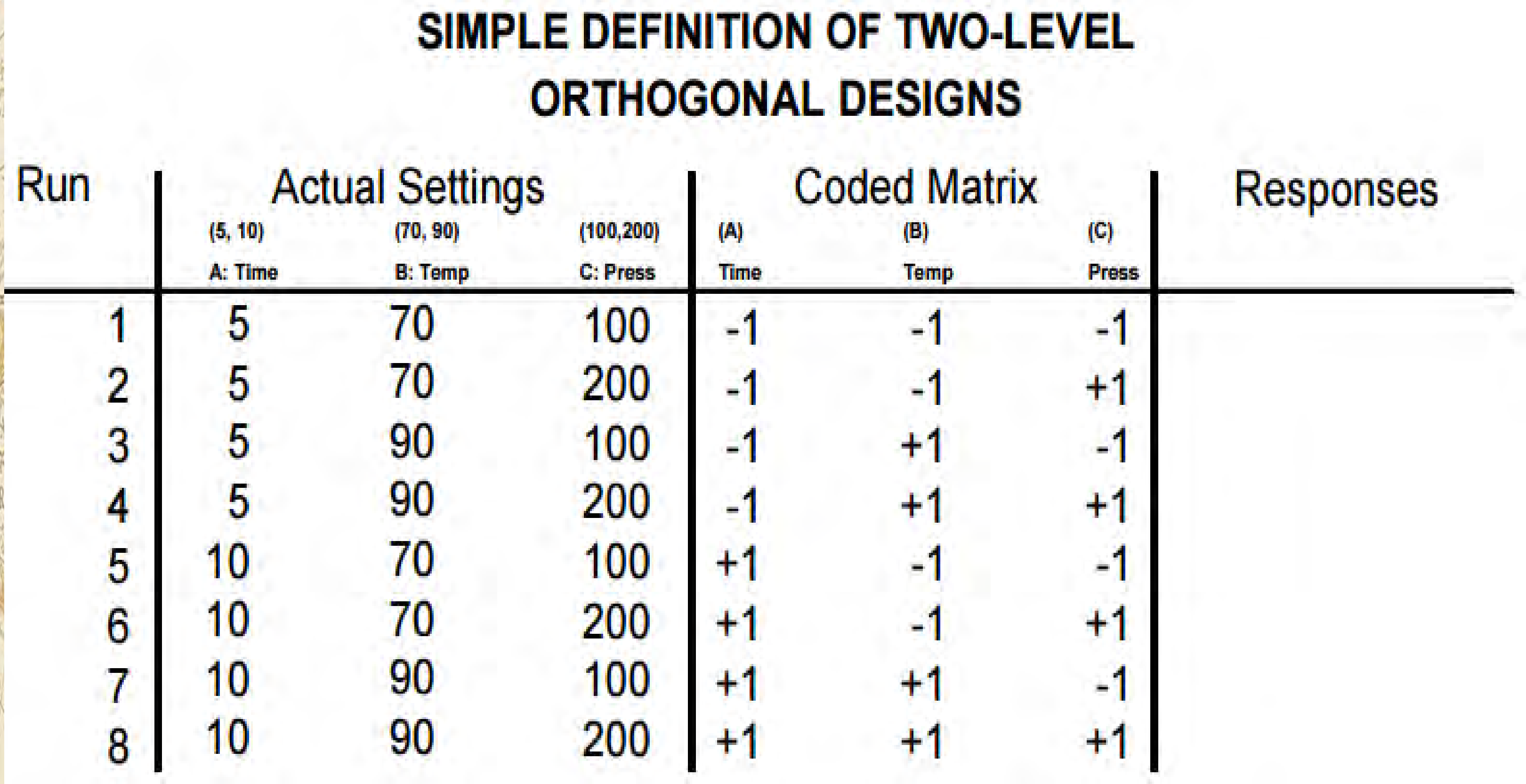
Figure 4: Main Effect of a Factor



The main effect of a factor is defined as the change in the response due to varying one factor from its low level, and keeping the other factors at their center-level.

PROCESS MODEL FOR DESIGN OF EXPERIMENT

Table 3: 2^3 Factorial DOE and the Associated Orthogonal Design Matrix



SIMPLE DEFINITION OF TWO-LEVEL
ORTHOGONAL DESIGNS

Run	Actual Settings			Coded Matrix			Responses
	(5, 10)	(70, 90)	(100,200)	(A)	(B)	(C)	
	A: Time	B: Temp	C: Press	Time	Temp	Press	
1	5	70	100	-1	-1	-1	
2	5	70	200	-1	-1	+1	
3	5	90	100	-1	+1	-1	
4	5	90	200	-1	+1	+1	
5	10	70	100	+1	-1	-1	
6	10	70	200	+1	-1	+1	
7	10	90	100	+1	+1	-1	
8	10	90	200	+1	+1	+1	

PROCESS MODEL FOR DESIGN OF EXPERIMENT

Consideration Should be Given to:

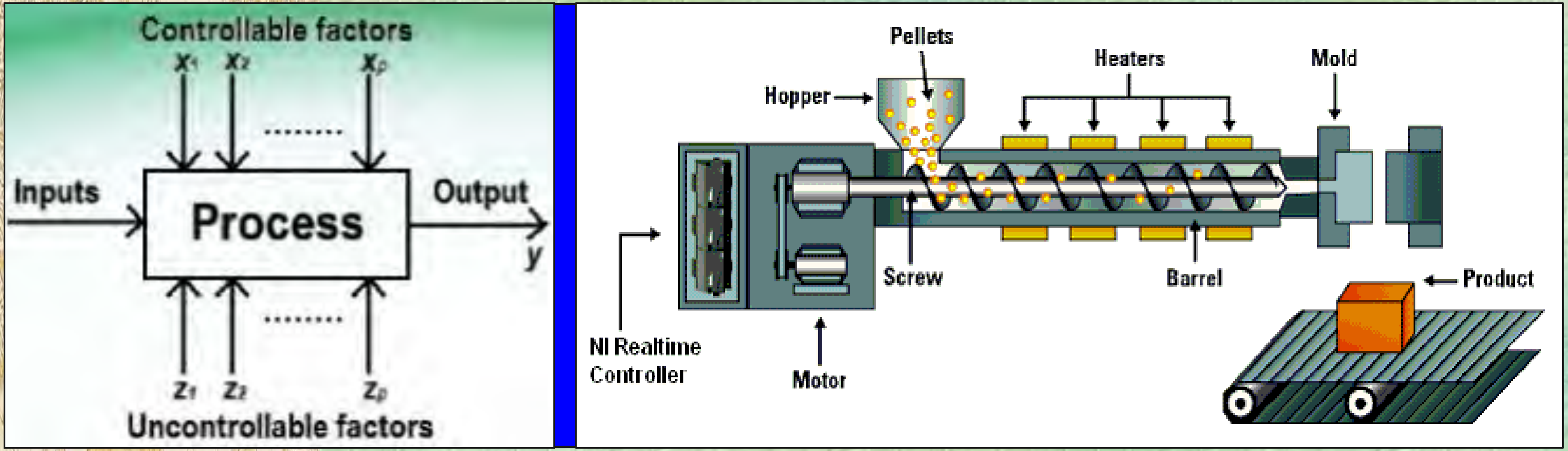
❑ Which variables are most influential on the response Y?

❑ Where to set the influential X's so that Y is almost near the desired nominal value?

❑ Where to set the influential X's so that the variability in Y is small?

❑ Where to set the influential X's so that the effects of the uncontrollable variables are minimized?

Figure 6: Injection Molding Process



PLANNING A DOE EXPERIMENT

What do you Need to Plan and Experiment?

□ **Measure Phase Deliverables**

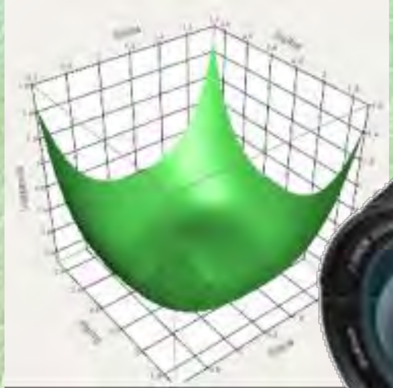
- Advocacy Team
- Baseline of Y response
- Problem Statement, including Y response
- Process map of process | Product Specification

□ **Analyze Phase Deliverables:**

- Analysis of Baseline Data
  - Graphs
  - F, t, and χ^2 Tests
  - ANOVA | Regression Analysis
- Potential Vital X's.

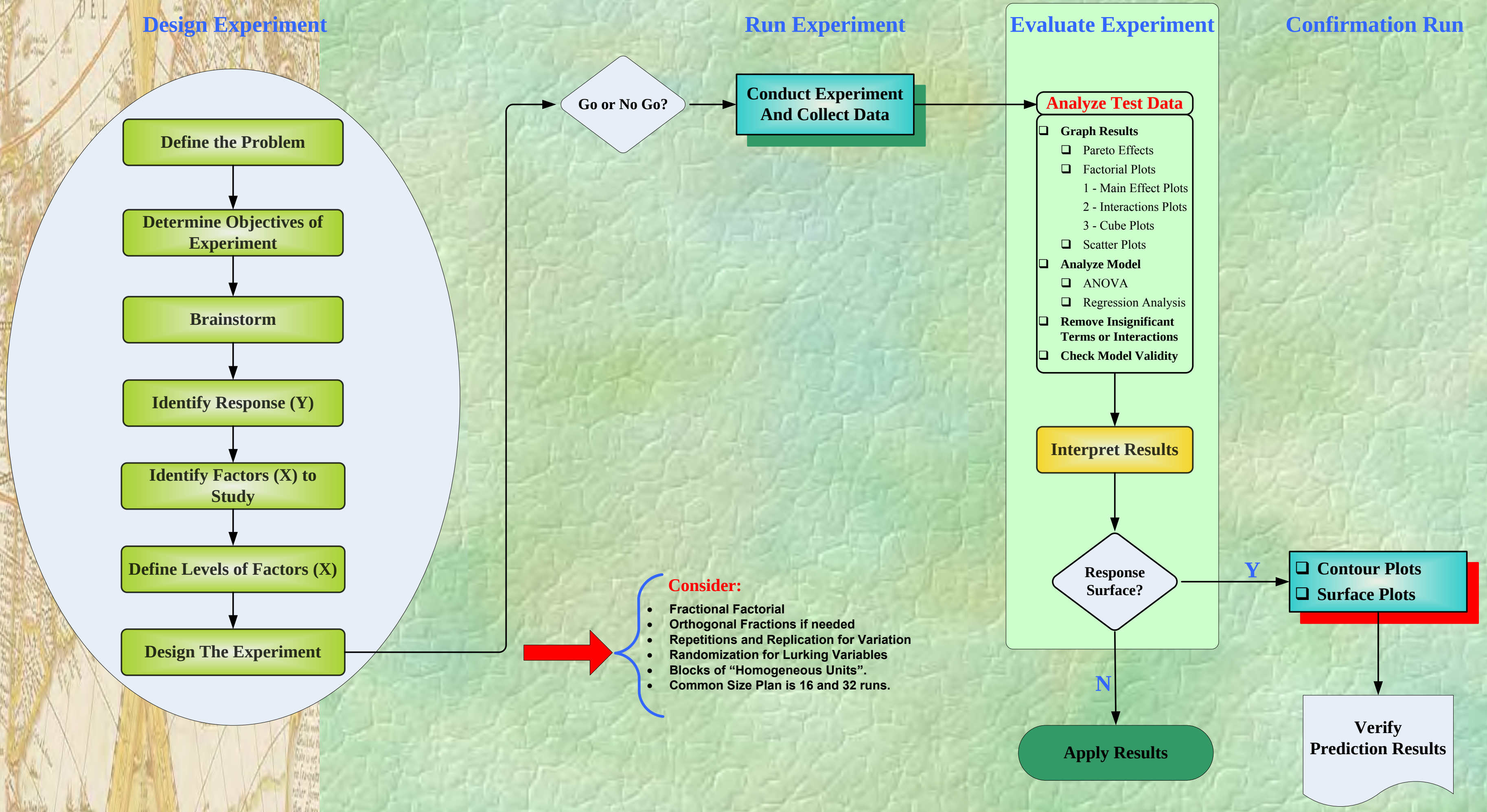
□ **Management Team Buy-in:**

- Time
- Cost
- Resources
- Support of DOE Strategy



EXPERIMENTAL DESIGN STEPS

Figure 9: The Experimental Design Process



- ❑ Graph Results
  - ❑ Pareto Effects
  - ❑ Factorial Plots
    - 1 - Main Effect Plots
    - 2 - Interactions Plots
    - 3 - Cube Plots
  - ❑ Scatter Plots
- ❑ Analyze Model
  - ❑ ANOVA
  - ❑ Regression Analysis
- ❑ Remove Insignificant Terms or Interactions
- ❑ Check Model Validity

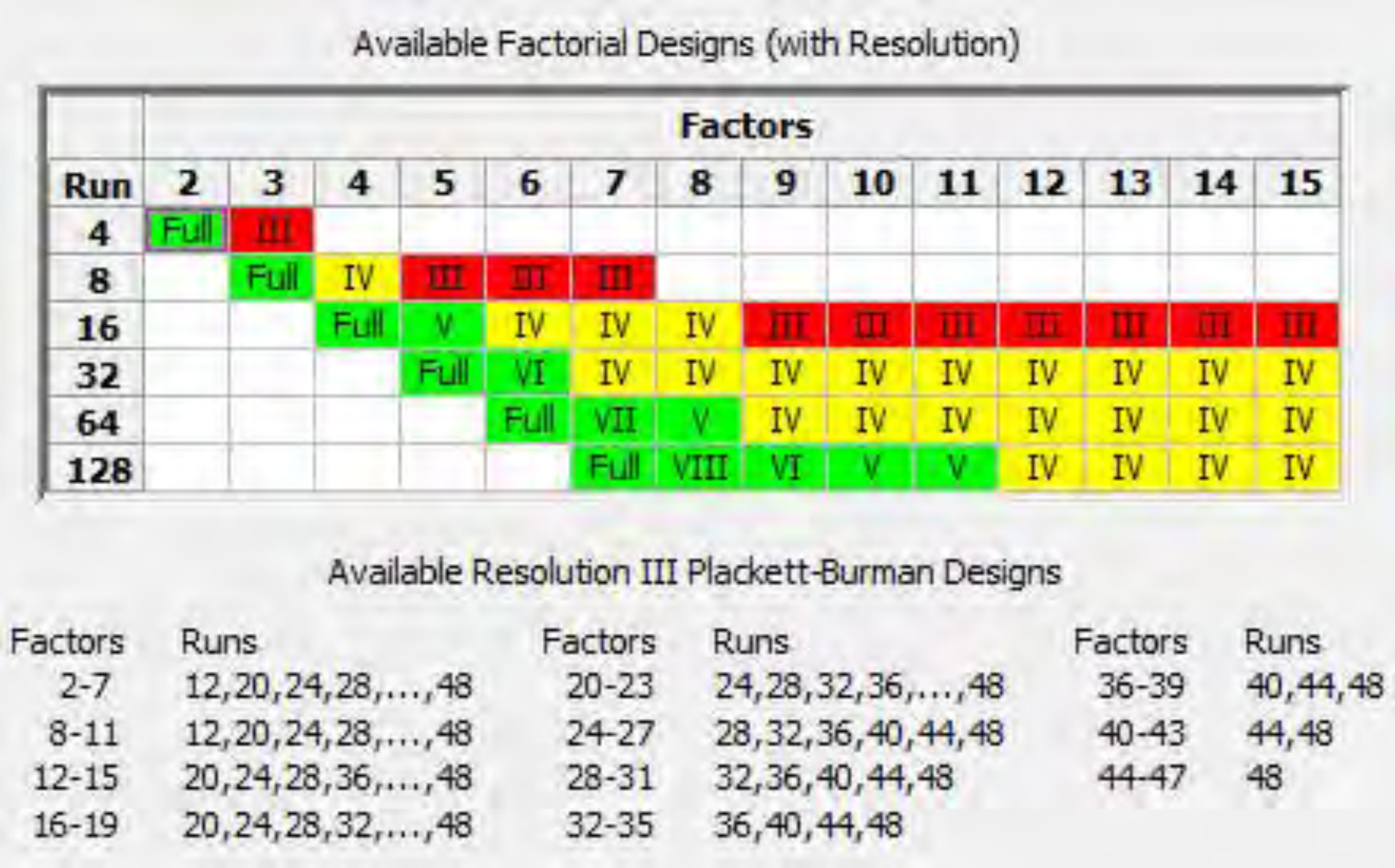
- ❑ Contour Plots
- ❑ Surface Plots

Consider:

- Fractional Factorial
- Orthogonal Fractions if needed
- Repetitions and Replication for Variation
- Randomization for Lurking Variables
- Blocks of “Homogeneous Units”.
- Common Size Plan is 16 and 32 runs.

EXPERIMENTAL DESIGN STRATEGIES

Figure 12: Available DOE Software Application Design Choices



Available Factorial Designs (with Resolution)

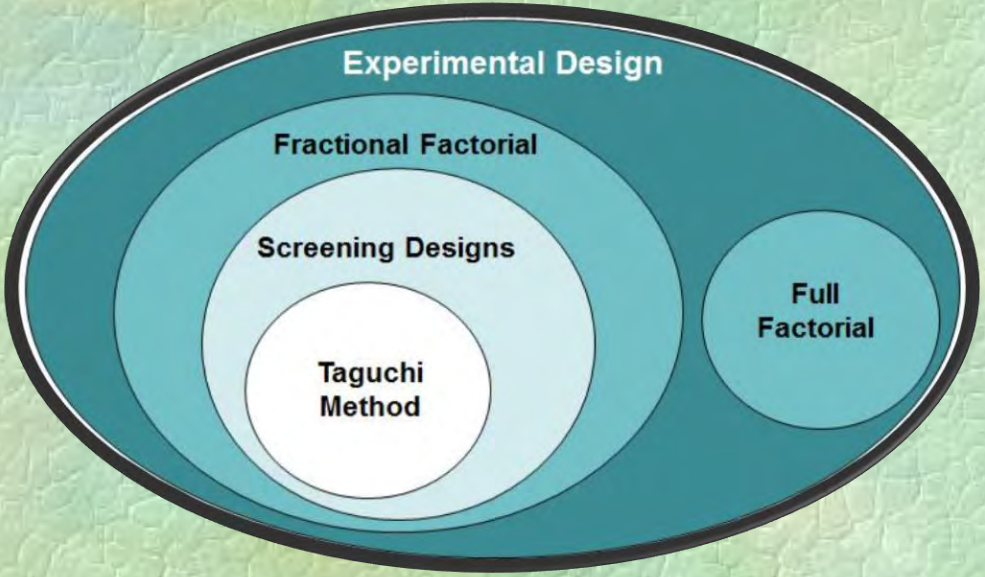
	Factors													
Run	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
4	Full	III												
8		Full	IV	III	III	III								
16			Full	V	IV	IV	IV	III	III	III	III	III	III	III
32				Full	VI	IV	IV	IV	IV	IV	IV	IV	IV	IV
64					Full	VII	V	IV	IV	IV	IV	IV	IV	IV
128						Full	VIII	VI	V	V	IV	IV	IV	IV

Available Resolution III Plackett-Burman Designs

Factors	Runs	Factors	Runs	Factors	Runs
2-7	12,20,24,28,...,48	20-23	24,28,32,36,...,48	36-39	40,44,48
8-11	12,20,24,28,...,48	24-27	28,32,36,40,44,48	40-43	44,48
12-15	20,24,28,36,...,48	28-31	32,36,40,44,48	44-47	48
16-19	20,24,28,32,...,48	32-35	36,40,44,48		

TYPES OF ENGINEERING DESIGN OF EXPERIMENTS

- **Discovery**
  - Usually involve hands on activities.
  - Design to generate new ideas or approaches.
  - May involve systems or processes that are not well understood or refined.
- **Hypothesis**
  - Seek to falsify specific hypothesis.
  - Closer to the traditional approach.
  - Used often in the attempt to prove a theory, idea, or approach.

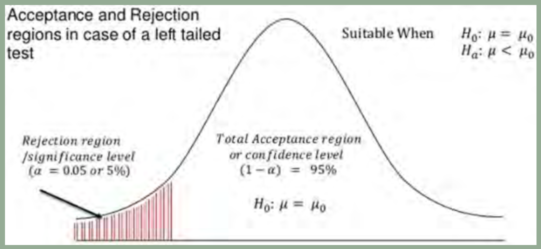


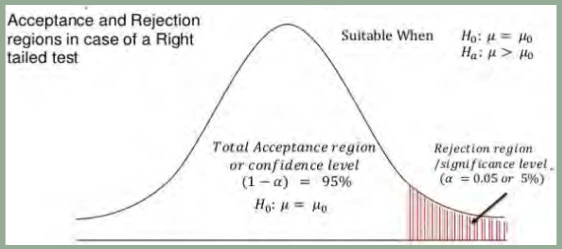
TYPES OF ENGINEERING DESIGN OF EXPERIMENTS

Simple Comparison Experiments

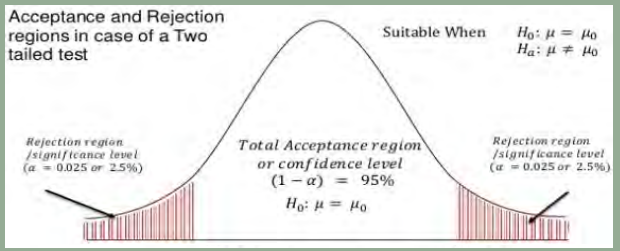
- ❑ One Factor – Multiple Levels.
- ❑ Objective of Experiment.
  - Compare two are more means, variances or probabilities.
  - Compare X vs. Y: [Better or Worse] – paired comparison is a special case of randomized block design.
- ❑ Major Considerations:
  - Sample Size
  - Structure of statistical hypothesis
  - Knowledge of distribution: Normal, F-statistics, χ^2 and other characteristics.

One Tailed Test


Acceptance and Rejection regions in case of a left tailed test
Suitable When
$H_0: \mu = \mu_0$
$H_a: \mu < \mu_0$
Rejection region /significance level (α = 0.05 or 5%)
Total Acceptance region or confidence level $(1-\alpha)$ = 95%
$H_0: \mu = \mu_0$


Acceptance and Rejection regions in case of a Right tailed test
Suitable When
$H_0: \mu = \mu_0$
$H_a: \mu > \mu_0$
Total Acceptance region or confidence level $(1-\alpha)$ = 95%
$H_0: \mu = \mu_0$
Rejection region /significance level (α = 0.05 or 5%)

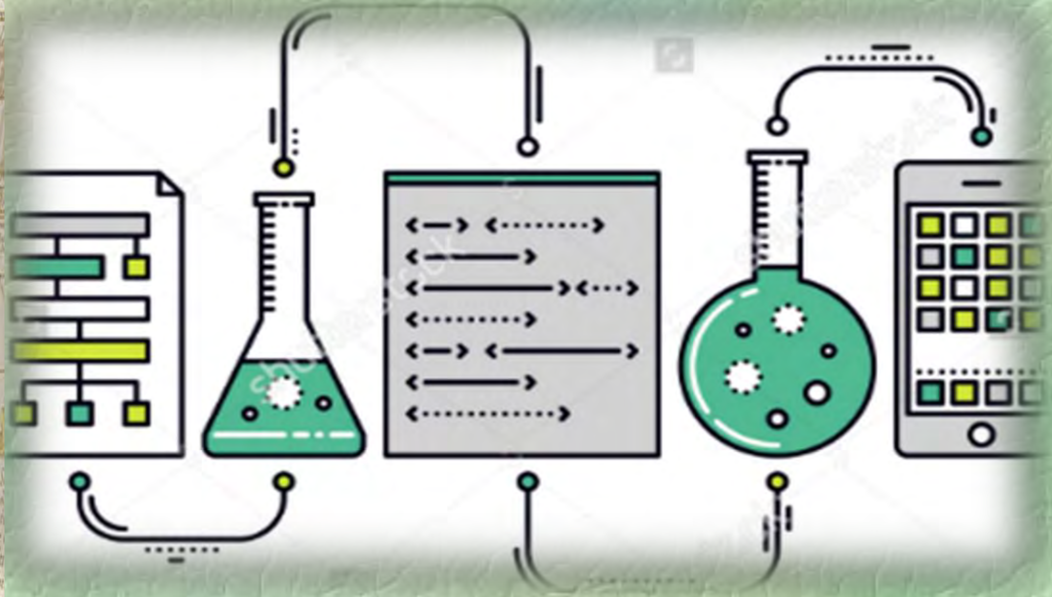
Two Tailed Tests


Acceptance and Rejection regions in case of a Two tailed test
Suitable When
$H_0: \mu = \mu_0$
$H_a: \mu \neq \mu_0$
Rejection region /significance level (α = 0.025 or 2.5%)
Total Acceptance region or confidence level $(1-\alpha)$ = 95%
$H_0: \mu = \mu_0$
Rejection region /significance level (α = 0.025 or 2.5%)

In general for Comparison use T-Critical Test Statistics

Conducting a Main Effects Experiment

- ❑ **The objective: Optimize the recipe in order to achieve a high judging score.**
- ❑ **The situation: We have time to bake 4 batches of cookies for the experimental judging.**



TAGUCHI METHOD OF EXPERIMENTATION

Assigning the Factors to the Array

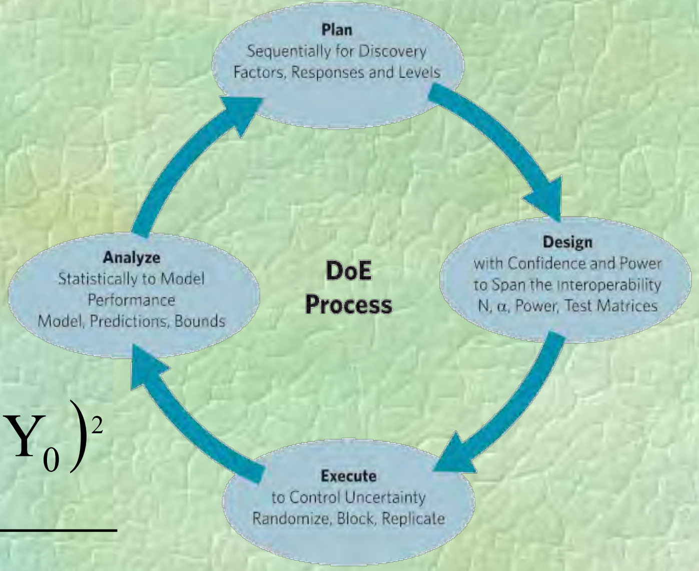
- ❑ The main effect experiment [screening] considers each factor as independent so assign them to array columns arbitrarily.
- ❑ The consideration of interactions and confounding is beyond the scope of example below.
- ❑ Screening experiments are often with many factors for further experimentation.

Table 11: Assigning Factors to The Array

	$L_4\,(2^3)$			$L_4\,(2^3)$		
Run No.	Temp	Time	Size	A	B	C
1	325	12	Sm	1	1	1
2	325	15	Lg	1	2	2
3	375	12	Lg	2	1	2
4	375	15	Sm	2	2	1

TAGUCHI METHOD OF EXPERIMENTATION

Mean Square Deviation



Plan
Sequentially for Discovery
Factors, Responses and Levels

Design
with Confidence and Power
to Span the Interoperability
N, α, Power, Test Matrices

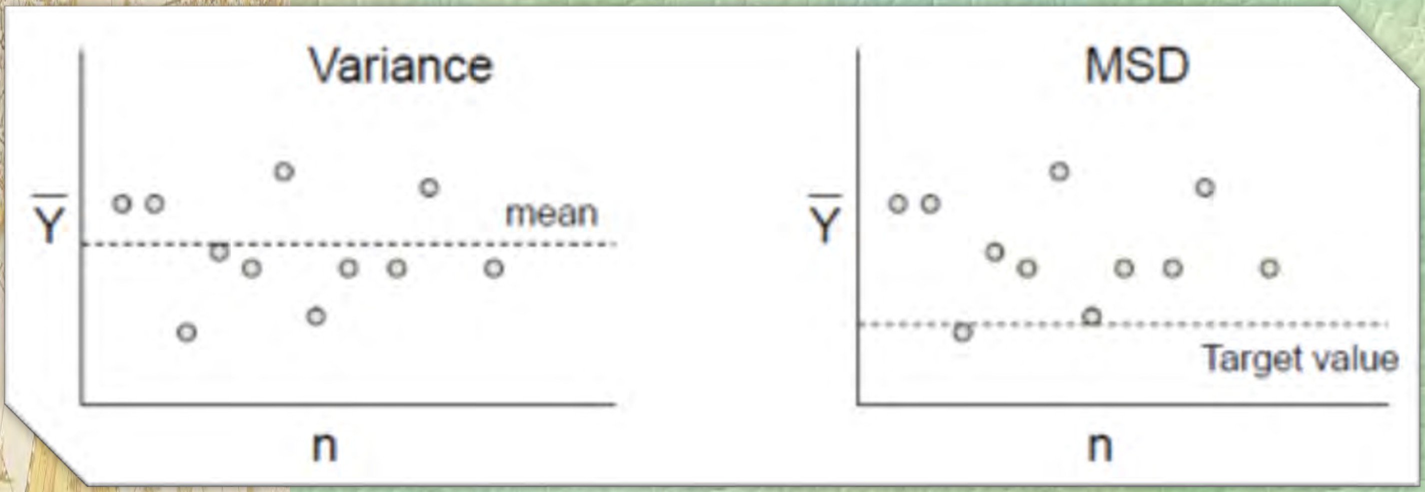
Execute
to Control Uncertainty
Randomize, Block, Replicate

Analyze
Statistically to Model
Performance
Model, Predictions, Bounds

DoE
Process

- ❑ **Variance:** $\sigma^2 = \dfrac{\sum_{i=1}^{n}(Y_i - \mu)^2}{n}$

- ❑ **MSD [Nominal is Best]:** $MSD = \dfrac{\sum_{i=1}^{n}(Y_i - Y_0)^2}{n}$



TAGUCHI METHOD OF EXPERIMENTATION

Three Types of Analysis Statistics

- ❑ **Signal to Noise Ratio:** $\mathrm{S/N} = -10\log(\mathrm{MSD})$

  In every case the larger the signal to noise ratio the better the results.

- ❑ **S-type smaller-is-better statistics:**

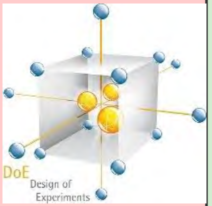
$$\mathrm{MSD} = \frac{(Y_1)^2 + (Y_2)^2 + \ldots\ldots\ldots\ldots\ldots\ldots\ldots + (Y_n)^2}{n}$$

- ❑ **B-type Bigger-is-better statistics:**

$$\mathrm{MSD} = \frac{\dfrac{1}{Y_1^2} + \dfrac{1}{Y_2^2} + \ldots\ldots\ldots\ldots\ldots\ldots\ldots + \dfrac{1}{Y_n^2}}{n}$$

- ❑ **N-type Nominal-is-best statistics:**

$$\mathrm{MSD} = \frac{(Y_1 - Y_0)^2 + (Y_2 - Y_0)^2 + \ldots\ldots\ldots\ldots\ldots\ldots\ldots + (Y_n - Y_0)^2}{n}$$



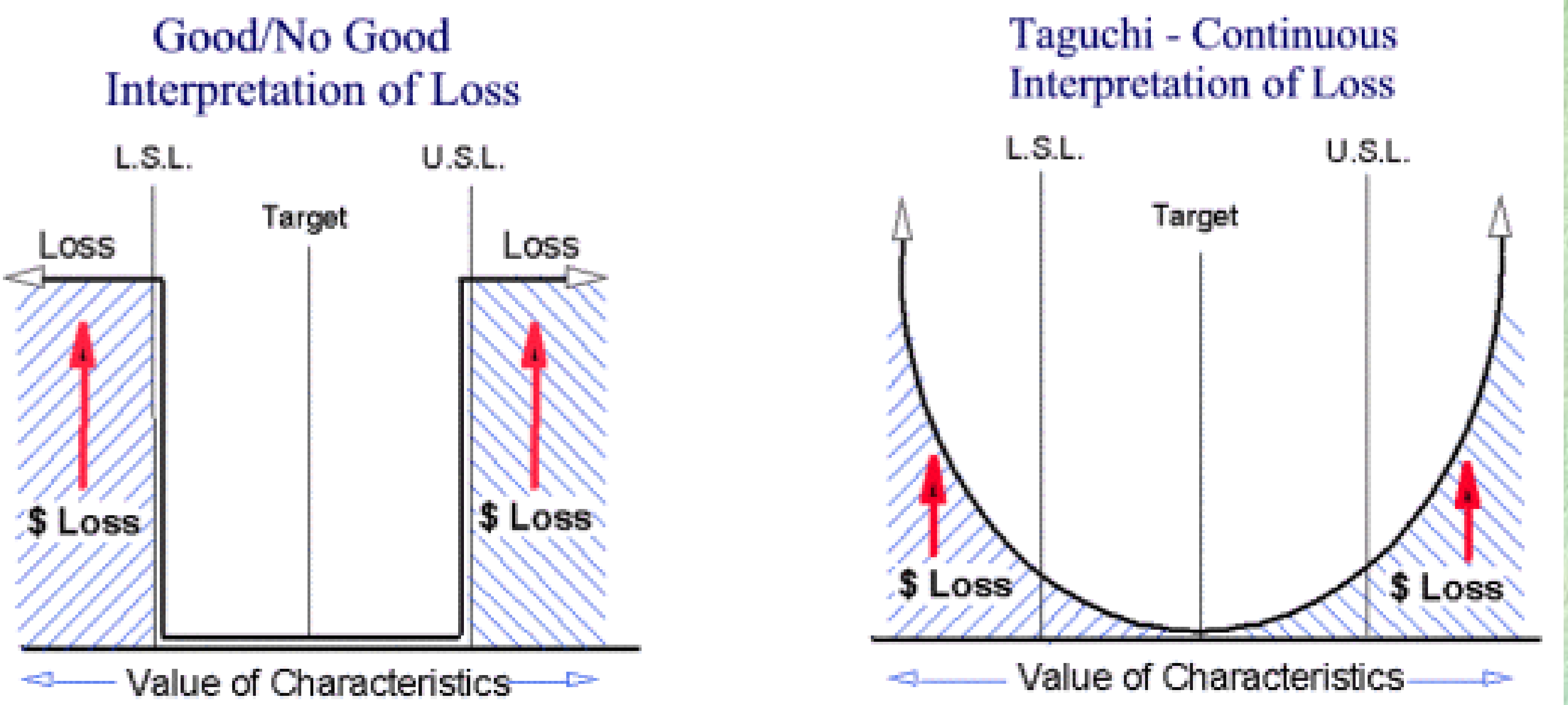
INTEGRATING LOSS FUNCTION WITTH DOE

Taguchi Loss Function Concepts

- Taguchi describes a continuous Loss Function that increases as a part deviates from the target, or nominal value (Figure 18).
- The Loss Function stipulates that society's loss due to poorly performing products is proportional to the square of the deviation of the performance characteristic from its target value.
- Taguchi adds this cost to society (consumers) of poor quality to the production cost of the product to arrive at the total loss (cost).
- Taguchi uses designed experiments to produce product and process designs that are more robust - less sensitive to part/process variation.

INTEGRATING LOSS FUNCTION WITTH DOE

Figure 18: Loss Function Representation with Respect to Target Value



Source: Morestream.com

APPLICATION OF TAGUCHI LOSS FUNCTION

Fuel Pump Noise Study

- ❑ In an experimental study of an automotive fuel pump noise, three 2 level factors were included as illustrated in Table 17.
- ❑ The Taguchi L_4 orthogonal array was used to define the four trial conditions.
- ❑ Six samples of each of the four trial conditions were tested and results were documented as shown in table 18.
- ❑ The levels were selected so that the trial condition 1 represents the *current design* of the fuel pump.
- ❑ If a decision is made to change the design to determine the optimum configuration, estimate the performance of the optimum design and the cost savings when the new fuel pump is produced.

APPLICATION OF TAGUCHI LOSS FUNCTION

Table 17: Fuel Pump Noise Study Example

Design Factors and Their Levels				Experiment will use L_4			
Columns	Factor Name	Level 1	Level 2	Trial | Column	1	2	3
1	Seal Thickness	Present	Thicker	Trial 1	1	1	1
2	Rotor Chuck Type	Present	New Design	Trial 2	1	2	2
3	Finger to Drive C1	Present	Increase	Trial 3	2	1	2
				Trial 4	2	2	1

Note: Three 2 Level factors studied | Objective: Design least noisy and best performance pump | Characteristics: Nominal the Best [SIQ = 70 Target].

APPLICATION OF TAGUCHI LOSS FUNCTION

Table 18: Original Observation and Their S|N Ratios

			Factors			Observation						Responses		
Trial Repetitions	Standard Order	Run Order	Seal Thickness	Rotor Chuck Type	Finger to Drive C_1	R_1	R_2	R_3	R_4	R_5	R_6	Y Mean	Y Std	Signal to Noise Ratio
1	3	1	1	1	1	67	85	87	65	59	76	73.1667	11.3563	-20.71
2	4	2	1	2	2	65	65	66	54	73	58	63.5	6.6558	-18.99
3	1	3	2	1	2	54	45	56	45	63	46	51.5	7.3959	-25.89
4	2	4	2	2	1	56	67	45	54	56	74	58.6667	10.2697	-23.36
														-88.95

Quality Characteristics: Nominal is Best

$$\text{Standard Deviation}(\text{SD}) = \sqrt{\sum_{i=1}^{n}\left(\text{Y1} - \overline{\text{Y}}\right)^2 / (n-1)}$$

$$\text{Mean Square Deviation}(\text{MSD}) = \frac{\sum_{i=1}^{n}\left(Y_i - Y_0\right)^2}{N}$$

APPLICATION OF TAGUCHI LOSS FUNCTION

Solution

- Target value quality characteristic = 70. MSD for repetition 1 is determined as follows:

$$MSD = \frac{\sum_{i=1}^{n}\left(Y_i - Y_0\right)^2}{N} = \frac{(67-70)^2 + (85-70)^2 + (87-70)^2 + (65-70)^2 + (59-70)^2 + (76-70)^2}{6} = 117.5$$

- S/N = -10 log(MSD) = -10 $\log_{10}$ {117.5} = -20.71
- Similarly for repetition 2: S/N = -10 $\log_{10}$ (MSD) = -10 log {79.167} = -18.9854
- Also for repetition 3: S/N = -10 $\log_{10}$ (MSD) = -10 log {387.833} = -25.8865
- And for repetition 4: S/N = -10 $\log_{10}$ (MSD) = -10 log {216.33} = -23.3512

APPLICATION OF TAGUCHI LOSS FUNCTION

Table 19: Analysis of Variance ANOVA Table

Column	Factor	DOF	Sum of Squares	Variance	Percent
1	Seal Thickness	1	22.801	22.801	82.97
2	Rotor Chuck Type	1	4.512	4.512	16.43
3	Finger to Drive	1	0.164	0.164	00.60
All other errors		0			
Total		3	27.48		100.00

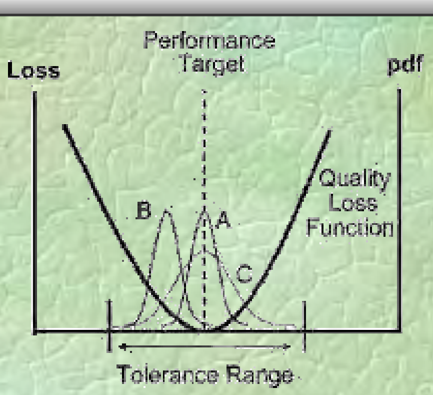
Assume that the following information is used:

Target value of quality characteristics	= 70
Tolerance value of quality characteristics	= ± 20
Cost of replacement/ rejection	= $45.00
Production Rate	= 20,000

APPLICATION OF TAGUCHI LOSS FUNCTION

Table 20: The Main Effects

Columns	Factor Name	Level 1	Level 2	$L_2 - L_1$	Level 3	Level 4
1	Seal Thickness	-19.85	-24.63	-4.78	0.00	0.00
2	Rotor Chuck Type	-23.30	-21.18	2.12	0.00	0.00
3	Finger to Drive C1	-22.04	-22.44	-0.40	0.00	0.00



APPLICATION OF TAGUCHI LOSS FUNCTION

Table 21: Estimate of the Optimum Condition of Design | Process

Factor Description	Level Description	Level	Contribution
Seal Thickness	Present Design	1	2.3875
Rotor Chuck Type	New Design	2	1.0625
Finger to Drive Clearance	Present Design	1	0.2025
Contribution from All Factors [Total]			3.6524
Current grand Average of Performance			-22.2375
Expected result at Optimum			18.5851

Calculations: 2.3875 + 1.0625 + 0.2025 = 3.6524 | -22.2375 + 3.6524 = -18.5851 | -88.95 ÷ 4 = 22.375

APPLICATION OF TAGUCHI LOSS FUNCTION

Table 22: Calculation of Loss

Item	Problem Definition	Values Defined or Determined
1	Target value of quality characteristics (m)	70.00
2	Tolerance of quality characteristics	20.00
3	Cost of rejection at production (per unit)	\$45.00
4	Unit produced per month (Total)	20,000
5	S/N Ratio of current design/part	-20.71
6	S/N Ratio of new design/part	-18.5851
	Computation of Loss Using Taguchi Loss Function	
7	Loss Function: L(y) = 0.11 x MSD = 0.11 * 117.5 | Also L(y) =	$K * (y – m)^2$
	K = Cost of replacement / $(\text{Tolerance})^2$ = 45/ $(20)^2$ = 0.1125	
	Before Experiment	
8	Loss/unit due to deviation from target in current design	\$12,953.00 * 12
	After Experiment	
9	Loss/unit due to deviation from target will be reduced from \$12,953.00 to:	\$7,941.00 * 12
	Monthly Savings	
10	If production were maintained at the improved condition, then based on 20,000 units/month	\$100246.90

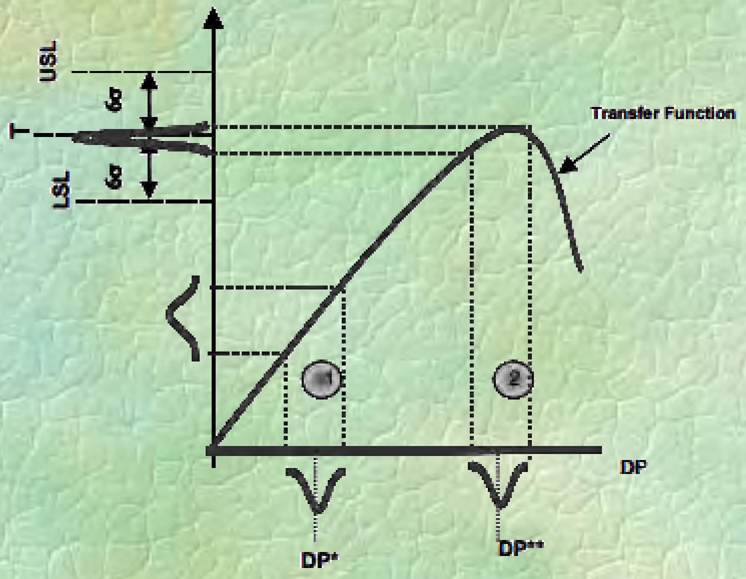
This estimate includes only those variables that have a significant contribution

RELIABILITY IMPROVEMENT THROUGH ROBUST DESIGN

Robust Design

- ❑ Robust design is concerned with the product/process functional requirement and methods to provide this function at lowest overall cost and targeted quality level under the variability produced by the noise factors.
- ❑ Robustness is defined as reducing the variation of the functional requirements of the system and having them on target as defined by the customer.
- ❑ The principal idea of robust design is that statistical testing of a product should be carried out at the design stage, the off-line stage, in order to make the product robust against the effects of variation in the manufacturing and use environments.

Figure 25: Robust Design



Elements of an Optimal Design Problem

- ❑ Objective function (Single or multi-objective)
- ❑ Design variables (Size, shape, topology, concept)
- ❑ Constraints
- ❑ Systems with uncertainty → Robust Design.

RELIABILITY IMPROVEMENT THROUGH ROBUST DESIGN

Design Optimization

- ❑ Table 27 shows the test matrix and partial results of a DOE used to determine reliability of a product.
- ❑ After the experimental data $y_{i,\ jk}$ are available, the experimenter is required to analyze these data to optimize the product design.
- ❑ This should be done following the steps outlined above and using the equations below to facilitate the calculations.
- ❑ Reliability is used as a quality characteristic. Since reliability R is a Larger-the-Better characteristics between 0 and 1, 1/R is a Smaller-the-Better type target at 1.
- ❑ The MSD of 1/R is: $MSD_i = \frac{1}{l}\sum_{j=1}^{l}\left(\frac{1}{R_{ij}} - 1\right)^2, \qquad i = 1, 2, \ldots\ldots\ldots\ldots\ldots, N$
- ❑ Where R_{ij} is the reliability estimate at the cross combination of row i and column j. l is the number of observation in the row.

RELIABILITY IMPROVEMENT THROUGH ROBUST DESIGN

Design Optimization Continued

- The Signal-to-Noise ratio is determined as follows:

$$\hat{\eta} = -10\log\left[\frac{1}{l}\sum_{j=1}^{l}\left(\frac{1}{R_{ij}}-1\right)^{2}\right], \qquad i = 1, 2, \ldots\ldots\ldots\ldots\ldots, N$$

Example Application

- Refer to table 27. Suppose that the reliability estimates in the first row are 0.92, 0.96, 0.80 and 0.87. Calculate the signal-to-noise ratio for this row.
- Substitute respective values in equation above and calculate the S/N value for the row.

$$\hat{\eta} = -10\log\left\{\frac{1}{4}\left[\sum_{j=1}^{l}\left(\frac{1}{0.92}-1\right)^{2} + \left(\frac{1}{0.96}-1\right)^{2} + \left(\frac{1}{0.80}-1\right)^{2} + \left(\frac{1}{0.87}-1\right)^{2}\right]\right\} = 16.3$$

- This process should be repeated for all rows to determine their respective S/N ratio. Optimal values is determined as discussed earlier.

RELIABILITY IMPROVEMENT THROUGH ROBUST DESIGN

Table 27: Cross Orthogonal Array with Reliability Estimates

										Outer Array				
									Z_1:	1	1	2	2	
Run		Inner Array – Factors and Interactions							Z_2	1	2	1	2	
Standard Order	Run Order	1	1	3	4	5	6	7	Z_3:	1	2	2	1	S|N Ratio
6	1	1	1	1	1	1	1	1		0.92	0.96	0.80	0.87	16.3
5	2	1	1	1	2	2	2	2		R_{21}	R_{22}	R_{23}	R_{24}	
2	3	1	2	2	1	1	2	2		R_{31}	R_{32}	R_{33}	R_{34}	
4	4	1	2	2	2	2	1	1		R_{41}	R_{42}	R_{43}	R_{44}	
3	5	2	1	2	1	2	1	2						
8	6	2	1	2	2	1	2	1						
1	7	2	2	1	1	2	2	1						
7	8	2	2	1	2	1	1	2		R_{81}	R_{82}	R_{83}	R_{84}	

THE ¼ FRACTION OF THE 2^K DESIGN

Example Application

- ❑ Components manufactured in an injection molding process are showing excessive shrinkage.
- ❑ This is causing problems in assembly operations downstream from the injection molding area.
- ❑ A quality improvement team has decided to use a designed of experiment to study the injection molding process so that shrinkage can be reduced.
- ❑ The team decide to integrate six factors: Mold Temperature (A), Screw Speed (B), Holding Time (C), Cycle Time (D), Gate Size (E), and Holding Pressure (F). Each at two levels.
- ❑ The objective is to characterize and learn how each factor affects shrinkage and also, how the factors interact.

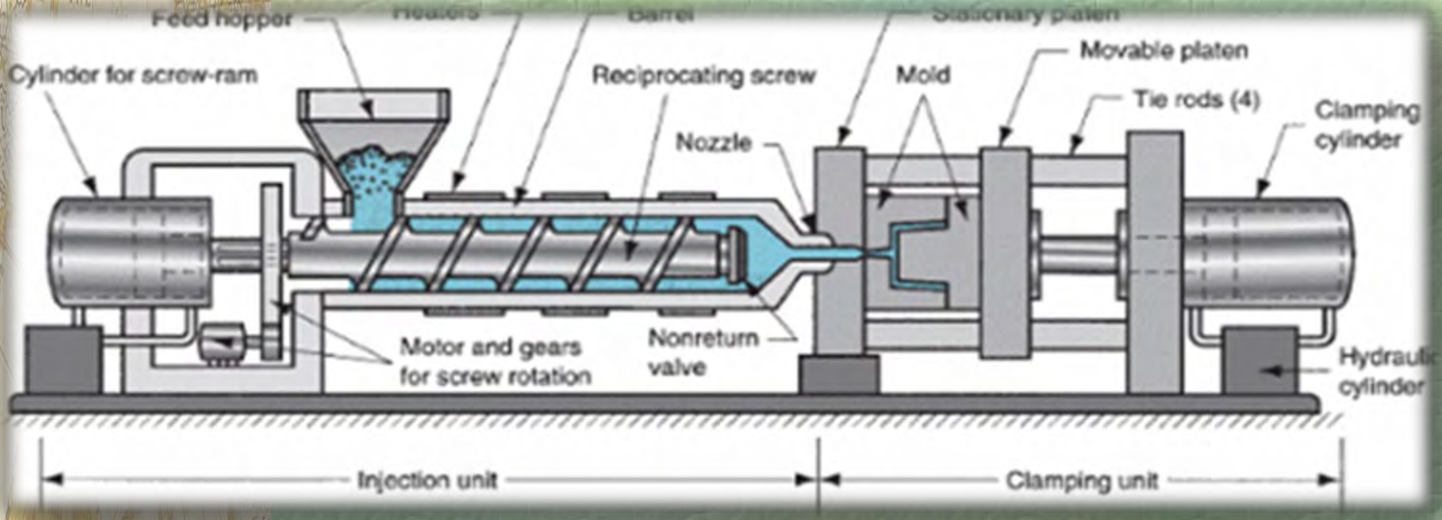
THE ¼ FRACTION OF THE 2^K DESIGN

Fractional Factorial Design

Factors:	8	Base Design:	6, 16	Resolution:	I
Runs:	16	Replicates:	1	Fraction:	1/16
Blocks:	1	Center pts (total):	0		

*** WARNING * Main effects are confounded with the mean (I)**

Design Generators: E = ABC, F = BCD, G = ABCE, H = BCDF



THE ¼ FRACTION OF THE 2^K DESIGN

Table 34: A 2^{6-2}_{IV} Design for Injection Molding

Std Order	Run Order	Center Pt	Blocks	Mold Temp	Screw Speed	Hold Time	Cycle Time	Gate Size	Hold Pressure	ABC	BCD	Observed Shrinkage (x 10)
14	1	1	1	1	-1	1	1	-1	-1	1	1	5
11	2	1	1	-1	1	-1	1	1	-1	1	1	34
4	3	1	1	1	1	-1	-1	-1	1	1	1	60
15	4	1	1	-1	1	1	1	-1	1	1	1	37
3	5	1	1	-1	1	-1	-1	1	1	1	1	32
8	6	1	1	1	1	1	-1	1	-1	1	1	60
5	7	1	1	-1	-1	1	-1	1	1	1	1	4
9	8	1	1	-1	-1	-1	1	-1	1	1	1	8
2	9	1	1	1	-1	-1	-1	1	-1	1	1	10
13	10	1	1	-1	-1	1	1	1	-1	1	1	16
16	11	1	1	1	1	1	1	1	1	1	1	52
12	12	1	1	1	1	-1	1	-1	-1	1	1	60
10	13	1	1	1	-1	-1	1	1	1	1	1	12
6	14	1	1	1	-1	1	-1	-1	1	1	1	15
1	15	1	1	-1	-1	-1	-1	-1	-1	1	1	6
7	16	1	1	-1	1	1	-1	-1	-1	1	1	26

THE ¼ FRACTION OF THE 2^K DESIGN

Table 35: Estimated Effects and Coefficients for Observed Shrinkage (coded units)

Term	Effect	Coef	SE Coef	T	P
Constant		27.313	2.511	10.88	0.000
Mold Temp	13.875	6.937	2.511	2.76	0.028
Screw Speed	35.625	17.813	2.511	7.09	0.000
Hold Time	-0.875	-0.438	2.511	-0.17	0.867
Cycle Time	1.375	0.688	2.511	0.27	0.792
Gate Size	0.375	0.187	2.511	0.07	0.943
Hold Pressure	0.375	0.188	2.511	0.07	0.943
Mold Temp * Screw Speed * Cycle Time	0.125	0.063	2.511	0.02	0.981
Mold Temp * Screw Speed * Hold Pressure	-4.875	-2.438	2.511	-0.97	0.364
S = 10.0423 PRESS = 3688.16 R-Sq = 89.40% R-Sq(pred) = 44.62% R-Sq(adj) = 77.28%					

$$\hat{Y} = \hat{\beta}_0 + \hat{\beta}_1 x_1 + \hat{\beta}_2 x_2 + \hat{\beta}_{12} x_1 x_2$$

$$= 27.3125 + 6.9775 x_1 + 17.8125 x_2 + 5.9375 x_1 x_2$$

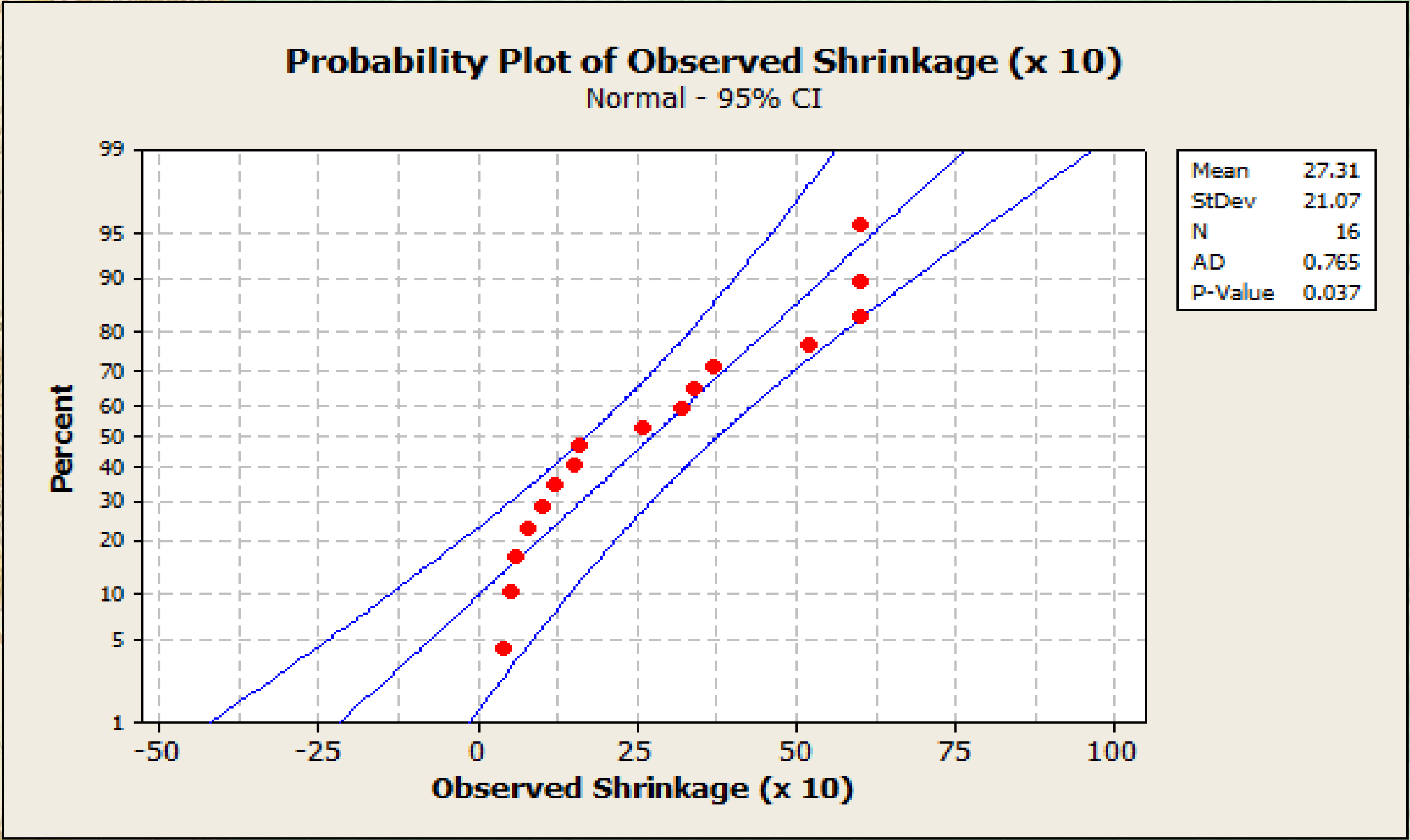
THE ¼ FRACTION OF THE 2^K DESIGN

Analysis of Variance for Observed Shrinkage (x 10) (coded units)

Source	DF	Seq SS	Adj SS	Adj MS	F	P
Main Effects	6	5858.38	5858.38	976.40	9.68	0.004
3-Way Interactions	2	95.13	95.13	47.56	0.47	0.642
Residual Error	7	705.94	705.94	100.85		
Total	15	6659.4433				

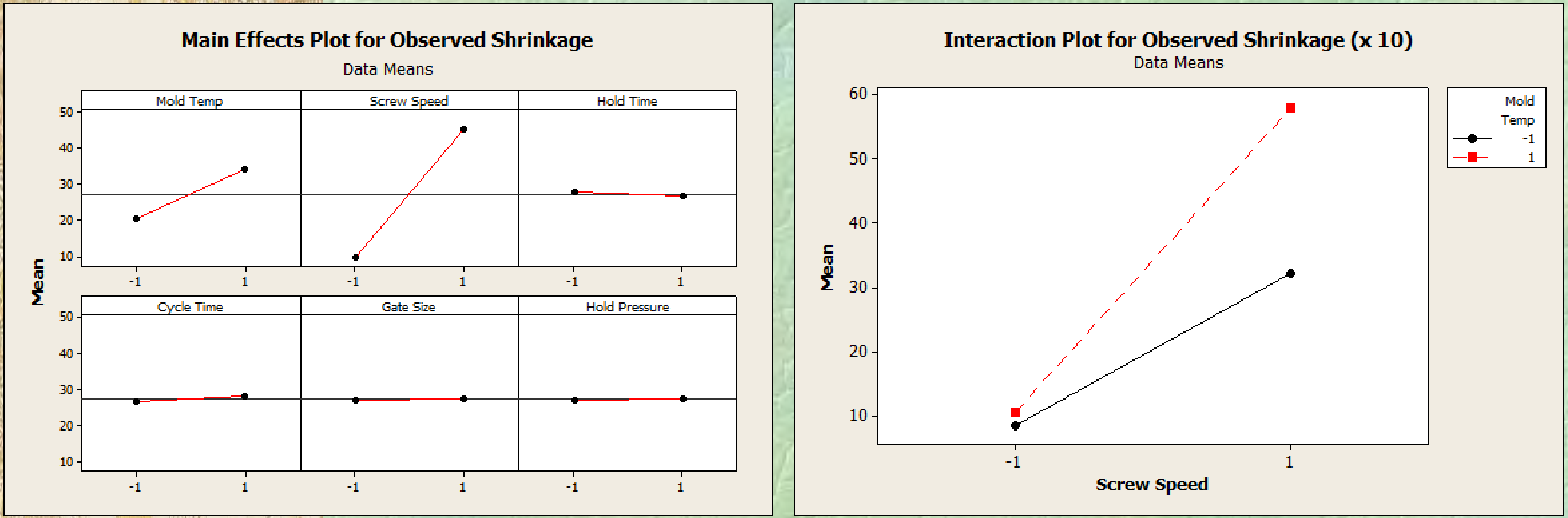
FRACTIONAL FACTORIAL DOE

Figure 36: Probability Plots for Part Shrinkage



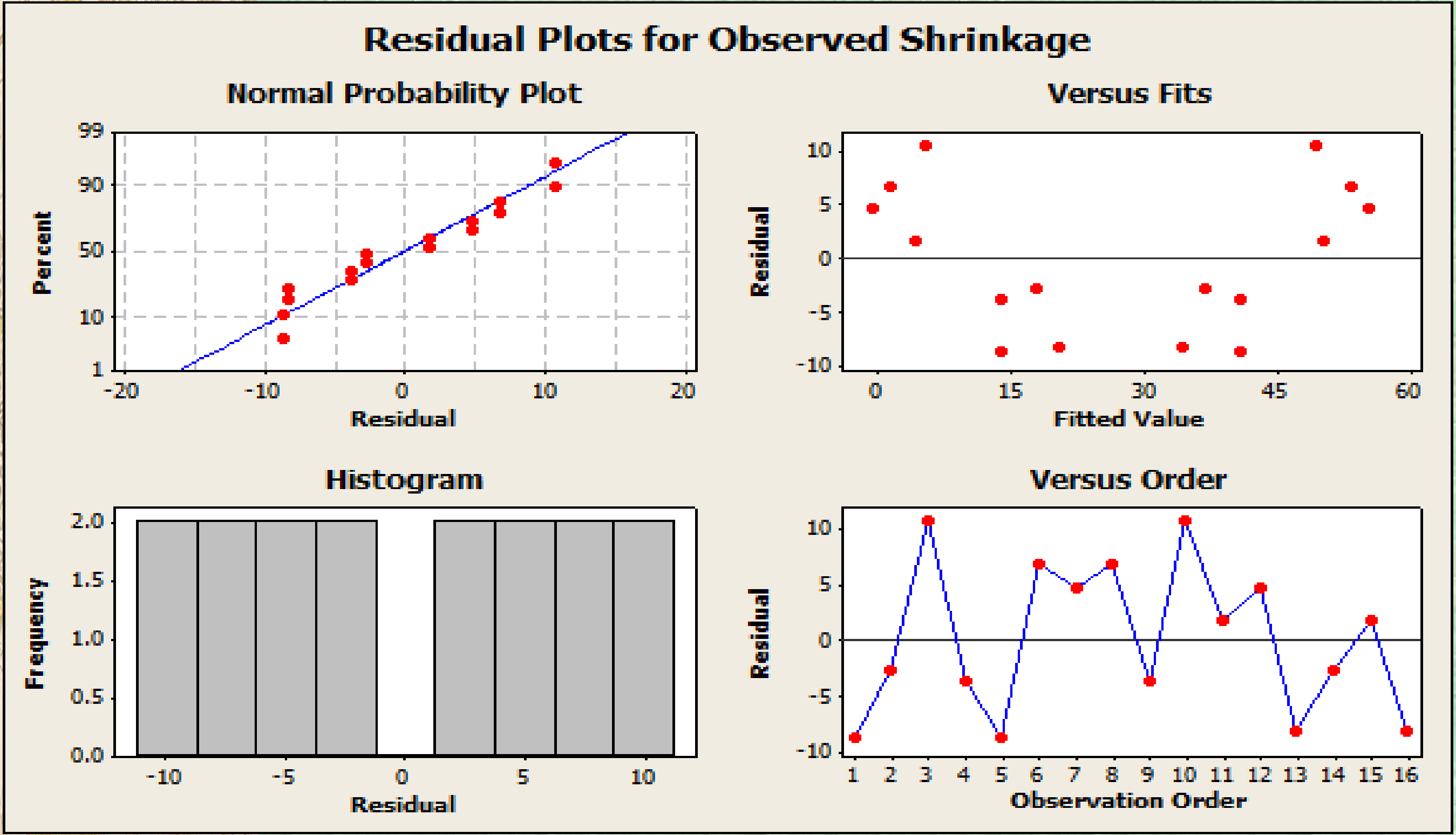
FRACTIONAL FACTORIAL DOE

Figure 37: Main Effects and Interaction Plots of Part Shrinkage



FRACTIONAL FACTORIAL DOE

Figure 38: Various Graphical Pots of Residuals



M4 - LEARNING OBJECTIVES

Participant Shall be able to:

- Identify means of reducing human error during design development.
- Identify and apply quantitative models for human behavior.
- Identify the principles the design of human machine interface seeks to embody.
- Learn the development of justifiable quantitative human error probabilities.
- Gain understanding of how to determine if provisions of suitable evidence that features included in the design are appropriate to general risk level.
- Gain understanding of how to determine if provisions of suitable evidence that features included in the design are appropriate to general risk level.
- Gain understanding of human factors expectations set by IEC 60601-1-6, IEC – 62366 and ANSI | AAMI HE – 75.
- Establish quantitative usability goals acceptance criteria for their company's products.
- Gain understanding of how to determine and quantify human reliability.
- Gain understanding of the extent to which human contributes to the general level of risk associated with the product design.

Adapt | Implement | Improve

HUMAN FACTORS ENGINEERING

What are Human Factors? Usability?

❑ **Human Factors**: **“…the application of knowledge about human capabilities (physical, sensory, emotional, and intellectual) and limitations to the design and development of tools, devices, systems, environments, and organizations….” (ANSI/AAMI HE75:2009, Introduction)**

❑ **Usability**: **“Characteristic of the user interface that establishes effectiveness, efficiency, ease of user learning and user satisfaction” (ISO/IE 62366:2007, Definition 3.17).**

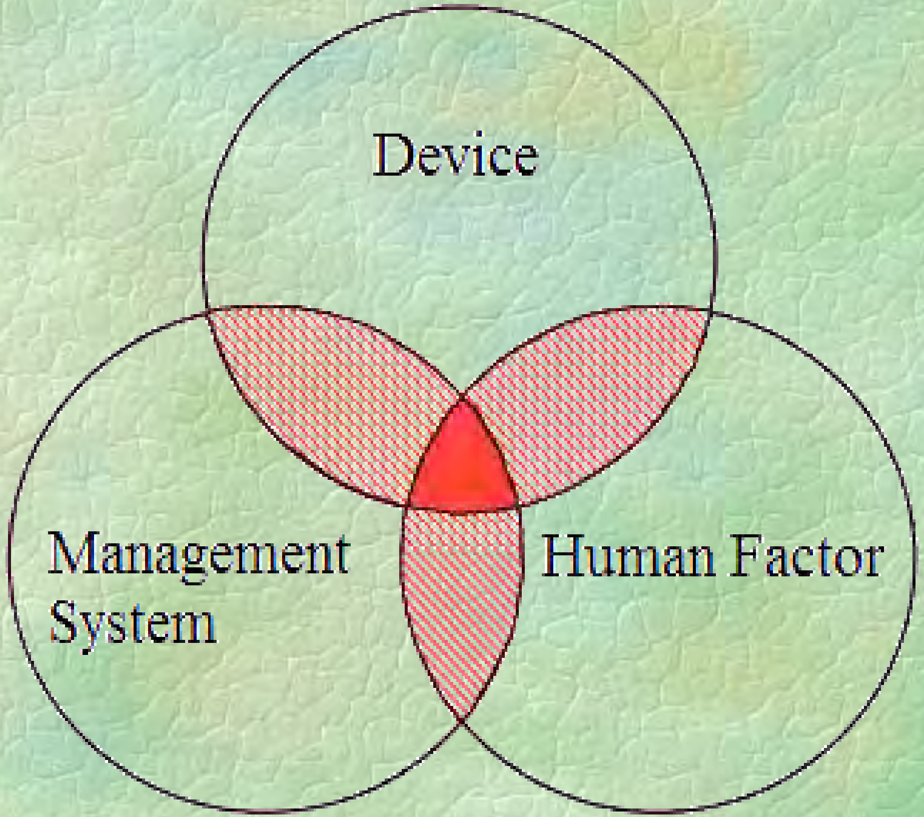
❑ **Human Reliability: The probability of successful performance of only those human activities necessary to make a system reliable or available.**

❑ **Human Error: Human Error is simply some human output which is outside the tolerances established by the system requirements in which the person operates.**

The application of human factors engineering will “create a human-system interface that will operate within human performance capabilities, meet system functional requirements, and accomplish mission \ functional objectives.”

HUMAN FACTORS ENGINEERING

Figure 1: Illustration of Human Factor



Human Factor may be defined as an integration and application of scientific knowledge about the behavior of human beings, device and management systems (procedures, training, etc.) to improve their interactions in the workplace.

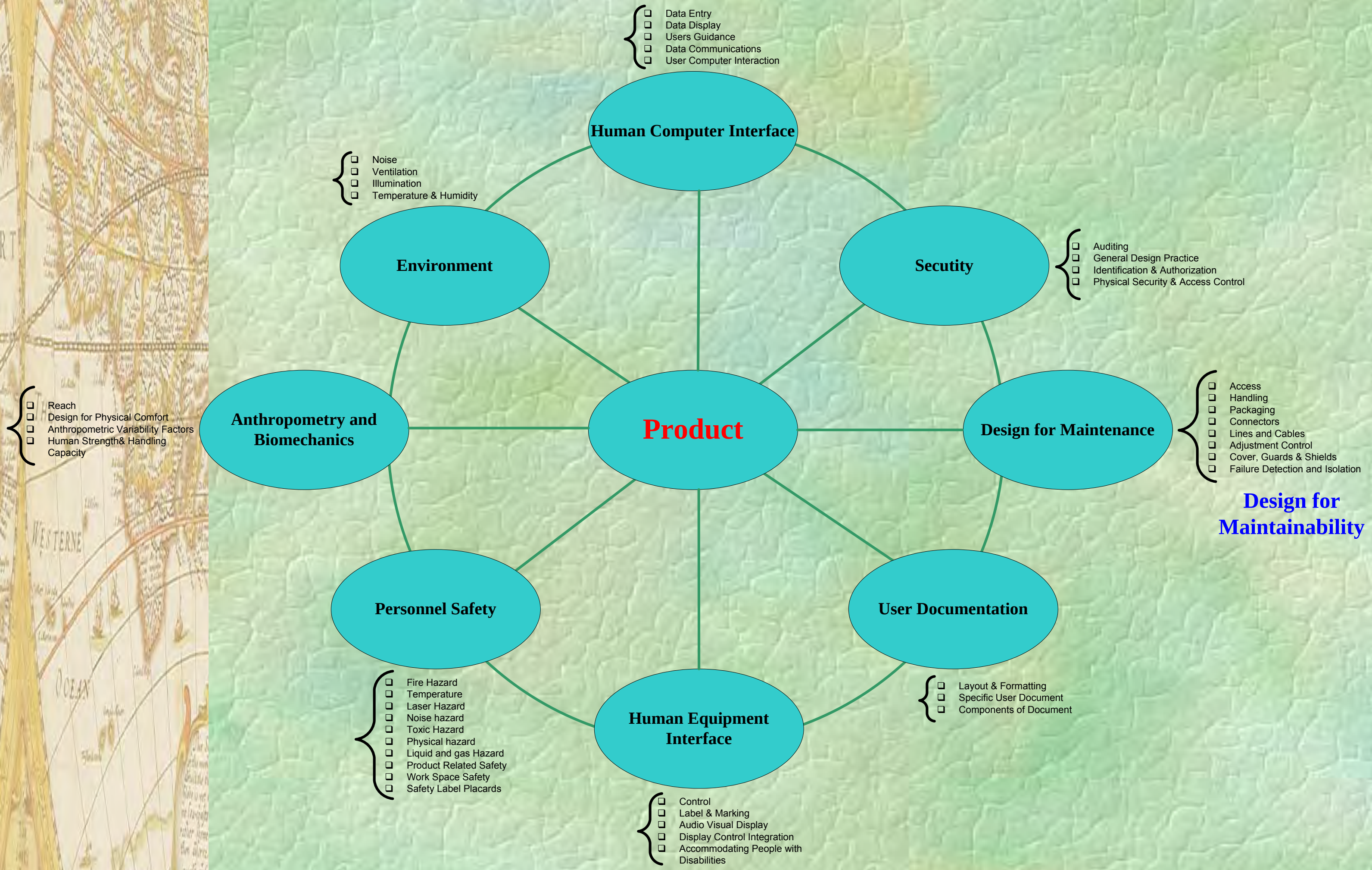
HUMAN FACTORS ENGINEERING

Objectives of Human Factors

- ❑ The first is to enhance the effectiveness and efficiency with which work and other activities are carried out. This includes such things as increased convenience of use, reduced errors and increased productivity.
- ❑ The second objective is to enhance certain desirable human values, including improved safety, reduced fatigue and stress, increased comfort, greater user acceptance, increased job satisfaction, and improved quality of life.
- ❑ To develop the optimal conditions for the user in work environment, to reduce physiological costs, to improve productivity, to facilitate instrument handling, to maximize the efficiency of operation and production system, and to minimize human errors ergonomics is essential.

HUMAN FACTORS ENGINEERING

Figure 4: Framework for Human Factors Engineering



Human Computer Interface

- Data Entry
- Data Display
- Users Guidance
- Data Communications
- User Computer Interaction

Environment

- Noise
- Ventilation
- Illumination
- Temperature & Humidity

Secutity

- Auditing
- General Design Practice
- Identification & Authorization
- Physical Security & Access Control

Anthropometry and Biomechanics

- Reach
- Design for Physical Comfort
- Anthropometric Variability Factors
- Human Strength& Handling Capacity

Product

Design for Maintenance

- Access
- Handling
- Packaging
- Connectors
- Lines and Cables
- Adjustment Control
- Cover, Guards & Shields
- Failure Detection and Isolation

Design for Maintainability

Personnel Safety

- Fire Hazard
- Temperature
- Laser Hazard
- Noise hazard
- Toxic Hazard
- Physical hazard
- Liquid and gas Hazard
- Product Related Safety
- Work Space Safety
- Safety Label Placards

User Documentation

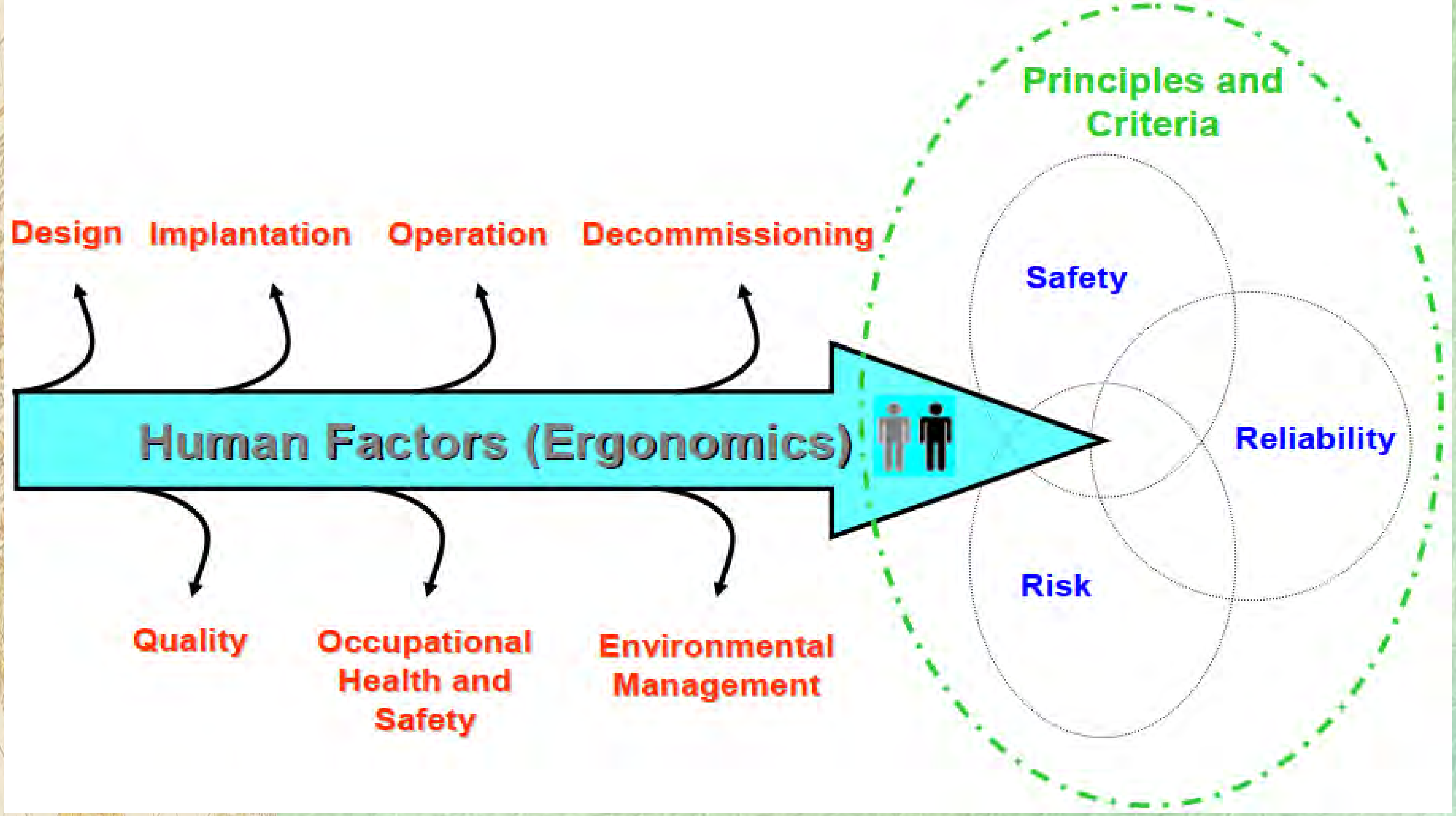
- Layout & Formatting
- Specific User Document
- Components of Document

Human Equipment Interface

- Control
- Label & Marking
- Audio Visual Display
- Display Control Integration
- Accommodating People with Disabilities

HUMAN FACTORS ENGINEERING

Figure 6: Overview of the Framework for Human Factors Integration.



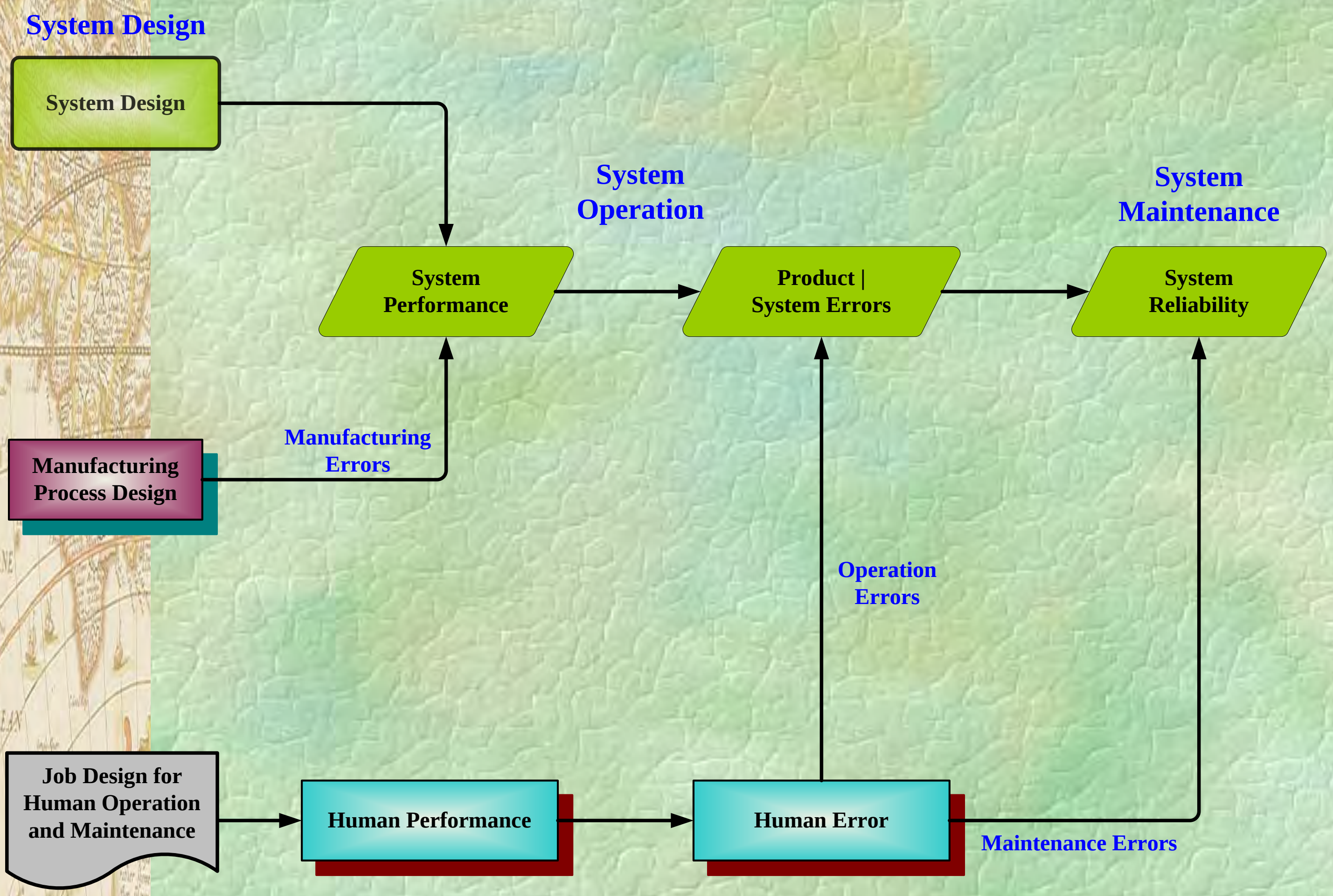
HUMAN FACTORS ANALYSIS

Table 2: Three Major Types of Human Factors Analysis

Item	Analysis Type	Description	Comments
1	▪ Visibility	▪ Determine visibility of operation or work area to operators and maintainers.	It may be important (e.g., for safety considerations) that a person be able to fully observed the operation or work area.
2	▪ Strength	▪ Used to determine the feasibility of activity sequences. Determine whether or not a person is able to carry out an activity that requires a certain level of human strength, i.e., to evaluate the ability of the person to carry, lift, hold, twist, push and pull objects in standing, bending, sitting, squatting,, lying, etc., body position.	Strength analysis can be one of the most important criteria for the evaluation of a task.
3	▪ Accessibility	▪ Performed to identify design problems related to the inability of personnel to access an operation or work area, i.e., to detect possible collisions during an activity.	Based on the size of men and women at a given percentile of the population.

HUMAN RELIABILITY CONSIDERATIONS FOR SYSTEMS

Figure 11: The Impact of Human on System and Process Reliability



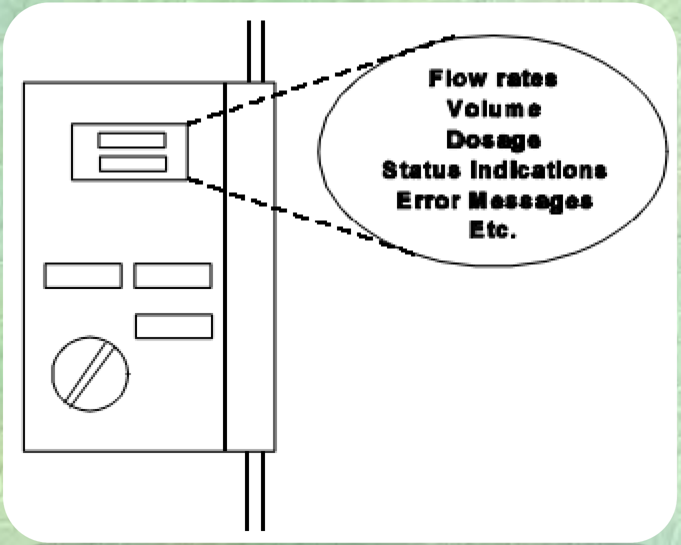
HUMAN RELIABILITY CONSIDERATIONS FOR SYSTEMS

Medical Device Application

❑ **The following are some problems that apply to many medical devices and can lead to errors:**

- **Illogical or cumbersome control sequences;**
- **Unfamiliar language, symbols, or codes;**
- **Inconsistencies among display formats;**
- **Conventions that contradict user expectations;**
- **Uncertain or no feedback after input;**
- **Functions that are hidden from the user;**
- **Missing or ambiguous prompts, symbols, or icons;**
- **Un-signaled resets or defaults;**
- **No status information;**
- **Missing lock-outs or interlocks; and**
- **Requirements for complex mental calculations.**

Figure 13: Infusion Pump



With current models, users often must retrieve and remember large amounts of information.

GENERAL PRODUCT DESIGN REQUIREMENTS

Table 6: Principles for Designing and Selecting Systems and Equipment

Item No	Design Factors	General Description and Criteria
1	Simplicity in design	▪ The system or equipment design should be as simple as possible, consistent with the desired human-machine system functions, and compatible with the expected maintenance concepts. Simplicity Means more reliable.
2	Hardware and interface standardization	▪ Equipment and human-machine interface designs shall be standardized to the degree practical and compatible with system functions and purposes.
3	Software standardization	▪ Software shall be as standardized as possible so that applications that address common functions employ the same user dialogues, interfaces, and procedures.
4	Standardization for maintenance	▪ Identical interfaces, fasteners, switches or breakers, and connectors shall be used throughout a unit of equipment. ▪ Similarly, control, display, marking, coding, labeling, and arrangement schemes shall be the same for common functions.
5	Distinctive identification, interfaces, and interconnections	▪ Units of equipment or modules that have different functions shall be distinctive in their appearance and identification. Equipment with different functions shall have distinctive interfaces (control and display features, and connectors) so they cannot be interconnected or used erroneously.
6	Design for common tools	▪ Whenever possible, system and equipment design shall minimize auxiliary equipment and the number of tools needed for maintenance by designing for common tools available in a maintainer's tool box.
7	Safety	▪ System and equipment design shall incorporate applicable system and personnel safety design criteria. These criteria include those that minimize human error under normal, degraded, or emergency conditions, and under adverse environments.
8	Fail-safe design	▪ A fail-safe design shall be provided for systems whose failure could cause catastrophic damage, injury to personnel, or inadvertent operation of equipment.
9	Ruggedness	▪ Systems and equipment shall be sufficiently rugged to withstand handling during operation, maintenance, supply, and transport within the environmental limits specified in the applicable product specification.

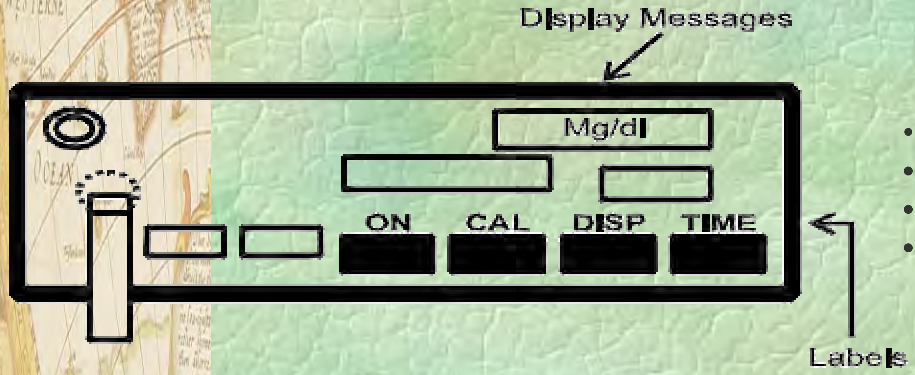
HUMAN FACTORS VALIDATION

Validate Safety of Use - FDA

❑ Demonstrates and provides evidence that a medical device, as designed, can be used safely and effectively:

- By people who are representative of the intended users
- Under expected use conditions
- For essential and critical (high-risk) tasks

Figure 14 - Blood Glucose Monitor



- Are displays and labels legible?
- Are strips easy to clean and insert?
- Is device compact and durable?
- How difficult are timing operations?

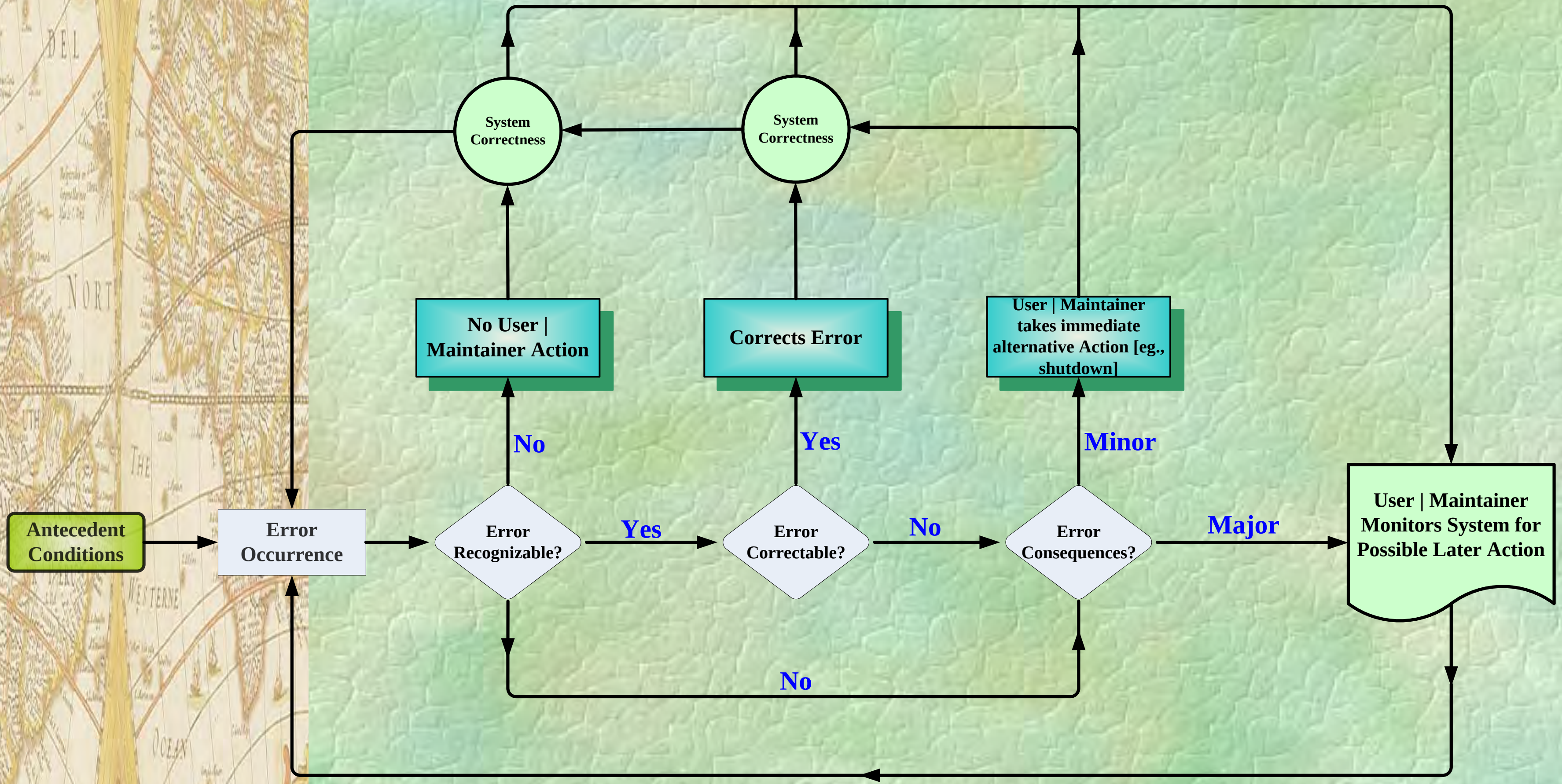
SYSTEM DESIGN ENVIRONMENTAL CONDITIONS

Table 9: Environmental Factor Consideration in Design

Item No.	Environmental Factor	Human Factor Consideration
1	Acoustic Noise	Consideration should be given to the effects of noise on device users, other workers, and the patient. All noise sources should be assessed.
2	Interruptions and Distractions	A medical device's intended user might be interrupted or distracted while using the device. Designers should account for the type and frequency of these interruptions in their designs so that interruptions do not adversely affect device use. Workplace stresses and interruptions in use environments can distract device users and lead to use errors.
3	Lighting	Device displays should be designed for viewing under the lighting conditions in intended use locations. It is important to consider the specific lighting environments in which a medical device will be used and to sample lighting levels in representative locations by means of light meters.
4	Temperature and Humidity	Medical devices should be designed to minimize their impact on surrounding temperatures and humidity levels that could affect the user's ability to use a device. Temperature and humidity extremes can degrade performance.
5	Surface Temperature	During normal use, the temperature of medical device surfaces and components that can come into contact with device users or patients should not exceed the limits specified in [ANSI/AAMI ES60601-1:2005].
6	Vibration	The vibration of visual displays should not significantly compromise user performance. Usability testing should be performed to assess the impact of expected vibration on critical functions of the device and on the incidence of use errors.

CHARACTERISTICS OF HUMAN ERROR

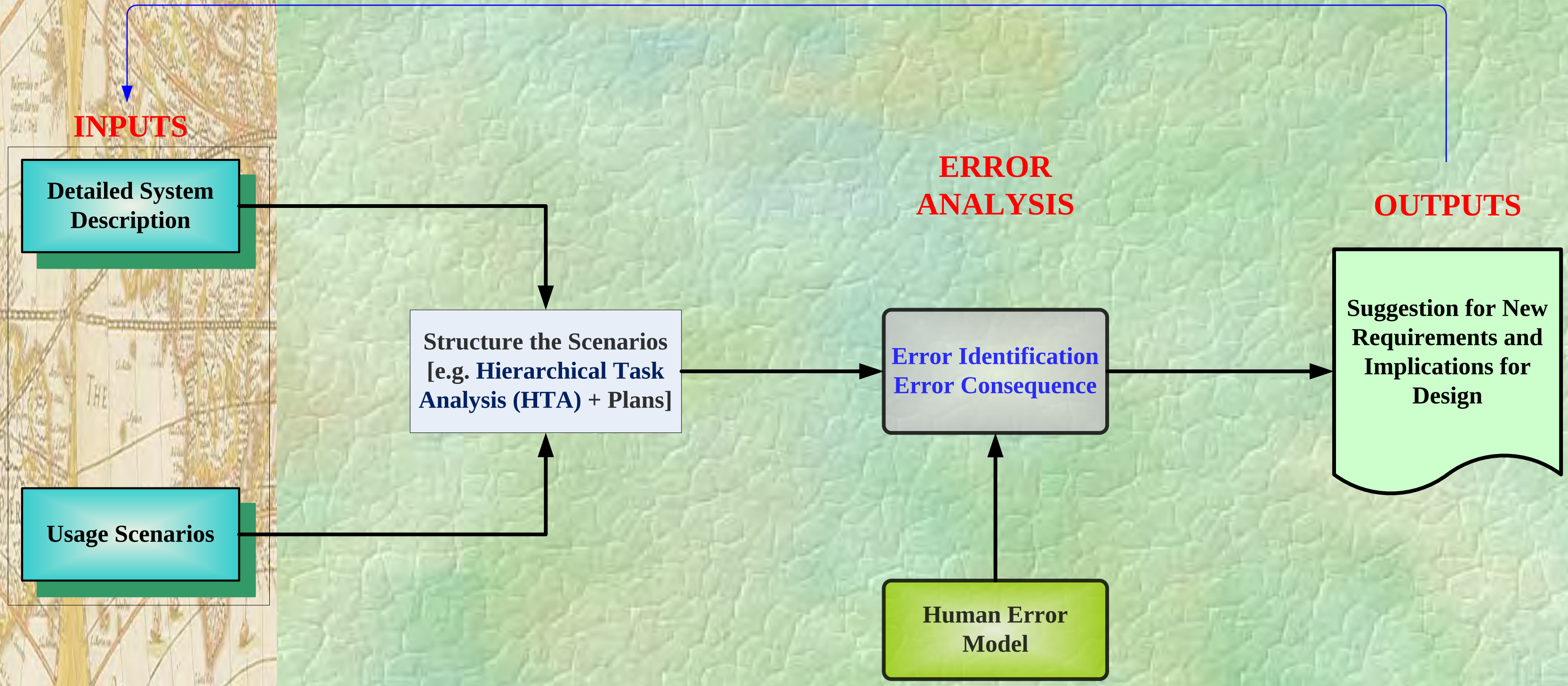
Figure 15: Flow Diagram Illustrating a Possible Error Recovery Sequence



Three Characteristics: Obviousness (for self detection or detection by another), Corrected [recovery], and its Consequences

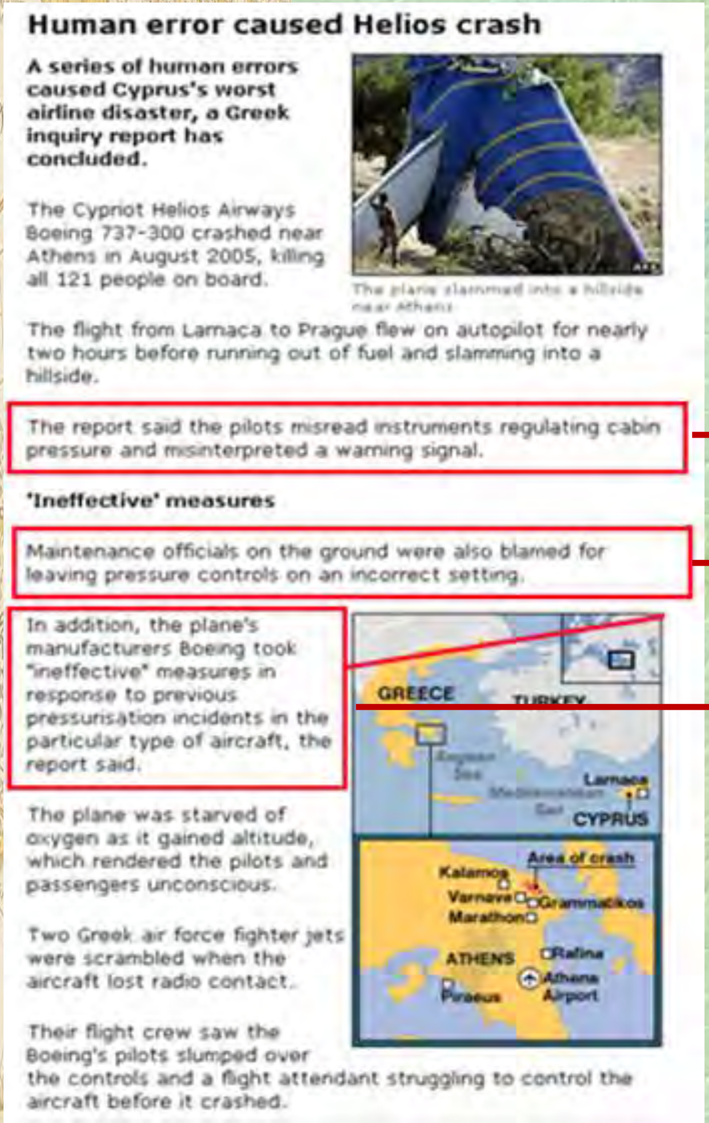
HUMAN ERROR ASSESSMENT METHOD APPLIED IN DESIGN

Figure 20: Technique for Human Error Assessment Process Early in System Design


INPUTS
Detailed System Description
Usage Scenarios
Structure the Scenarios [e.g. Hierarchical Task Analysis (HTA) + Plans]
ERROR ANALYSIS
Error Identification
Error Consequence
Human Error Model
OUTPUTS
Suggestion for New Requirements and Implications for Design

Technique for Human Error Assessment (THEA). The method has been applied to several real world case studies and has demonstrated its suitability in evaluating a design for its vulnerability to human interaction failures which may become problematic once the design becomes operational.

HUMAN ERROR EXAMPLE



Human error caused Helios crash

A series of human errors caused Cyprus's worst airline disaster, a Greek inquiry report has concluded.

The Cypriot Helios Airways Boeing 737-300 crashed near Athens in August 2005, killing all 121 people on board.

The plane slammed into a hillside near Athens

The flight from Larnaca to Prague flew on autopilot for nearly two hours before running out of fuel and slamming into a hillside.

The report said the pilots misread instruments regulating cabin pressure and misinterpreted a warning signal.

'Ineffective' measures

Maintenance officials on the ground were also blamed for leaving pressure controls on an incorrect setting.

In addition, the plane's manufacturers Boeing took "ineffective" measures in response to previous pressurisation incidents in the particular type of aircraft, the report said.

The plane was starved of oxygen as it gained altitude, which rendered the pilots and passengers unconscious.

Two Greek air force fighter jets were scrambled when the aircraft lost radio contact.

Their flight crew saw the Boeing's pilots slumped over the controls and a flight attendant struggling to control the aircraft before it crashed.

Human errors may affect design and procedures, as well as decisions or actions for controlling transients or in reacting to perturbations and hardware failures.

- ❑ **Pilot misread instruments AND misinterpreted warning signals**
- ❑ **Maintenance left pressure control in wrong setting**
- ❑ **Manufacturer did not respond adequately to previous similar incidents.**

Extract taken from BBC News Site
http://news.bbc.co.uk/1/hi/world/europe/6036507.stm?ls

HUMAN ERRORS CAUSING USER-INTERFACE DESIGN PROBLEMS

User-interface medical device design-related problems that, directly or indirectly, cause users errors

- Poorly designed labels.
- Ambiguous or difficult to read displays.
- Confusing device operating instructions.
- Unnecessary confusing or intrusive device alarms.
- Poor device designing requiring unnecessary complex installation and maintenance tasks.
- Complex or unconventional arrangements of items such as controls, displays, and tubing.

HUMAN ERRORS ANALYSIS METHODS FOR MEDICAL DEVICE

User-interface medical device design-related problems that, directly or indirectly, cause users errors:

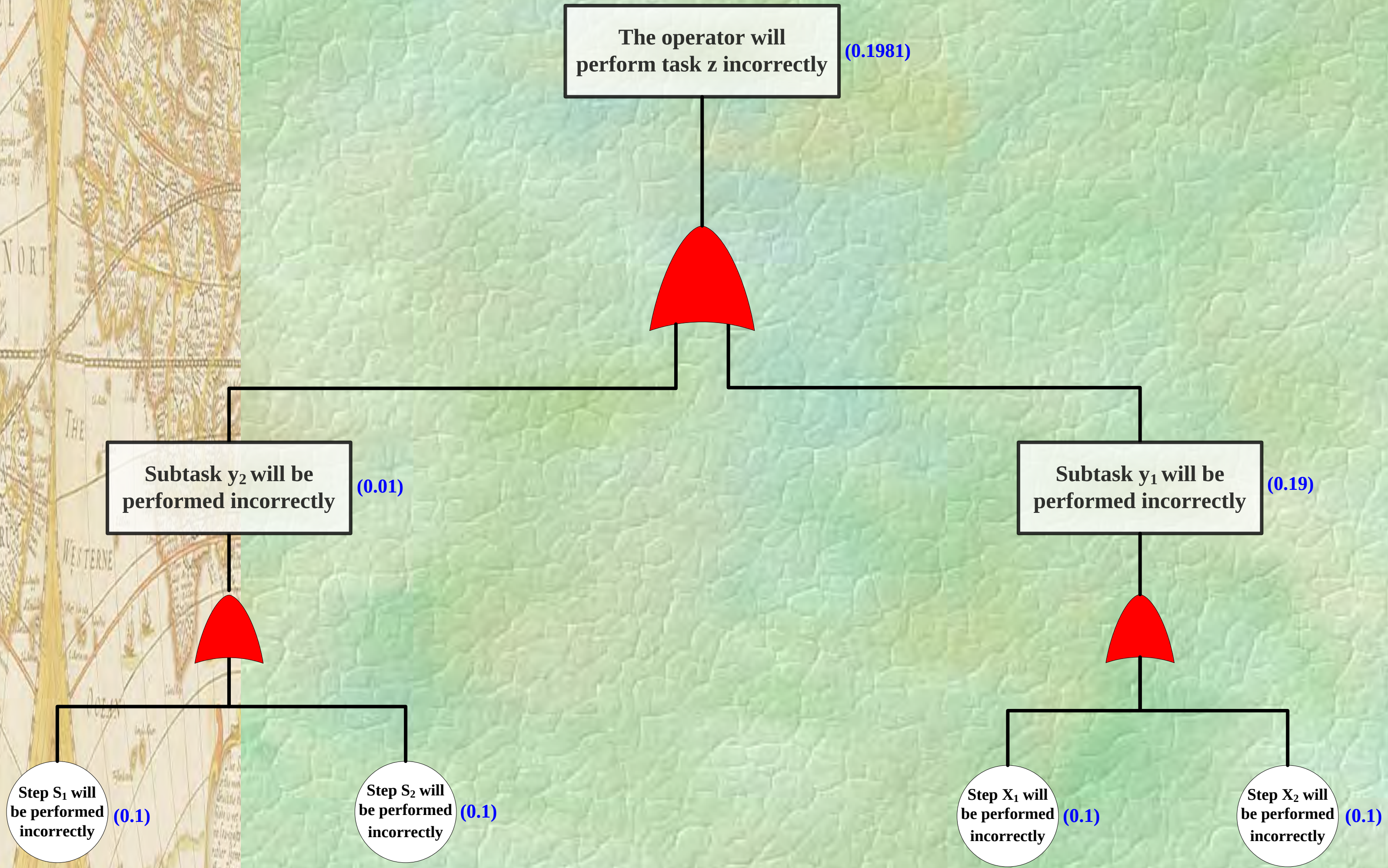
- ❑ FMEA
- ❑ Barrier Analysis.
- ❑ Force Field Analysis.
- ❑ Root Cause Analysis.
- ❑ Markov Model
- ❑ Fault Tree Analysis (FTA).
- ❑ Man-Machine System Analysis (MMSA).

Barrier Analysis

- ❑ This method is based on the premise that an item possesses various types of energy (e.g., pharmaceutical reactions, mechanical impact, and heat) that can cause property damage and injuries.
- ❑ The method basically attempts to identify various types of energies associated with items and appropriate barriers to stop them from reaching humans or property.

HUMAN ERRORS IN MEDICAL DEVICES

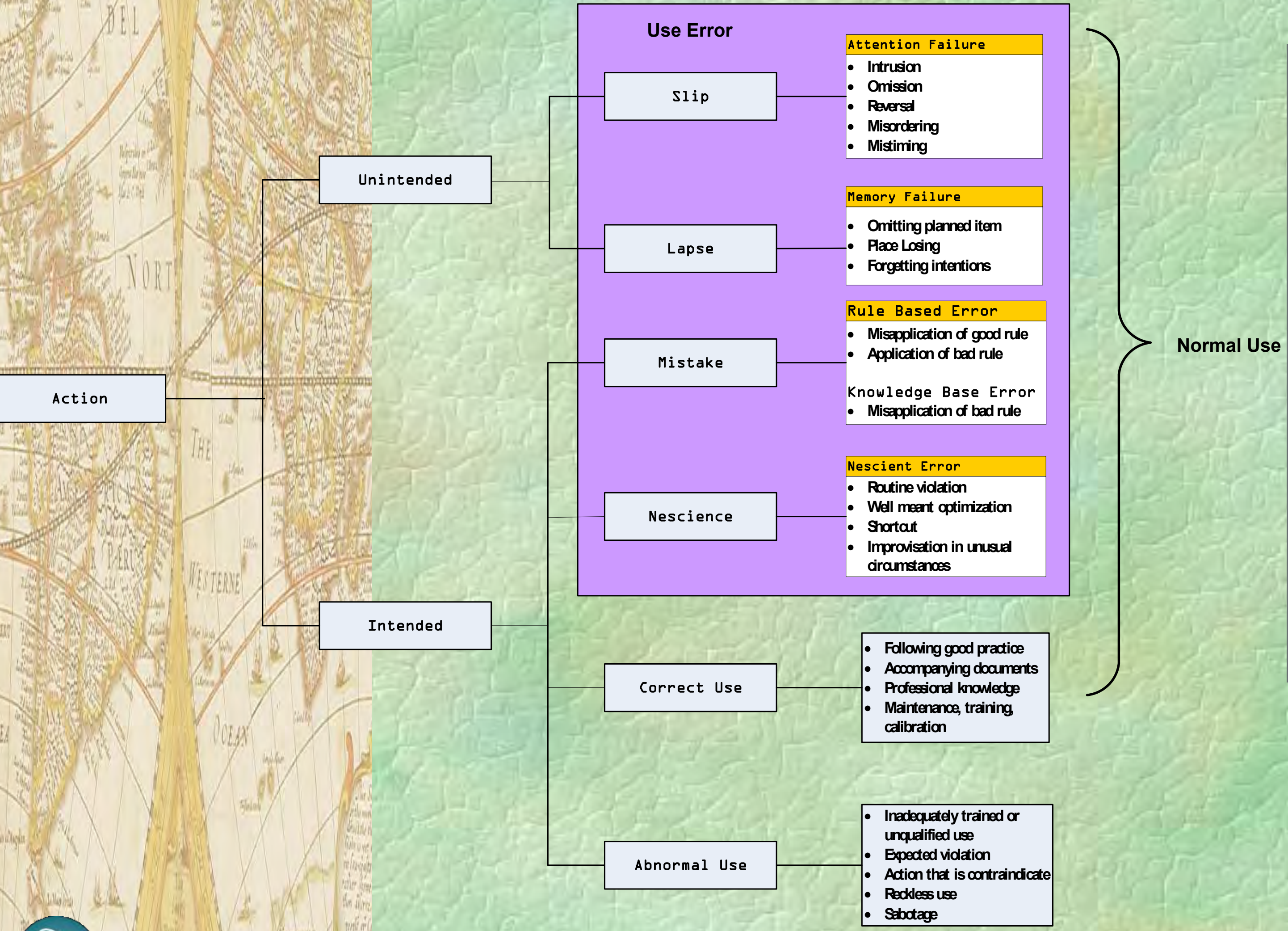
Figure 23: Fault Tree for Medical Device Operator Performing Task Z Incorrectly



The operator will perform task z incorrectly
(0.1981)
Subtask y_2 will be performed incorrectly
(0.01)
Subtask y_1 will be performed incorrectly
(0.19)
Step S_1 will be performed incorrectly
(0.1)
Step S_2 will be performed incorrectly
(0.1)
Step X_1 will be performed incorrectly
(0.1)
Step X_2 will be performed incorrectly
(0.1)

MANAGING THE RISK OF USE ERROR

Figure 26: Erroneous, correct, and abnormal use and examples of use error [Adapted from IEC 62366:2007]



Use Error

Action

Unintended

Intended

Slip

Attention Failure
- Intrusion
- Omission
- Reversal
- Misordering
- Mistiming

Lapse

Memory Failure
- Omitting planned item
- Place Losing
- Forgetting intentions

Mistake

Rule Based Error
- Misapplication of good rule
- Application of bad rule

Knowledge Base Error
- Misapplication of bad rule

Nescience

Nescient Error
- Routine violation
- Well meant optimization
- Shortcut
- Improvisation in unusual circumstances

Correct Use
- Following good practice
- Accompanying documents
- Professional knowledge
- Maintenance, training, calibration

Abnormal Use
- Inadequately trained or unqualified use
- Expected violation
- Action that is contraindicate
- Reckless use
- Sabotage

Normal Use

Reducing error risk: A brief guide

1. Identify critical human tasks.
2. Identify error potential:
   a. What errors are possible?
   b. What are the potential consequences of those errors?
3. Identify performance-shaping factors:
   a. People-level factors.
   b. Job-level factors.
   c. Organisation-level factors.
4. Evaluate existing controls:
   a. Are controls in place to prevent error?
   b. Are controls in place to mitigate error?
   c. Is error risk ALARP?
5. Develop additional controls:
   a. Eliminate the opportunity for error.
   b. Prevent – lower the likelihood of error.
   c. Reduce – facilitate error identification and recovery.
   d. Mitigate the consequences of error.

FACTS AND FIGURES ON HUMAN ERRORS IN MAINTENANCE

Some of the facts and figures associated with human error in maintenance are as follows:

- ❑ A study of electronic equipment revealed that 30% of failures were due to operation and maintenance error.
- ❑ The breakdown of this statistic shows abnormal or accidental condition (12%), manhandling (10%), and faulty maintenance (8%).
- ❑ In 1993, a study of 122 maintenance occurrences involving human factors concluded that the categories of maintenance error breakdowns were incorrect installations (30%), omissions (56%), incorrect parts (8%), and other (6%).
- ❑ A study of various tasks such as adjust, align, and remove indicates a human reliability mean of 0.9871. This means that one should expect errors by maintenance personnel on the order of 13 times in 1000 attempts
- ❑ In 1979 in a DC-10 accident at O'Hare Airport in Chicago, 272 persons died because of improper maintenance procedures
- ❑ A study of maintenance operations among commercial airlines revealed that 40 to 50% of the time the elements removed for repair were not defective.

USABILITY APPLICATION IN DESIGN OF MEDICAL DEVICE

Medical Device

- ❑ Any instrument, apparatus, implement, machine, appliance, implant, in vitro reagent or calibrator, software, material or other similar or related article, intended by the MANUFACTURER to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of:
  - ▪ Diagnosis, prevention, monitoring, treatment or alleviation of disease,
  - ▪ Diagnosis, monitoring, treatment, alleviation of or compensation for an injury,
  - ▪ Investigation, replacement, modification, or support of the anatomy or of a physiological process,
  - ▪ Supporting or sustaining life,
  - ▪ Disinfection of MEDICAL DEVICES,
  - ▪ Providing information for medical purposes by means of in vitro examination of specimens derived from the human body.

USABILITY APPLICATION IN DESIGN OF MEDICAL DEVICE

Why is Usability Important?

- ❑ Defined in ISO 9241:
  - A measure of the effectiveness, efficiency and satisfaction with which specified users can achieve specified goals in a particular environment.
- ❑ Poor Usability Results in:
  - Anger and Frustration
  - Costs Money
  - Higher error Rates
  - Equipment Damage
  - Loss of Customer Loyalty
  - Physical and Emotional Injury
  - Decreased Productivity in the Workplace

Examples of Poor Design

- ❑ Door Handles
  - Handles *afford* pulling
  - Trapped between doors
  - Using a flat plate would *constrain* the user to push
- ❑ Wireless PowerPoint slide controller
  - Short press to go forward
  - Long press to go backward
- ❑ Refrigerator Temperature Control
  - One cooling unit
  - Two compartments and two controls

USABILITY APPLICATION IN DESIGN OF MEDICAL DEVICE

Content of the Usability Test Plan

❑ The usability test plan should describe the following:

A. Purpose
B. Setting
C. Participants
D. Prototypes or simulations
E. Methodology or test protocol
F. Usability objectives
G. Data collection
H. Data analysis
I. Reporting
J. Tasks

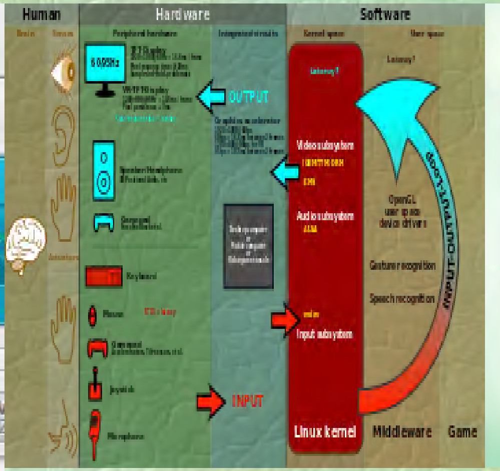
❑ Methodology or Test Protocol

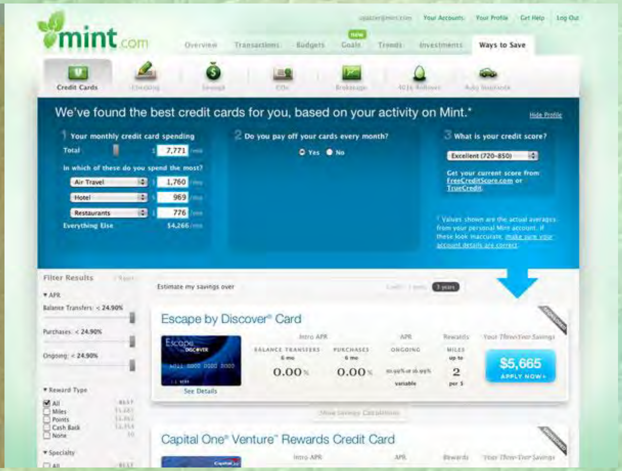
- The method description in a usability testing plan, its actual protocol, and the subsequent report are much like the methodology section of any scientific report.
- The usability test plan should describe the usability study methodology and related test protocols in enough detail that another researcher or designer could replicate the study.
- It should cover all of the items relating to logistics [testing locations, number of participants, size of testing staff, duration of testing session, video recording, note takers, and data logging software].

FUNDAMENTALS OF SOFTWARE USER INTERFACE

Sample Software–User Interfaces

- ❑ Embedded software–user interfaces—those found in special-purpose medical devices—are plentiful.
- ❑ Examples include patient monitors, infusion pumps, and defibrillators. These devices tend to incorporate a set of dedicated controls, such as a number pad, a four-way cursor control, and special-purpose keys that allow users to interact effectively with the associated user interface.
- ❑ It is common for the software–user interface of larger medical devices to be based on a personal computer (PC) application running within a commercial operating system (e.g., Windows™) on a conventional computer screen.



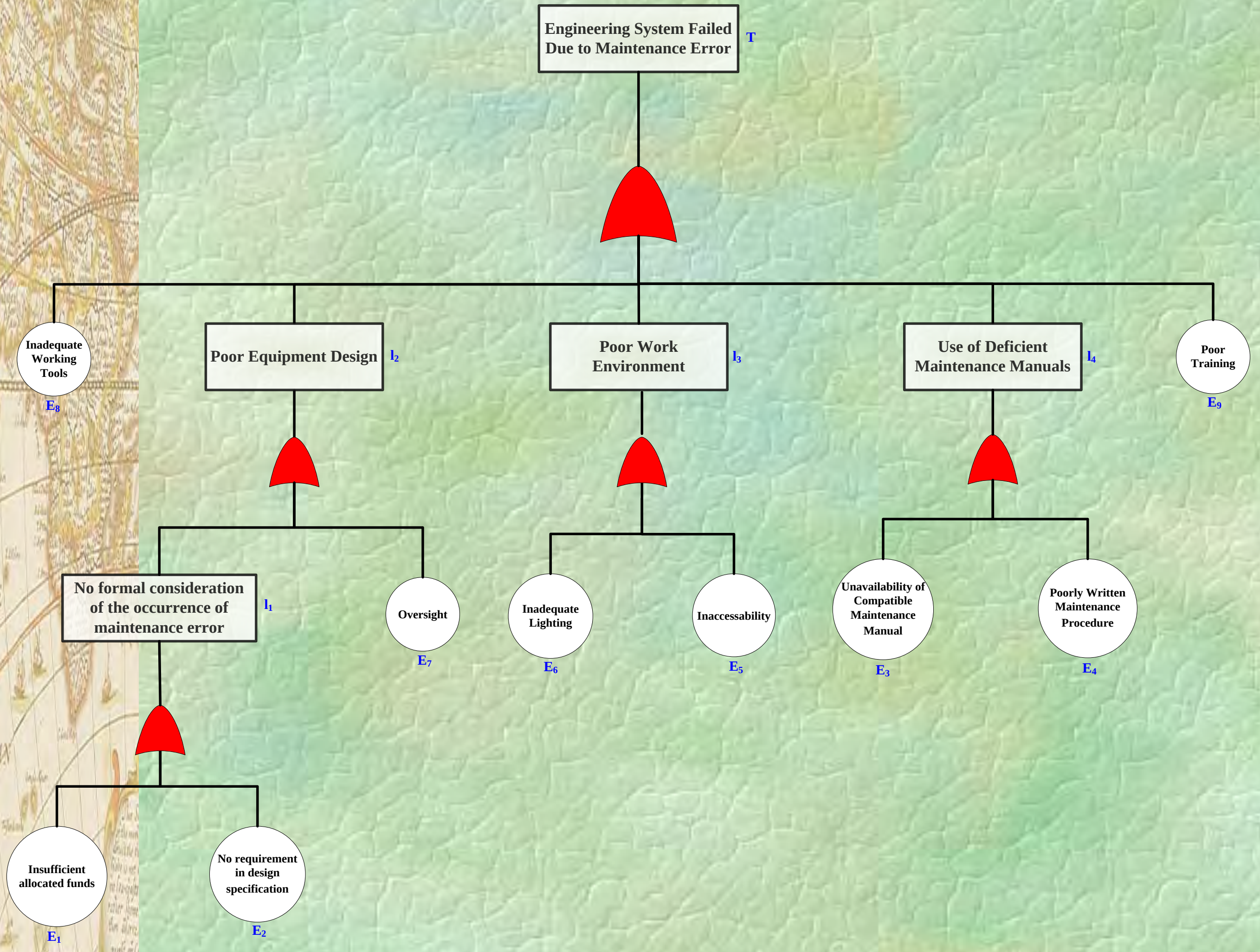


We've found the best credit cards for you, based on your activity on Mint.*

Your monthly credit card spending
Do you pay off your cards every month?
What is your credit score?
Excellent (720-850)
Air Travel
Hotel
Restaurants
Everything Else
Filter Results
Escape by Discover® Card
$5,665
APPLY NOW
Capital One® Venture℠ Rewards Credit Card

PREDICTING THE OCCURRENCE OF HUMAN ERROR IN MAINTENANCE

Figure 37: Fault Tree Diagram


Engineering System Failed Due to Maintenance Error
T
Inadequate Working Tools
E_8
Poor Equipment Design
I_2
Poor Work Environment
I_3
Use of Deficient Maintenance Manuals
I_4
Poor Training
E_9
No formal consideration of the occurrence of maintenance error
I_1
Oversight
E_7
Inadequate Lighting
E_6
Inaccessability
E_5
Unavailability of Compatible Maintenance Manual
E_3
Poorly Written Maintenance Procedure
E_4
Insufficient allocated funds
E_1
No requirement in design specification
E_2

M5 – SEC 2 - LEARNING OBJECTIVES

Participant shall be able to:

- **Identify the different methods of stress application and determine the type of accelerated stress.**
- **Identify the required inputs and distinguish between ALT, HASS, and HALT.**
- **Determine the appropriate stress parameter to accelerate.**
- **Utilize ALT model to estimate and quantify the life of an item or product through accelerated life data analysis.**
- **Utilize ALT model to assess and demonstrate component reliability, operating life or MTTF.**
- **Develop and understanding of how to design | develop ALT test plan, determine the number of units to be tested.**
- **Explain how Design and Analysis of Experiment is used to support ALT.**

Adapt | Implement | Improve

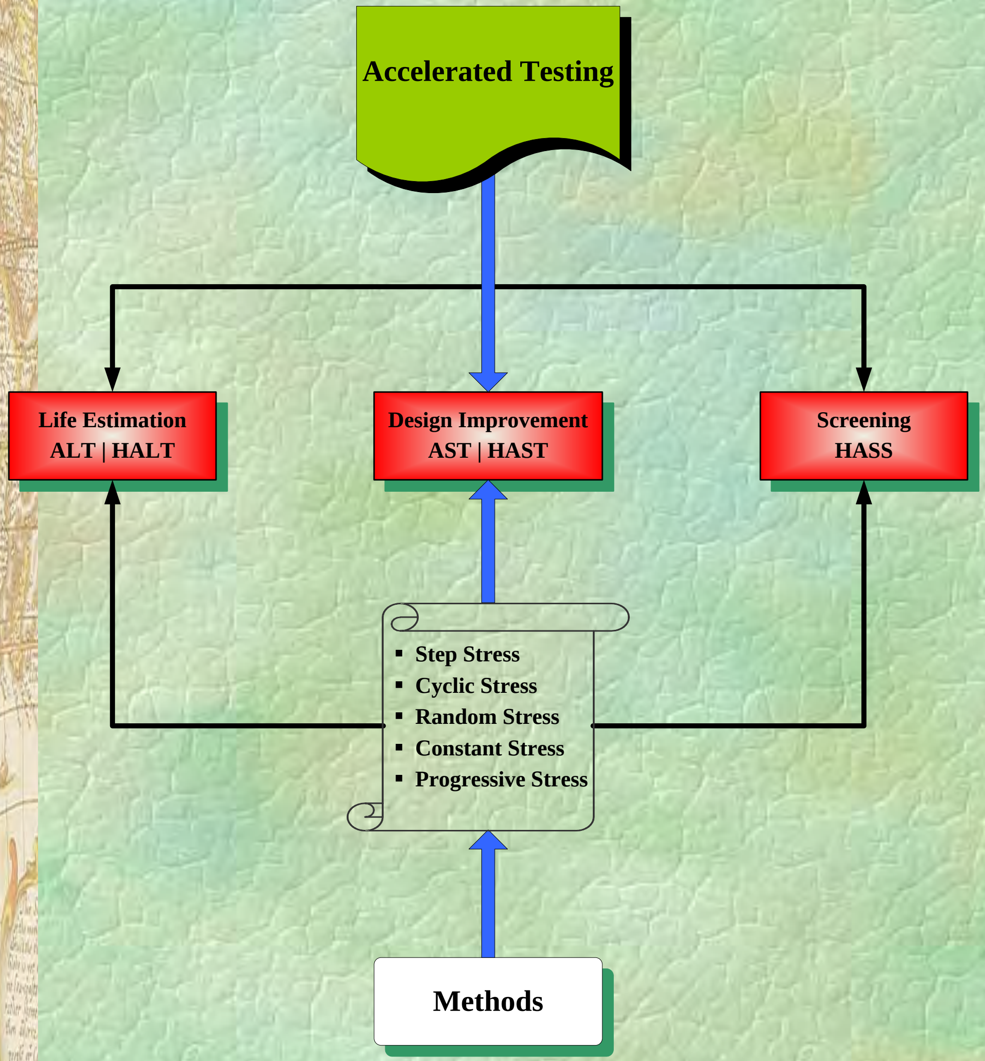
APPLICATION OF ACCELERATED LIFE TESTS

Scope And Purpose

- Accelerated testing allows designers to make predictions about the life of a product:
  - By developing a model that correlates reliability under accelerated conditions to reliability under normal conditions.
- The purpose of accelerated testing is to determine and verify product performance in an expedient manner:
  - By utilizing a variety of high environmental or operational stress levels, singularly or in combination, with the purpose of determining the expected life span of a part or product in a shortened test time
- Timing: Accelerated life test can be performed at any phase of product development cycle. Concept and planning phase is however the best time for application.
- Benefits: The major rational for performing accelerated life testing is to reduce product test time, resulting in schedule and cost benefits.

APPLICATION OF ACCELERATED LIFE TESTING

Figure 1: Accelerated Testing



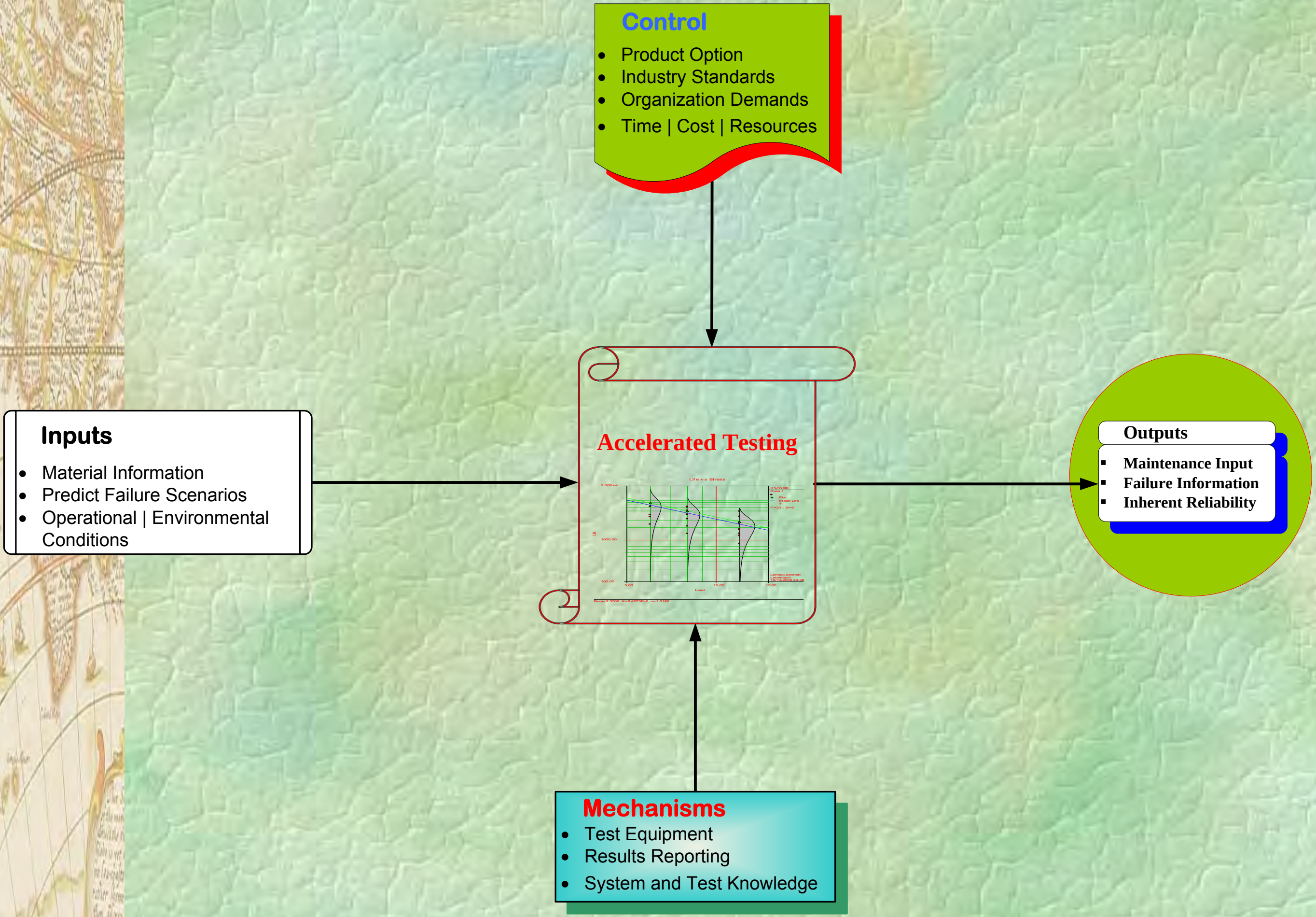
WHY IMPLEMENT ACCELERATED LIFE TESTING

Table 2: Summary of Reasons for and Applications for ALT

Item No.	Reasons for ALT	Application of ALT
1	Improve yields	Detecting failure modes
2	Reduce field return	Assessing component reliability
3	Better quality product	Evaluating the effects of stress on life
4	Identify process failure	Demonstrating component reliability
5	Reduce field service costs	To determine the product design capability
6	Reduce DOA | Early life failures	Comparing two or more competing products
7	Sales advantages | Customer satisfaction	To predict reliability and reduce the liability related to field failure

GENERAL CONCEPT OF ACCELERATED TESTING

Table 3: Concepts of Accelerated Life Testing



Control
- Product Option
- Industry Standards
- Organization Demands
- Time | Cost | Resources

Inputs
- Material Information
- Predict Failure Scenarios
- Operational | Environmental Conditions

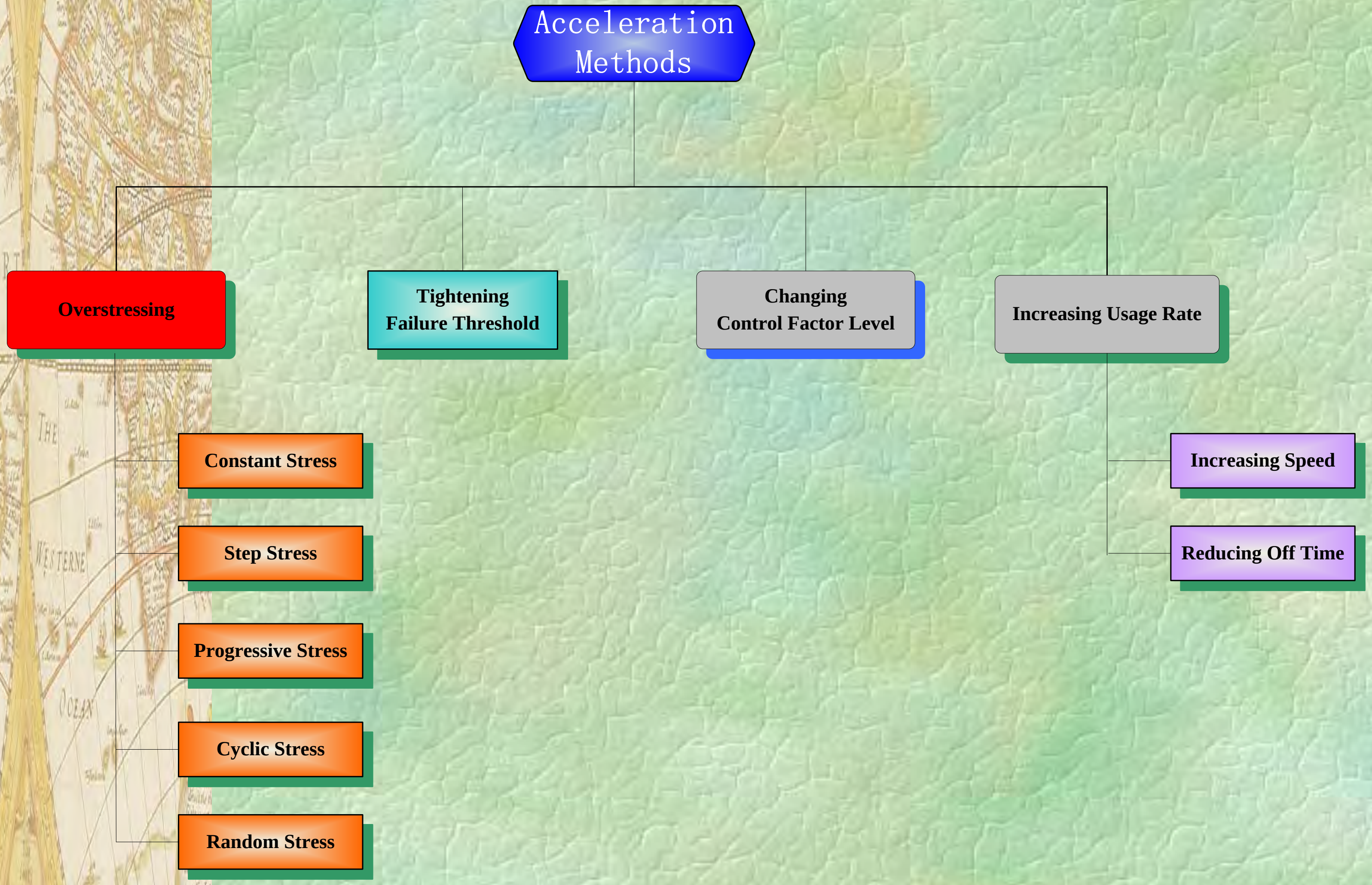
Accelerated Testing

Outputs
- Maintenance Input
- Failure Information
- Inherent Reliability

Mechanisms
- Test Equipment
- Results Reporting
- System and Test Knowledge

METHODS OF APPLYING ACCELERATED STRESS

Figure 5: Classification of Acceleration Methods



Overview of ALT Test Plans

- 3 Level 4:2:1 Allocation Plan

Recommends three stress levels using the same approach described above for the 3 Level Best Traditional Plan. The proportion of test units tested at the high, mid and low stress levels will be calculated to be as close as 4:2:1 as possible as illustrated in table 14.

Let's say for example you specified that 300 units are available in the Total Number for a power element, then this plan will recommend testing 171 units at the high level, 86 at the mid level and 43 at the low level.

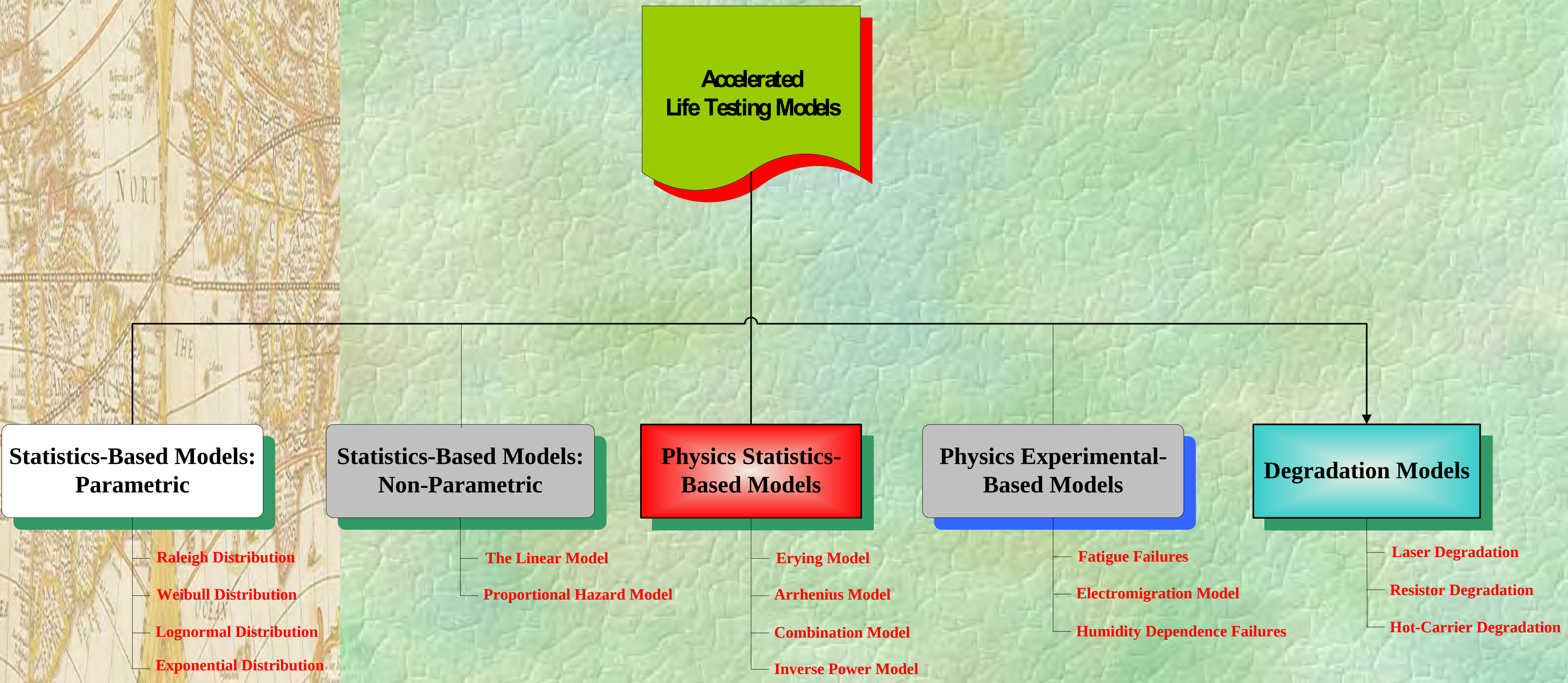
Table 14: Statistically Optimum Test Plan – Weibull Distribution

Temp °C	Proportion of Test Unit Allocated	Number of Test Units Allocated	Probability of Failure	Expected Number of Test Units Failing
50	0.000	-	0.001	-
78	0.456	171	0.03	5
98	0.728	86	0.24	21
120	1.000	43	0.90	39

Reference 1 provides additional details of how the stress levels are determined and other parameters shown in table

MODELS APPLIED IN ACCELERATED LIFE TESTING

Figure 11: Models for Accelerated Life Testing



Accelerated Life Testing Models

Statistics-Based Models: Parametric
- Raleigh Distribution
- Weibull Distribution
- Lognormal Distribution
- Exponential Distribution

Statistics-Based Models: Non-Parametric
- The Linear Model
- Proportional Hazard Model

Physics Statistics-Based Models
- Erying Model
- Arrhenius Model
- Combination Model
- Inverse Power Model

Physics Experimental-Based Models
- Fatigue Failures
- Electromigration Model
- Humidity Dependence Failures

Degradation Models
- Laser Degradation
- Resistor Degradation
- Hot-Carrier Degradation

STATISTICS BASED MODEL APPLICATION OF ALT

Numerical Example – Inverse Power Relationship:

LebenTech Design Assurance engineer design three tests, each with eight units to evaluate the reliability of a type of surface mount electrolytic capacitor. The tests were conducted at elevated voltage levels of 80, 100, and 120V, respectively.

All units were run to failure, where a failure is said to have occurred when the capacitance drifts more than 25%.

- The failure times in hours are illustrated in table 12. Estimate the mean life at rated voltage of 50V. If a capacitor ran for 1500 hours without a failure at 120V, calculate the equivalent time the capacity would have survived at the rated voltage.
- The Inverse Power relationship can be written as: $L = \dfrac{A}{V^b}$

Where L is the nominal Life, V the voltage stress, and A and B are constants dependent on material properties, product design, failure criteria and other factors.

STATISTICS BASED MODEL APPLICATION OF ALT

Table 12: Life Data at Elevated Voltage

	Voltage [V]		
	80	100	120
Life [Hr]	1770	1090	630
	2448	1907	848
	3230	2147	1121
	3445	2645	1307
	3538	2903	1321
	5809	3357	1357
	6590	4135	1984
	6744	4381	2331
Mean Life [Hr]	4197	2821	1362

STATISTICS BASED MODEL APPLICATION OF ALT

Solution

For the convenience of data analysis, we transform the above equation into a linear relationship as: $\mathrm{In}(L) = a + b\ \mathrm{In}(V)$

Where a = In(A) and b = -B. Both a and b are estimated from test data. The accelerated factor between the two stress level is:

$$A_f = \left(\frac{V'}{V}\right)^B$$

- The mean life at an elevated voltage is the average of the lifetimes at that voltage. The resulting mean lives are illustrated in tables 12 and 13.
- Then we use the equation above to fit the mean life data at each voltage level. Simple linear regression analysis shown in figure 19 gives:

  $\hat{a} = 20.07$ and $\hat{b} = -2.683$
- The regression line and raw data are plotted in figure 19. The estimates of A and B are: $\hat{A} = \exp(20.07) = 5.203 \times 10^8$ and $\hat{B} = 2.683$

STATISTICS BASED MODEL APPLICATION OF ALT

Solution Continues

The mean life at 50V is: $\hat{L}_{50} = \left(\dfrac{5.203 \times 10^{8}}{50^{2.683}} \right) = 14.39 \text{ Hours}$

The acceleration factor between 50 and 120V:

$$\hat{A}_f = \left(\frac{V'}{V} \right)^{B} = \left(\frac{120}{50} \right)^{2.683} = 10.47$$

- Then 1500 hours at 120V is equivalent to 1500 x 10.47 = 15,705 hours at 50V.
- That is if a capacitor ran for 1500 hours at 120V without failure, it would have survived 15,705 hours at 50V.

STATISTICS BASED MODEL APPLICATION OF ALT

Table 13: Log Life Data at Elevated Voltage

	Voltage [In V]		
	In [80] = 4.8	In [100] = 4.6	In [120] = 4.8
Log Life [Hr]	7.5	7.0	6.4
	7.8	7.6	6.7
	8.1	7.7	7.0
	8.1	7.9	7.2
	8.2	8.0	7.2
	8.7	8.1	7.2
	8.8	8.3	7.6
	8.8	8.4	7.8
Mean Log Life [Hr]	8.3	7.9	7.2

Log Life: In [1770] = 7.478

STATISTICS BASED MODEL APPLICATION OF ALT

Solution Continues

Regression Analysis: In Life Cap versus In Volt

The regression equation is: In Life Cap = 20.07 - 2.683 In Volt

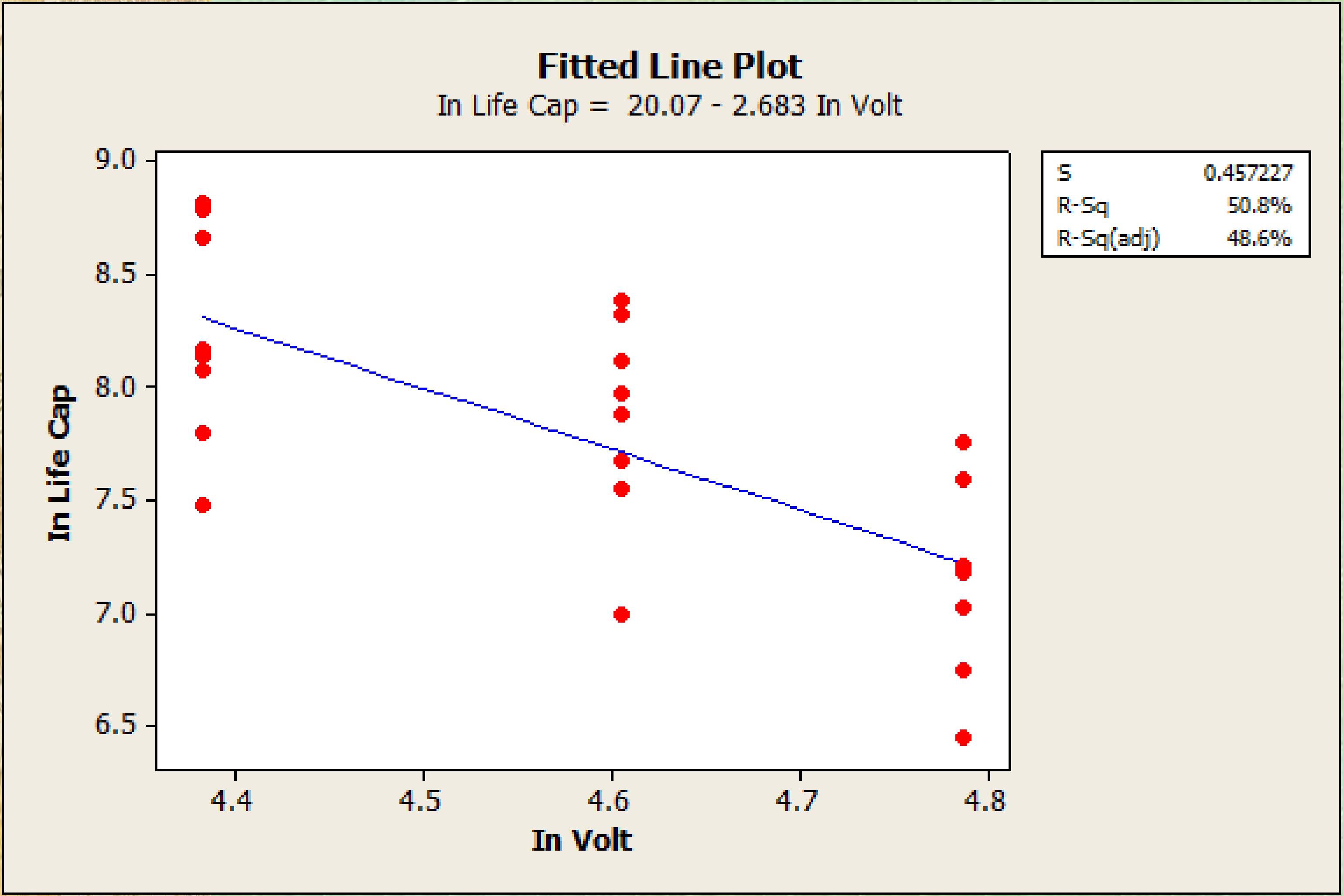
S = 0.457227   R-Sq = 50.8%   R-Sq(adj) = 48.6%

Analysis of Variance

Source	DF	SS	MS	F	P
Regression	1	4.74878	4.74878	22.72	0.000
Error	22	4.59925	0.20906		
Total	23	9.34803			

STATISTICS BASED MODEL APPLICATION OF ALT

Figure 19: Regression line Fitted to Mean Life of Capacitor



STATISTICS BASED MODEL APPLICATION OF ALT

Figure 20: Probability Plot for Failure at Different Voltage Levels

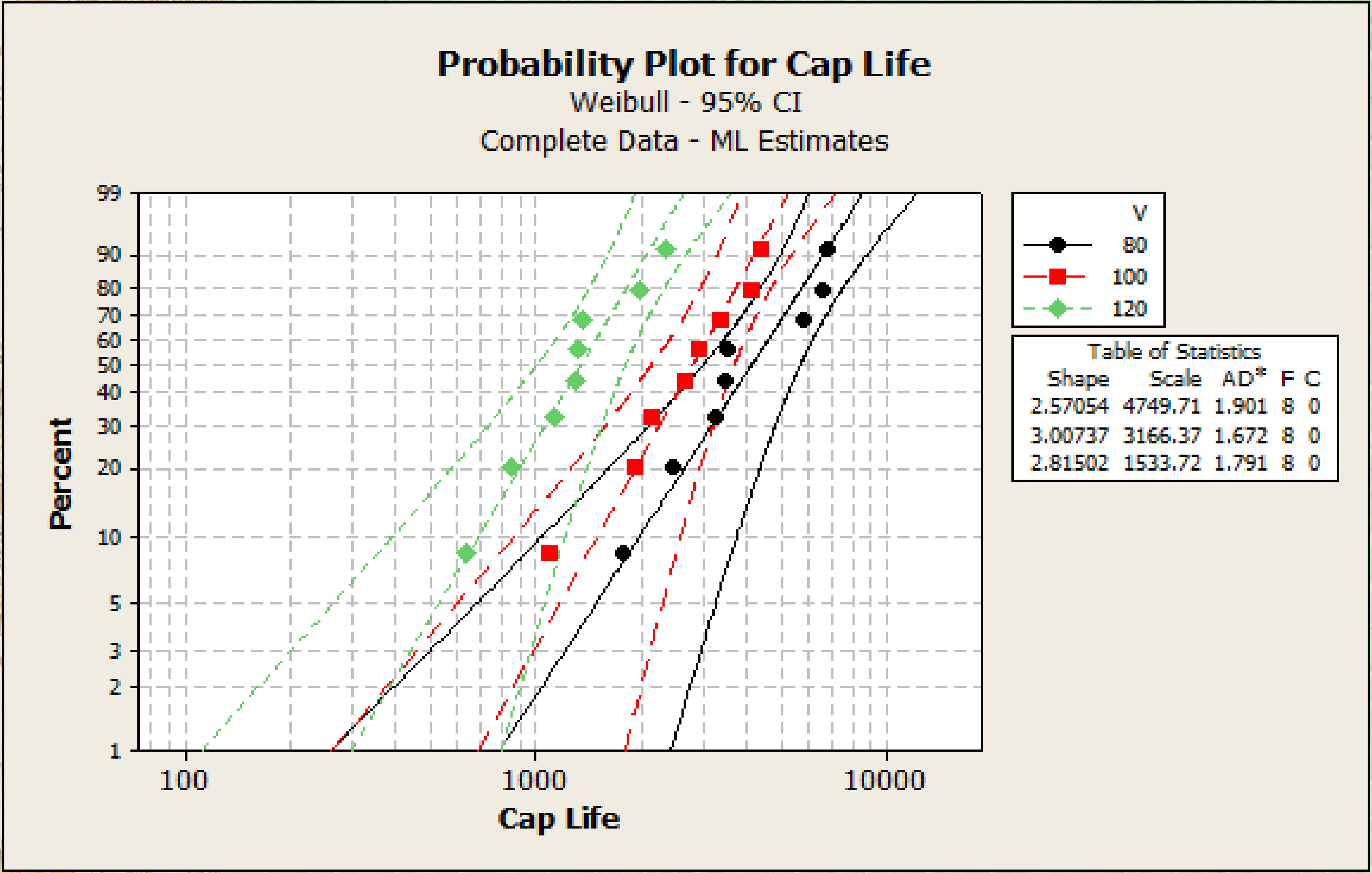
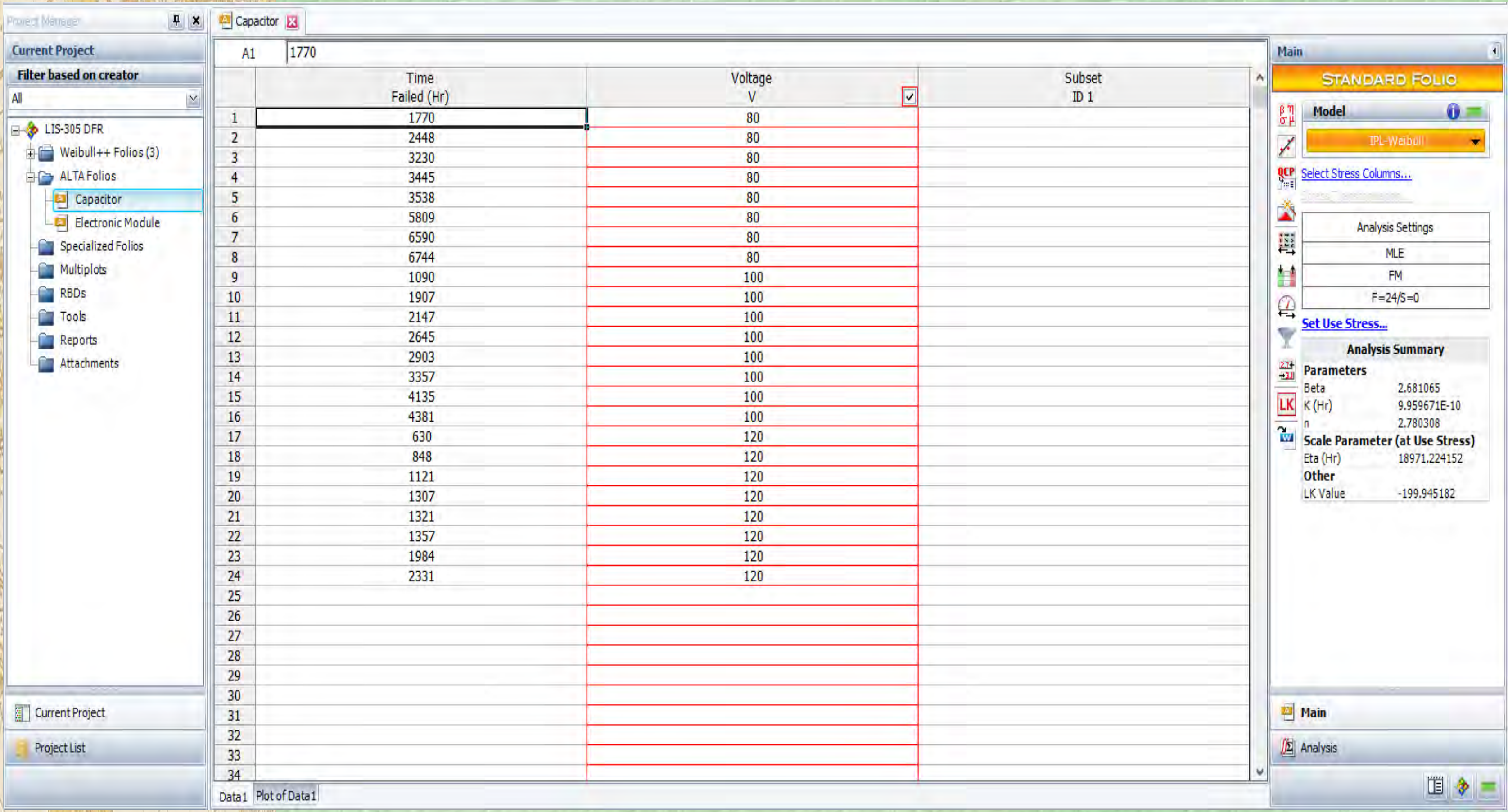


Table of Statistics

Shape	Scale	AD*	F	C
2.57054	4749.71	1.901	8	0
3.00737	3166.37	1.672	8	0
2.81502	1533.72	1.791	8	0

GRAPHICAL REPRESENTATION

Figure 21: Data Setup for ALT Data Analysis at Various Voltage



A1 1770

	Time Failed (Hr)	Voltage V ☑	Subset ID 1
1	1770	80	
2	2448	80	
3	3230	80	
4	3445	80	
5	3538	80	
6	5809	80	
7	6590	80	
8	6744	80	
9	1090	100	
10	1907	100	
11	2147	100	
12	2645	100	
13	2903	100	
14	3357	100	
15	4135	100	
16	4381	100	
17	630	120	
18	848	120	
19	1121	120	
20	1307	120	
21	1321	120	
22	1357	120	
23	1984	120	
24	2331	120	
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			

Model: IPL-Weibull

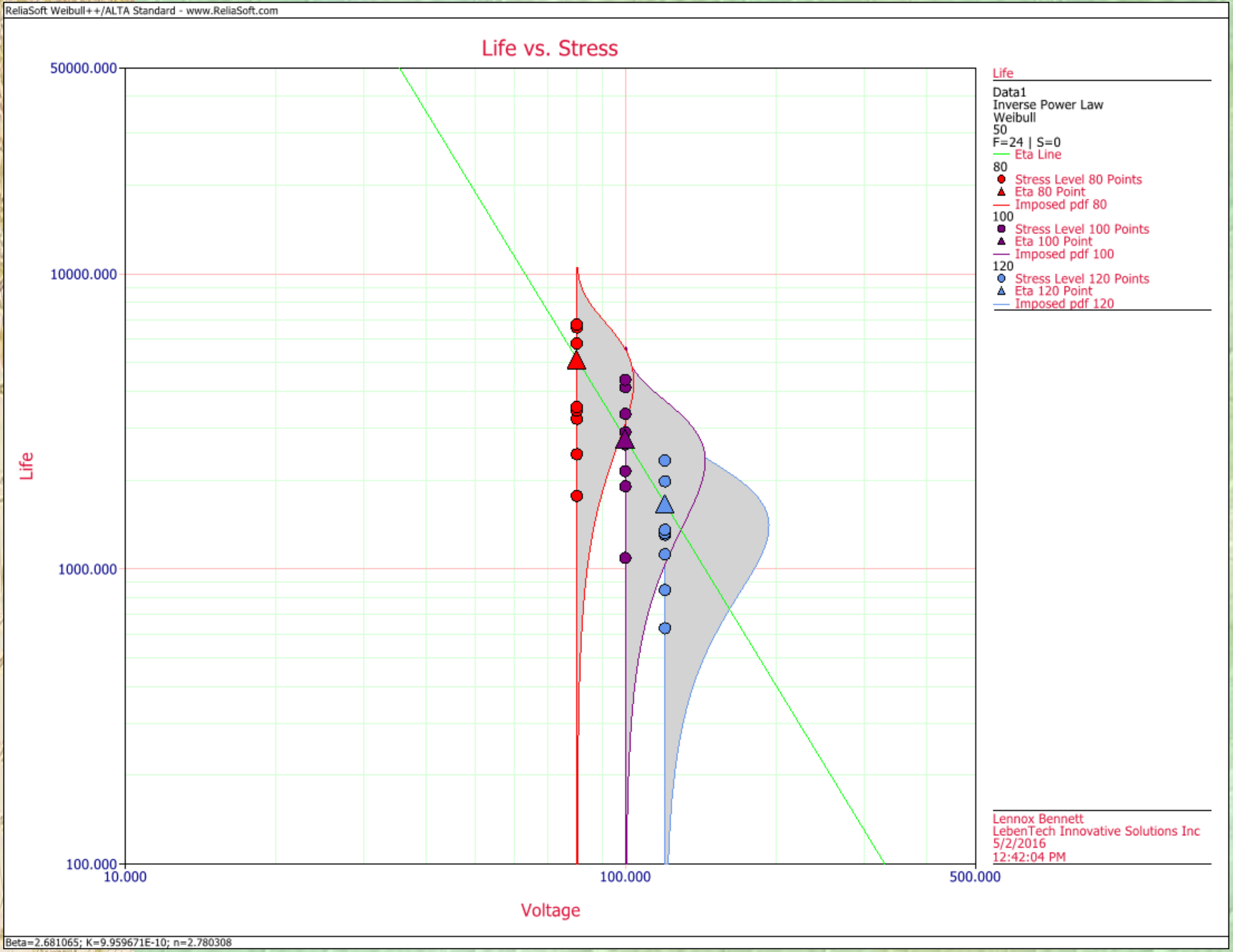
Analysis Settings
MLE
FM
F=24/S=0

Analysis Summary	
Parameters	
Beta	2.681065
K (Hr)	9.959671E-10
n	2.780308
Scale Parameter (at Use Stress)	
Eta (Hr)	18971.224152
Other	
LK Value	-199.945182

Numerical Example – Voltage | Graphical Solution

GRAPHICAL REPRESENTATION

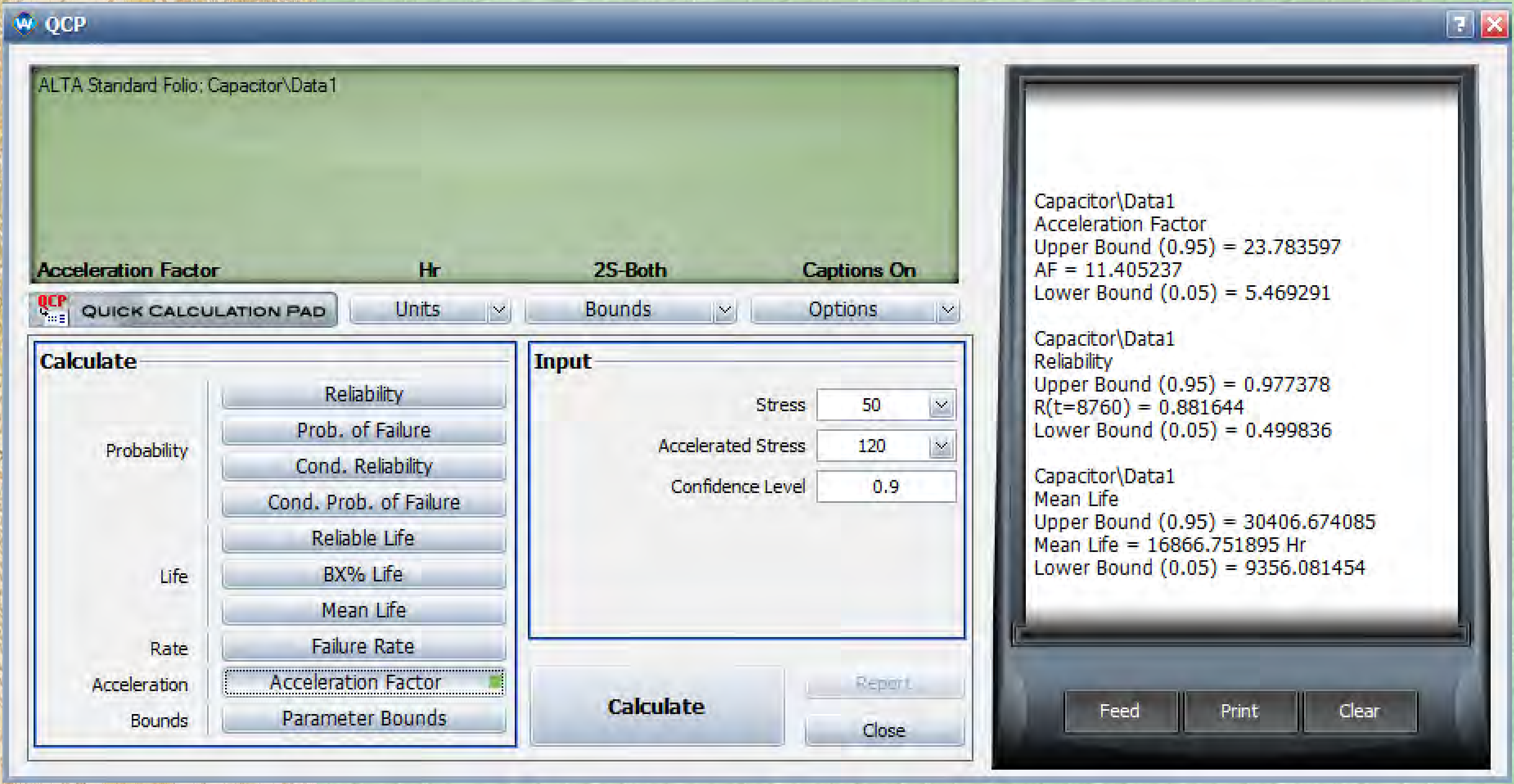
Figure 22: Life Stress Relationship at Various Voltage Levels


ReliaSoft Weibull++/ALTA Standard - www.ReliaSoft.com

Beta=2.681065; K=9.959671E-10; n=2.780308

GRAPHICAL REPRESENTATION

Figure 23: Utilizing Reliasoft QCP to Determine Model Parameters



ALTA Standard Folio: Capacitor\Data1

Acceleration Factor   Hr   2S-Both   Captions On

Stress: 50

Accelerated Stress: 120

Confidence Level: 0.9

```
Capacitor\Data1
Acceleration Factor
Upper Bound (0.95) = 23.783597
AF = 11.405237
Lower Bound (0.05) = 5.469291

Capacitor\Data1
Reliability
Upper Bound (0.95) = 0.977378
R(t=8760) = 0.881644
Lower Bound (0.05) = 0.499836

Capacitor\Data1
Mean Life
Upper Bound (0.95) = 30406.674085
Mean Life = 16866.751895 Hr
Lower Bound (0.05) = 9356.081454
```

M6 - LEARNING OBJECTIVES

Participant Shall be able to:

- Utilize results of risk analysis to prioritize design improvements.
- Identify and distinguish between the elements of risk analysis.
- Develop risk analysis process flow for their company's products.
- Gain understanding of how to select the appropriate risk assessment tool for design evaluation.
- Utilize principles of risk assessment to estimate the value of risk.
- Gain understanding of how to recognize and determine critical path of Product Liability Analysis.
- Identify elements of liability claims.
- Recognize if the failure of their company product could potentially cause a chain of events with safety | liability implications.
- Identify circumstances when product design compromise reliability of the component.

Adapt | Implement | Improve

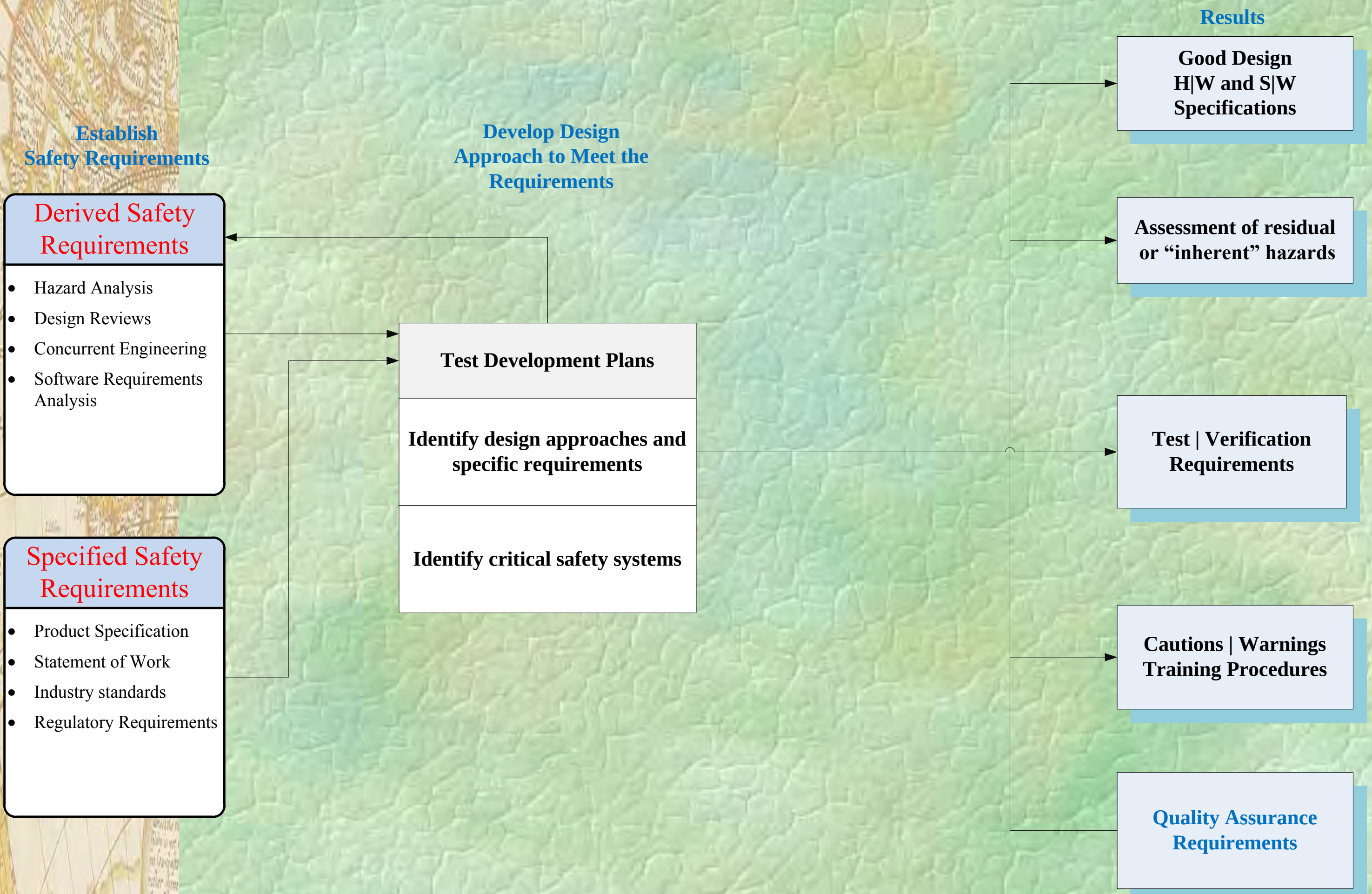
NEED FOR ENGINEERING RISK AND SAFETY ANALYSIS

Demand for Risk Analysis

- The need for risk and safety analysis is driven by: excessive warranty cost, product unreliability, and product recall leading to liability damage.
- Product required to satisfy certification, or FDA Regulatory Requirements.
- Product required to meet specific standards [MIL-STD-882C, ISO 14971, AAMI HE75: 2009] or Safety Integrity Level (SIL) requirements.
- Uncertainty and risk target requirement of safety critical systems.
- Engineering assessment required to quantify the product acceptable risk criterion.
- Product specification requirement and contract obligation.
- Quantification of product residual risk and confirmation of acceptable level of probability of failure.

PRODUCT SAFETY ENGINEERING ASSESSMENT

Figure 6-1: System Safety Approach



Establish Safety Requirements

Derived Safety Requirements

- Hazard Analysis
- Design Reviews
- Concurrent Engineering
- Software Requirements Analysis

Specified Safety Requirements

- Product Specification
- Statement of Work
- Industry standards
- Regulatory Requirements

Develop Design Approach to Meet the Requirements

Test Development Plans

Identify design approaches and specific requirements

Identify critical safety systems

Results

Good Design H|W and S|W Specifications

Assessment of residual or "inherent" hazards

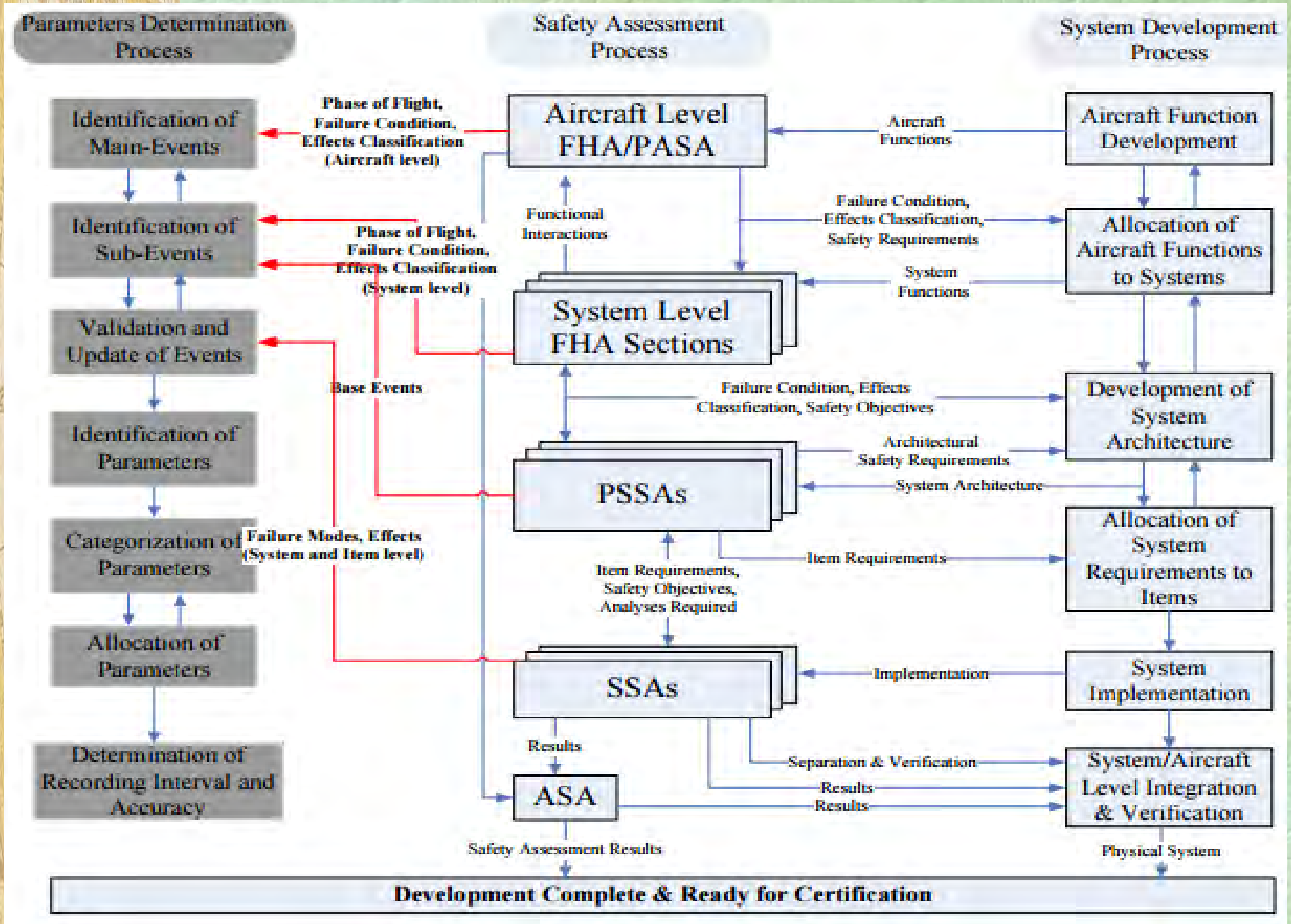
Test | Verification Requirements

Cautions | Warnings Training Procedures

Quality Assurance Requirements

SAFETY ENGINEERING ASSESSMENT - AVIATION

Figure 6-3: The Process for Determination of Airborne Recorded Parameters



Parameters Determination Process

Safety Assessment Process

System Development Process

Identification of Main-Events

Identification of Sub-Events

Validation and Update of Events

Identification of Parameters

Categorization of Parameters

Allocation of Parameters

Determination of Recording Interval and Accuracy

Phase of Flight, Failure Condition, Effects Classification (Aircraft level)

Phase of Flight, Failure Condition, Effects Classification (System level)

Base Events

Failure Modes, Effects (System and Item level)

Aircraft Level FHA/PASA

Functional Interactions

System Level FHA Sections

PSSAs

Item Requirements, Safety Objectives, Analyses Required

SSAs

Results

ASA

Safety Assessment Results

Aircraft Functions

Failure Condition, Effects Classification, Safety Requirements

System Functions

Failure Condition, Effects Classification, Safety Objectives

Architectural Safety Requirements

System Architecture

Item Requirements

Implementation

Separation & Verification

Results

Results

Aircraft Function Development

Allocation of Aircraft Functions to Systems

Development of System Architecture

Allocation of System Requirements to Items

System Implementation

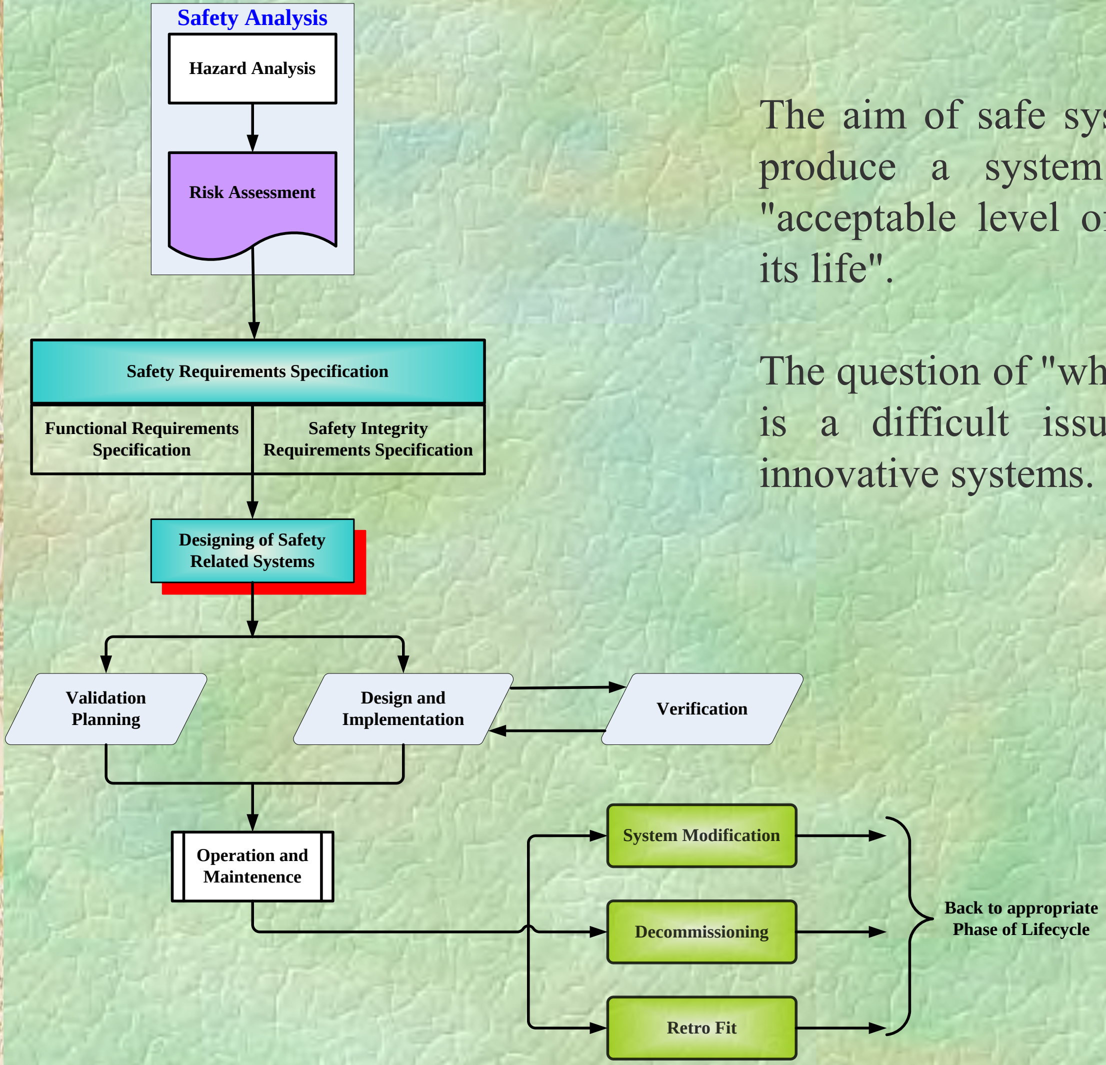
System/Aircraft Level Integration & Verification

Physical System

Development Complete & Ready for Certification

PRODUCT SAFETY ENGINEERING ASSESSMENT

Figure 6-5: The Safety Lifecycle Model for Critical System

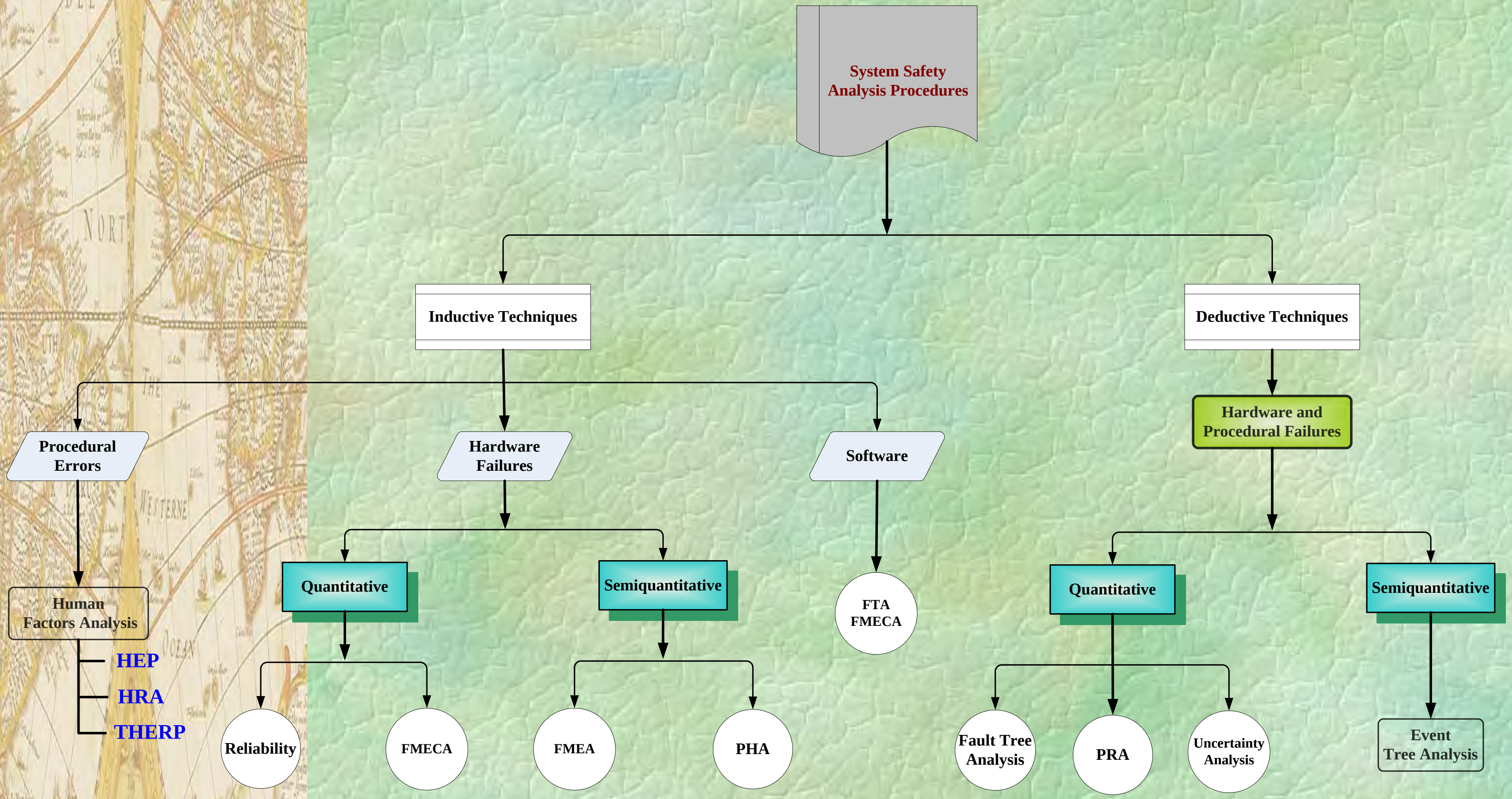

Safety Analysis
Hazard Analysis
Risk Assessment
Safety Requirements Specification
Functional Requirements Specification
Safety Integrity Requirements Specification
Designing of Safety Related Systems
Validation Planning
Design and Implementation
Verification
Operation and Maintenence
System Modification
Decommissioning
Retro Fit
Back to appropriate Phase of Lifecycle

The aim of safe system design is to produce a system which has an "acceptable level of risk throughout its life".

The question of "what is acceptable?" is a difficult issue for new and innovative systems.

PRODUCT SAFETY ENGINEERING ASSESSMENT

Figure 6-6: Types of System Safety Analysis



System Safety Analysis Procedures

Inductive Techniques

Deductive Techniques

Procedural Errors

Hardware Failures

Software

Hardware and Procedural Failures

Human Factors Analysis

HEP

HRA

THERP

Quantitative

Semiquantitative

FTA FMECA

Quantitative

Semiquantitative

Reliability

FMECA

FMEA

PHA

Fault Tree Analysis

PRA

Uncertainty Analysis

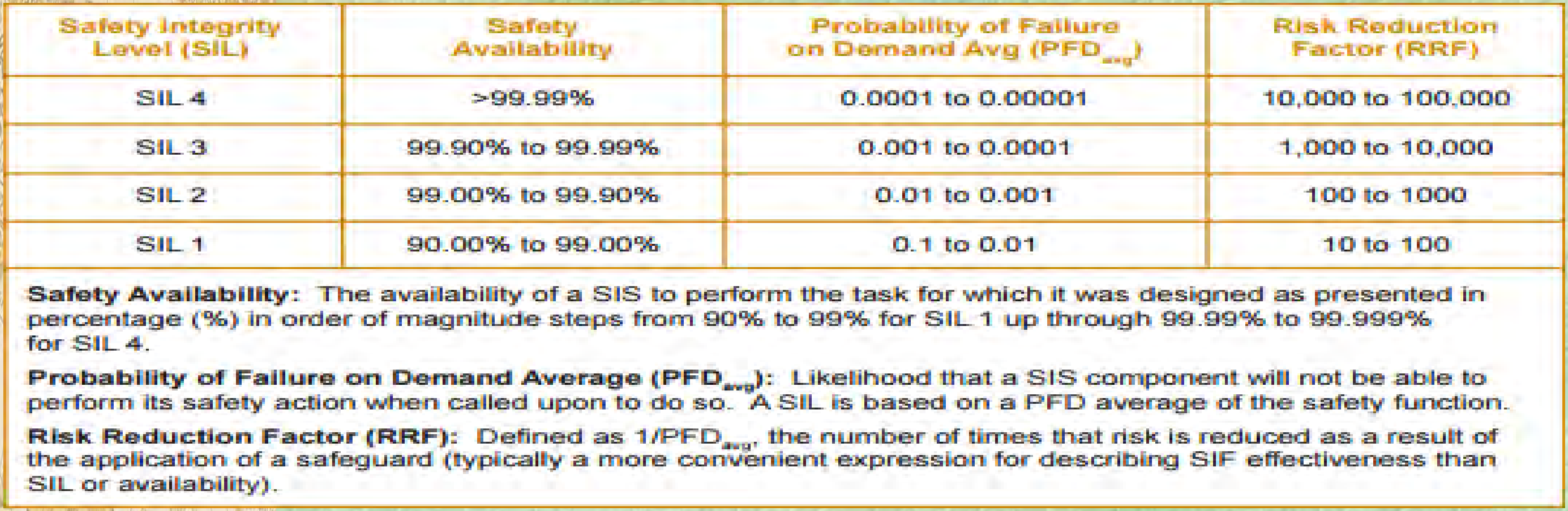
Event Tree Analysis

SAFE FAILURE FUNCTION

Analysis of Safety Risk

- Failure can happen in a safe or dangerous way.
- Detection mechanisms are software enabled in the context of complex systems (involving microcomputers).
- SFF is represented by: $SFF = 1 - \frac{\lambda_{du}}{\lambda_{Total}}, \; \lambda_{Total} = \lambda_{du} + \lambda_{dd} + \lambda_{su} + \lambda_{sd}$

Table 6-3: Safety Instruments Performance Requirements



Safety Integrity Level (SIL)	Safety Availability	Probability of Failure on Demand Avg (PFD_{avg})	Risk Reduction Factor (RRF)
SIL 4	>99.99%	0.0001 to 0.00001	10,000 to 100,000
SIL 3	99.90% to 99.99%	0.001 to 0.0001	1,000 to 10,000
SIL 2	99.00% to 99.90%	0.01 to 0.001	100 to 1000
SIL 1	90.00% to 99.00%	0.1 to 0.01	10 to 100

Safety Availability: The availability of a SIS to perform the task for which it was designed as presented in percentage (%) in order of magnitude steps from 90% to 99% for SIL 1 up through 99.99% to 99.999% for SIL 4.

Probability of Failure on Demand Average (PFD_{avg}): Likelihood that a SIS component will not be able to perform its safety action when called upon to do so. A SIL is based on a PFD average of the safety function.

Risk Reduction Factor (RRF): Defined as $1/PFD_{avg}$, the number of times that risk is reduced as a result of the application of a safeguard (typically a more convenient expression for describing SIF effectiveness than SIL or availability).

PRODUCT SAFETY ENGINEERING ASSESSMENT

Hazard Tracking Purpose and Objectives

Hazard tracking is recommended as a means to effectively managed hazard analysis data and facilitate a hazard discovery and hazard risk mitigation process. Objectives for performing analysis include:

- Provides a means to effectively influence product design and to ensure safety is optimized in new system.
- Provide data and information necessary to efficiently and effectively managed risk associated with safe operation of the device.
- Provides a means for documenting approaches, decisions and actions taken to eliminate or reduce risk of hazards.
- Provides a method for closed loop tracking of actions and/or decisions and ensure information is accessible and available when required.
- Provide means for effectively organizing, managing, and updating hazard data.

Figure 6-16 provides a graphical illustration of the proposed closed loop tracking process.

VERIFYING COMPLIANCE OF SAFETY REQUIREMENTS

Verification of Design for Safety

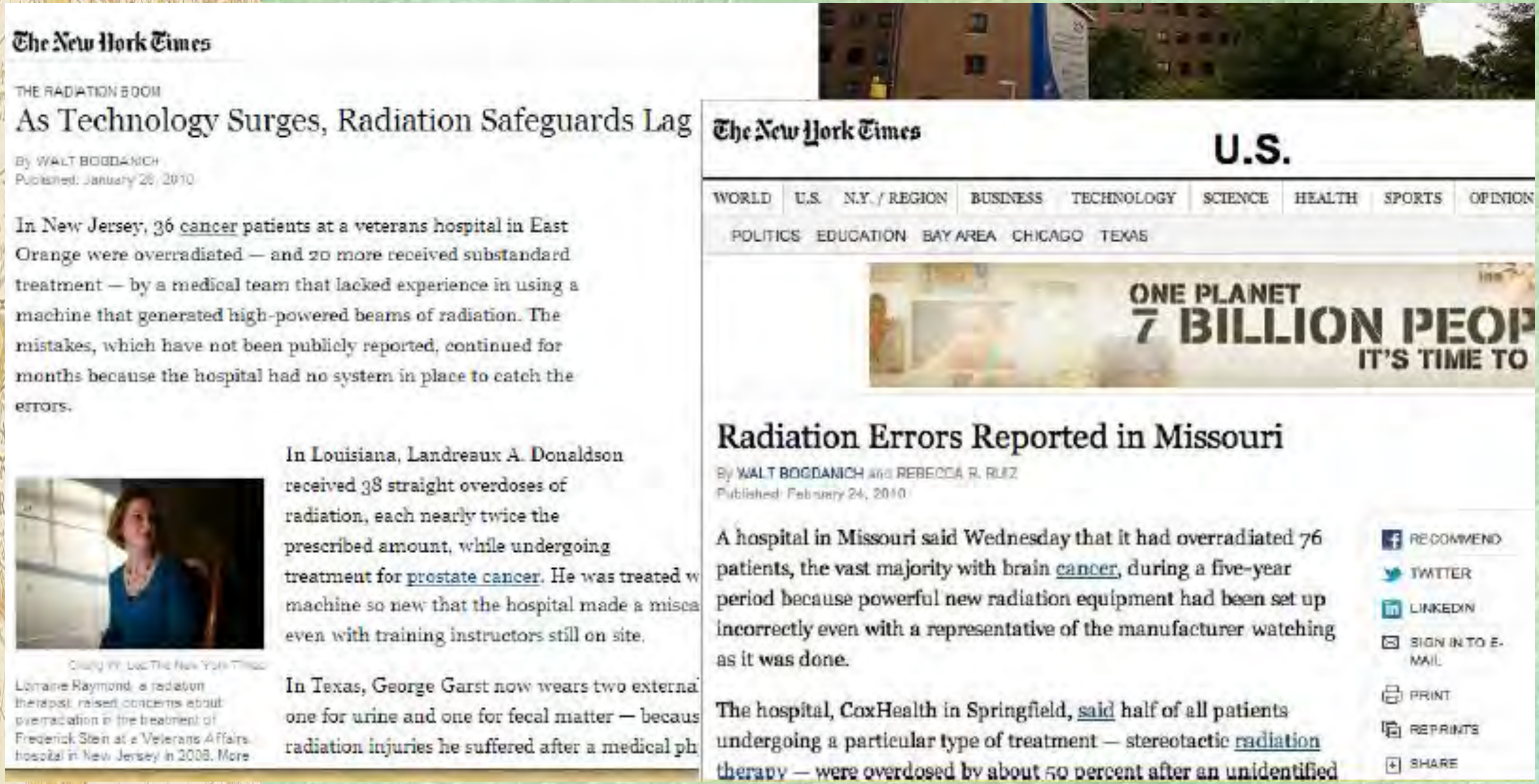
- Compliance with requirements or standards is defined as implementing and verifying that all process, activities [analysis] and task identified on product functional specification and specific standard or regulation.
- Compliance Testing: IEC 60601, MIL-STD-882E, and DO - 278B.
- Certification: Satisfactory fulfillment of requirements.
- Risk Assessment: Verify Product is design for minimum risk.
- Validation of safety of use [Effectiveness of risk control] – Human Factor
  1. Validating specific design modification.
  2. Validating overall device use safety.
- Verification of product reliability: Prove that safety control requirements are properly met.

Verification involve the ability to demonstrate that a product design complies with the objectives and outputs defined in the applicable safety standard.

– Proactive Innovative Solutions for Success and Competitive Advantages

MEDICAL DEVICE SAFETY ANALYSIS APPLICATION

Figure 6-19: Articles Relating to Inadequacies in Medical Device System



The New York Times

THE RADIATION BOOM

As Technology Surges, Radiation Safeguards Lag

By WALT BOGDANICH
Published: January 26, 2010

In New Jersey, 36 cancer patients at a veterans hospital in East Orange were overradiated — and 20 more received substandard treatment — by a medical team that lacked experience in using a machine that generated high-powered beams of radiation. The mistakes, which have not been publicly reported, continued for months because the hospital had no system in place to catch the errors.

Chang W. Lee/The New York Times

Lorraine Raymond, a radiation therapist, raised concerns about overradiation in the treatment of Frederick Stein at a Veterans Affairs hospital in New Jersey in 2008. More

In Louisiana, Landreaux A. Donaldson received 38 straight overdoses of radiation, each nearly twice the prescribed amount, while undergoing treatment for prostate cancer. He was treated w machine so new that the hospital made a misca even with training instructors still on site.

In Texas, George Garst now wears two externa one for urine and one for fecal matter — becaus radiation injuries he suffered after a medical ph

Radiation Errors Reported in Missouri

By WALT BOGDANICH and REBECCA R. RUIZ
Published: February 24, 2010

A hospital in Missouri said Wednesday that it had overradiated 76 patients, the vast majority with brain cancer, during a five-year period because powerful new radiation equipment had been set up incorrectly even with a representative of the manufacturer watching as it was done.

The hospital, CoxHealth in Springfield, said half of all patients undergoing a particular type of treatment — stereotactic radiation therapy — were overdosed by about 50 percent after an unidentified

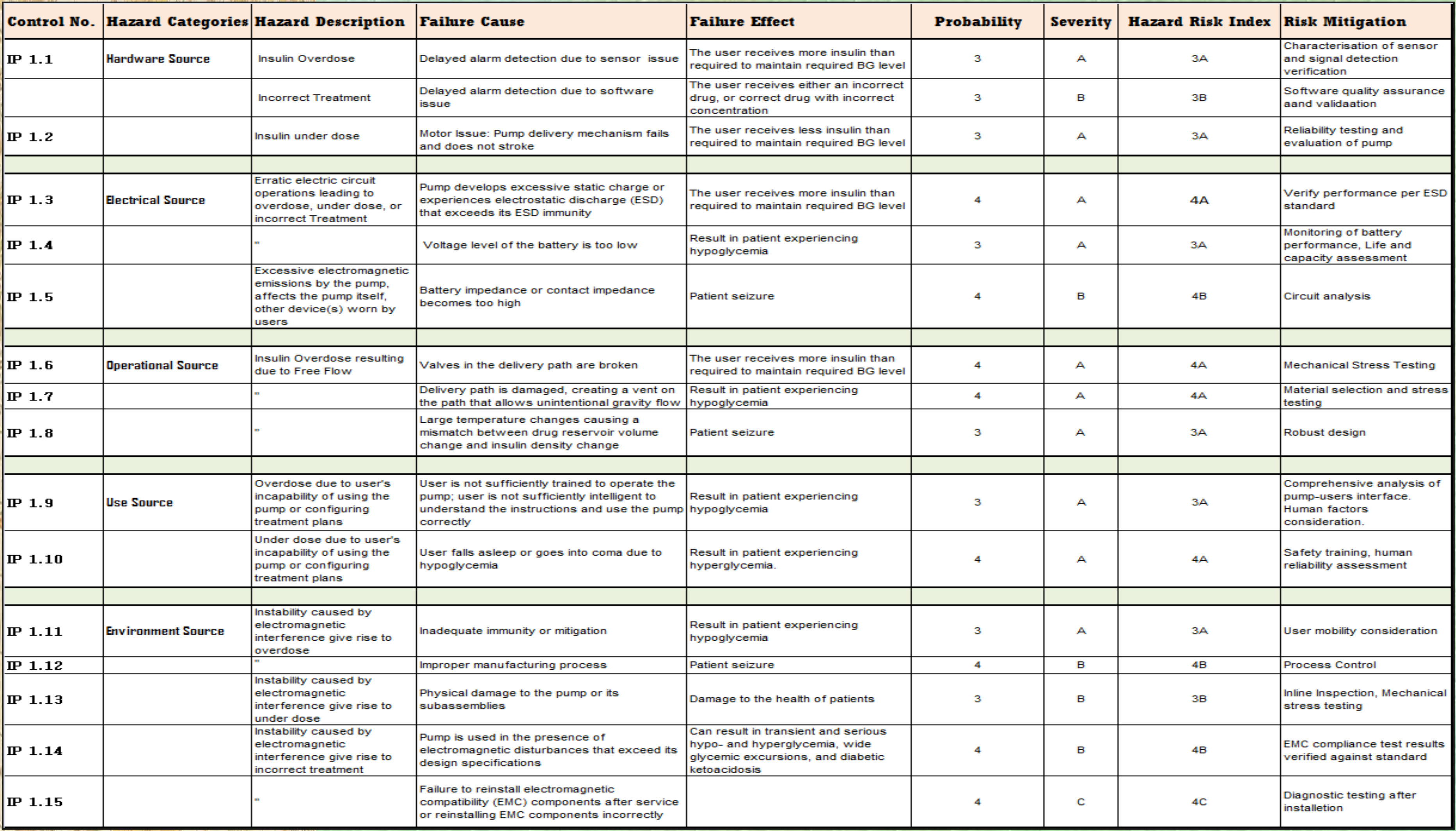
MEDICAL DEVICE SAFETY ANALYSIS APPLICATION

Table 6-4: Application of FMEA to the Proton Beam Radiotherapy System

System Function Specification	Potential Failure Mode | Error	Potential Causes of Failure | Error	SEV	Potential Effects of Failure | Error	OCC	Current Design Control / Mitigation		DET	RPN	Risk Reduction	Controlled Index
						Method of Prevention	Detection Means				
Definition of dose calculation parameters	Improper selection of physical beam model and/or calculation grid	Human Error due to time pressure or inadequate skill	7	Wrong dose distribution	4	Training and instruction manual		5	140	2	14
Target selection of dose presription for each target	Wrong setting of dose prescription type	Human Error	8	Wrong delivery	3	Human Error Analysis	Human Reliability	4	96		
Couch origin of coordinates identification for absolute positioning	Wrong definition of couch origin of coordinates [small amounts in terms of 2 - 3 mm]	Human Error	5	Unintended normal tissue irradiated or CTV missing	4	Training plus operating instructions	FTA of Human Error	6	120	2	10
Deliver accurate dose of radiation to patient	Inadvertent radiation [laser]	Control System Failure	9	Unintended normal tissue irradation	8	Redundant processor	Alarm	2	144	3	27
				Serious adverse clinical outcome		Scatter correction capability					
Deliver radiation dose to within absolute 5% and 5 mm	IV Overdose	Error in dose calculated	7	Delivery accuracy compromise and patent get harm [injury]	4	PHA, FMECA, and FTA application	Perform verification and validation testing	7	196	3	21
		Calibration	7	Toxicity	2	PM schedue		2	28		
		Dose delivery	7		6	Statistical analysis of dose delivery	Acceptance testing	5	210	2	14

MEDICAL DEVICE SAFETY ANALYSIS APPLICATION

Table 6-5: Preliminary Hazard Analysis Generic Insulin Infusion Pump



Control No.	Hazard Categories	Hazard Description	Failure Cause	Failure Effect	Probability	Severity	Hazard Risk Index	Risk Mitigation
IP 1.1	Hardware Source	Insulin Overdose	Delayed alarm detection due to sensor issue	The user receives more insulin than required to maintain required BG level	3	A	3A	Characterisation of sensor and signal detection verification
		Incorrect Treatment	Delayed alarm detection due to software issue	The user receives either an incorrect drug, or correct drug with incorrect concentration	3	B	3B	Software quality assurance aand validaation
IP 1.2		Insulin under dose	Motor Issue: Pump delivery mechanism fails and does not stroke	The user receives less insulin than required to maintain required BG level	3	A	3A	Reliability testing and evaluation of pump
IP 1.3	Electrical Source	Erratic electric circuit operations leading to overdose, under dose, or incorrect Treatment	Pump develops excessive static charge or experiences electrostatic discharge (ESD) that exceeds its ESD immunity	The user receives more insulin than required to maintain required BG level	4	A	4A	Verify performance per ESD standard
IP 1.4		"	Voltage level of the battery is too low	Result in patient experiencing hypoglycemia	3	A	3A	Monitoring of battery performance, Life and capacity assessment
IP 1.5		Excessive electromagnetic emissions by the pump, affects the pump itself, other device(s) worn by users	Battery impedance or contact impedance becomes too high	Patient seizure	4	B	4B	Circuit analysis
IP 1.6	Operational Source	Insulin Overdose resulting due to Free Flow	Valves in the delivery path are broken	The user receives more insulin than required to maintain required BG level	4	A	4A	Mechanical Stress Testing
IP 1.7		"	Delivery path is damaged, creating a vent on the path that allows unintentional gravity flow	Result in patient experiencing hypoglycemia	4	A	4A	Material selection and stress testing
IP 1.8		"	Large temperature changes causing a mismatch between drug reservoir volume change and insulin density change	Patient seizure	3	A	3A	Robust design
IP 1.9	Use Source	Overdose due to user's incapability of using the pump or configuring treatment plans	User is not sufficiently trained to operate the pump; user is not sufficiently intelligent to understand the instructions and use the pump correctly	Result in patient experiencing hypoglycemia	3	A	3A	Comprehensive analysis of pump-users interface. Human factors consideration.
IP 1.10		Under dose due to user's incapability of using the pump or configuring treatment plans	User falls asleep or goes into coma due to hypoglycemia	Result in patient experiencing hyperglycemia.	4	A	4A	Safety training, human reliability assessment
IP 1.11	Environment Source	Instability caused by electromagnetic interference give rise to overdose	Inadequate immunity or mitigation	Result in patient experiencing hypoglycemia	3	A	3A	User mobility consideration
IP 1.12		"	Improper manufacturing process	Patient seizure	4	B	4B	Process Control
IP 1.13		Instability caused by electromagnetic interference give rise to under dose	Physical damage to the pump or its subassemblies	Damage to the health of patients	3	B	3B	Inline Inspection, Mechanical stress testing
IP 1.14		Instability caused by electromagnetic interference give rise to incorrect treatment	Pump is used in the presence of electromagnetic disturbances that exceed its design specifications	Can result in transient and serious hypo- and hyperglycemia, wide glycemic excursions, and diabetic ketoacidosis	4	B	4B	EMC compliance test results verified against standard
IP 1.15		"	Failure to reinstall electromagnetic compatibility (EMC) components after service or reinstalling EMC components incorrectly		4	C	4C	Diagnostic testing after installation

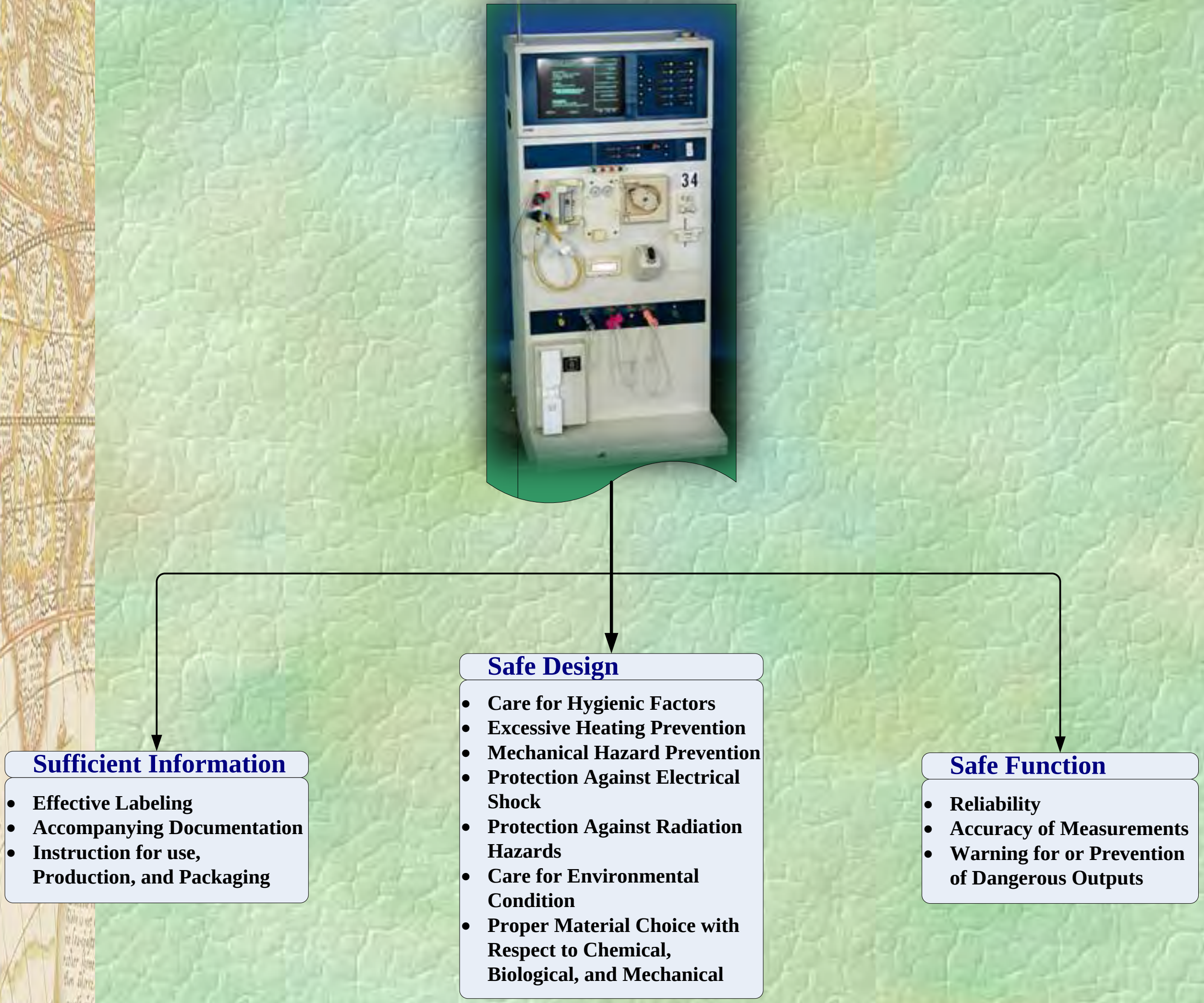
MEDICAL DEVICE SAFETY ANALYSIS APPLICATION

Table 6-6: Preliminary Hazard Analysis Risk Index Matrix

Semi Quantitative Probability Levels	Qualitative Severity Levels				
	E - Negligible	D - Minor	C - Serious	B - Critical	A - Catastrophic
1 - Frequent	1E	1D	1C	1B	1A
2 - Probable	2E	2D	2C	2B	2A
3 - Occasional	3E	3D	3C	3B	3A
4 - Remote	4E	4D	4C	3B	4A
5 - Improbable	5E	5D	5C	5B	5A

MEDICAL DEVICE RELATED SAFETY REQUIREMENTS

Figure 6-23: Categories of Medical Device Safety-Related Requirements



Sufficient Information

- Effective Labeling
- Accompanying Documentation
- Instruction for use, Production, and Packaging

Safe Design

- Care for Hygienic Factors
- Excessive Heating Prevention
- Mechanical Hazard Prevention
- Protection Against Electrical Shock
- Protection Against Radiation Hazards
- Care for Environmental Condition
- Proper Material Choice with Respect to Chemical, Biological, and Mechanical

Safe Function

- Reliability
- Accuracy of Measurements
- Warning for or Prevention of Dangerous Outputs

SOFTWARE SAFETY ANALYSIS

Basic Concepts

- Software must be considered in the context of system safety. Some of the essential concepts in safety analysis are:

  1. Risk: The possibility of undesired outcome.
  2. Safety: Freedom from risk.
  3. Mishap: Unintended events that results in a loss [Also called accidents].
  4. Hazard: State of system that could lead to a mishap.
  5. Software Hazard: A software condition that could lead to an unsafe condition in hardware.

- Qualitative Risk: In a qualitative assessment of risk, possible outcomes are ranked in terms of severity (e.g., *catastrophic, probable, critical, marginal, negligible*) and hazard level (e.g., *frequent, probable, occasional, remote improbable, impossible*).

SOFTWARE SAFETY ANALYSIS

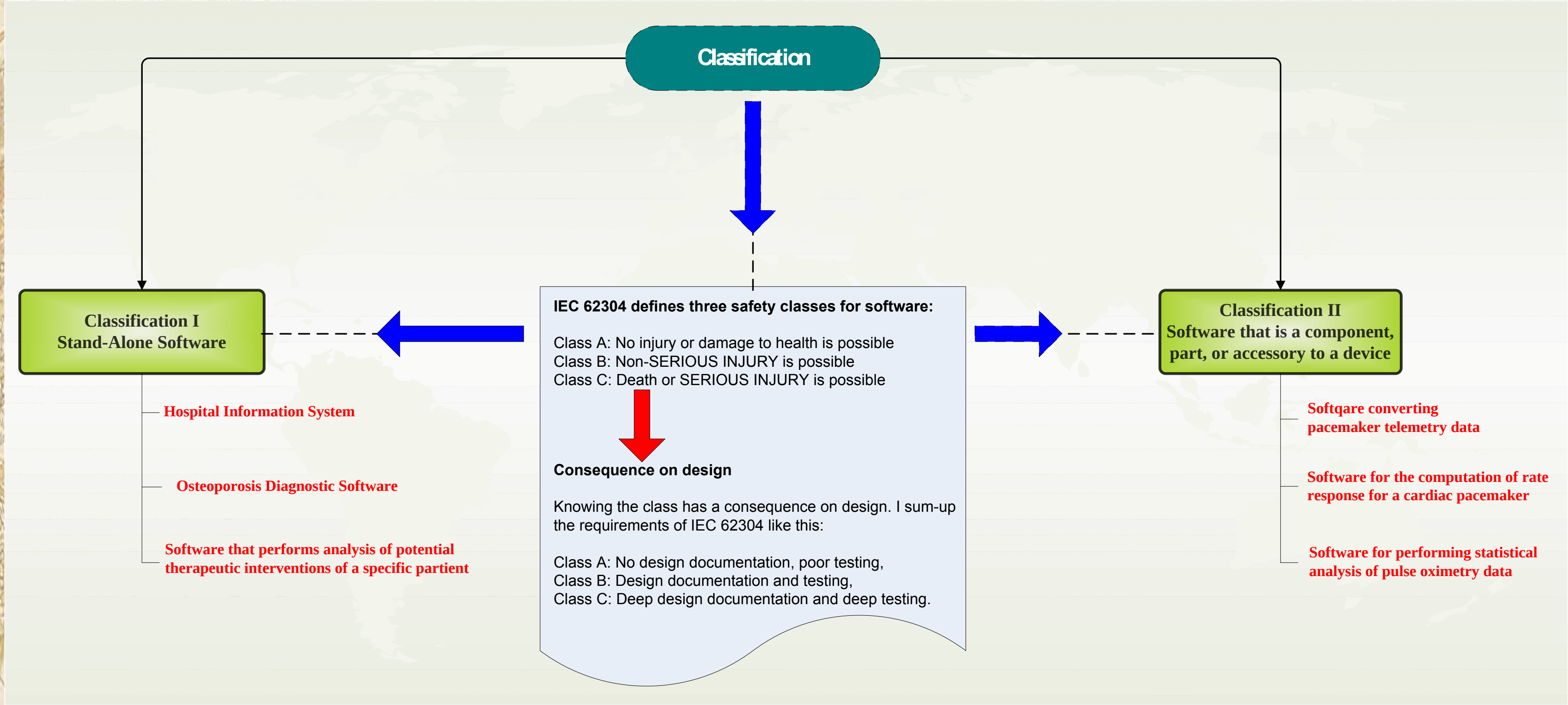
Table 6-7: Basic Causes of Software Safety Problems

Item	Cause	Description
1	▪ Specification Error	▪ The software specification defines what [and sometimes] the software is performed. If a software/hardware interface is not planned properly, unforeseen safety problems may occur.
2	▪ Design Error	▪ Errors such as incorrect algorithms, lack of self-tests or fault tolerance, and incorrect interfaces can result in safety problems.
3	▪ Coding Error	▪ Includes errors such as incorrect signs, endless loops, unused logic, syntax errors, etc., generally results in *reliability and quality* problems, rather than safety-related problems.
4	▪ Hardware-Induced Error	▪ Includes failure that results in the [undesired] transformation of a bit in a word, potentially changing the meaning of a software instruction.

Source: System Reliability Toolkit

SOFTWARE SAFETY APPLICATION

Figure 6-26: Classification of Medical Device Software



Classification

Classification I
Stand-Alone Software

- Hospital Information System
- Osteoporosis Diagnostic Software
- Software that performs analysis of potential therapeutic interventions of a specific partient

IEC 62304 defines three safety classes for software:

Class A: No injury or damage to health is possible
Class B: Non-SERIOUS INJURY is possible
Class C: Death or SERIOUS INJURY is possible

Consequence on design

Knowing the class has a consequence on design. I sum-up the requirements of IEC 62304 like this:

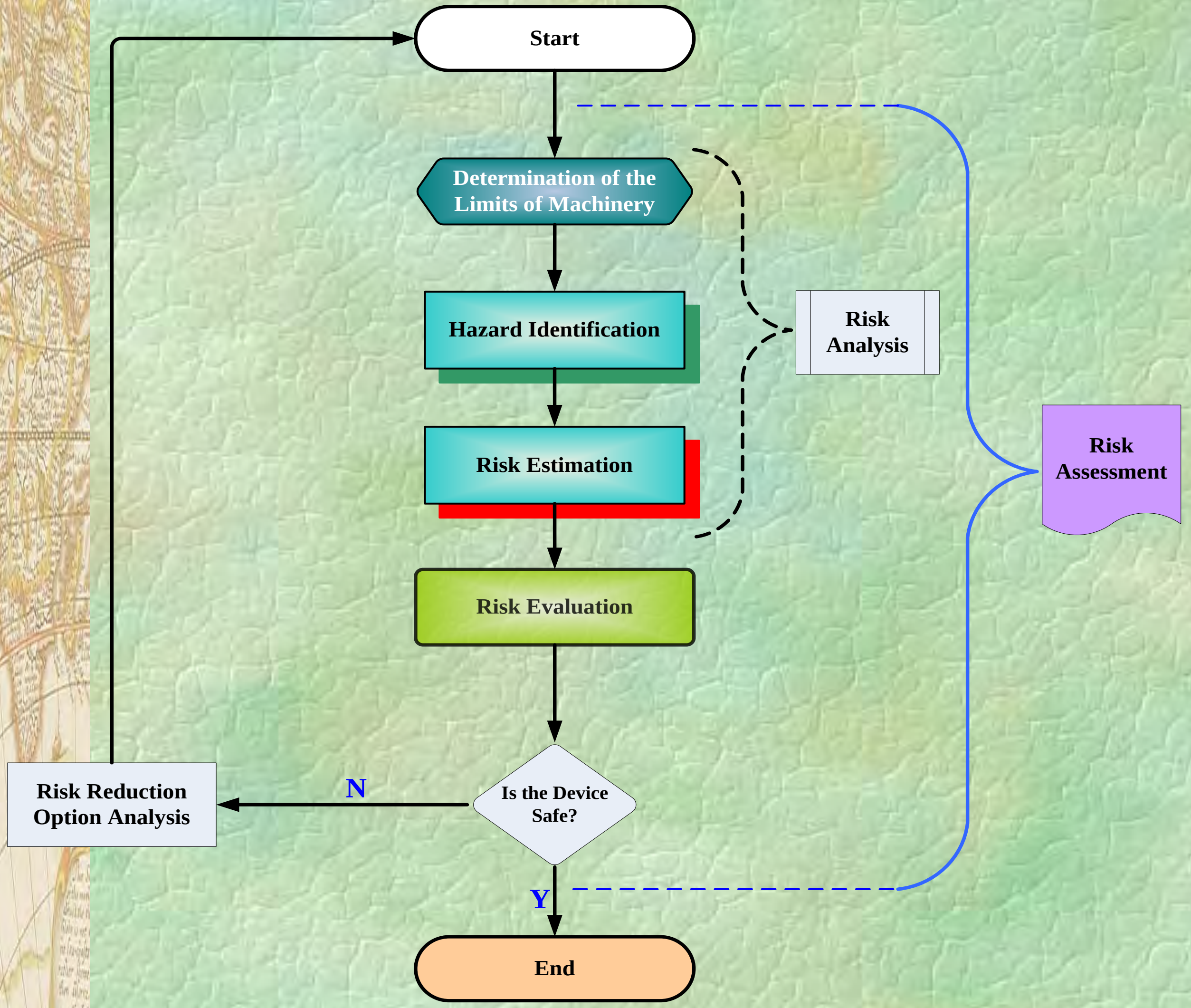
Class A: No design documentation, poor testing,
Class B: Design documentation and testing,
Class C: Deep design documentation and deep testing.

Classification II
Software that is a component, part, or accessory to a device

- Softqare converting pacemaker telemetry data
- Software for the computation of rate response for a cardiac pacemaker
- Software for performing statistical analysis of pulse oximetry data

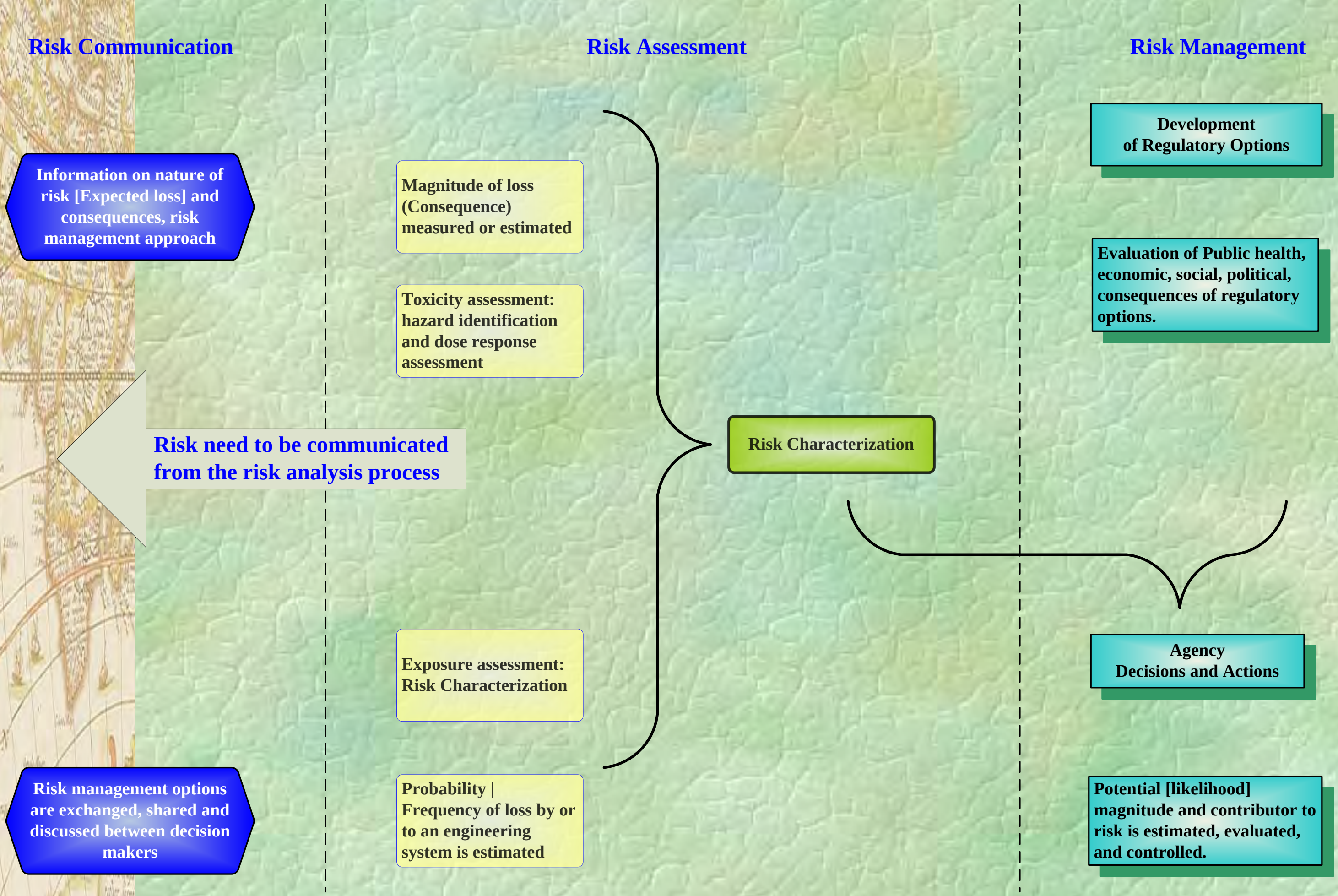
ENGINEERING RISK ASSESMENT OF PRODUCT DESIGN

Figure 6-28: Representation of the Risk Assessment Procedure – EN 1050



ELEMENT AND TYPES OF RISK ANALYSIS

Figure 6-29: Elements of Product Design Risk Analysis



Risk Communication

Risk Assessment

Risk Management

Information on nature of risk [Expected loss] and consequences, risk management approach

Risk need to be communicated from the risk analysis process

Risk management options are exchanged, shared and discussed between decision makers

Magnitude of loss (Consequence) measured or estimated

Toxicity assessment: hazard identification and dose response assessment

Exposure assessment: Risk Characterization

Probability | Frequency of loss by or to an engineering system is estimated

Risk Characterization

Development of Regulatory Options

Evaluation of Public health, economic, social, political, consequences of regulatory options.

Agency Decisions and Actions

Potential [likelihood] magnitude and contributor to risk is estimated, evaluated, and controlled.

– Proactive Innovative Solutions for Success and Competitive Advantages

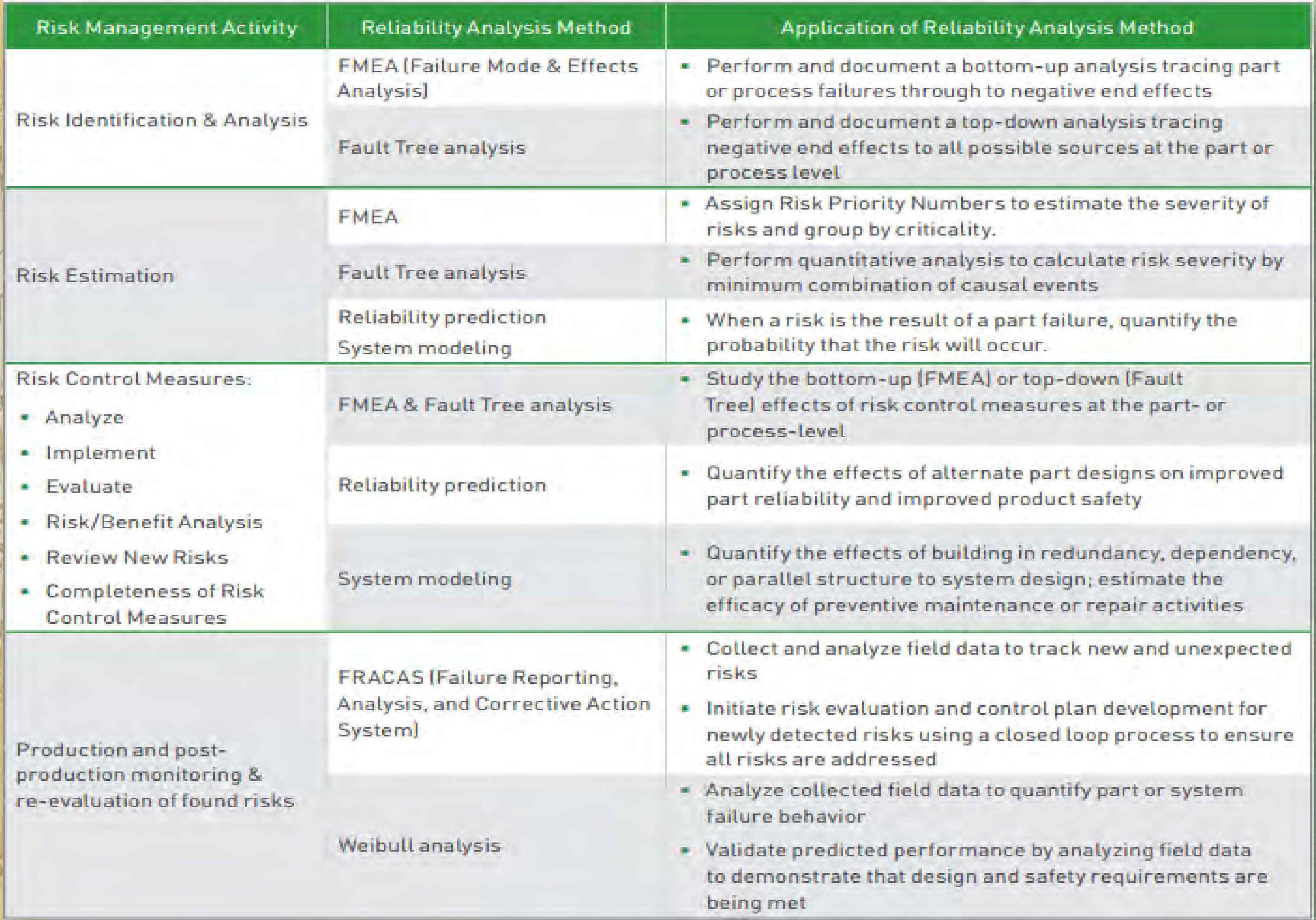
ELEMENT AND TYPES OF RISK ASSESSMENT

Table 6-10: Categories of Risk Analysis that Accounts for Potential Loss

Item	Risk Analysis Categories	Description of Application
1	❑ Health Risk Analysis	❑ Involves estimating potential diseases and losses of life affecting, humans, animals, and plants.
2	❑ Safety Risk Analysis	❑ Involve estimating potential harms caused by accidents occurring due to natural events [climate conditions, earthquakes, brush fires], or human made products, technologies, and systems [i.e., aircraft crashes, technology obsolescence, or failure].
3	❑ Security Risk Analysis	❑ Involve estimating access and harm caused due to war, terrorism, riot, crime, and misappropriation of information [national security information, intellectual property].
4	❑ Financial Risk Analysis	❑ Involve estimating potential individual, institutional and societal monetary losses such as currency fluctuations, interest rate, share market, market loss, bankruptcy, and miss appropriation of funds.
5	❑ Environmental Risk Analysis	❑ Involve estimating loss due to noise, contamination, and pollution in ecosystem [water, land, air] and in space.

RISK ASSESMENT APPLIED TO MEDICAL DEVICES

Table 6-17: Reliability Analysis Methods Used to Support Risk Management

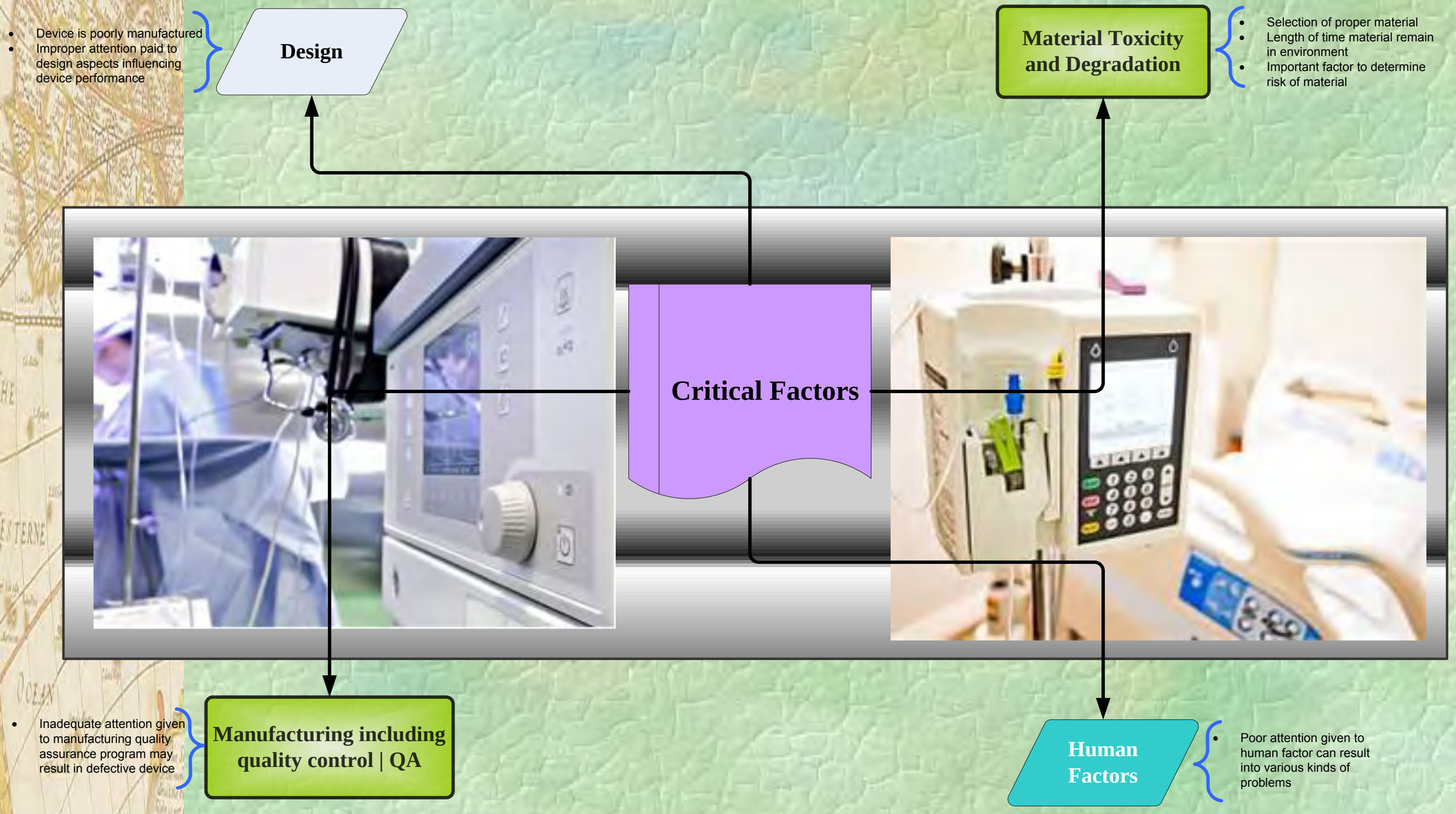


Risk Management Activity	Reliability Analysis Method	Application of Reliability Analysis Method
Risk Identification & Analysis	FMEA (Failure Mode & Effects Analysis)	▪ Perform and document a bottom-up analysis tracing part or process failures through to negative end effects
	Fault Tree analysis	▪ Perform and document a top-down analysis tracing negative end effects to all possible sources at the part or process level
Risk Estimation	FMEA	▪ Assign Risk Priority Numbers to estimate the severity of risks and group by criticality.
	Fault Tree analysis	▪ Perform quantitative analysis to calculate risk severity by minimum combination of causal events
	Reliability prediction System modeling	▪ When a risk is the result of a part failure, quantify the probability that the risk will occur.
Risk Control Measures: ▪ Analyze ▪ Implement ▪ Evaluate ▪ Risk/Benefit Analysis ▪ Review New Risks ▪ Completeness of Risk Control Measures	FMEA & Fault Tree analysis	▪ Study the bottom-up (FMEA) or top-down (Fault Tree) effects of risk control measures at the part- or process-level
	Reliability prediction	▪ Quantify the effects of alternate part designs on improved part reliability and improved product safety
	System modeling	▪ Quantify the effects of building in redundancy, dependency, or parallel structure to system design; estimate the efficacy of preventive maintenance or repair activities
Production and post-production monitoring & re-evaluation of found risks	FRACAS (Failure Reporting, Analysis, and Corrective Action System)	▪ Collect and analyze field data to track new and unexpected risks ▪ Initiate risk evaluation and control plan development for newly detected risks using a closed loop process to ensure all risks are addressed
	Weibull analysis	▪ Analyze collected field data to quantify part or system failure behavior ▪ Validate predicted performance by analyzing field data to demonstrate that design and safety requirements are being met

Source: ptc.com – Methods for managing product reliability and risk in the medical device field

FACTORS IMPACTING MEDICAL DEVICES RISK ASSESSMENT

Figure 6-35: Factors Critical to Medical Device Assessment



Critical Factors

Design

- Device is poorly manufactured
- Improper attention paid to design aspects influencing device performance

Material Toxicity and Degradation

- Selection of proper material
- Length of time material remain in environment
- Important factor to determine risk of material

Manufacturing including quality control | QA

- Inadequate attention given to manufacturing quality assurance program may result in defective device

Human Factors

- Poor attention given to human factor can result into various kinds of problems

TYPES OF PRODUCT LIABILITY

Product Liability

- Negligence - legal
- Strict Liability - legal
- Breach of warranty – legal
- Defects
- Failure to warn

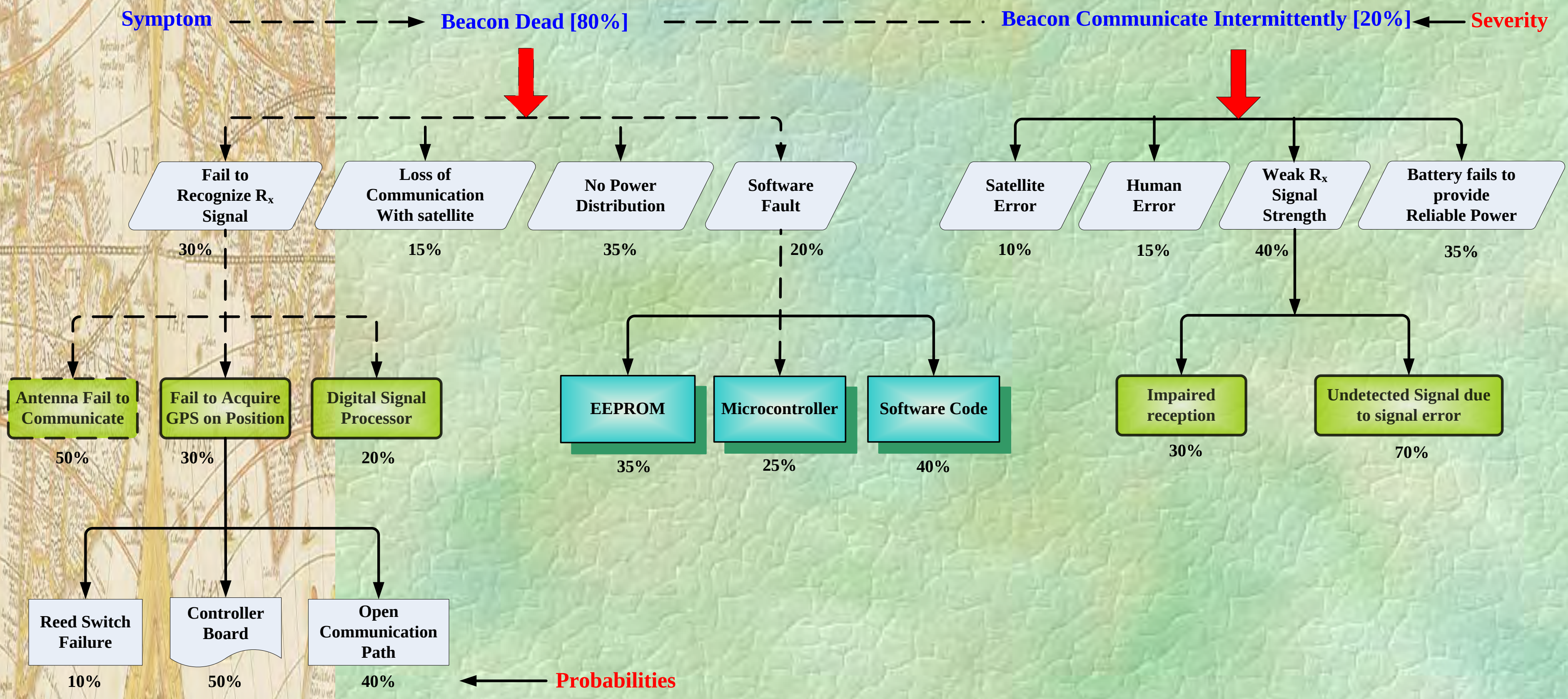
Negligence

- You owe a duty of care to another
- The standards for that care have been breached
- As a result a compensable injury results
- There are damages or injury to the plaintiff

Risk assessments help reduce exposure to hazards and can assist in building a successful defense against a product liability claim.

PRODUCT PREVENTION LIABILITY ANALYSIS

Figure 6-43: Product Liability Analysis – Emergency Beacon



PREVENTION OF PRODUCT LIABILITY

Guidelines to Prevent Manufacturing Defect

- Use proper labels and warnings about the use of the product.
- Use proper process control, quality control and inspection techniques to reduce manufacturing defects.
- Build all safety features and devices as part of the basic product instead of making them available as optional equipment.
- Use statistical sampling techniques to evaluate the adherence of production employees to design and manufacturing specifications.
- If the potential risk of the product in causing injuries is high, consider using 100 percent inspection instead of statistical sampling.
- Document all inspection, quality control, and testing activities and report the results to the product design and development department.

ECONOMIC MODELS FOR PRODUCT WARRANTIES

Example Application

- A turbine engine with a manufacturer's cost of \$1500 is sold under a 20,000 an hour PRW policy. The failure rate of the engine is 3 x 10^{-5} hours of operation. Assume the engine functions during its useful life. Find the expected unit warranty cost.

Solution

- Substituting respective information in equation 7.4 for the exponential distribution.

$$E[X(w)] = c_0\left[1 - e^{-\lambda w}\right] - \frac{c_0}{\lambda w}\int_0^w t\lambda e^{-\lambda t}dt$$

$$= c_0\left(1 - e^{-\lambda w}\right) - \frac{c_0}{\lambda w}\left[1 - (1 + \lambda w)e^{-\lambda w}\right] \text{.............Eqn 7.5}$$

- For the case where c_0 = \$1500, w = 20,000 hours and λ= 3 x 10^{-5} hours of operation :

M7 - LEARNING OBJECTIVES

Participant Shall be able to:

- ♦ **Determine optimum warranty period.**
- ♦ **Perform statistical analysis of product warranty data.**
- ♦ **Identify and be able to use different cost models.**
- ♦ **Utilize warranty data for prediction of future claims.**
- ♦ **Identify types of warranty and ways to classify them.**
- ♦ **Identify factors involved in establishing a particular warranty policy.**
- ♦ **Utilize warranty data to identify opportunities for quality and reliability improvements.**
- ♦ **Identify methods of analyzing warranty data, and use warranty data to estimate reliability.**

Adapt | Implement | Improve

PRODUCT WARRANTY CONCEPTS

Warranty Functions

Warranties are tools. Their optimal use is determined by their contribution to production of higher quality commercial and consumer products within appropriate life-cycle costs. The following warranty functions are classified with those process characteristics in mind:

Assurance Validation: Warranties help assure buyer that the seller delivers a product whose design and manufacture, as well as materials and workmanship, conform to contractual | design specifications.

Incentivization. Warranties ostensibly incentivize the contractor as a matter of course. This function, however, becomes truly distinctive when guarantee provisions define penalties for failure to achieve target parameters and/or rewards for "over achievement" of such targets.

Insurance: Every warranty provides a measure of insurance against the risks of repair or replacement costs. This function becomes noteworthy or dominant when the warranty protects the buyer against substantial contingent losses due to support costs or to inadequacies in periods extending significantly into the post-acceptance.

PRODUCT WARRANTA DATA ANALYSIS

Warranty Data Mining

- Product Data: This data typically include product serial number, production data, plant identification, sales data, sales region, price, accumulated use, warranty repair history, and others which are analyzed for different purposes.
- Failure Data: When a failure is claimed the repair service provider should record the data associated with the failure, such as customer complaint symptoms, use conditions at failure, and accumulated use. After the failure is fixed, the diagnosis findings, failure modes, failed part number, causes, and post fix test results documented (Use of FRACAS, CAPA).
- Repair Data: Such data should contain labor time and cost, part number serviced, cost of parts replaced, technician work identification and affiliation, date of repair and others.

When failures are claimed, information about the failed products is disclosed to the manufacturer. Such information is precious and credible and should be analyzed thoroughly to support business and engineering decision making.

PRODUCT WARRANTA DATA ANALYSIS

Warranty Data Mining Strategy

♦ Approach utilized will depend on a specific product and database. The strategy represented here consist of four steps:

1. **Define the objective of the warranty analysis**: General objective can include but not limited to, determination of monetary reserves for warranty, estimation of field reliability, projection of warranty repairs.

2. **Determine the data scope**: In this step the analysis should clearly define what specific warranty data [product, failure, repair] in each category are needed to achieve the objective .

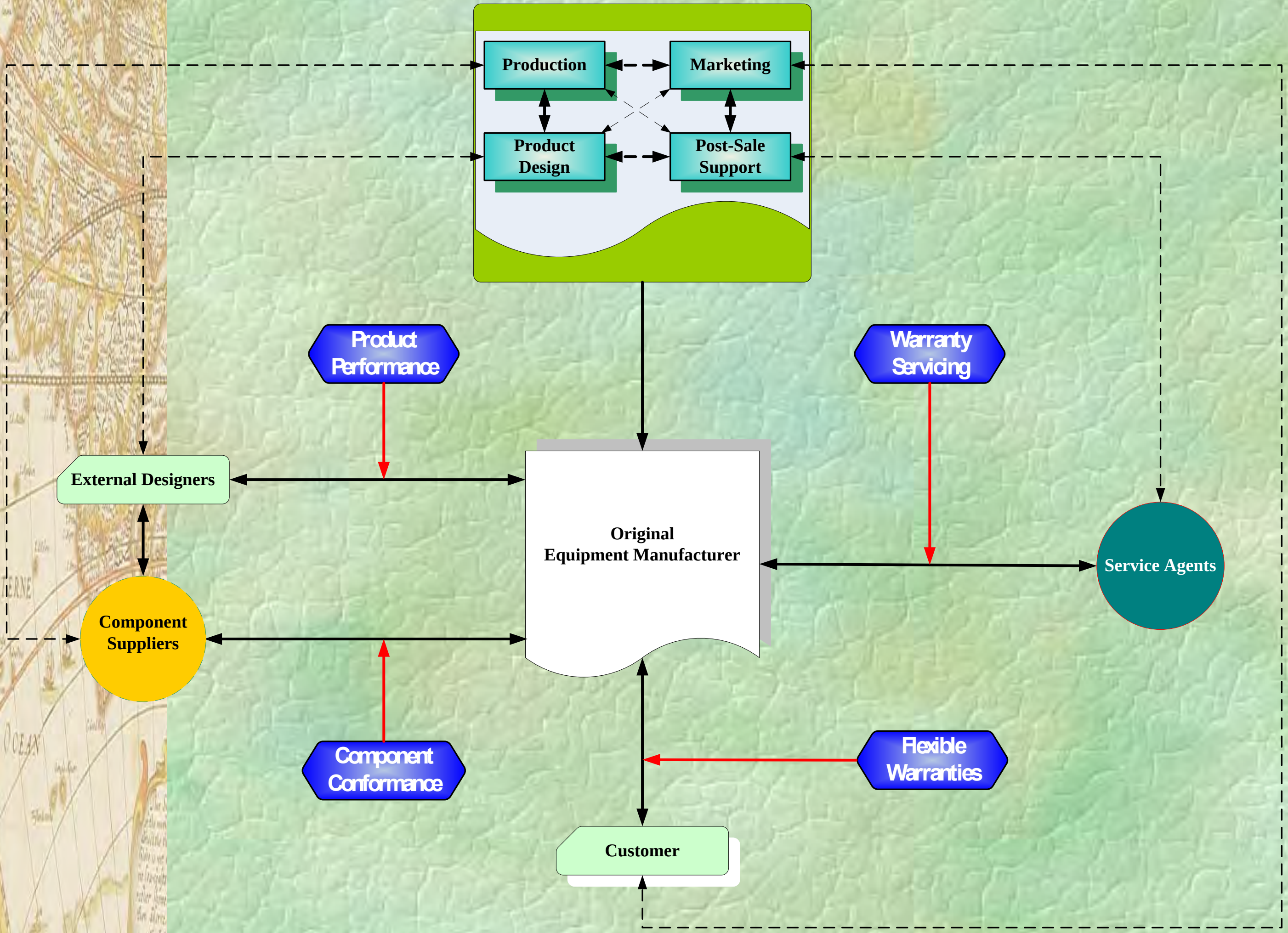
3. **Create data search filters and launch the search**: In relation to warranty database, a filter is a characteristic of a product, failure or repair.

4. **Format the data representation**: Manipulate data into to format with which subsequent data analysis are efficient.

Data mining is a computer assisted process of searching and analyzing enormous amount of data and extracting the meaning of the data. Data mining uses a variety of tools, including statistical analysis, decision tree, neural net, principal component and factor analysis.

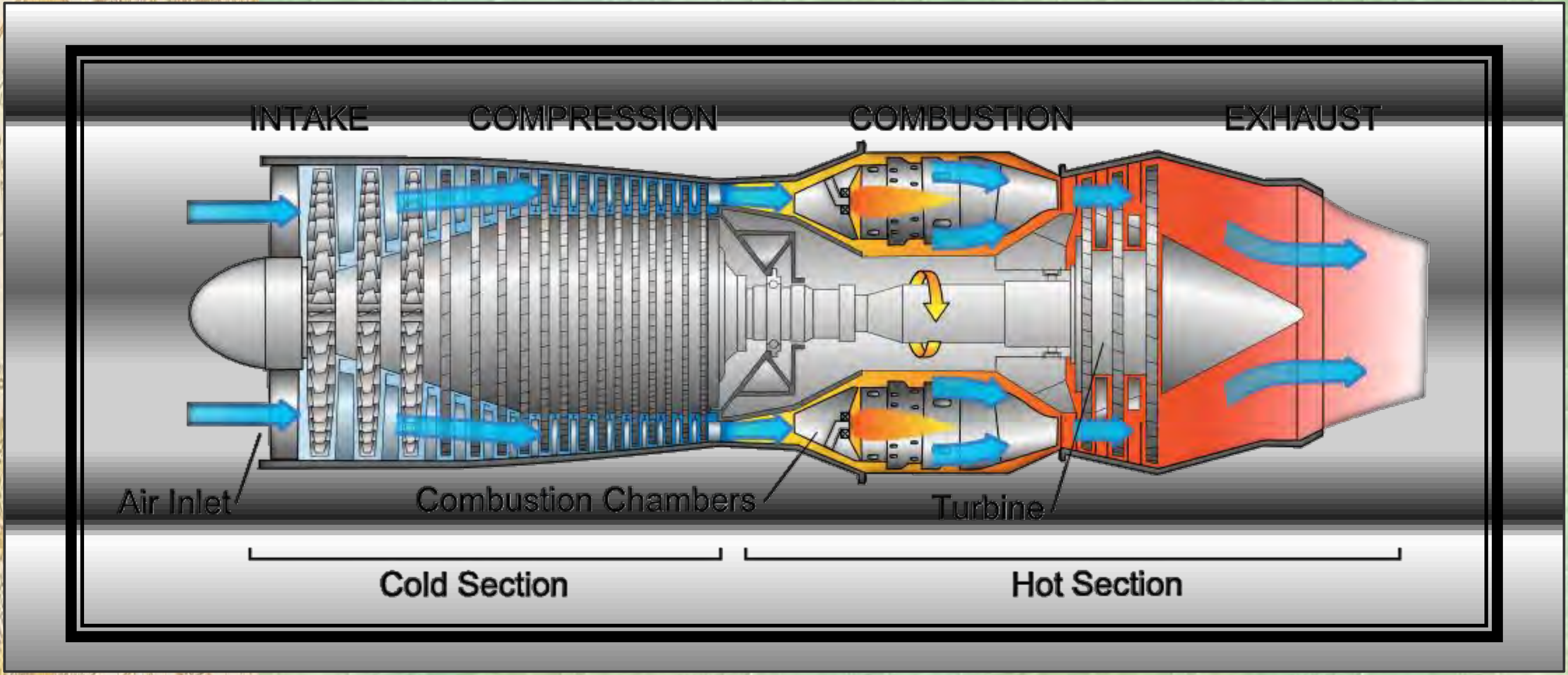
PRODUCT RELIABILITY AND WARRANTY

Figure 1: Framework for Study of Product Warranty



ECONOMIC MODELS FOR PRODUCT WARRANTIES

Solution Continues



$$E[X(20{,}000)] = \$1500\left(1-e^{-3x10^{-5}(20{,}000)}\right) - \frac{1500}{(3\,x\,10^{-5})(20{,}000)}\ x\left\{1-\left[1+(3\,x\,10^{-5})\,x\,(20{,}000)\right]e^{-3\,x\,10^{-5}(20{,}000)}\right\}$$

$$=(1500)(0.4512)-(2500)\{1-(1.6)x(0.54881)\}$$

$$=676.8-304.76=\$372.76$$

DETERMINE OPTIMUM WARRANTY PERIODS

Exponential Failure Times

- For failure times represented by an exponential distribution, as in the case during the useful life of a product, the number of failures during warranty, N[w], is Poisson and M[w] = λ and optimum warranty can be determined by:

$$w^* = \frac{2b_0b_1 - c_1\lambda}{2b_1^2} \quad \text{.....................Eqn 7.11}$$

Example Application

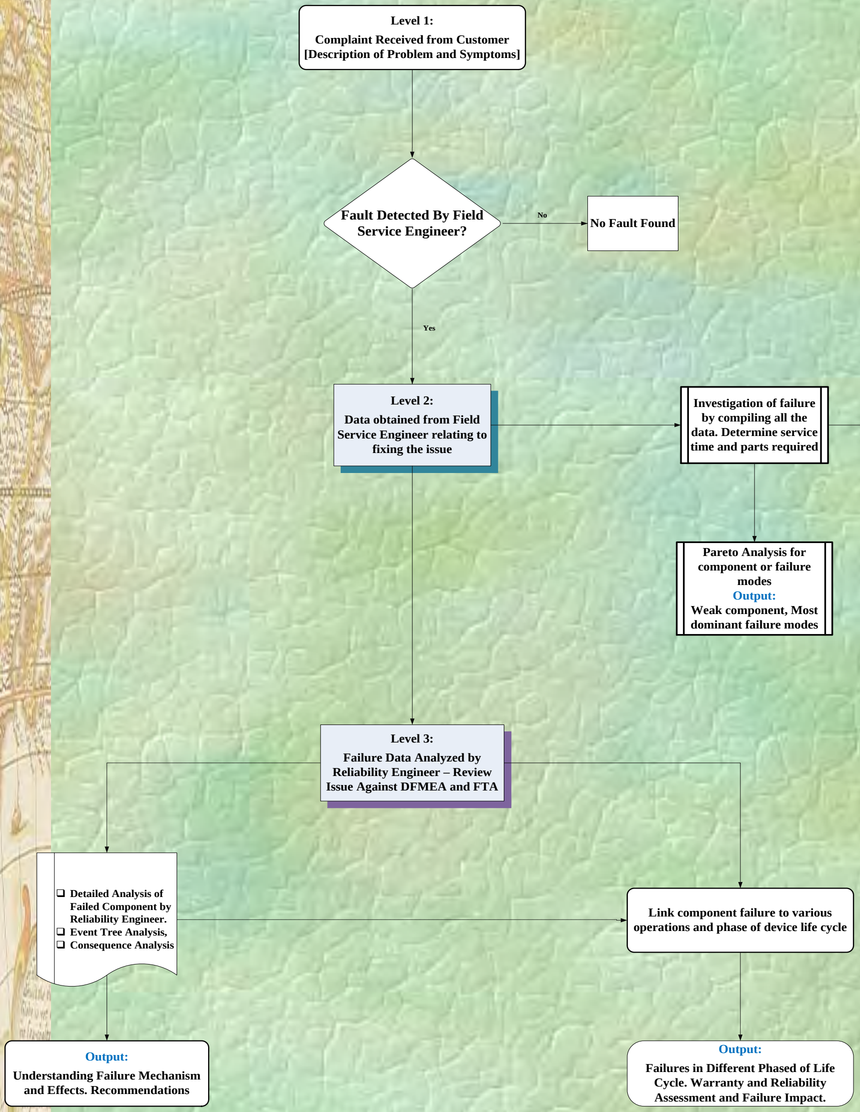
- Let's utilize the example from Thomas [1999] where a non-repairable item costs $1000. Failures occurs during useful life at a rate of 0.5 per year, each cost the manufacturer $1000.

- Without the warranty, the manufacturer estimates that it would be necessary to incur a cost of $2500 to market the item and, with warranty, the marketing costs would decline as B[w] = [50 – 10 w]^2. Thus c_1 = 1,000, λ= 0.5, b_0 = 10, b_1 = 10 and K = 2,500.

$$w^* = \frac{2*(50)*(10) - (1{,}000)*(0.5)}{2 \text{ x } (10)^2} = 2.5 \text{ years}$$

Reliability Assessment of Deployed System

Figure 10: Three Levels of Data Analysis



Level 1:
Complaint Received from Customer
[Description of Problem and Symptoms]

Fault Detected By Field Service Engineer?

No

No Fault Found

Yes

Level 2:
Data obtained from Field Service Engineer relating to fixing the issue

Investigation of failure by compiling all the data. Determine service time and parts required

Investigation of failure by grouping and categorizing of data [Relevant and Non-relevant Failures].

Investigation of failure by fault or defect code

Pareto Analysis for component or failure modes
Output:
Weak component, Most dominant failure modes

Gather information for CAPA | FRACAS, Failure Analysis team. Graph failure for trend
Output:
Detect sudden changes | Trend of issue

Time Series Plot, Trend Plot, New defect category
Output:
Detect sudden changes | Trend of issue

Level 3:
Failure Data Analyzed by Reliability Engineer – Review Issue Against DFMEA and FTA

- ❑ Detailed Analysis of Failed Component by Reliability Engineer.
- ❑ Event Tree Analysis,
- ❑ Consequence Analysis

Link component failure to various operations and phase of device life cycle

Output:
Understanding Failure Mechanism and Effects. Recommendations

Output:
Failures in Different Phased of Life Cycle. Warranty and Reliability Assessment and Failure Impact.

DESIGN FOR WARRANTY COST REDUCTION

Table 7: Design Phase Warranty Cost Reduction Strategies

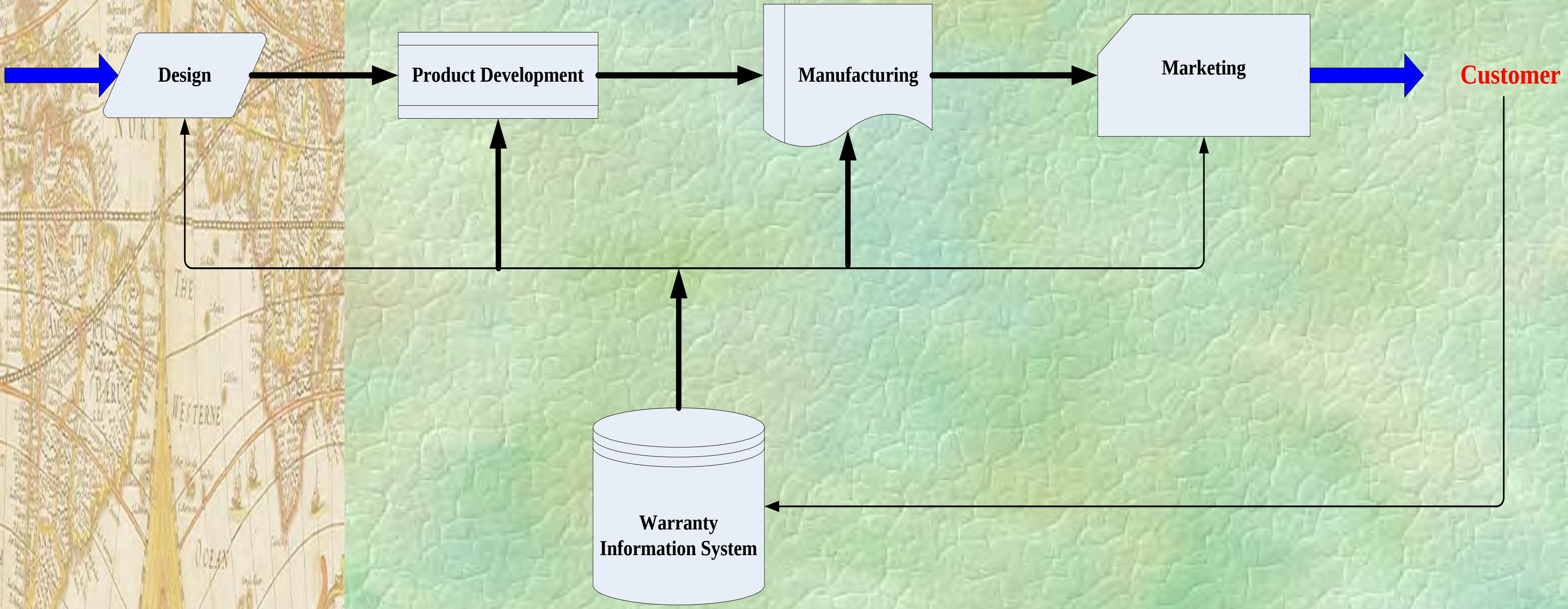
$$W_c \cong \sum_{i=1}^{M} N_i * \left({}_{STD}\,Cost_i + C_{material} \right)$$

Item	Reduce Number of Occurrences	Reduce Events Process Cost
1	▪ Design out the event occurrence 1. Modify product features 2. Change how product works 3. Implement feature differently	▪ Designing new (cheaper processes) 1. Design process around new technology 2. Design process to meet new market needs 3. Optimize process to reduce variability
2	▪ Reduce the number of occurrences 1. Improve SW | FW robustness 2. Increase HW reliability [reduce AFR]	▪ Switching to a cheaper process 1. ID features or capabilities needed to support different process
3	▪ Proactive Application of Design for X 1. Design for Assembly 2. Design for Reliability 3. Design for Manufacturing	▪ Reduce Standard Process Cost by: 1. Outsourcing 2. Product Changes 3. Process improvements 4. Supply chain re-engineering

Source: Adapted from Robert H Mueller, M.S., CQE Ops A La Carte & The Marisan Group

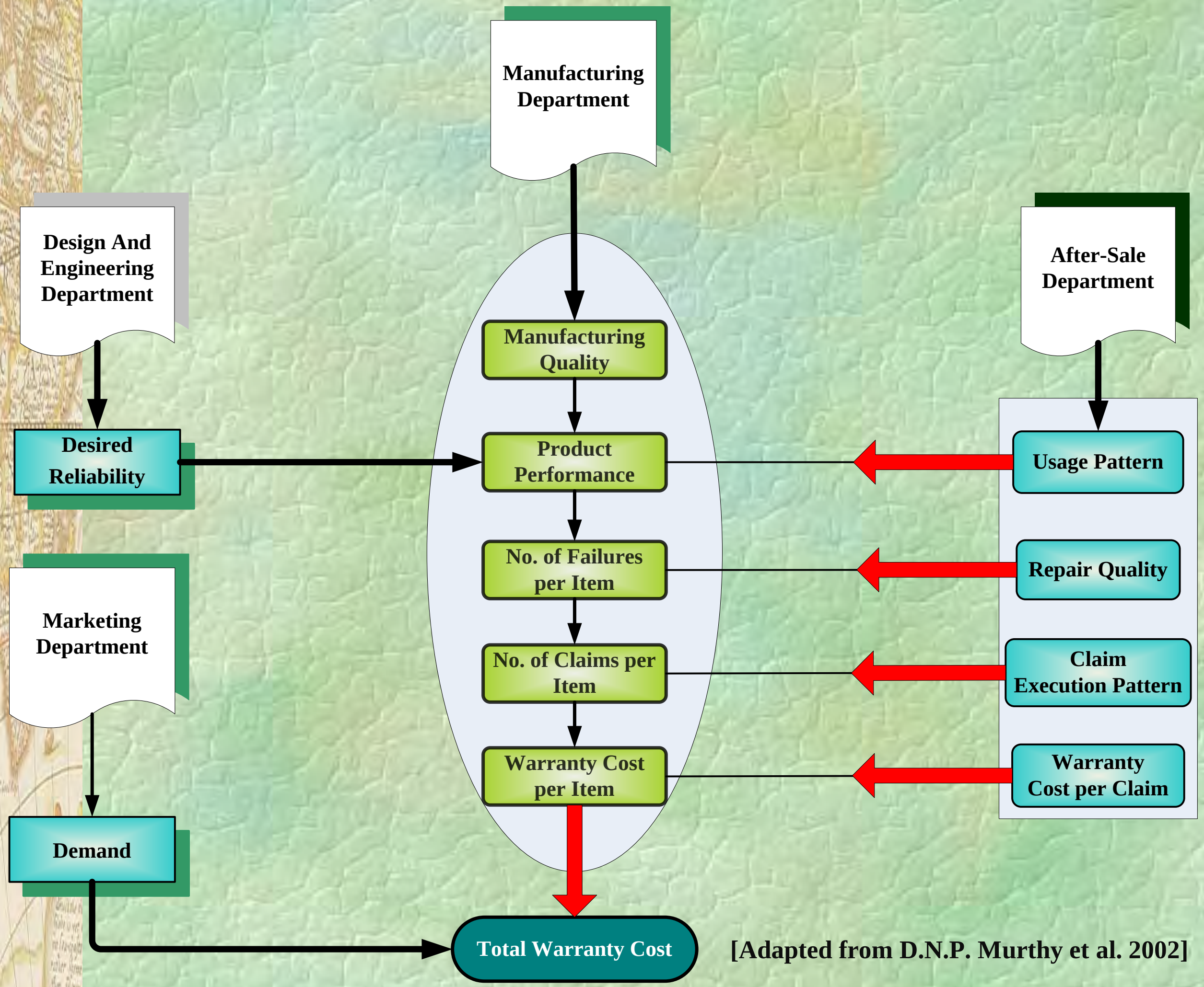
ELEMENTS OF WARRANTY COSTS

Figure 12: Product Development Model with Warranty



SYSTEM CHARACTERIZATION FOR WARRANTY COSTS

Figure 15: Integrated Model for Total Warranty Costs



[Adapted from D.N.P. Murthy et al. 2002]

WARRANTY COST MODELS APPLICATION

Non-renewing Warranty – FRW Policy Example 2

- A notebook computer can be manufactured at a cost of $150 and sold with a FRW policy. Units failing during warranty will be replaced at a cost to the manufacturer of $150.
- The mean time to failure is 2.5 years and failure times are distributed Erlang with cumulative distribution function (cdf) as follows:

$$F(t) = 1 - (1 + 0.8t)e^{-0.8t}, \ t \geq 0$$

- This represents a standard form of Erlang distribution with λ = 0.8 and k = 2; therefore, applying the single-failure assumption in equation 7.16 for the expected cost gives:

$$C_s(w) \approx C_0 + C_1 F(w)$$

$$C_s(w) = 150 + 150\left(1 - (1 + 0.8w)e^{-0.8w}\right), \ w \geq 0$$

$$C_s(w) = 300 - 150(1 + 0.8w)e^{-0.8w}, \ w \geq 0$$

M7 - INTERACTIVE EXERCISE

Simple Warranty Example:

Let's assume that a manufacturer of GPS devices plans to offer a 6-month warranty on the devices that cost \$150 each to produce. The expectation is to sell 15,000 devices and an internal test program indicates that the Mean-Time-To-Failure (MTTF) is 4 years after a stress-screening period. How much should the production cost be increased to cover the warranty cost?

W = 6 months
C_0 = \$150 (without warranty cost)
MTTF = 48 months
N = 15,000 units

The expected number of failures is:

$$F(t) = N\left[1 - e^{-\left(t/MTTF\right)}\right]$$

So that the number of failures over the interval dt is:

$$df = \left(\frac{N}{MTTF}\right) e^{-\frac{t}{MTTF}} dt$$

M8 – SEC 1 - LEARNING OBJECTIVES

Participant shall be able to:

- Develop understanding of specifying software reliability requirements.
- Distinguish between the different methods of allocating reliability to modules.
- Identify and utilize different design analysis methods to validate software design during development.
- Understand how the reliability of the software system can be measured and how growth models are used to predict reliability.
- Distinguish between formal specification (specification errors & omission) and formal verification (programming & some decision errors).
- Identify means of verifying that the specified dependability attributes (reliability, availability, safety and security) have been met by the system.

Adapt | Implement | Improve

SOFTWARE RELIABILITY OVERVIEW

DFR Fundamentals

Reliable software will be achieved through the implementation of structured software design methodology, independent testing, design reviews, verification, validation, and quality evaluation audits. These coordinated efforts are described in the Software Development Plan.

The design assurance and reliability engineer are responsible for the collection and analysis of operational software problem data obtained from software Problem Trouble Reports. The analysis activities can include:

- Problem Density Analysis - the problems per thousand lines of source code are tracked and analyzed.

SOFTWARE RELIABILITY OVERVIEW

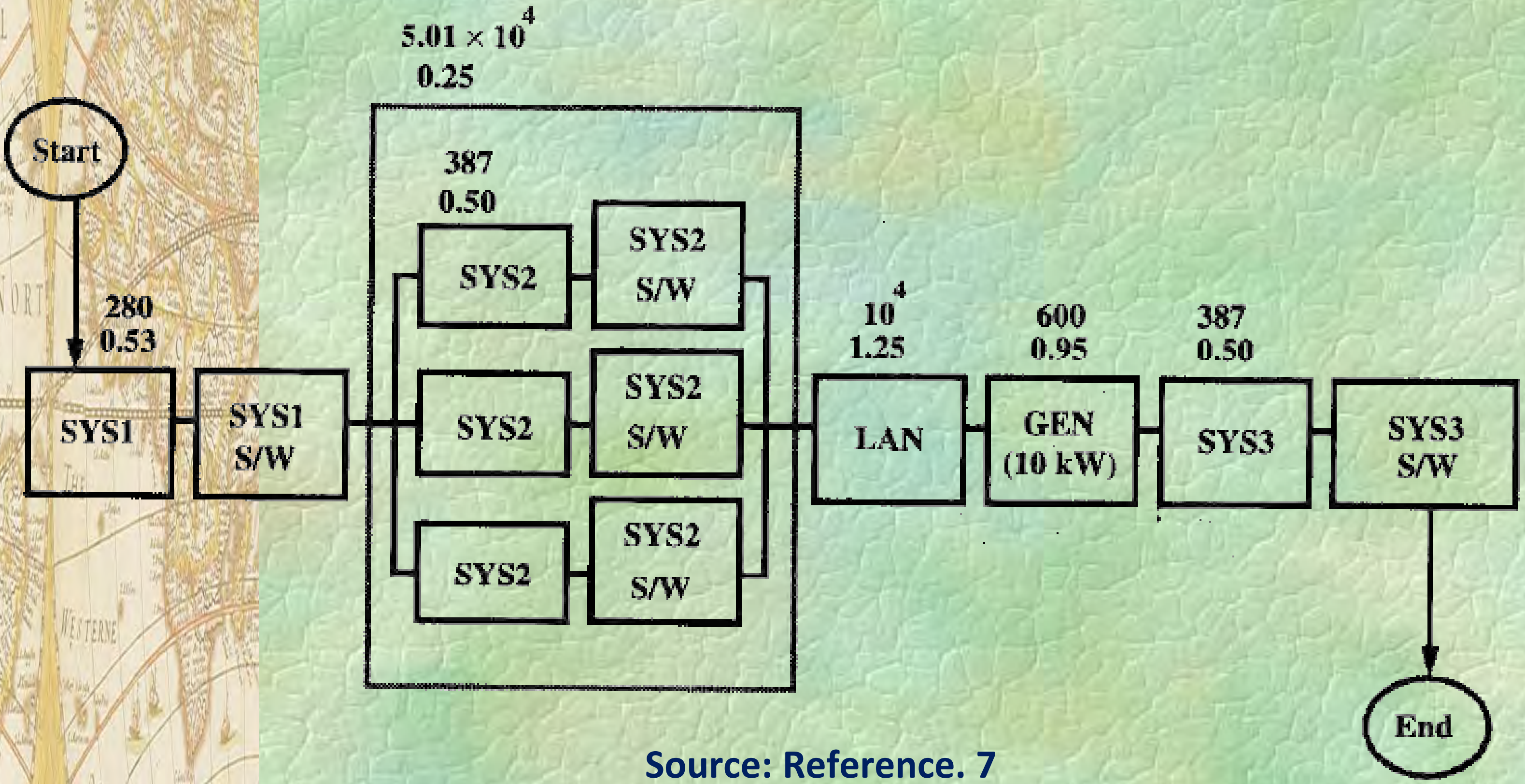
DFR Fundamentals

- Problem Category Analysis - The Software Problem Trouble Reports are categorized by problem (software/code, documentation, design, logic) and investigated.
- Open Problem Analysis - Priorities are assigned to the open problems for analysis. Reliability and safety problems will receive a high priority.
- Problem Cause Analysis – It is recommended for trend analysis to be performed to identify both good and bad trends. If the trend is significant, the root cause is determined, so the appropriate steps can be taken.

The analysis of operational software will indicate where more attention to reliability/quality is required. It also provides indicators as to where improved techniques should be instituted throughout the project.

SOFTWARE RELIABILITY OVERVIEW

Figure 2: Representative Example of Predicting Reliability



Source: Reference. 7

Reliability modeling methods are used to model combined HW/SW systems for the purposes of reliability estimation and allocation need to accurately assess the interdependence between individual software elements, the hardware platforms on which these software elements execute, and the services provided by the system being analyzed.

SOFTWARE RELIABILITY DEFINITIONS AND BASIC CONCEPTS

General Perspectives:

- Software reliability is defined as the probability of failure-free software operation for a specified period of time in a specified environment [ANSI91].
- Software Quality also includes factors such as functionality, usability, performance, serviceability, capability, installability, maintainability and documentation.
- A software system is an interacting set of software subsystems that is embedded in a computing environment that provides input to the software system and accepts service (outputs) from the software.
- Expected Service (or 'behavior') of a software system is a time-dependent sequence of output that agrees with the initial specification from which the software implementation has been derived [for the verification purpose] or which agrees with that system users have perceived the correct values to be [for the validation purpose].

SOFTWARE RELIABILITY DEFINITIONS AND BASIC CONCEPTS

General Perspectives:

- **Failures** – **A failure occurs when the user perceives that the program ceases to deliver the expected service.**

Table 1: Failure Severity Class Classification

Severity Class	System Capability Impact
1	Basic Service Interruptions - Catastrophic
2	Basic Service Degradation - Major
3	Inconvenience, Immediate Correction Necessary
4	Minot Effect, Correction Deferrable

- **Outage** – **An outage is a special case of a failure that is defined as a loss or degradation of service to a customer for a period of time [called outage duration].**
- **A failure resulting in the loss of functionality of the entire system is called a system outage.**

SOFTWARE RELIABILITY DEFINITIONS AND BASIC CONCEPTS

Common Types of System

- **Command Driven System** – A system in which the emphasis is on commands developed to support user's functionality and operational profile. Utilizes the software command to accomplish a function/operation.
- **Data Driven System**
  1. Financial billing systems are commonly data-driven.
  2. Reliability you want to evaluate is the probability of generating a correct bill.
  3. An operational profile must be developed for each subsystem.
- **Occurrence Probabilities** – In general there are two ways to determine occurrence probabilities for operations:
  1. Count the occurrence of operations in the field.
  2. Rely on estimates derived by refining the functional profile.

SOFTWARE RELIABILITY DEFINITIONS AND BASIC CONCEPTS

Understanding Operating Profile

- **Operation Profile** – A profile can be defined as a set of distinct [only one can occur at a time] alternatives called elements, each with a probability that it will occur.
- If element A occurs 70% of the time and element B 30% for example, the profile is A, 0.7 and B, 0.3.
- **Functional Profile** – A functional profile is a user-oriented profile of functions, not the operations that actually implement them.
- The operational profile, which is a quantitative characterization of how the system will be used, is very essential in software reliability engineering.

SOFTWARE RELIABILITY DEFINITIONS AND BASIC CONCEPTS

Understanding Operating Profile

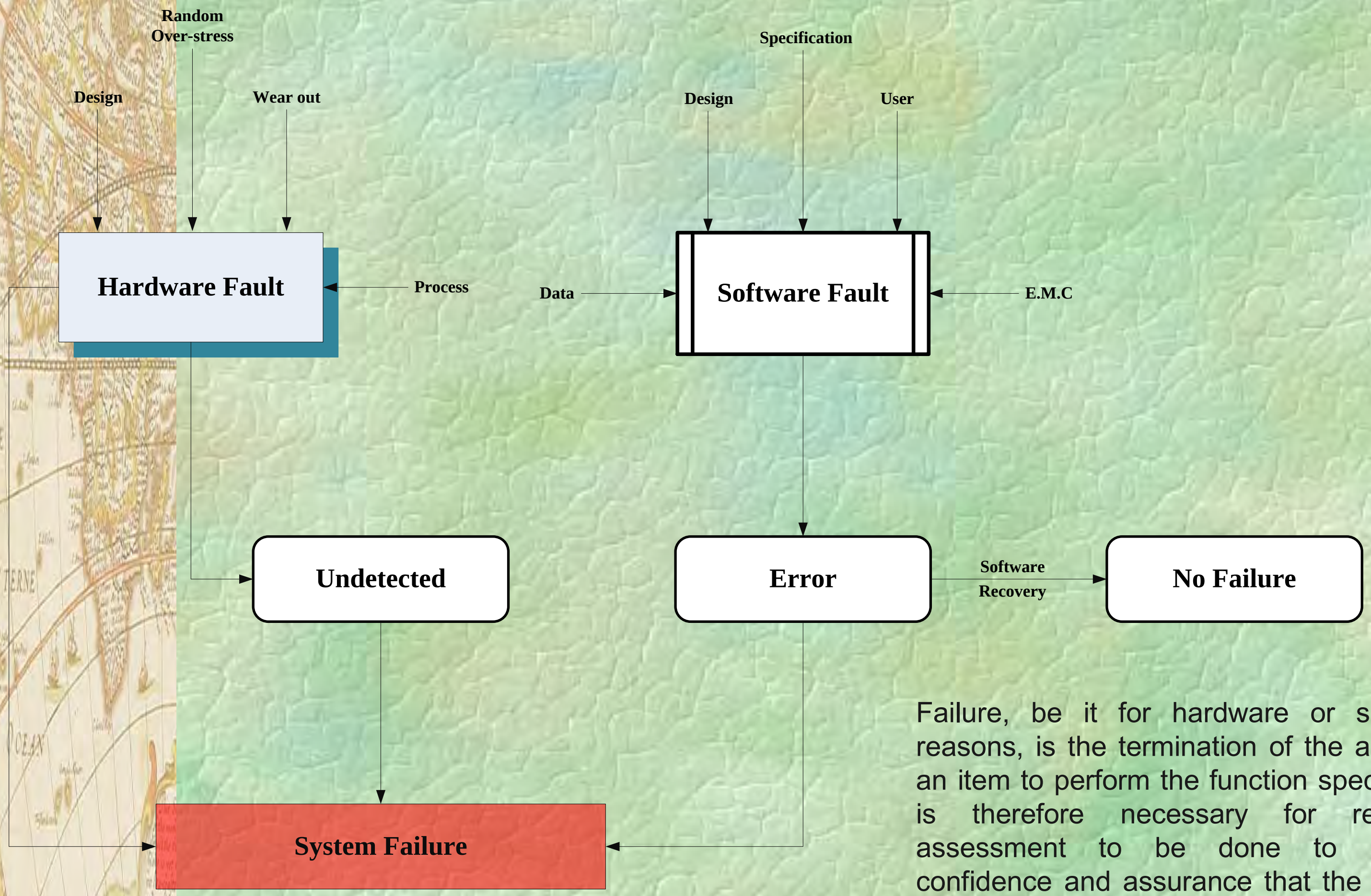
- **Example** – In a PBX application, there are 80 telephone additions, 70 removals, and 800 relocations or changes per month. Online-directory updating represents 5 percent of the total use in system administration mode.
- Lets assume that the occurrence probabilities for the system-administration mode is 0.02.

Table 2: Sample Initial Functional Profile Segment

Function	System Administration Mode Occurrence Probability	Overall Occurrence Probability
Relocation | Change	0.80	0.0160
Addition	0.08	0.0016
Removal	0.07	0.0014
Online-directory updating	0.05	0.0010

SOFTWARE RELIABILITY DEFINITIONS AND BASIC CONCEPTS

Figure 4: Software Failures in a Programmable System



Failure, be it for hardware or software reasons, is the termination of the ability of an item to perform the function specified. It is therefore necessary for reliability assessment to be done to provide confidence and assurance that the system will perform as intended over its design life.

SOFTWARE RELIABILITY DEFINITIONS AND BASIC CONCEPTS

- **Mean Time to Repair [MTTR]** – **This represents the expected time until a system will be repaired after a failure is observed.**
- **Availability** - **This is the probability that a system is available when needed.**
- **Typically it is measured by:** $\text{Availabili ty} = \dfrac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}$
- **Failure Data collection** - **Two types of failure data, namely** ***failure-count data and time-between-failures data, can be collected for the purpose of software reliability measurement.***

Table 6: Time – Based Failure Specification

Failure Number	Failure Time (sec)	Failure Interval (sec)
1	5	5
2	15	10
3	30	15
4	40	10
5	55	15
6	60	5
7	75	15

SOFTWARE RELIABILITY DEFINITIONS AND BASIC CONCEPTS

Table 7: Failure – Based Failure Specification

Time (sec)	Cumulative Failures	Failure Interval
15	2	2
30	5	3
45	8	3
80	9	1
120	11	2
150	15	4
200	20	5

- **Software Reliability Measurement** – Measurement of software reliability includes two types of activities:
  1. **Reliability Estimation** – This activity determines the current software reliability based on applying statistical inferences techniques to failure data obtained during system test or system operation.
  2. **Reliability Prediction** - This activity determines the current software reliability based upon available software metrics and measures .

DESIGNING SOFTWARE FOR RELIABILITY

Good Reliability Design Engineering would:

- **Use redundancy | diversity for reliability.**
- **Use consistent error handling.**
- **Use quality development tool.**
- **Use good architectural infrastructure.**
- **Utilize built-in application health checks.**
- **Follow established application design guidelines.**
- **Incorporate reliability requirements in the specification.**

Design Concepts

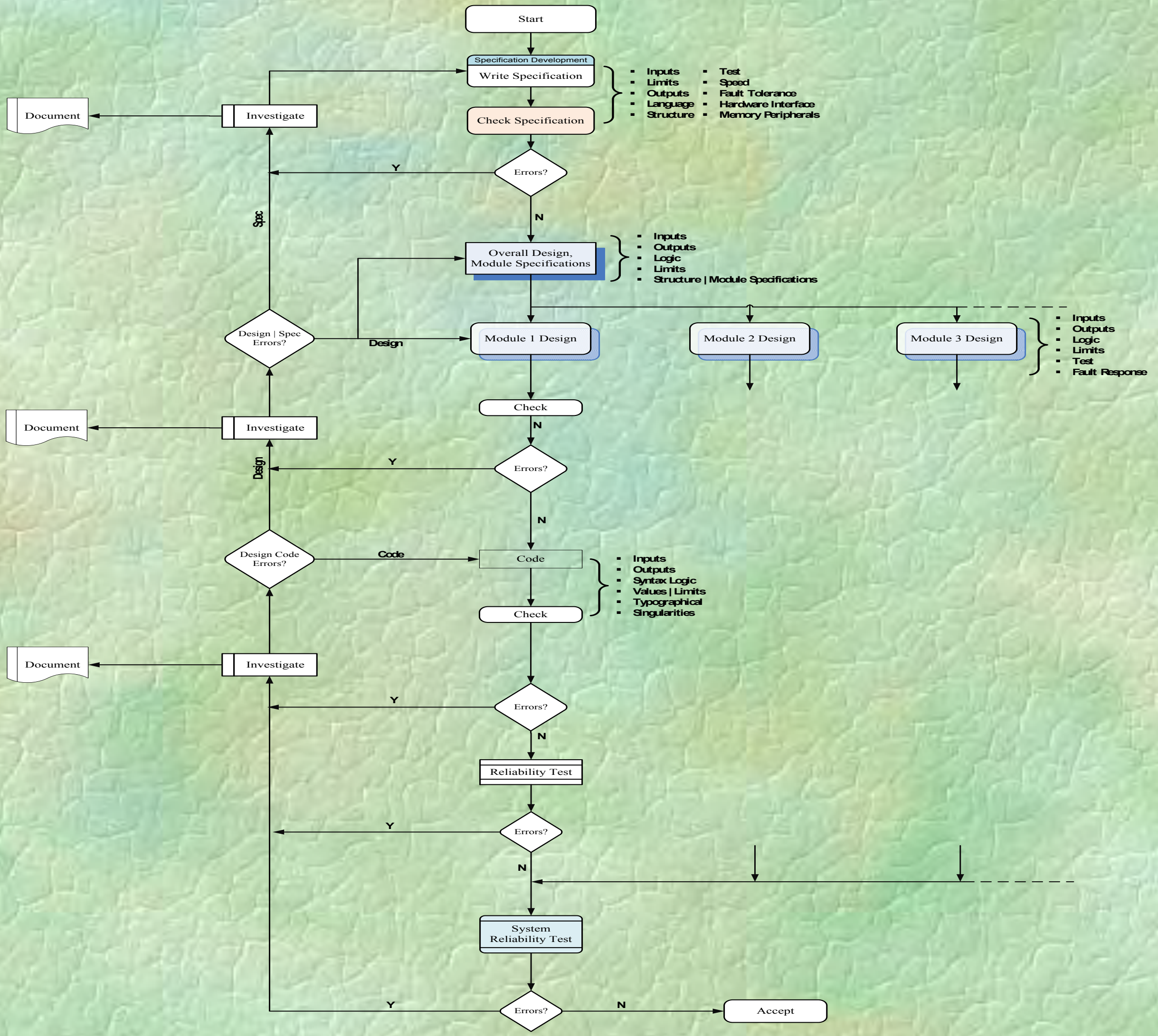
1. **The process of designing for reliability involves looking at the application's expected usage pattern, specifying the reliability profile, and engineering the software architecture with intention of meeting the profile.**

2. **DFR includes ensuring that data input and data transformations, error-free state management, and non-corrupting recovery from detected failure conditions are pertinent elements of an application to operate failure free.**

3. **Creating a high-reliability application depends on the entire software development life cycle from early design specifications, through building and testing, to deployment and ongoing operational maintenance.**

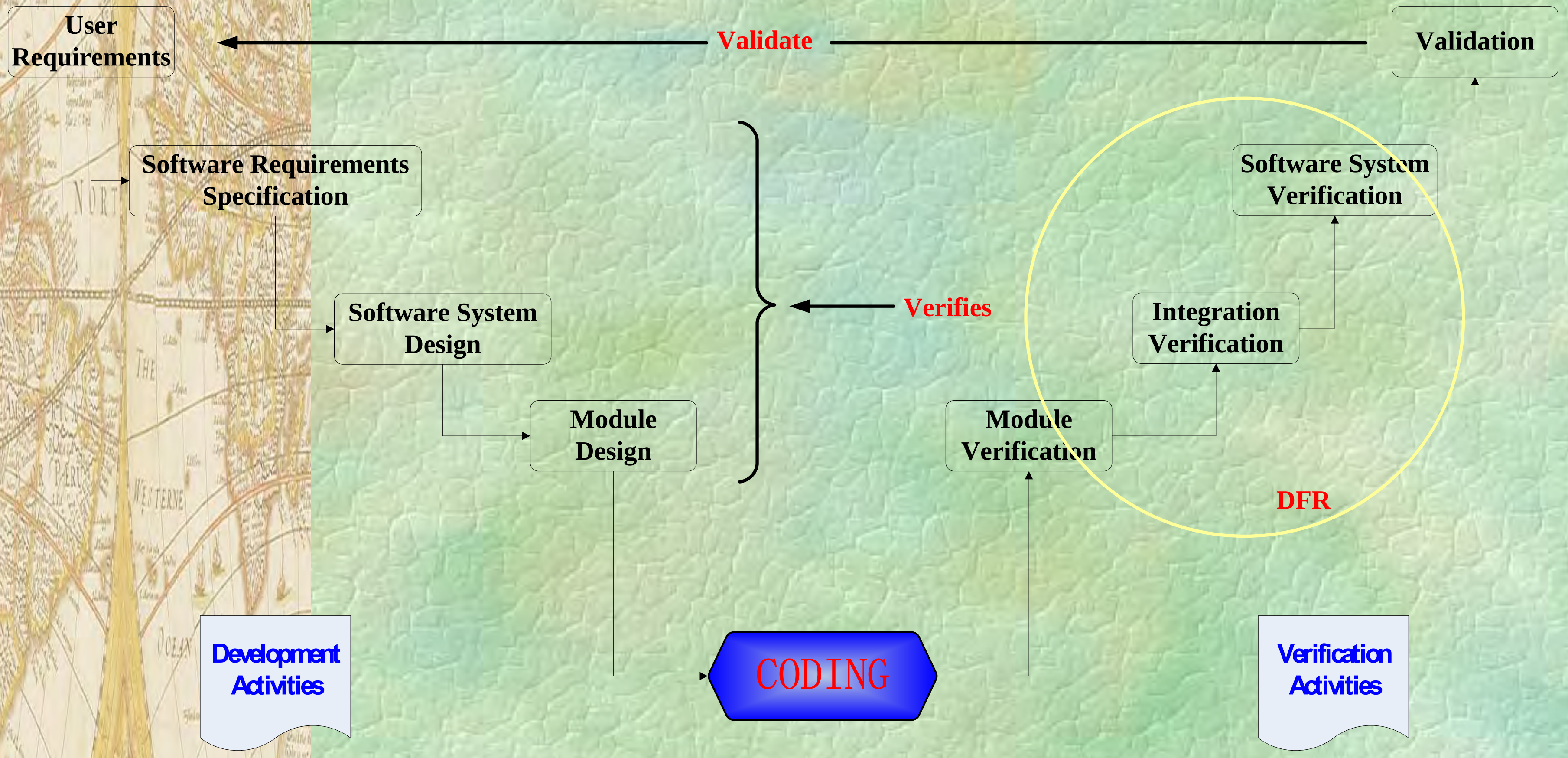
FUNDAMENTAL ELEMENTS OF SOFTWARE DEVELOPMENT

Figure 6: Software Development Process for Reliability



FUNDAMENTAL ELEMENTS OF SOFTWARE DEVELOPMENT

Figure 8: Relationship of Software Development and Verification and Validation Activities



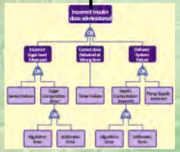
– Proactive Innovative Solutions for Success and Competitive Advantages

SOFTWARE DESIGN VERIFICATION

Figure 9: Software Verification Techniques

Software Verification

- Dynamic Testing Techniques
  - Stress Tests
  - Random Tests
  - Structure Tests
    - Loop Testing
    - Random Testing
    - Basic Path Testing
  - Functional Tests
    - Domain Testing
    - Data Flow Testing
    - Finite State Testing
    - Transition Flow Testing
    - Behavioral Control Flow Testing
  - Performance Tests
- Static Verification Technique
  - Fault Tree Analysis

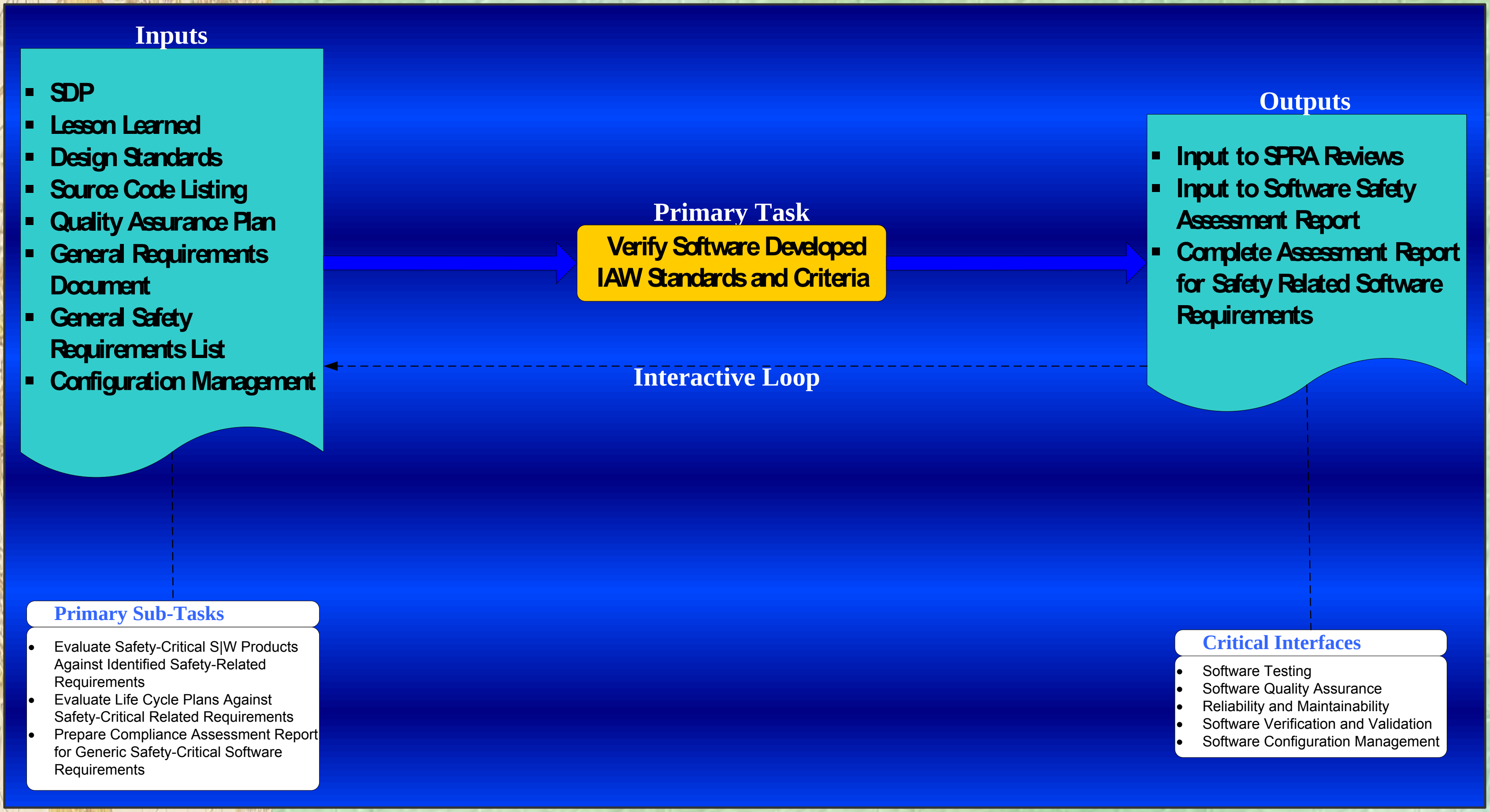


  - Modeling Techniques
    - Petri Nets
    - Finite State Machines
    - Rate Monotonic Analysis
  - Technical Reviews
  - Inspection
  - Walkthrough
  - Formal Verification
- Verification Activities
  - Module Verification
    - Computational Errors
      - Precision Errors
      - Mixed Mode Operation
      - Incorrect Initialization
      - Incorrect Arithmetic Precedence
    - Error Handling
    - Exception Handling
    - * Always Structural or White Box Testing
  - Integration Verification
  - System Verification
  - Change Verification
  - Verifying Safety
  - Verification Measurement
    - **Test Coverage**
    - **Reliability Modeling**
      - Weibull Model
      - Rayleigh Model
      - Reliability Growth Model
    - * Completeness & Reliability

Static Analysis Tool Developed by AdaCoreb: CodePeer, GNATPro, SPARK Pro, Qgen Model-Based Development Tool

PRINCIPLE OF VERIFICATION AND VALIDATION

Figure 10: Software Requirement Verification – Safety Critical Design



Inputs

- SDP
- Lesson Learned
- Design Standards
- Source Code Listing
- Quality Assurance Plan
- General Requirements Document
- General Safety Requirements List
- Configuration Management

Primary Task

Verify Software Developed IAW Standards and Criteria

Outputs

- Input to SPRA Reviews
- Input to Software Safety Assessment Report
- Complete Assessment Report for Safety Related Software Requirements

Interactive Loop

Primary Sub-Tasks

- Evaluate Safety-Critical S|W Products Against Identified Safety-Related Requirements
- Evaluate Life Cycle Plans Against Safety-Critical Related Requirements
- Prepare Compliance Assessment Report for Generic Safety-Critical Software Requirements

Critical Interfaces

- Software Testing
- Software Quality Assurance
- Reliability and Maintainability
- Software Verification and Validation
- Software Configuration Management

Software Reliability Specifications

Specifying Reliability Requirements

- To specify reliability requirements, use one or more of the three methods described below. The methods are:

  1. Release Date
  2. System Balance
  3. Life Cycle Cost Optimization

- The first approach is used when the release date is particularly critical. Generally appropriate for flight system facing a fixed launch time, or commercial systems aiming at delivery within a profit window.

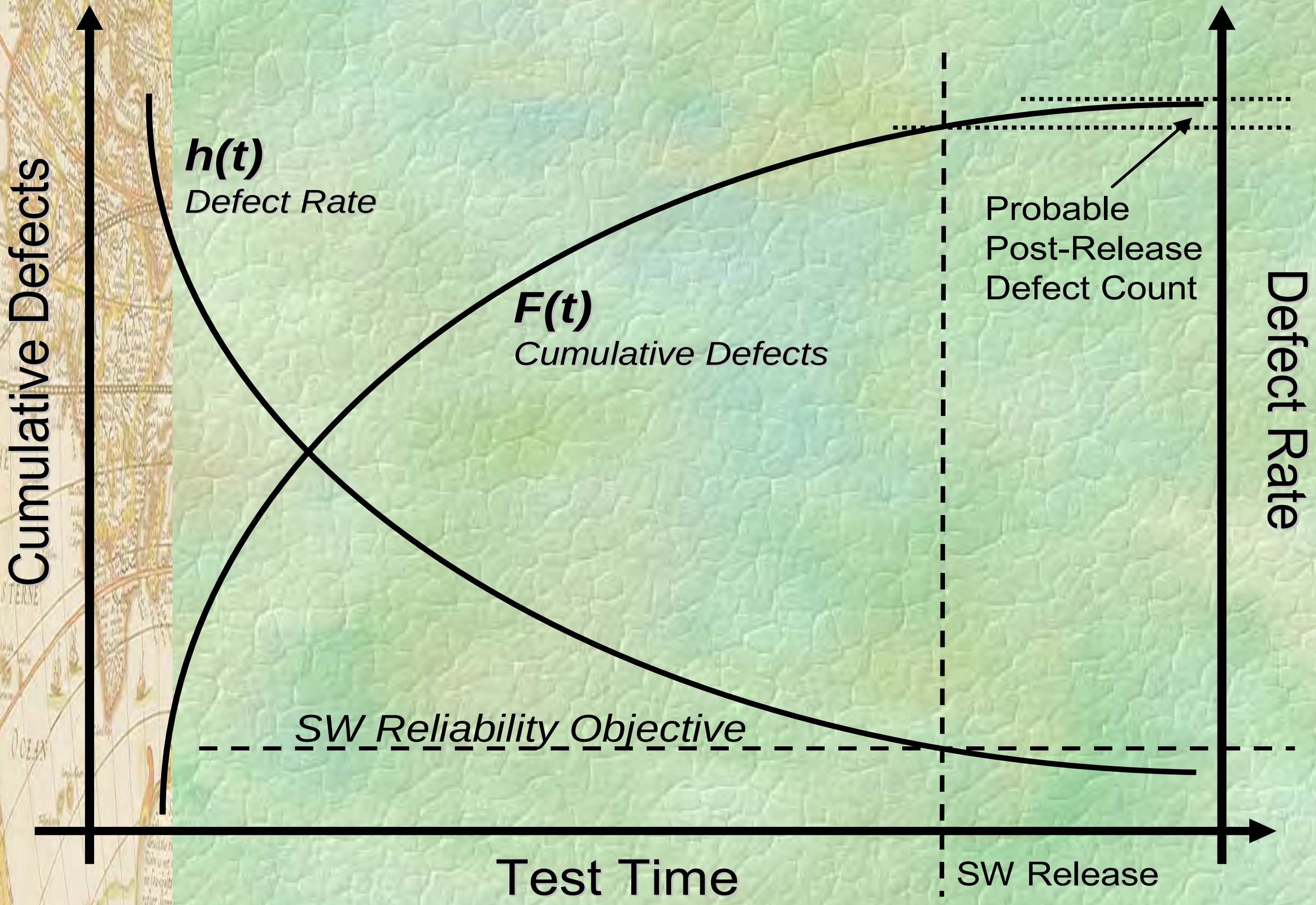
- The system balance method is primarily used to allocate reliabilities among components of a system based on the overall reliability requirements.

- The basis of the third approach, is the assumption that reliability improvement is obtained by more expensive testing.

- It is possible to use one of these methods for developing the requirements for one component of the system, and another for a separate component.

SOFTWARE RELIABILITY OBJECTIVES

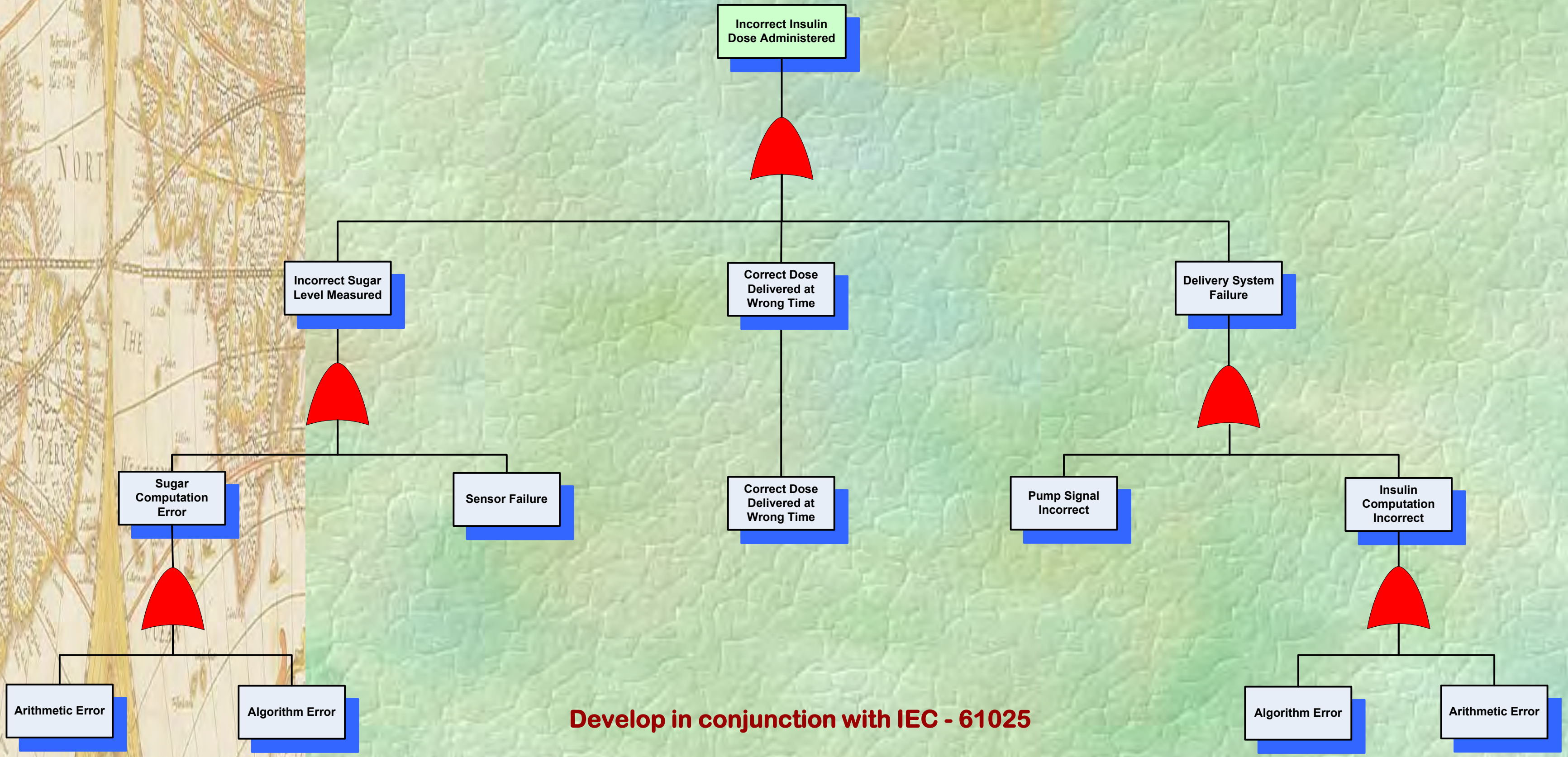
Figure 11: Relationship Between Defect Rate And Reliability Objectives



– Proactive Innovative Solutions for Success and Competitive Advantages

SOFTWARE DESIGN ANALYSIS

Figure 14: Fault Tree for Insulin Delivery System



Incorrect Insulin Dose Administered
Incorrect Sugar Level Measured
Correct Dose Delivered at Wrong Time
Delivery System Failure
Sugar Computation Error
Sensor Failure
Correct Dose Delivered at Wrong Time
Pump Signal Incorrect
Insulin Computation Incorrect
Arithmetic Error
Algorithm Error
Algorithm Error
Arithmetic Error

Develop in conjunction with IEC - 61025

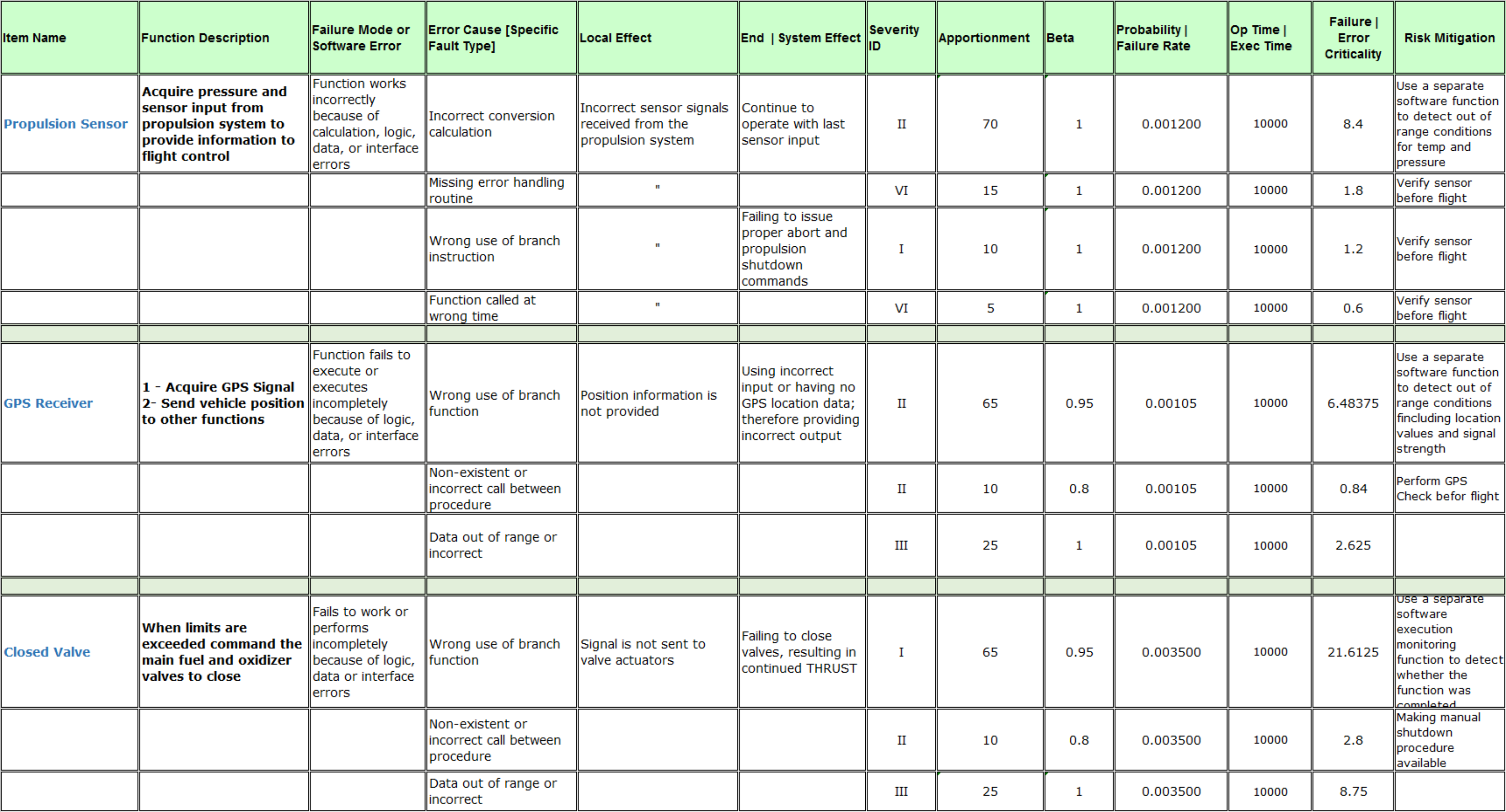
SOFTWARE DESIGN ANALYSIS

Table 16: Example DFMEA of a Control CSCI for a MESA System

<table>
<tr><th>Item</th><th>System Function Specification</th><th>Potential Failure Mode | Error</th><th>Potential Effects of Failure | Error</th><th>S
E
V</th><th>Potential Causes of Failure | Error</th><th>O
C
C</th><th colspan="2">Current Design Control / Mitigation</th><th>D
E
T</th><th>R
P
N</th><th>Corrective Action</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Method of Prevention</td><td>Detection Means</td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>CSCI Control Signals</td><td>The Control CSCI acts as the host coordinator for the MESA systemand maintains communication with all remote computers</td><td>Host | Remote Computers out of synch [Closed vs. Open loops]</td><td>Inadvertent motion of hardware [ST, Sphere, OTSS]</td><td>9</td><td>Valid Host signal sent to remote and invalid mode [Closed vs. Open loops]</td><td>5</td><td>Static Analysis</td><td>Dynamic Analysis</td><td>5</td><td>225</td><td>Incorporate a loop synchronization algorithm</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Sphere HWCI Control Signals</td><td>Sphere Control shall the sphere encoder and control line movements</td><td>Sphere control software generates erroneous motion command</td><td>Undesired command motion of sphere</td><td>9</td><td>Data initialization failure</td><td>4</td><td>PHA</td><td>Automated self checking of software</td><td>3</td><td>108</td><td>Incorporate software analysis checking to ensure valid motion commands are generated</td></tr>
<tr><td></td><td></td><td></td><td></td><td>8</td><td>Undesired movement value generated</td><td>5</td><td>FMECA</td><td>verification testing</td><td>5</td><td>200</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td>9</td><td>Invalid incremental movement calculation</td><td>6</td><td>FTA</td><td>Automated self checking of software</td><td>6</td><td>324</td><td></td></tr>
</table>

SOFTWARE DESIGN ANALYSIS

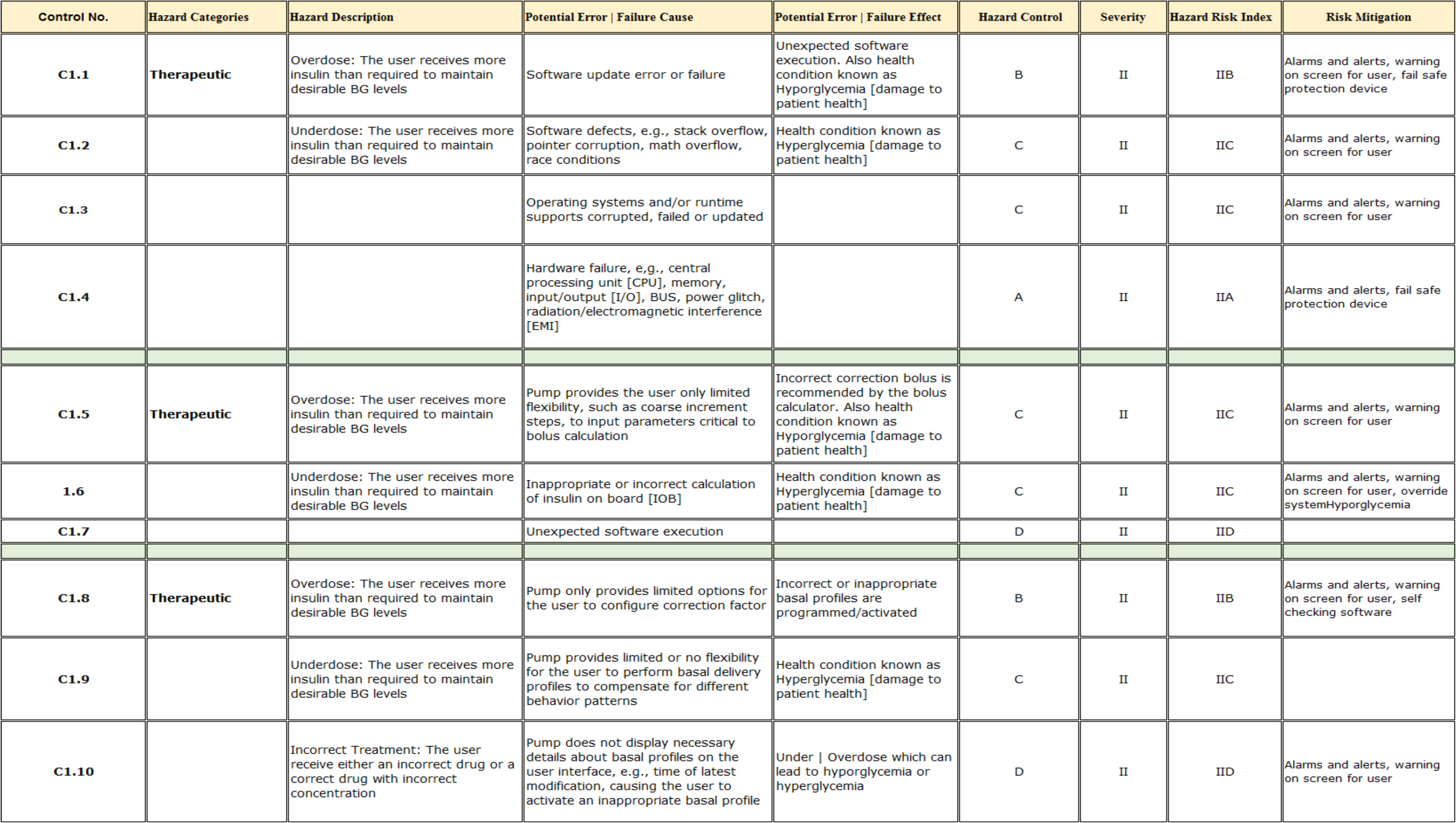
Table 17: Hypothetical FMECA – Software and Computing System



Item Name	Function Description	Failure Mode or Software Error	Error Cause [Specific Fault Type]	Local Effect	End | System Effect	Severity ID	Apportionment	Beta	Probability | Failure Rate	Op Time | Exec Time	Failure | Error Criticality	Risk Mitigation
Propulsion Sensor	**Acquire pressure and sensor input from propulsion system to provide information to flight control**	Function works incorrectly because of calculation, logic, data, or interface errors	Incorrect conversion calculation	Incorrect sensor signals received from the propulsion system	Continue to operate with last sensor input	II	70	1	0.001200	10000	8.4	Use a separate software function to detect out of range conditions for temp and pressure
			Missing error handling routine	"		VI	15	1	0.001200	10000	1.8	Verify sensor before flight
			Wrong use of branch instruction	"	Failing to issue proper abort and propulsion shutdown commands	I	10	1	0.001200	10000	1.2	Verify sensor before flight
			Function called at wrong time	"		VI	5	1	0.001200	10000	0.6	Verify sensor before flight
GPS Receiver	**1 - Acquire GPS Signal 2- Send vehicle position to other functions**	Function fails to execute or executes incompletely because of logic, data, or interface errors	Wrong use of branch function	Position information is not provided	Using incorrect input or having no GPS location data; therefore providing incorrect output	II	65	0.95	0.00105	10000	6.48375	Use a separate software function to detect out of range conditions fincluding location values and signal strength
			Non-existent or incorrect call between procedure			II	10	0.8	0.00105	10000	0.84	Perform GPS Check befor flight
			Data out of range or incorrect			III	25	1	0.00105	10000	2.625	
Closed Valve	**When limits are exceeded command the main fuel and oxidizer valves to close**	Fails to work or performs incompletely because of logic, data or interface errors	Wrong use of branch function	Signal is not sent to valve actuators	Failing to close valves, resulting in continued THRUST	I	65	0.95	0.003500	10000	21.6125	Use a separate software execution monitoring function to detect whether the function was completed
			Non-existent or incorrect call between procedure			II	10	0.8	0.003500	10000	2.8	Making manual shutdown procedure available
			Data out of range or incorrect			III	25	1	0.003500	10000	8.75	

SOFTWARE DESIGN ANALYSIS

Table 18: Preliminary Hazard Analysis Generic Insulin Infusion Pump



Control No.	Hazard Categories	Hazard Description	Potential Error | Failure Cause	Potential Error | Failure Effect	Hazard Control	Severity	Hazard Risk Index	Risk Mitigation
C1.1	Therapeutic	Overdose: The user receives more insulin than required to maintain desirable BG levels	Software update error or failure	Unexpected software execution. Also health condition known as Hyporglycemia [damage to patient health]	B	II	IIB	Alarms and alerts, warning on screen for user, fail safe protection device
C1.2		Underdose: The user receives more insulin than required to maintain desirable BG levels	Software defects, e.g., stack overflow, pointer corruption, math overflow, race conditions	Health condition known as Hyperglycemia [damage to patient health]	C	II	IIC	Alarms and alerts, warning on screen for user
C1.3			Operating systems and/or runtime supports corrupted, failed or updated		C	II	IIC	Alarms and alerts, warning on screen for user
C1.4			Hardware failure, e,g., central processing unit [CPU], memory, input/output [I/O], BUS, power glitch, radiation/electromagnetic interference [EMI]		A	II	IIA	Alarms and alerts, fail safe protection device
C1.5	Therapeutic	Overdose: The user receives more insulin than required to maintain desirable BG levels	Pump provides the user only limited flexibility, such as coarse increment steps, to input parameters critical to bolus calculation	Incorrect correction bolus is recommended by the bolus calculator. Also health condition known as Hyporglycemia [damage to patient health]	C	II	IIC	Alarms and alerts, warning on screen for user
1.6		Underdose: The user receives more insulin than required to maintain desirable BG levels	Inappropriate or incorrect calculation of insulin on board [IOB]	Health condition known as Hyperglycemia [damage to patient health]	C	II	IIC	Alarms and alerts, warning on screen for user, override systemHyporglycemia
C1.7			Unexpected software execution		D	II	IID	
C1.8	Therapeutic	Overdose: The user receives more insulin than required to maintain desirable BG levels	Pump only provides limited options for the user to configure correction factor	Incorrect or inappropriate basal profiles are programmed/activated	B	II	IIB	Alarms and alerts, warning on screen for user, self checking software
C1.9		Underdose: The user receives more insulin than required to maintain desirable BG levels	Pump provides limited or no flexibility for the user to perform basal delivery profiles to compensate for different behavior patterns	Health condition known as Hyperglycemia [damage to patient health]	C	II	IIC	
C1.10		Incorrect Treatment: The user receive either an incorrect drug or a correct drug with incorrect concentration	Pump does not display necessary details about basal profiles on the user interface, e.g., time of latest modification, causing the user to activate an inappropriate basal profile	Under | Overdose which can lead to hyporglycemia or hyperglycemia	D	II	IID	Alarms and alerts, warning on screen for user

This is a medical device software - IEC 62304 [Use in conjunction with ISO 14971]

SOFTWARE DESIGN ANALYSIS

Table 19: Safety-Critical Function Matrix

	Safety-Critical Functions						
CSCI | CSU Name	1	2	3	4	5	6	Ratings
INIT	M		M	M			M
SIGNAL		H	M				H
DIHZ					H		H
CLEAR				H		H	H
BYTE							N

H - High: The CSCI or CSU is directly involved with a critical factor
M - Medium: The CSCI or CSU is indirectly involved or subordinate to a critical factor
N - None: The CSCI or CSU does not impact a safety-critical function.

ALLOCATING RELIABILITY TO SOFTWARE

Table 24: Failure Rate Allocation Based on Criticality

Steps	Description Details of Step Requirements
1	Determine the failure rate goal of the software: λ_s
2	Determine the number of software CSCIs in the aggregate: N
3	For each ith CSCI, i = 1, 2,…………., N determine its criticality factor c_i. The lower the c_i the more critical the CSCI.
4	Determine τ_i the total active time of the ith CSCI, i = 1, 2,…………., N. Determine T the operation time of the aggregate.
5	Compute the failure rate adjustment factor K: $K = \frac{\sum_{i=1}^{N} c_i * \tau_i}{T}$
6	Compute the allocated failure rate goal of each CSCI $\lambda_i = \lambda_s \left(C_i / K \right)$ [Divide K makes the allocated CSCI failure rates build up to the aggregate failure rate goal].

ALLOCATING RELIABILITY TO SOFTWARE

Solution

It is estimated for the Laser to be used to support approximately 1100 potential cases over 10-year service life. Since item 1 control module has the lowest value this indicates that the first CSCI of the software aggregate is the most critical. Let’s Compute the Adjustment Factor K: Substituting respective values in equation below:

$$K = \frac{\sum_{i=1}^{N} c_i * \tau_i}{T} = \frac{(1 \times 0.5) + (4 \times 1.5) + (3 \times 1.5) + (4 \times 1.0) + (5 \times 0.75)}{5.5} = 3.41$$

Then, the allocated failure rate goals of the software CSCI are tabulated in Table 22:

Table 26: Control Module Failure Rate Allocations

Module	Equation	Computation	Allocated Failure Rate
λ_1	λ_s (c_1/K)	0.001 (1/3.41)	0.00029326
λ_2	λ_s (c_2/K)	0.001 (2/3.41)	0.00058651
λ_3	λ_s (c_3/K)	0.001 (3/3.41)	0.00087976
λ_4	λ_s (c_4/K)	0.001 (4/3.41)	0.00117302
λ_5	λ_s (c_5/K)	0.001 (5/3.41)	0.00159236

SOFTWARE RELIABILITY PREDICTIONS AND ESTIMATION MODELS

Table 27: Comparing Prediction and Estimation Models

Issues	Prediction Models	Estimation Models
Data Reference	Utilized Historical Data	Uses data from current software development effort
When Used In Development Cycle	Usually made prior to development or test phases, can be used as early as concept phase	Usually made later in life cycle (After some data has been collected); not typically used in concept or development phases
Time Frame	Predict reliability at some future time	Estimate reliability at either present or some future time

The estimation of remaining errors in the software is the deciding factor for the release of the software or the amount of more testing which is required. Software growth reliability models are used for the correct estimation of the remaining errors.

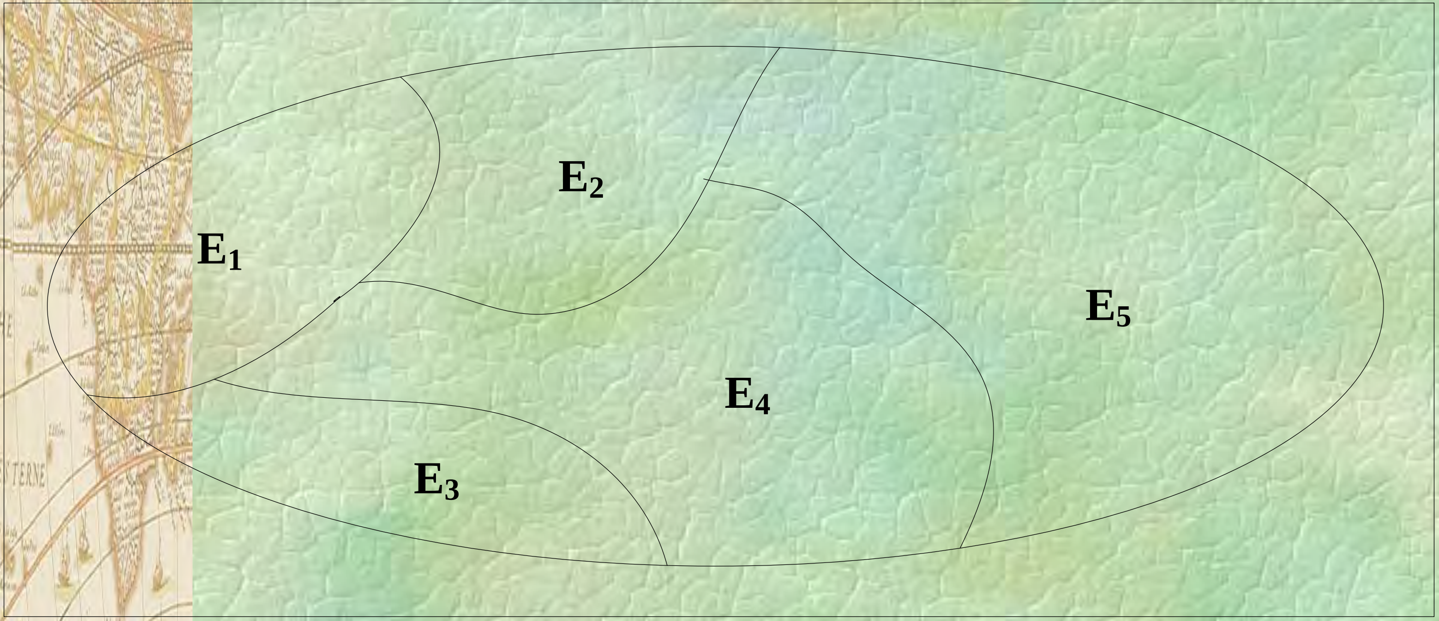
SW RELIABILITY MODEL Applications

Example Applications

- Table 30 illustrates an example using Figure 22 Input Domain. Each row represents the data of each equivalence class, i.e., E1, E2, E3, E4, and E5. The estimated reliability of the Input Domain is 1 minus the sum of the equivalence class reliabilities from the fifth column.
- As calculated for this example the total estimated reliability of this Input Domain is 0.94.
- **Summary of Input Domain Modeling Steps:**
  1. Determine the operational profile
  2. Define a partition of the input domain and assign operational probabilities to the equivalence classes in the partition
  3. Define failures
  4. Select a set of test cases for each equivalence class
  5. Run the tests
  6. Estimate the reliability.

SW RELIABILITY MODEL Applications

Figure 22: Input Domain Partitioned Into Sub-domains



SW RELIABILITY MODEL Applications

Table 30: Example of Input Domain Model Calculation

Equivalence class	Parameters			
	$P(E_1)$	n_1	f_1	$P(E_i)\frac{f_i}{n_i}$
1	0.20	20	2	0.0200
2	0.15	30	1	0.0050
3	0.50	40	2	0.0250
4	0.10	20	1	0.0050
5	0.05	30	3	0.0050
Total Estimated Reliability = $1-\sum P(E_1)\frac{f_1}{n_1} = 1-0.00600=0.9400$				

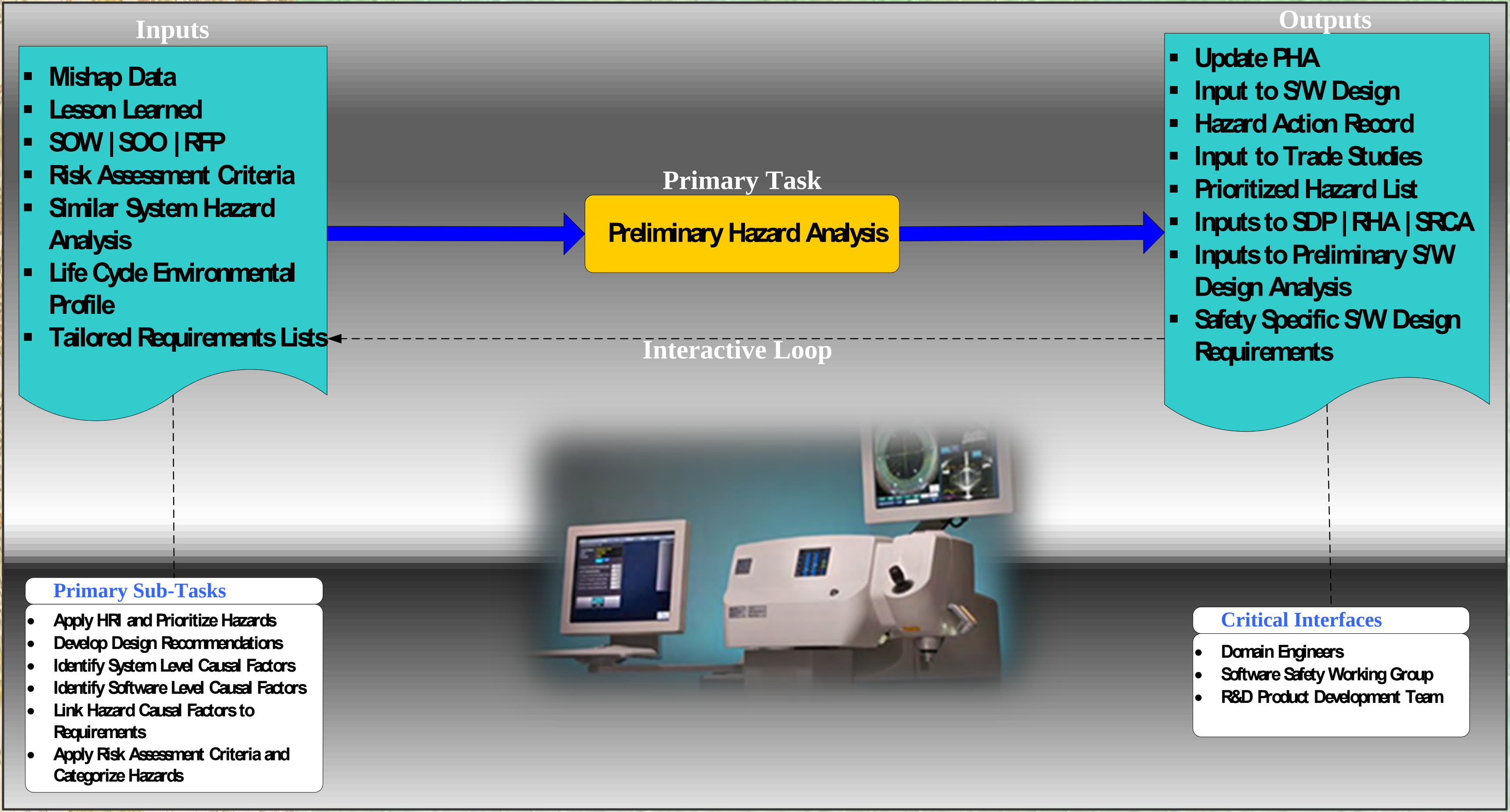
SOFTWARE IN SAFETY CRITICAL SYSTEMS

Classification of Critical Systems

- Software controlled systems where failures can result in significant economic losses, physical damage or threats to human life are usually called critical systems.
- The system may be software-controlled so that the decisions made by the software and subsequent actions are safety critical.
- Software is extensively used for checking and monitoring other safety critical components in a system.
- Types of Critical Systems:
  1. Safety Critical Systems – A system whose failure may result in injury, loss of life, or major environment damage [Laser eye surgery device].
  2. Mission Critical Systems - A system whose failure may result in the failure of some goal-directed activity [navigation system of spacecraft]
  3. Business Critical Systems - A system whose failure may result in the failure of the business using that system [customer account system in a bank].
- Embedded software systems whose failure can cause the associated hardware to fail and directly threaten people [Insulin pump control system].

DERIVE SAFETY-CRITICAL SOFTWARE REQUIREMENTS

Figure 28: Preliminary Hazard Analysis



Inputs

- Mishap Data
- Lesson Learned
- SOW | SOO | RFP
- Risk Assessment Criteria
- Similar System Hazard Analysis
- Life Cycle Environmental Profile
- Tailored Requirements Lists

Primary Task

Preliminary Hazard Analysis

Outputs

- Update PHA
- Input to S/W Design
- Hazard Action Record
- Input to Trade Studies
- Prioritized Hazard List
- Inputs to SDP | RHA | SRCA
- Inputs to Preliminary S/W Design Analysis
- Safety Specific S/W Design Requirements

Interactive Loop

Primary Sub-Tasks

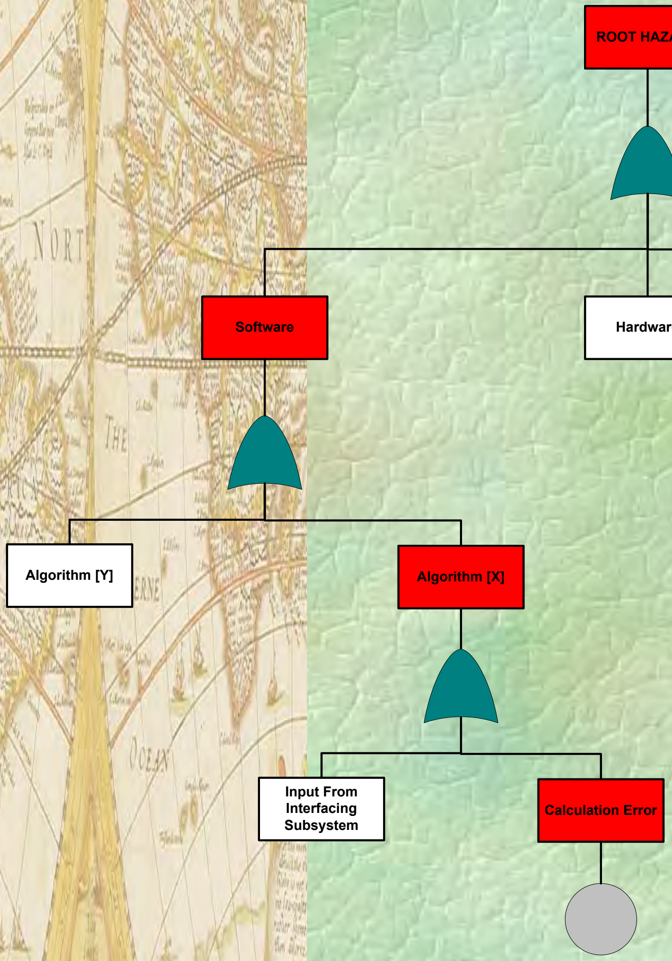
- Apply HRI and Prioritize Hazards
- Develop Design Recommendations
- Identify System Level Causal Factors
- Identify Software Level Causal Factors
- Link Hazard Causal Factors to Requirements
- Apply Risk Assessment Criteria and Categorize Hazards

Critical Interfaces

- Domain Engineers
- Software Safety Working Group
- R&D Product Development Team

MATURED SOFTWARE SAFETY REQUIREMENTS

Figure: 29 – In-Depth Hazard Cause Analysis



Root Analysis

- Interface
- Failure Mode
- Hazard Analysis

In-Depth Analysis

- Algorithm
- Calculations
- Sequence Timing
- CSU and SRS Requirements

– Proactive Innovative Solutions for Success and Competitive Advantages

EVALUATING SOFTWARE SAFETY

Safety Analysis Techniques

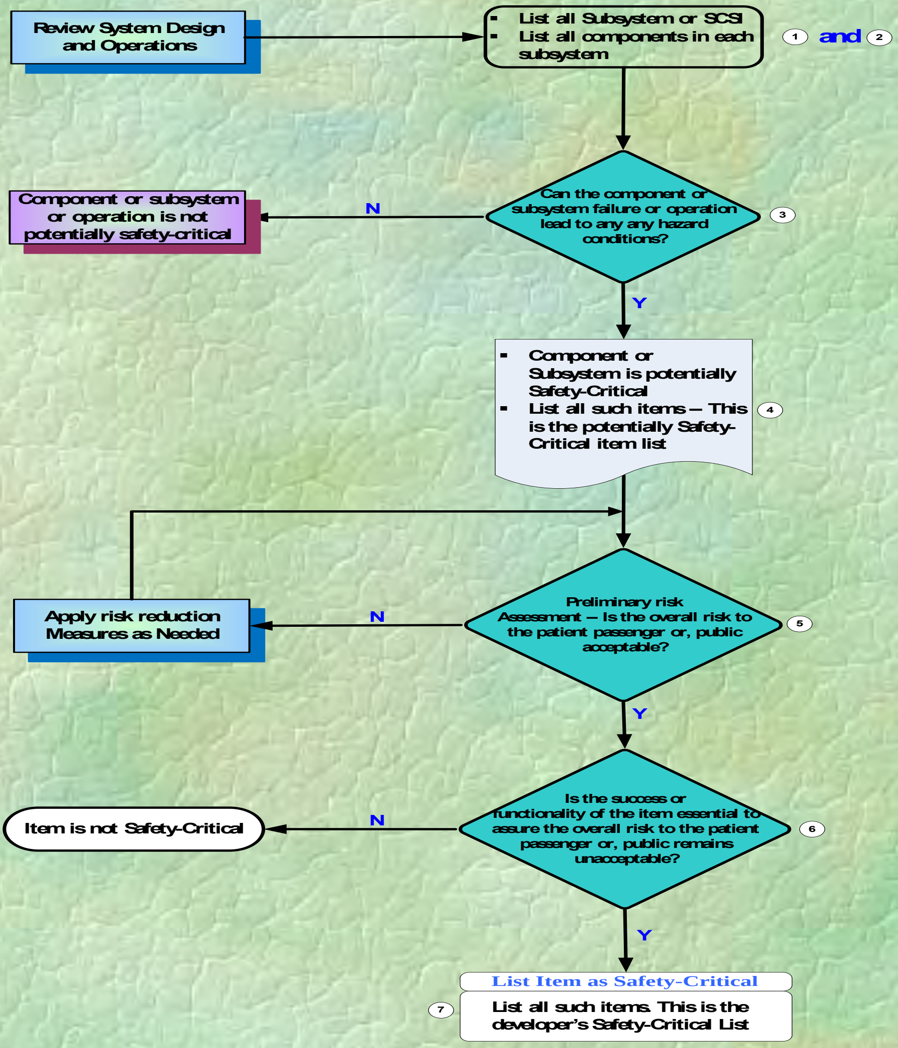
- Current Analysis techniques and methodologies available for conducting software safety analyses includes:

  1. Petri net Analysis
  2. Code Walk Through
  3. Design Walk Through
  4. Sneak Circuit Analysis
  5. Safety Cross Check Analysis
  6. Software Fault Tree Analysis
  7. Preliminary Hazard Analysis
  8. Failure Modes and Effect Analysis
  9. Software | Hardware Integrated Critical Path Analysis

- A systematic, logical, disciplined System Safety Process generally consists of one or more of these analyses and procedures undertaken as part of the design and development effort to ensure system safety.

SAFETY CRITICALITY ASSESSMENT

Figure: 31 – Flowchart of Safety-Critical Methodology



Review System Design and Operations

- List all Subsystem or SCSI
- List all components in each subsystem

1 and 2

Can the component or subsystem failure or operation lead to any any hazard conditions?

3

N

Component or subsystem or operation is not potentially safety-critical

Y

- Component or Subsystem is potentially Safety-Critical
- List all such items – This is the potentially Safety-Critical item list

4

Preliminary risk Assessment – Is the overall risk to the patient passenger or, public acceptable?

5

N

Apply risk reduction Measures as Needed

Y

Is the success or functionality of the item essential to assure the overall risk to the patient passenger or, public remains unacceptable?

6

N

Item is not Safety-Critical

Y

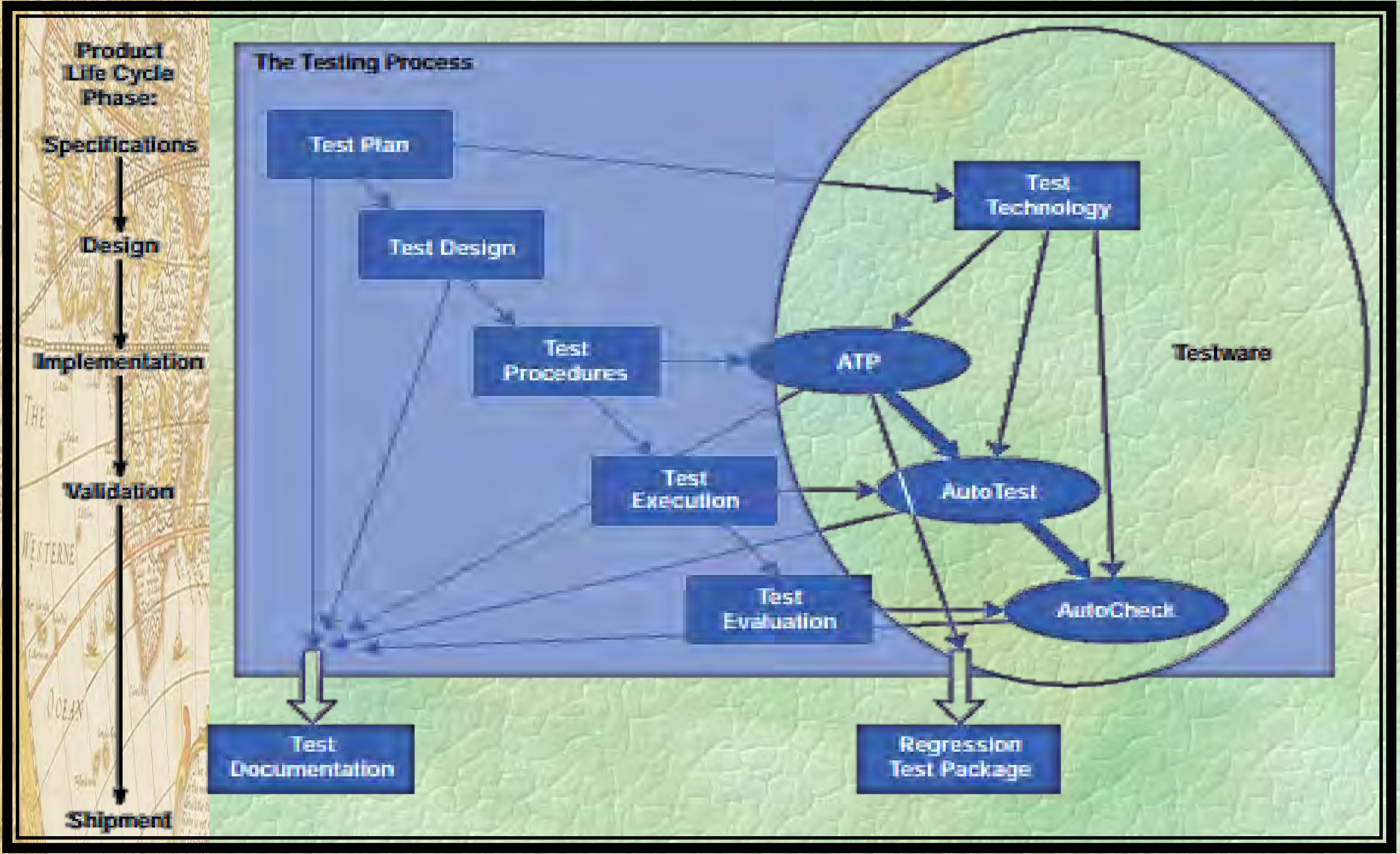
List Item as Safety-Critical

7

List all such items. This is the developer's Safety-Critical List

Testing Safety-Critical Software

Figure: 32 – The Software Testing Process for HP OmniCare Patient Monitors.

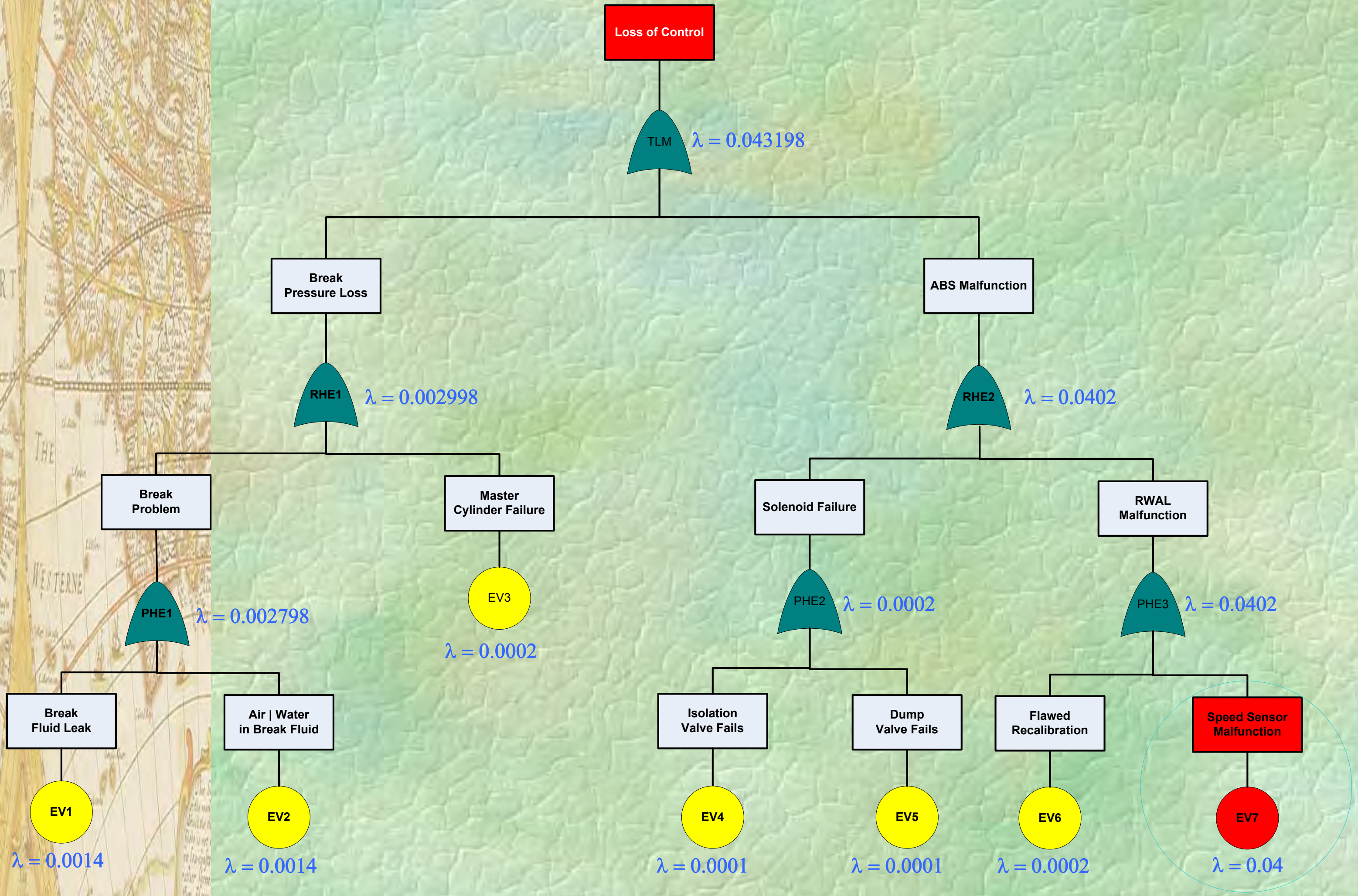


Source: June 1997 Hewlett-Packard Journal

Copyright © 2016 LEBENTECH ® – Proactive Innovative Solutions for Success and Competitive Advantages

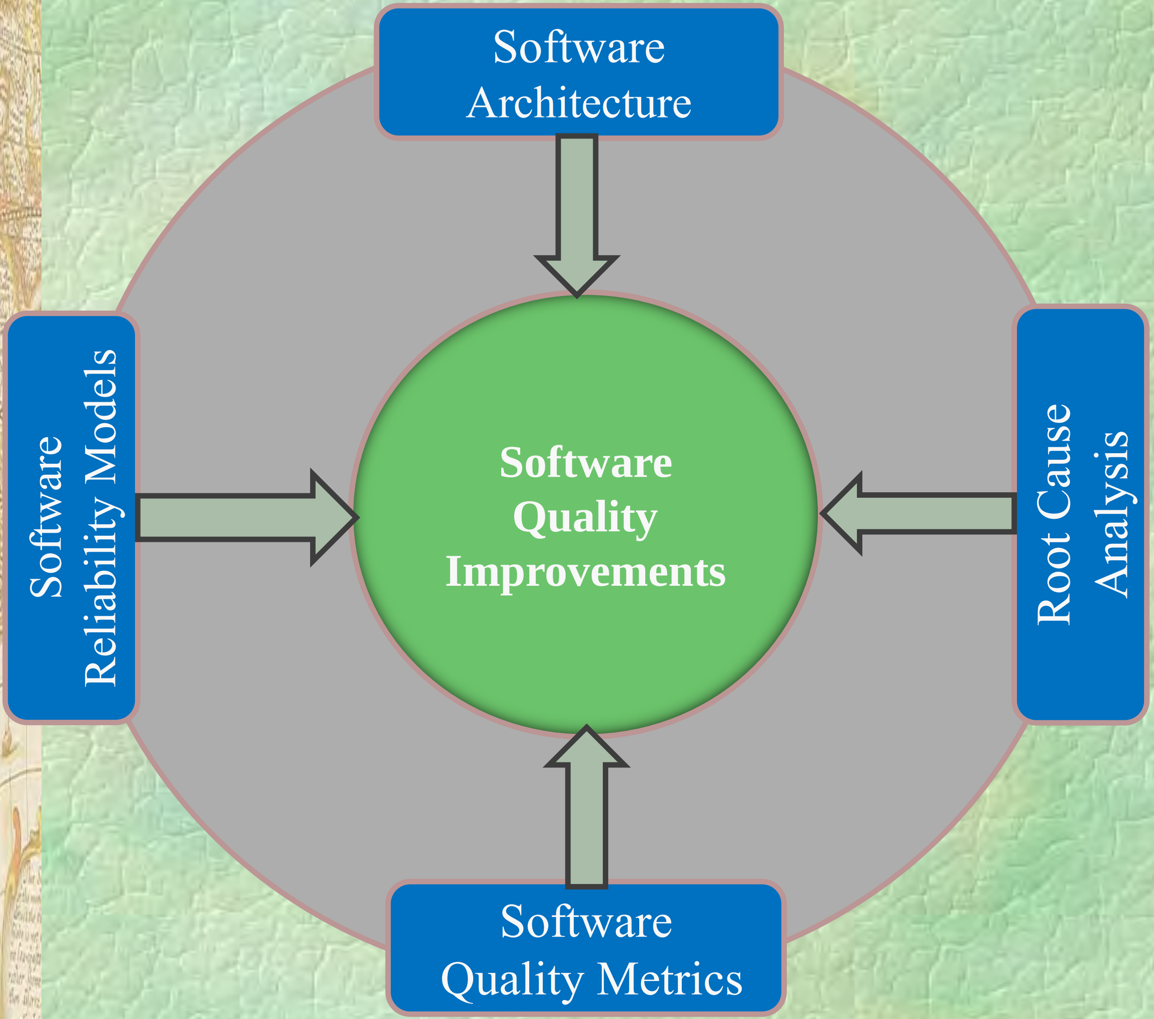
CASE STUDY APPLICATION

Figure 35: ABS Fault Tree Analysis – Faulty Sensor Case



SOFTWARE DESIGN RELIABILITY IMPROVEMENT

Figure 36: Software Quality Improvement Factors



M8 – SEC 2 - LEARNING OBJECTIVES

Participant shall be able to:

- Distinguish between defect testing and statistical testing and identify rules that governs testing.
- Identify sequence of stages to achieve design for reliability in future.
- List one or more reasons for testing software and identify specific phase of the lifecycle when specific testing is executed.
- Utilize test coverage methodology to determine software reliability.
- Understand the various testing methods that can be used to discover software faults and strategies that can be applied to determine reliability.
- Distinguish between defect testing, functional testing, statistical usage testing and acceptance testing.
- Learn how to select an acceptance sampling plan for reliability demonstration.

Adapt | Implement | Improve

SOFTWARE RELIABILITY PLANNING

Early Test Design

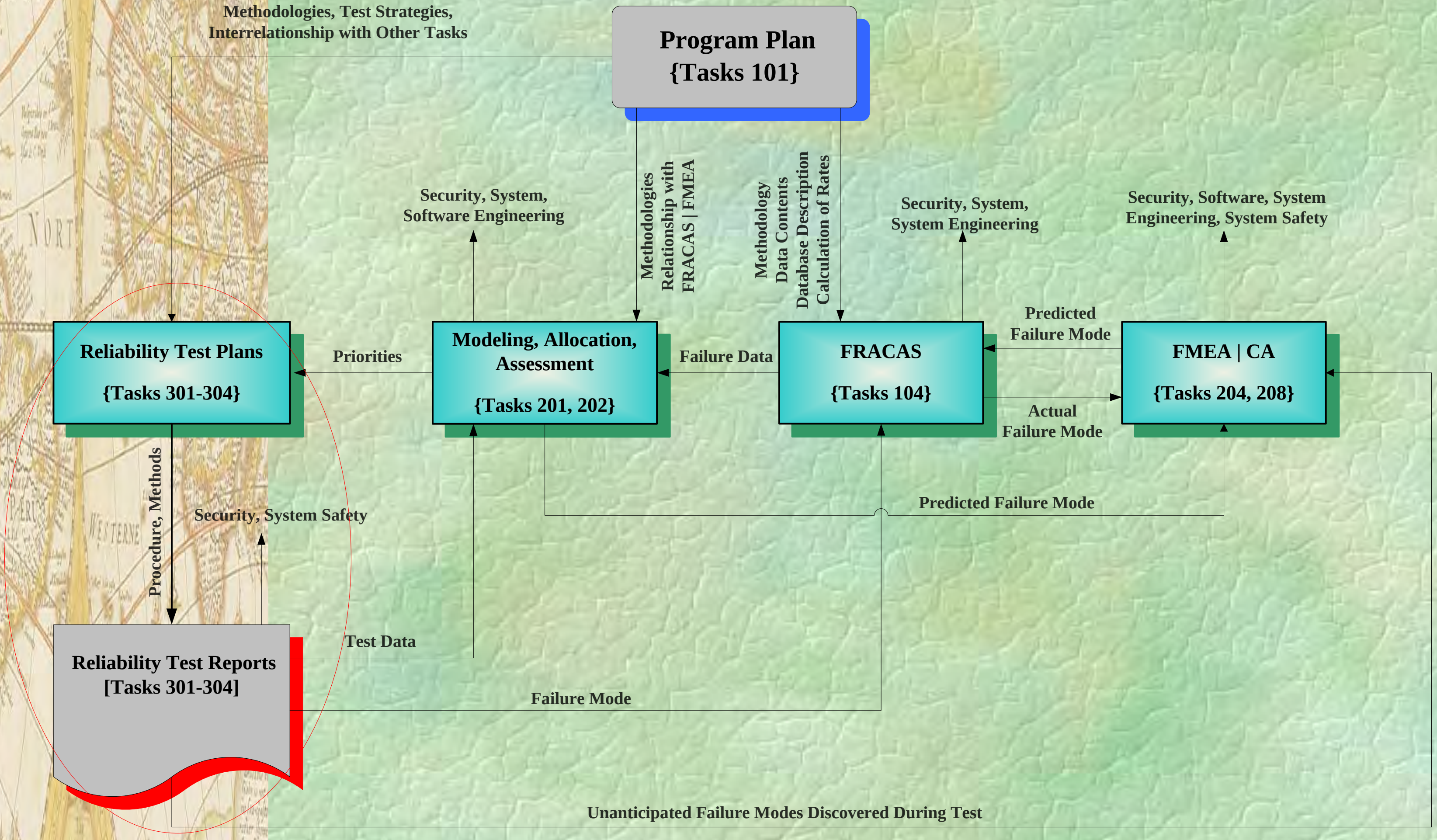
- Test Design find faults.
- Faults found early are cheaper to fix
- Most significant faults found first
- Faults prevented, not built inst design
- No additional effort, re-schedule test design
- Changing requirements caused by test design

Software testing involves executing and implementation of the software with test data and examining the outputs of the software and its operational behavior to check that it is performing as required.

Early test design helps to build quality, stops fault multiplication

SOFTWARE RELIABILITY PLANNING

Figure 1: Reliability Program for a Software-intensive System



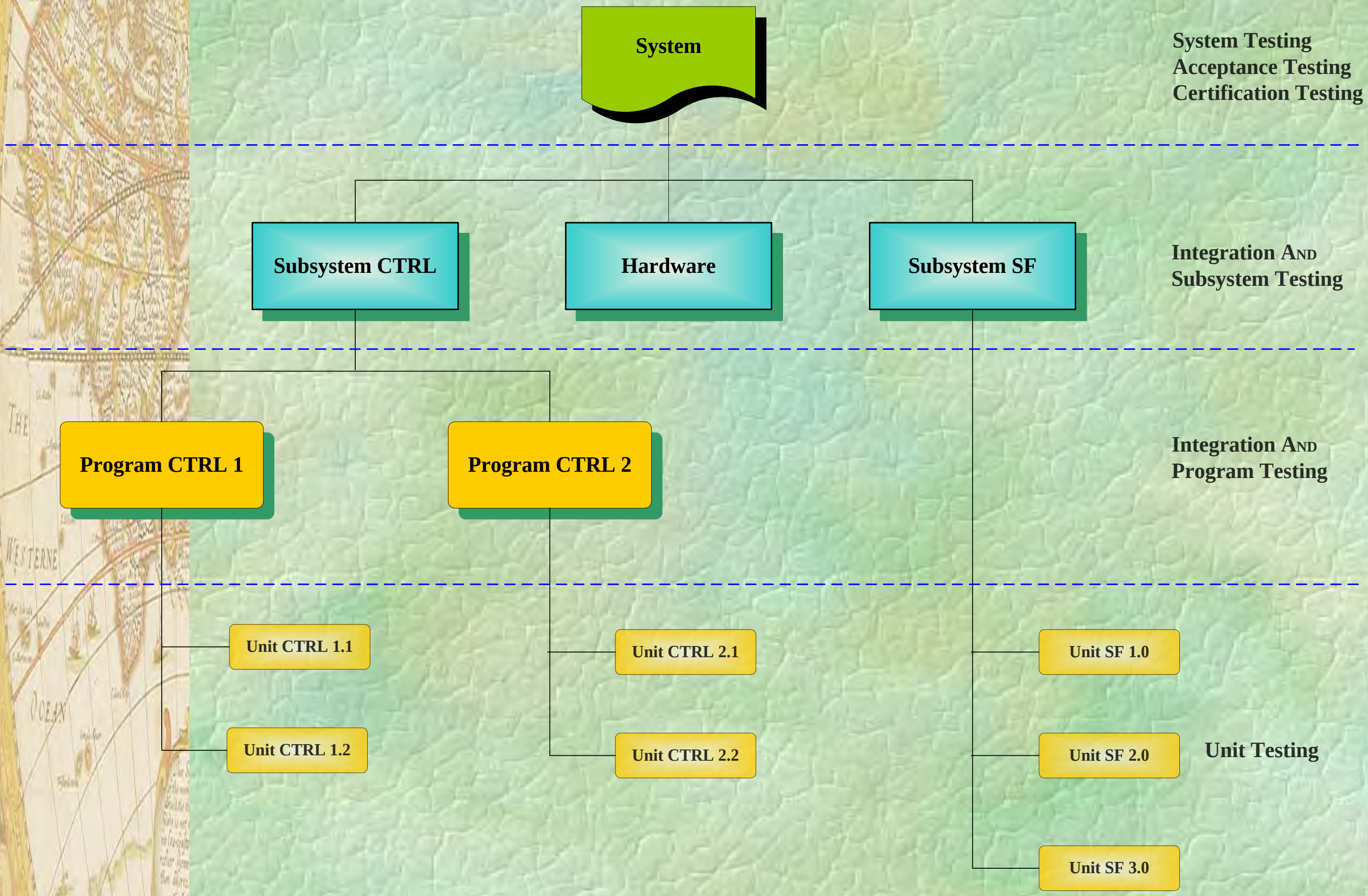
SOFTWARE VERIFICATION AND VALIDATION PLANNING

Table 1: Reasons for Testing Software

Item No.	Reason	Comments
1	Detect, expose and correct defect	Defect can be in a code, requirements and/or design. Gives programmers information they can use to prevent future defects
2	Demonstrate that requirements have been satisfied	The rationale for any test should be directly traceable to a customer requirement
3	Assess whether the software is suitable to meet the customer's need	Give management the information it needs to assess potential risks associated with the product
4	Calibrate Performance	Measuring processing speed, response times, resource consumptions, throughput and efficiency
5	Measure Reliability	Quantify the reliability of the software for the customer [reliability demonstration], or for internal improvements [reliability growth] prior to delivery to customer
6	Ensure change modifications have not introduce new faults	Referred to as regression testing
7	Establish due diligence for protection against product liability litigations	May provide some level of protection against [justifiably or unjustifiably] dissatisfied customer

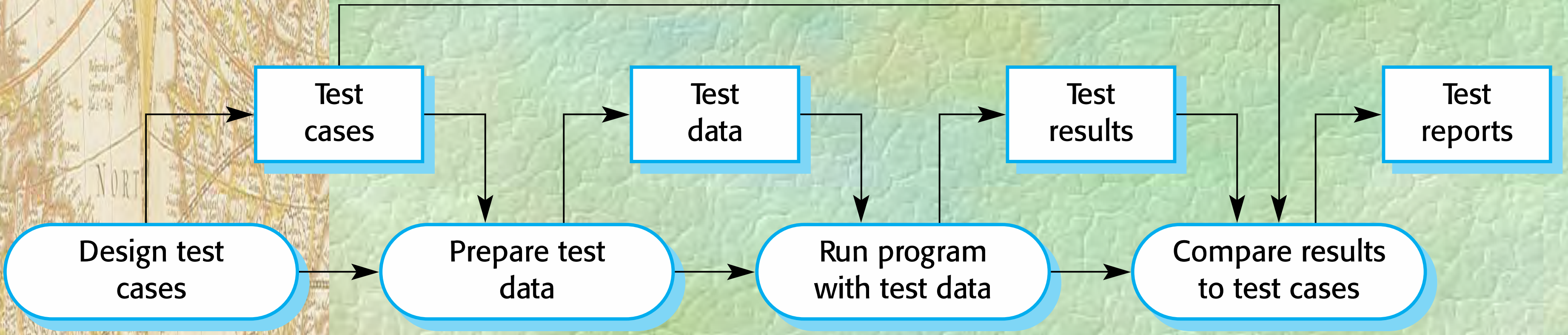
SOFTWARE VERIFICATION AND VALIDATION PLANNING

Figure 4: Level Of Software Testing



A Model of the Software Testing Process

Figure 8: The Defect Testing Process



- Defect testing is intended to find inconsistencies between a program a specification.
- These inconsistencies are usually due to program faults or defects.
- The tests are designed to reveal the presence of defects in the system rather than to stimulate operational use.

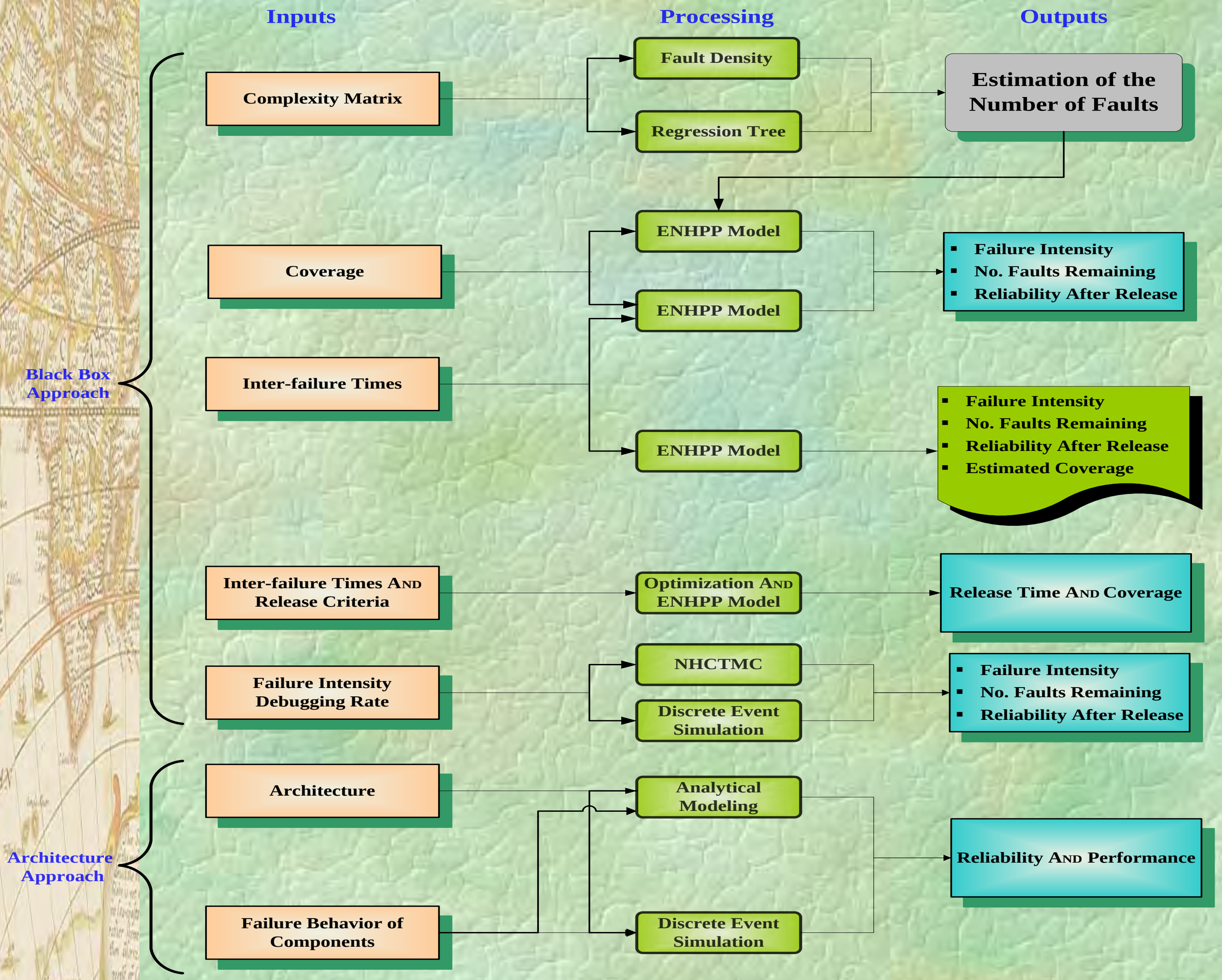
SOFTWARE VERIFICATION AND VALIDATION PLANNING

Table 2: Summary of Key Tests Executed in Software Validation

Item No.	Software Test	Comments
1	Unit	Demonstrates correct functionality of critical software elements
2	Interface	Shows that critical computer software units execute together as specified
3	System	Demonstrates the performance of the software within the overall system
4	Stress	Confirms the software will not cause hazards under abnormal circumstances, such as unexpected input values or overload conditions
5	Regression	Demonstrates changes made to the software did not introduce conditions for new hazards
6	Statistical Testing	This type of testing is used to test the program's performance and reliability and check how it works under operational conditions
7	Acceptance Testing	Verifies software acceptability based on input of operational usage that are generated

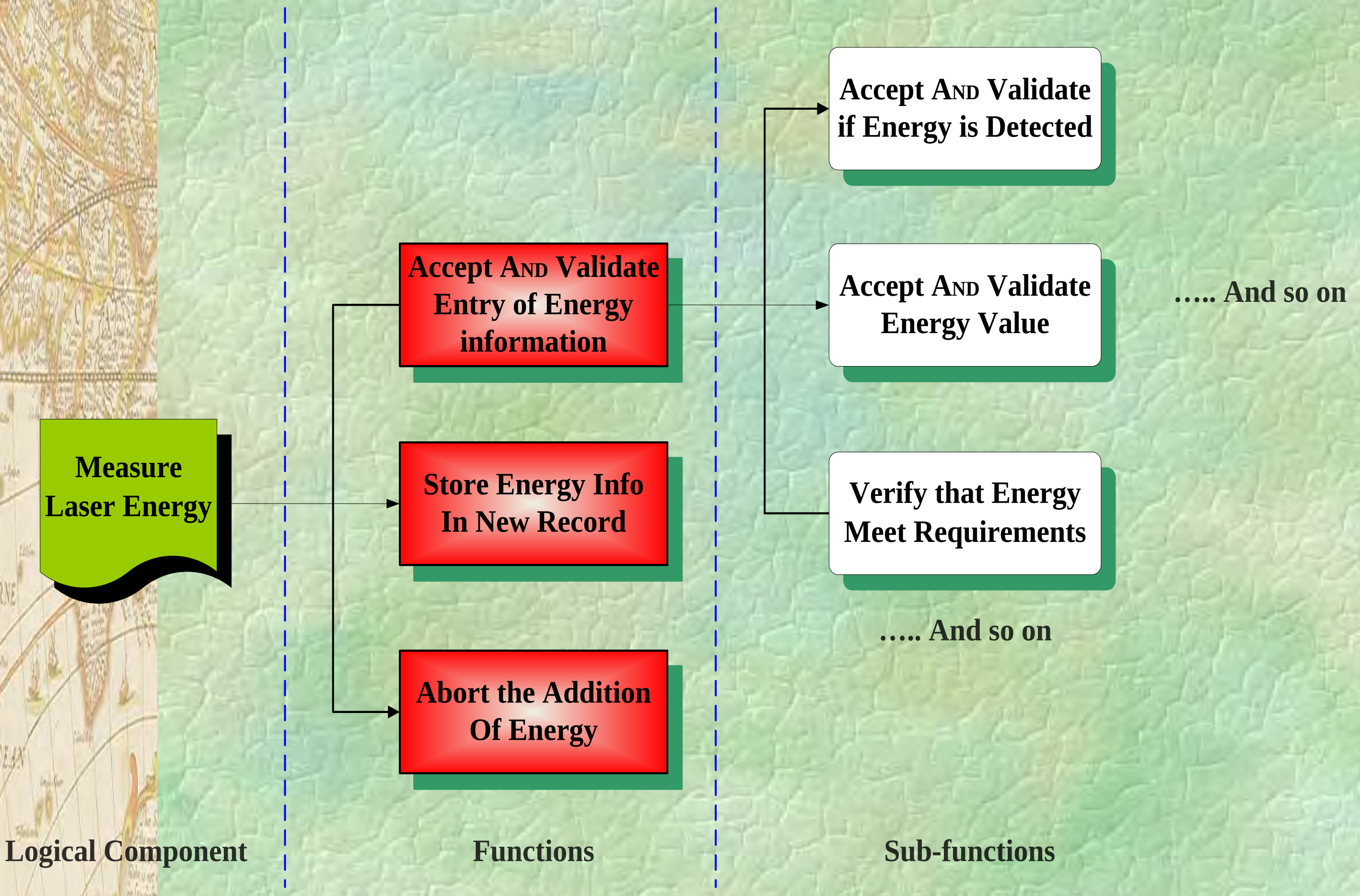
SOFTWARE TESTS WITH SPECIFIC OBJECTIVES

Figure 20: Architecture SREPT


Inputs
Processing
Outputs
Black Box Approach
Complexity Matrix
Fault Density
Regression Tree
Estimation of the Number of Faults
Coverage
ENHPP Model
ENHPP Model
Failure Intensity
No. Faults Remaining
Reliability After Release
Inter-failure Times
ENHPP Model
Failure Intensity
No. Faults Remaining
Reliability After Release
Estimated Coverage
Inter-failure Times And Release Criteria
Optimization And ENHPP Model
Release Time And Coverage
Failure Intensity Debugging Rate
NHCTMC
Discrete Event Simulation
Failure Intensity
No. Faults Remaining
Reliability After Release
Architecture Approach
Architecture
Analytical Modeling
Reliability And Performance
Failure Behavior of Components
Discrete Event Simulation

FUNCTIONAL SYSTEM TESTING

Figure 17: Function and Sub-function List Example



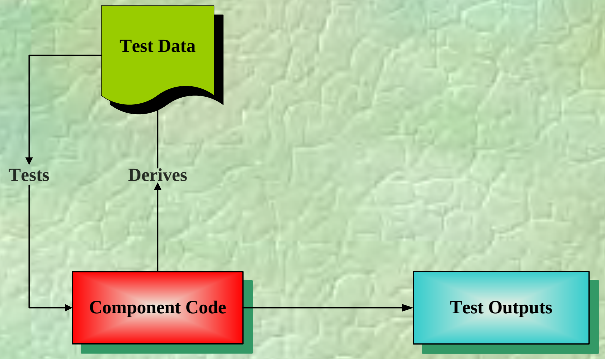
Measure Laser Energy
Accept And Validate Entry of Energy information
Store Energy Info In New Record
Abort the Addition Of Energy
Accept And Validate if Energy is Detected
Accept And Validate Energy Value
Verify that Energy Meet Requirements
….. And so on
….. And so on
Logical Component
Functions
Sub-functions

SOFTWARE TESTS WITH SPECIFIC OBJECTIVES

White Box Testing Methodology

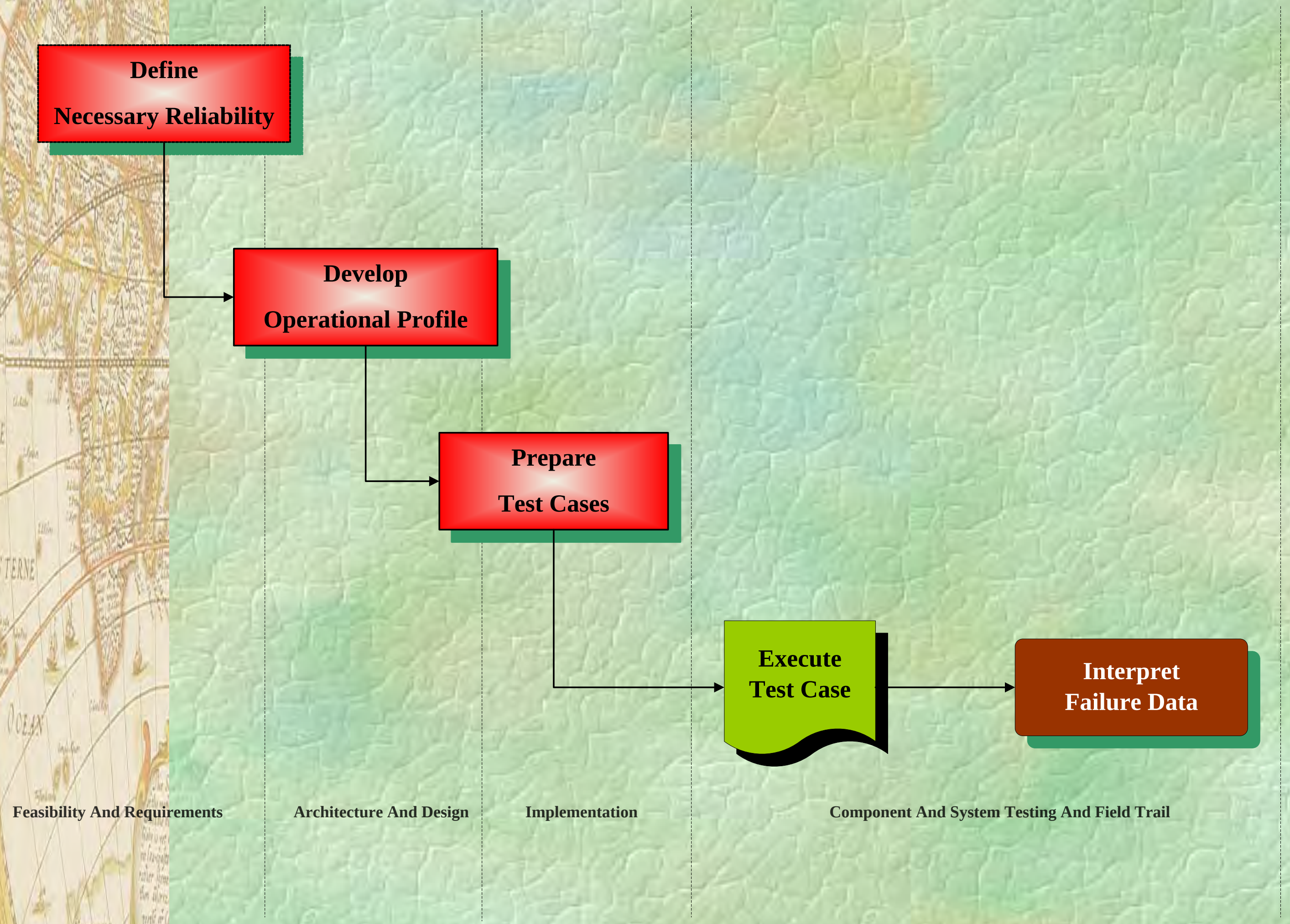
- White Box testing, or structural testing, which is an analysis of the details of the structure of the program, coding, language, and data base design.
- Structural testing is an approach to testing where the tests are derived from knowledge of the software structure's and implementation.
- Structural testing is usually applied to relatively small program units such as sub-routines or the operations associated with an object.
- The analysis of the code can be used to determine how many test cases are needed to guarantee that all the statements in the program or component are executed at least once during the testing process.

Figure 21: Structural Testing



SOFTWARE RELIABILITY TESTING PROCESS

Figure 6: Software Reliability Engineering Testing Process [SRETP]



SW TEST COVERAGE APPLICATION

Example Application

- Table 7 list the respective proportional variable, corresponding ratios and one weighting scheme.

Table 7: Test Coverage Weightage Factors

Variables	Ratios	Weighted Importance	Value
a	0.95	W_1	0.10
b	0.99	W_2	0.15
c	0.98	W_3	0.15
d	0.96	W_4	0.60

- For the purpose of test coverage reliability, it has been analytically determined that the total number of failure modes addressed (parameter “d”) is the most important.
- The total number of inputs tested (parameter “b”) and the total number of functions verified (parameter “c”) are equally important.
- Of the least important is the total number of independent path tested (parameter “a”).

SW TEST COVERAGE APPLICATION

Example Application

- The resulting test coverage reliability is calculated to be:

$$R = \frac{(0.95 * 0.10) + (0.99 * 0.15) + (0.98 * 0.15) + (0.96 * 0.60)}{0.10 + 0.15 + 0.15 + 0.60} = \frac{0.9665}{1} = 0.9965$$

- A second weighting scheme of w1 = 0.05, w2 = 0.25, w3 = 0.25, and w4 = 0.45, using the same values for the four proportional variables, provides different results:

$$R = \frac{(0.95 * 0.25) + (0.99 * 0.25) + (0.98 * 0.25) + (0.96 * 0.45)}{0.05 + 0.25 + 0.25 + 0.45} = \frac{0.972}{1} = 0.972$$

- Comparing the two weighted results with the test coverage reliability when all factors are weighted equally:

$$R = \frac{(0.95 * 1) + (0.99 * 1) + (0.98 * 1) + (0.96 * 1)}{1 + 1 + 1 + 1} = \frac{3.88}{4} = 0.97$$

SOFTWARE TESTS WITH SPECIFIC OBJECTIVES

Reliability | Qualities

- It is very important to understand the quality characteristics you want to verify during testing.
- Determine the approach based on your reliability testing objectives and apply methods based anticipated output.
- Software Reliability:
  1. System will be reliable – How to test this?
  2. 2 failures per year over ten years
  3. Mean Time Between Failures [MTBF]
  4. Reliability Growth Models
- Other Qualities
  1. Maintainability, portability, adaptability, etc.

SOFTWARE ACCEPTANCE TESTING

Software Reliability Testing

This is the final stage in the testing process before the system is accepted for operational use. At this stage the recommendation is for the software engineer to provide data for the system test instead of simulated data. It is expected that this test will reveal errors and omission in the system requirement definitions. It should also reveal requirement problems where system's facilities do not really meet the user's need or the system performance is unacceptable.

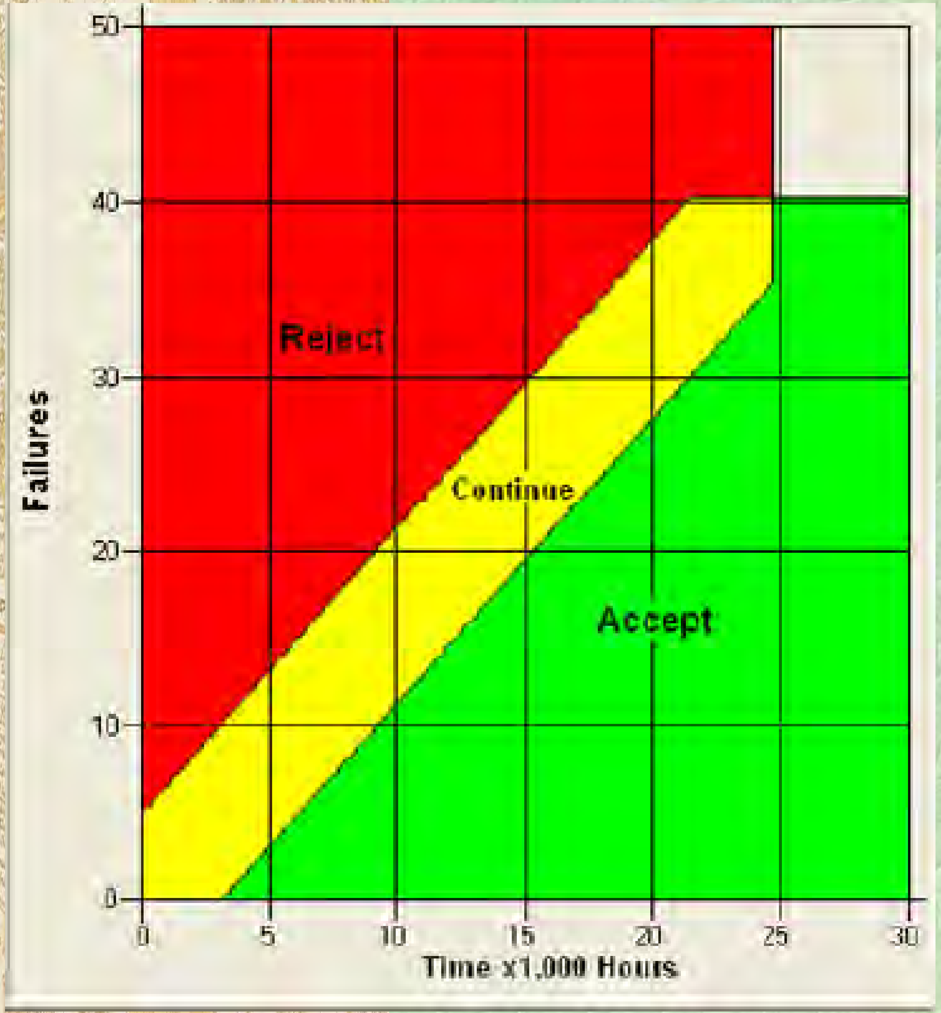
Software System shall be verified and accepted by performing Reliability Demonstration Test (RDT). The Failure Free Execution Test/Fix Duration Test shall be executed to accept or reject software performance. Producer's and consumer's risk shall range from 10% (Low risk) to 30% (High risk).

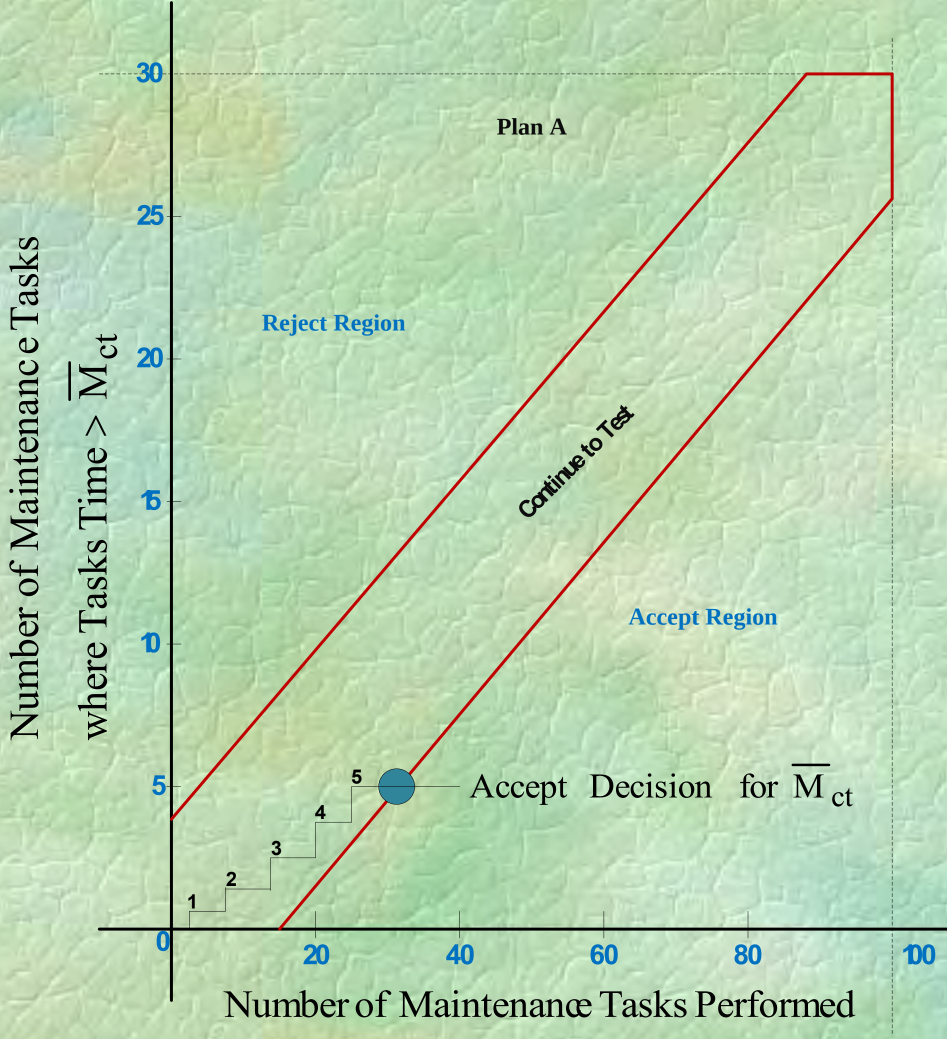
For Fixed Test Plan: Lower MTBF θ_1 = X Hours, Producer's and Consumer's risk = 20% and Reliability Goal = 1000 hours to failure.

For Failure Free Execution Test Plan: λ_1 = 0.0001 Failures/Hr, Producer's and Consumer's risk = 30%, and reliability goal for software λ_0 = 0.00005 Failures /Hr

SOFTWARE DESIGN ANALYSIS

Figure 24: **Reliability Demonstration Testing**





Further Application of Software Reliability Model

Musa’s Basic Model

- Assumption: Decrement in failure intensity function is constant.
- Results: Failure intensity is a function of average number of failures experienced at any given point in time [= failure probability]:

$$\lambda(\mu)=\lambda_0\left[1-\frac{\mu}{v_0}\right]$$

- Where:

  1. $\lambda(\mu)$: Failure Intensity
  2. λ_0: Initial failure intensity at start of execution
  3. μ: Average total number of failures at a given point in time
  4. -v_0 = Total number of failures over infinite time

Further Application of Software Reliability Model

Example 1

- Let’s assume that we are at some point in time t time units in the life cycle of a software system after it has been deployed.
- Let’s also assume that the program will experience 120 failures over infinite execution time. During the last t time unit interval 60 failures have been observed [and counted0. The initial failure intensity was 10 failures per CPU hour.
- Compute the current [at t] failure intensity:

Solution

$$\lambda(\mu)=\lambda_0\left[1-\frac{\mu}{v_0}\right]$$

- Substitute respective values in equations

$$\lambda(60)=10*\left[1-\frac{60}{120}\right] = 5\left[\frac{\text{failures}}{\text{CPU Hour}}\right]$$

Achieving Design for Reliability

Sequence of Stages to Achieve DFR

- To achieve reliable system design, fault tolerance mechanism needs to be in place. A typical response to system or software faults during operation includes a sequence of stages:
- **Fault Confinement.** This stage limits the spread of fault effects to one area of the system, thus preventing contamination of other areas. Fault-confinement can be achieved through use of self-checking acceptance tests, exception handling routines, consistency checking mechanisms, and multiple requests/confirmations.
- **Fault Detection.** This stage recognizes that something unexpected has occurred in the system. Fault latency is the period of time between the occurrence of a software fault and its detection.
  1. Off-line techniques such as diagnostic programs can offer comprehensive fault detection, but the system cannot perform useful work while under test.
  2. On-line techniques, such as watchdog monitors or redundancy schemes, provide a real-time detection capability that is performed concurrently with useful work.
- **Diagnosis.** This stage is necessary if the fault detection technique does not provide information about the failure location and/or properties.

Achieving Design for Reliability

Sequence of Stages to Achieve DFR

- **Reconfiguration**. This stage occurs when a fault is detected and a permanent failure is located.
  1. The system may reconfigure its components either to replace the failed component or to isolate it from the rest of the system.
  2. Successful reconfiguration requires robust and flexible software architecture and the associated reconfiguration schemes.
- **Recovery**. This stage utilizes techniques to eliminate the effects of faults. Two basic recovery approaches are based on: fault masking, retry and rollback.
  1. Fault-masking techniques hide the effects of failures by allowing redundant, correct information to outweigh the incorrect information. To handle design (permanent) faults, N-version programming can be employed.
  2. Retry, on the other hand, attempts a second try at an operation and is based on the premise that many faults are transient in nature.
- **Restart.** This stage occurs after the recovery of undamaged information. Depending on the way the system is configured, hot restart, warm restart, or cold restart can be achieved.

CONCLUSION

Why should Companies Invest in Software Reliability?

- Will Determine Whether Defects are Predicted.
  1. Before code is written or
  2. During testing or Never
- Performance Measurements Accessed
  1. Normalized fielded defects [defect density]
  2. Minimize probability of late delivery
  3. Magnitude of late deliveries as a percentage of original schedule
  4. Existence of development practices, organization philosophy, methods, tools, process.
  5. Type of application, industry, duty cycle
  6. Product characteristics related to requirements, design, and code.

Source: Ann Marie Neufelder – These factors were measured on 28 real organizations developing real time software.

THE END

Thank You
for
Listening

Questions
and
Comments