Reliability Issues From A Management Perspective

H. Paul Barringer, P.E.
Barringer & Associates, Inc., P. O. Box 3985, Humble, TX 77347-3985
Phone: 281-852-6810, FAX: 281-852-3749, e-mail: hpaul@barringer1.com

Abstract

Reliability for businesses begins with management. Management must communicate with a clear reliability policy statement. The policy can mobilize actions for considering cost of alternatives to prevent or mitigate failures, which require knowledge about times to failure, and failure modes, found by reliability technology. Justifications for reliability improvements require knowing: 1) when things fail, 2) how things fail, and 3) conversions of failures into time and money statements. Reliability engineering principles help define when and how things fail to provide facts for life cycle costs comparisons. This helps decide the lowest long-term cost of ownership driven by a single estimator called net present value for converting hardware issues and alternatives into money issues. Several short examples illustrate the methodology.

Reliability

Components, equipment, systems, and people are not perfect and free from failures. In a naïve, simplistic and deterministic view we can have perfection. However, in the real world we fall short of perfection, as perfection exists only in a fantasy world. Everything fails—in the end the worms have us all and the same is true for our systems. A natural law of entropy expresses the lowest energy state is a failure—buildings always fall down, they never fall up. Thus we spend time and resources mitigating effects of failures. Nothing lasts forever without failure. Consider the status of the seven ancient wonders of the world, learned by every school child, and only one exists intact today (the pyramids—and they're starting to look a little ragged!).

Reliability is the probability that a component, system, or process will function without failure for a specified length of time when operated correctly under specified conditions. Reliability engineering is concerned with predicting and avoiding failures—this is a strategic task. To quantify reliability issues it is important to know ***why***, ***how***, ***how often***, and ***costs*** of failures. Reliability issues are bound to the physics of failure mechanisms so the failure mechanisms can be mitigated. In the real world all potential failures are seldom well known or well understood, and prediction of failures is inherently a probabilistic problem where reliability analysis is a probabilistic process.

Reliability is not the same as availability even though both are described as a value between 0 and 1. Availability tells the percent of time the system is alive and ready for use if called upon, and stream factors define the actual online times as a percentage of up time. Reliability addresses the probability for a failure free interval under specific conditions. The complement to the sweet portion of reliability (absence of failures) is the probability of failure--the sour part of reliability.

Risk assessment models connect money with failures in a simple equation: $Risk = (probability of failure during a specified time interval and under specific conditions)*($Consequence of the failure event). $Risks always exist, and they are never zero. How much $Risk is affordable becomes a business issue. If the business organization is risk averse, then perhaps $Risk values must be less than say $10,000, or if risk accepting, then less than say $100,000. Set the actual $Risk value as a business decision rather than "backing into it" by failure to make a decision. Society expects planning for success and rejects abnormal $Risks.

What does your reliability policy say?

Management presents important issues to the organization with policy statements. Policies define specific areas of concern and indicate the desired outcome. Policies increase decisiveness by removing uncertainty about action required to meet the objective. Policy statements communicate information to the staff in general terms for detailed implementation by procedures in a consistent fashion through individual acceptance and individual commitment. Good policies reduce the potential for bad events such as inefficiency, counter productivity, inappropriate risk taking, and conflicts over requirements so that nothing is implemented because of the void.

Modern organizations have safety policies and quality policies. Before safety and quality policies, both areas originally operated with "Everyone knows what to do, we don't need a policy." Prior to policies injury rates were high and quality was poor. After policies it was clear the safety goal was zero injuries and the quality goal was full conformance to the requirements. Reliability issues need a clear and concise policy statement to avoid fuzzy interpretations.

Management has the responsibility to approve, distribute, educate, and train the organization in the requirements for reliability as a display of leadership. If management thinks, "everyone knows the requirements for reliability", expect the '50's mentality that will result in the same inconsistent results observed before safety and quality policies were taken seriously. When "everyone knows" (but few really know), expect to find inappropriate risks are taken without a consistent plan and the lack of consistency will exist within the organization where too many decisions are made on first costs rather than life time costs using net present value considerations for alternatives (notice the word alternatives is plural).

Without a reliability policy, pipeline managers only rely on the minimum standards from:

- AIAA (**http://store.aiaa.org**) recommended practices for software reliability;
- AIChE (**http://www.aiche.org/pubcat**) guidance for layers of protection and guidelines for preventing human error in process safety;
- API (**http://www.api.org**) standards, publications and recommended practices for pipelines;
- IEC (**http://www.iec.ch/seatop-e.htm**) reliability, dependability, and functional safety instrumented systems for the process industry guidelines and standards;
- IEEE (**http://shop.ieee.org/store**) reliability of power, instruments, and software and a variety of testing programs along with design details and guides for improving reliable human performance, safety systems for nuclear plants, maintenance standards, interconnecting networks for multiprocessors, computers and telecommunication systems, recommended practices for emergency and standby power systems, uninterruptible power system guides, and mission critical facility operations;
- ISA (**http://www.isa.org/reference/search.cfm**) standards for safety instrumented systems (SIS) for process safety (now a OSHA preferred standard); emergency shutdown systems; and
- USDOT (**http://ops.dot.gov/sear.htm**) pipeline safety regulations.

Individual minimum standards are similar to individual business tactics. First you must have a planned strategy and then you develop the tactics. Remember, the above standards/guidelines are **minimum requirements** set by outside interest. Minimum standards do not address extra requirements for business issues and potential for community outrage problems from pipeline failures. Minimum requirements may not be affordable for protecting your business interests. It is unwise to have too few reliability requirements, and it is foolish to require too many burdensome requirements.

Management must set the reliability policy (the general directive for what is intended). Policy drives procedures (step-by-step instructions for implementing policies). Procedures drive the rules (statements to take or not take actions).

Reliability policies must integrate safety, quality, risk, and financial requirements for the company to achieve the business objectives. Reliability policies must be understandable to the common person and come from top levels of management for credibility, legitimacy, constancy of purpose for improvements, and setting the organization to work for a common objective.

Management has a big role in reliability issues, which guide design of equipment and continues through maintenance of equipment and systems. Management must address the issues and state the general requirements so everyone understands. The issue of reliability is to provide a failure free environment for equipment and systems. Management must think in terms of a chess game—pawns will be lost (pumps, valves, instrumentation), but don't loose the king, which is the process (pressure integrity and product delivery system protecting human safety and environmental situations).

Issues for procedures

Procedures follow a policy and should address time/costs, etc. issues. Procedures may require establishment of assumed values or calculated values for communicating to the organization the high cost of certain failures. The fact that a human life is priceless does not compute but society allows certain risks, which then allow calculated values for communication purposes, as time/costs is the language of commerce, decisions, and action. Examples could be:

Assumed values-

- Spill loss of 1 gallon of undesirable fluids = $500
- Spill loss of 100 gallons of undesirable fluids = $3,000
- Spill loss of 1,000 gallons of undesirable fluids = $250,000
- Spill loss of 10,000 gallons of undesirable fluids = $1,900,000
- Spill loss of 100,000 gallons of undesirable fluids = $20,000,000
- Violation of Clean Waters Act provides civil penalties of $25,000/day or $1,000/bbl of spilled material or $3,000/bbl for "gross negligence"—if proposed Pipeline Safety Improvement Act S2438 is approved the maximum fines will increase to $100,000 for a single violation and to $1 million for a series of safety violations.

Calculated values -

- Accidental death of one person at (10^{-4}) = $2,500,000, multiply by 4 for disablement
- Accidental death of 10 people at (10^{-6}) = $250,000,000, ditto for disablement

Assumed values only for communication purposes-

- Other items to provide guidelines for failure events or failure avoidance including lists of applicable specifications and regulations for compliance audits.
- If the events occur in a sensitive area increase the cost by a factor of 5, if the events occur in a benign environment, reduce the cost by a factor of 5.

Please note: These numbers are quantified merely to convert humanitarian and violation issues into money (the language of business) so business trade-off decisions can be made, and the values **are not intended** to be guidance values for lawyers, **nor** do they represent callous viewpoints about the value of human life.

The point for inclusion of failure details into the procedures is to convert failure issues into money as a guideline for the organization to think about tradeoffs so everyone can react in a logical fashion to make honest and unemotional decisions concerning reliability matters. The probability of failure for one person at 10^{-4} (Taylor 1994) is the same as reliability = 0.9999 and 10^{-6} is reliability = 0.999999. Reliability values for discussions about humans are more palatable and less emotional than probabilities for human failure! Also note the $Risks for humans is a lower allowed value than $Risk for other typical business events.

Reliability Models

Reliability engineers discuss issues with reliability and availability models with a challenge, which is balanced against a capacity for handling the challenge of adverse conditions (Modarres 1999). Pipeline components, systems, and processes have a specific inherent capacity to handle challenges. In general, when the challenge is less than the capacity we have success; and when not, then we have failure. The failure mechanisms are physical processes attacking the models.

Typical reliability models are:

Stress-Strength models where stress represents aggregation of challenges and external conditions, and strength represents the variability of conditions affecting the capacity of system to repel the challengers attempting to cause failure.

Damage-Endurance models are similar to stress-strength models but the stress causes damages that are irreversible and cumulative such as corrosion, wear, embrittlement, and fatigue. Failure occurs when the cumulative damage exceeds the capacity of the component or system capacity to cope with the insults.

Challenge-Response models are conditions where components or systems fail but the failure is not identified until a challenge occurs due to a critical event, as compared to typical situations such as those that occur from the passage of time/cycles, etc.

Tolerance-Requirements models have failures only when the performance characteristics fall outside of some predetermined fixed limits and gradual degradation occurs based on use or time.

Mechanical failure mechanisms are physical processes, which lead to or result from some sort of stress (think of stress is general terms). The three broad classes are:

Stress-induced failure mechanisms are the cause or result of permanent or temporary stresses and are categorized by brittle fracture, buckling, yield, impact, ductile fracture, or elastic deformation.

Strength-reduced failure mechanisms lead directly or indirectly to failure and are categorized by wear, corrosion, cracking, diffusion, creep, radiation damage, or fretting.

Stress-increased failure mechanisms have a direct effect on increasing the applied stress and are categorized by fatigue, radiation, thermal-shock, impact, and fretting.

Electrical failure mechanisms are often more complicated than the typical mechanical system because of device and the packages in which they reside. Thus electrical/electronic failure mechanisms are often divided into three broad classes:

Electrical stress mechanisms result from voltage levels that damage devices or degrade electrical/electronic characteristics and are categorized by human error, uncontrolled currents, uncontrolled voltages, localized heating/melting, and latent damage, resulting in later failures.

Intrinsic failure mechanisms are related to the electrical/electronic element and categorized by electrically active layers in semiconductor chips, infant mortality problems built into the devices by manufacturing/design problems, gate oxide breakdown, ionic contamination, surface charge spreading, and hot electrons.

Extrinsic failure mechanisms are external failure mechanisms stemming from device packaging problems and problems with interconnections and undesirable environmental conditions.

Each failure mechanism can be accelerated in the field by unexpected combinations of events. The events are often triggered by a situation acting as a catalyst for failure.

The age-old technique for coping with these challenge events has been to make the components, systems, and processes very strong and keep the loads very low. For example, Roman bridges built for horses and chariots now carry heavy trucks with great success.

Another method of mitigating some failures is by maintenance engineering techniques, however, maintenance cannot restore strengths never existing in original designs. Thus direct replacement maintenance efforts cannot improve the inherent reliability, but only restore to the original values following deterioration—however, upgrade replacements can provide greater capacity.

Reliability Engineering vs. Maintenance Engineering

Reliability engineering is concerned with the strategic task of predicting and avoiding failures. Maintenance engineering is concerned with quickly restoring failures to an operating condition as a tactical task.

A current management fad is to take a maintenance mentality organization and change job titles to include the word reliability. This provides style but no substance, as tools and approaches for reliability and maintenance are different as night and day. Then management

wonders why the new "reliability" organization continues to function as before when the maintenance approach was fast repairs, which were considered the key to success as dictated by a maintenance organization.

Both reliability engineering and maintenance engineering have roots in each others territory and thus must know about each others roles, responsibilities, and tools Consider this analogy observed in most local fire departments: *reliability is to the fire marshal as maintenance is to fire fighters*. Reliability technology predicts failures and with the use of longer-range tools reduces the cost of failures.

Preventing failures costs money for equipment, procedures, and nurturing of the system. Repairing failures costs money. Thus both reliability and maintenance activities are ruled by money just as improvement decisions are always about money and alternatives. Improvement projects require engineering details converted into costs for yearly time buckets so as to correctly define cash outflows. Many companies use 20-year intervals for study periods.

Engineering is responsible for defining when failures will occur so they can be priced-out in net present value (NPV) worksheets, and this relies on predictions from reliability engineers. Of course the mode of failure also provides information about severity of the failure. The cost of failures must also include gross margin losses from production outages and cutbacks (when appropriate)—this is particularly true for continuous process operations, like pipelines, when the production is "sold out".

Reliability Engineering Tools

For reliability issues we talk about the sweet part—the absence of failures. We quantify reliability issues by measuring the failures, which is the sour part. Failure of equipment and processes always occur as a natural outgrowth from the laws of physics and changes in entropy of the system. It is easy to kill equipment. It is very difficult to make equipment survive. Table 1 shows a short list of reliability tools used for predicting failures and finding cost effective alternatives.

Table 1

Short List Of Reliability Engineering Principles Tools

- **Mean time between failures indices**
- **TPM and reliability principles**
- **Preparing reliability data for analysis**
- **Decision trees merging reliability and costs**
- **Weibull, normal, & log-normal probability plots**
- **Corrective action for Weibull failure**
- **Models & Monte Carlo simulations**
- **Pareto distributions for vital problems**
- **Fault tree analysis**
- **Design review**
- **Load/strength interactions**
- **Software reliability tools**
- **Sudden death and simultaneous testing**
- **Failure recording, analysis and corrective action**
- **Failure mode effect analysis**
- **Bathtub curves for modes of failure**
- **Availability, maintainability, capability**
- **Critical items significantly affecting safety/costs**
- **Quality function deployment**
- **Mechanical components testing for interactions**
- **Electronic device screening and de-rating**
- **Quality function deployment**
- **Reliability testing strategies**
- **Accelerated testing**
- **Contracting for reliability**
- **Reliability growth models and displays**
- **Cost of unreliability**
- **Reliability policies and specifications**
- **Reliability audits**
- **Management's role in reliability improvements**

The three regimes for equipment failure are: 1) infant mortality, 2) chance failures, and 3) wear out failures, which are connected to failure rates. Human errors are usually chance failures.

Infant mortality and old age wear out failures are superimposed on chance failures to obtain the typical bathtub failure curve where we typically think of chance failures having a lower failure rate than either wear out failures or infant mortality failures. The idealized bathtub curve is seldom observed for equipment—we have fewer pieces of equipment than we have human failures (deaths) and all human deaths in civilized societies must be reported to government agencies (mandatory reporting for equipment failures is not required).

The death of most equipment must be analyzed with Weibull analysis small samples using (Abernethy 2000) for each failure mode, and software makes the analysis task easy (Fulton 2001). In many cases a simple arithmetic technique of MTBF or MTTF is frequently used as a reliability precursor mixtures of failure modes that occur.

Most reliability tools are practical engineering tools seldom studied in depth at most universities. Usually the tools must be learned as supplements of continuing education either by home study or by short courses—see the reading list (Barringer 2001 a).

A simple precursor of reliability is a criterion called mean time to failure for non-repairable items and mean time between failures for repairable items. Consider the seal MTTF details in Figure 1 showing the effects of a change in failure criteria caused by new regulations.

This MTTF data from production, maintenance, and purchasing records

Remember: MTTF is a yardstick—not a micrometer!!

Chemical Plant ANSI Pump Life

Year	Number Of Unspared Pumps	Number Of Spared Pumps	Total Hours Of Pump Operation	Number Of Seal Failures	Seal MTTF (yrs)	Seal Failure Rate (fail/hr)	Conditions
1985	937	2996	21,330,000	1083	2.25	50.8E-6	No
1986	943	2996	21,380,000	937	2.60	43.8E-6	Emission
1987	950	2998	21,450,000	1156	2.12	53.9E-6	Monitoring
1988	950	3008	21,500,000	1127	2.18	52.4E-6	
1989	953	3012	21,540,000	1003	2.45	46.6E-6	
1990	955	3028	21,630,000	1689	1.46	78.1E-6	
1991	957	3036	21,680,000	1628	1.52	75.1E-6	
1992	963	3048	21,790,000	1581	1.57	72.6E-6	
1993	955	3038	21,670,000	1517	1.63	70.0E-6	Emission
1994	951	3026	21,580,000	1487	1.66	68.9E-6	Monitoring

Refinery API Pump Life

Year	Number Of Unspared Pumps	Number Of Spared Pumps	Total Hours Of Pump Operation	Number Of Seal Failures	Seal MTTF (yrs)	Seal Failure Rate (fail/hr)	Conditions
1985	313	1542	9,500,000	415	2.61	43.7E-6	No
1986	313	1542	9,500,000	398	2.72	41.9E-6	Emission
1987	313	1548	9,520,000	380	2.86	39.9E-6	Monitoring
1988	310	1560	9,550,000	361	3.02	37.8E-6	
1989	305	1580	9,590,000	343	3.19	35.8E-6	
1990	295	1580	9,500,000	535	2.03	56.3E-6	
1991	290	1590	9,500,000	481	2.25	50.6E-6	
1992	280	1598	9,450,000	403	2.68	42.6E-6	
1993	270	1602	9,380,000	354	3.02	37.7E-6	Emission
1994	265	1610	9,370,000	278	3.85	29.7E-6	Monitoring

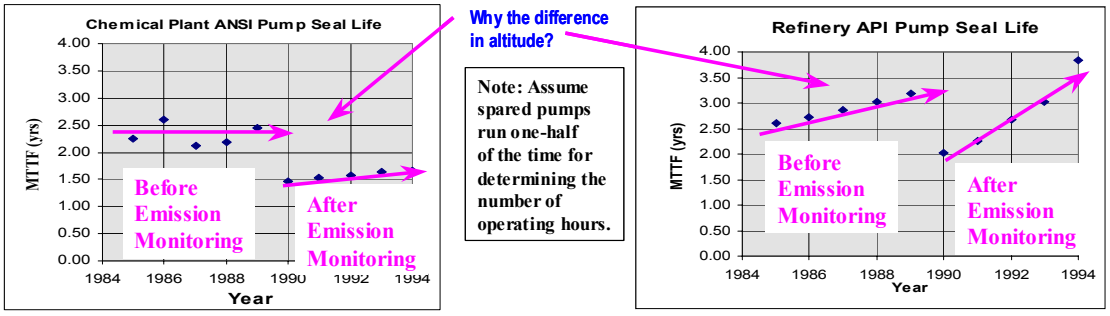

Figure 1: MTTF Before And After Regulatory Changes

Pipelines operating in high-consequence areas (HCA) sensitive to environmental damage should expect MTTF as experienced in Figure 1. The cause for MTTF decline in Figure 1 results from a more severe criteria for failure. MTTF/MTBF indicators help forecast the number of pump repairs expected during a time interval and thus help plan maintenance demands on resources and costs.

Some systems are simple series models without redundancy as shown in Figure 2 where failure of a single device causes the entire system to fail. Other systems are more durable by use of redundancies as shown in Figure 3. Redundancy means two or more devices providing backups to reduce system risks for failure.

Frequently, instruments and control systems employ reliability strategies for failure rate mitigation, using the principles of redundancies as the heart of safety integrity levels (SIL). SIL is described in ANSI/ISA-84.01-1996, Application of Safety Instrumented Systems for the Process

Industry, with draft technical report ISA-dTR84.02. Likewise IEC61508-1 (General Requirements), -2 (Requirements), -3 (Software), -4 (Definitions), -5 (Examples for SIL), -6 (Application Guidelines), and -7 (Overview of Techniques and Measures) for functional safety of electrical/electronic/programmable electronic safety related systems are available from Internet sites listed above and many details for electrical/electronic reliability apply to mechanical systems.

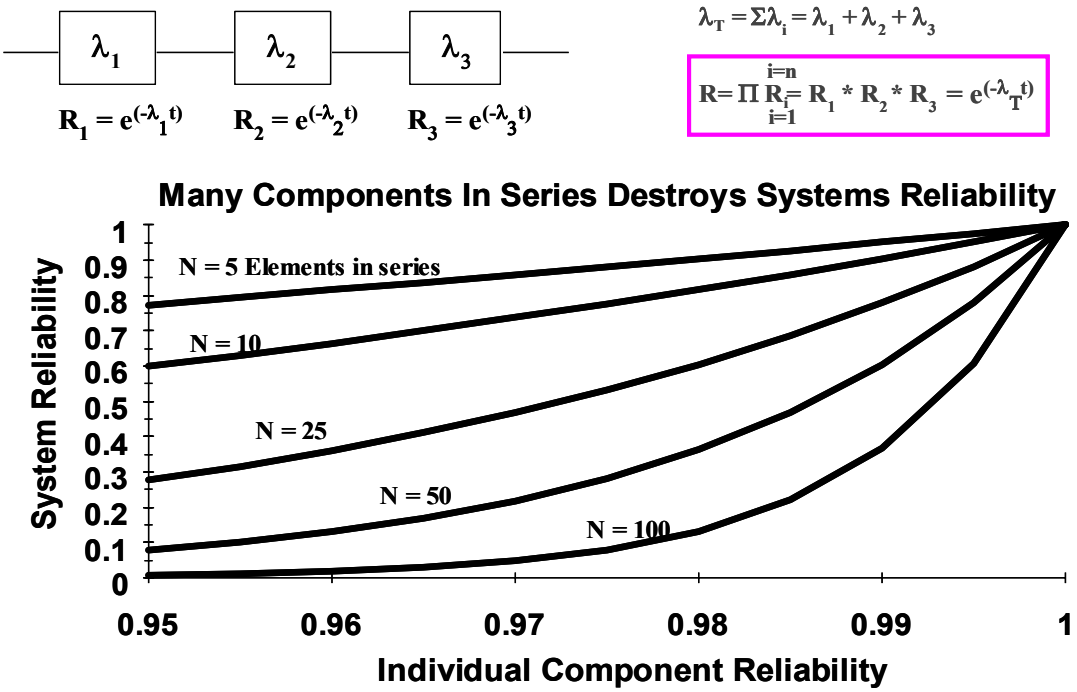

Figure 2: Simple Series System Reliability Model

If a single safety device has a reliability of 0.95 for one year and the consequence of failure is $20,000,000. The financial exposure, $risk = (probability of failure)*($consequence), is 0.05*$20,000,000 = $1,000,000 which is a very large financial exposure suggesting use of redundancy to mitigate the risk. If a similar device is placed in parallel, the system reliability as shown by the reliability model in Figure 3 is R = 1-(1-0.95)*(1-0.95) = 0.9975 and the financial exposure is 0.0025*20,000,000 = $50,000. If a third device is placed in parallel, the reliability is R = 1-(1-0.95)*(1-0.95)*(1-0.95) = 0.999875 and the financial exposure is 0.000125*20,000,000 = $2,500 which is a modest exposure and $Risks are mitigated by redundancies (see Table 3 below for financial justification details).

The financial risk for the triple (or more) redundancy requires more investment. Better grade redundant safety devices or a different method is needed for reducing failure consequence such as layers of protection analysis (LOPA) (Gruhn 1998) for keeping risks below an amount of say $10,000 (and this monetary risk level is also an issue for procedures driven by a management policy). The financial outcome and can be calculated with standard NPV calculation sheets as the sustaining "cost" is know for each year and acquisition cost for each scenario can be estimated.

For those needing modeling/calculation assistance, the no-cost RAPTOR block diagram software developed by the US Air Force is available for building complex reliability models (Barringer 2001b). Data is required to drive all reliability models and a limited Weibull database is available (Barringer 2001c), and data for reliability models should come from your own failure database which reflects: 1) grade of equipment purchased, 2) maintenance/operating strategies employed, and 3) organization of the database to clean the data using good practices such as inclusion of suspended (censored) data, and identification of the data taxonomy (CCPS 1998).

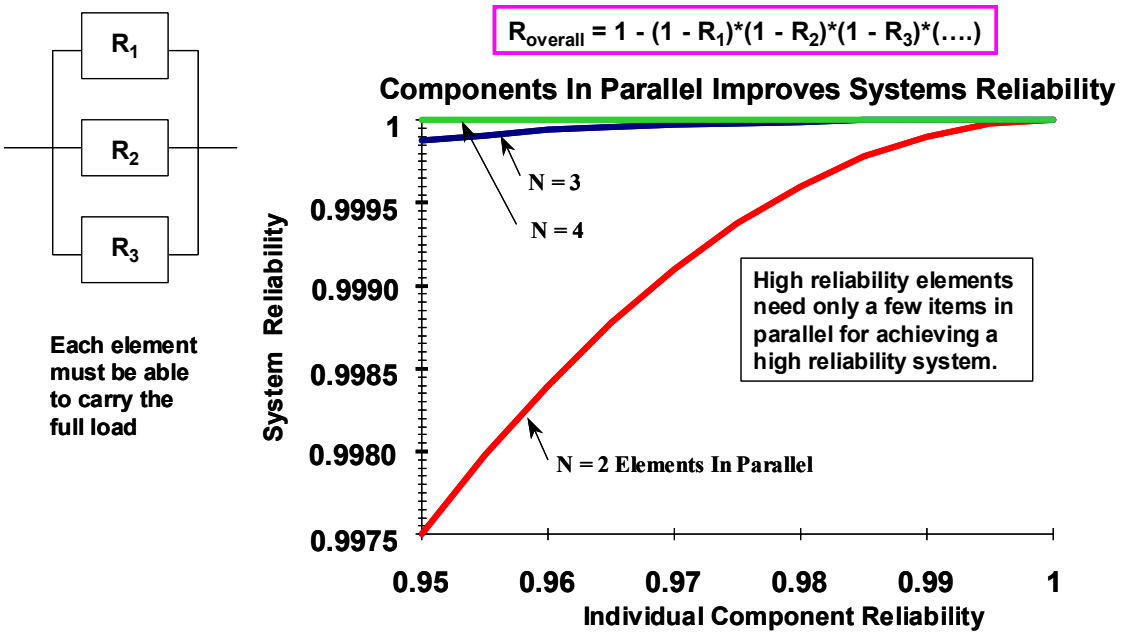

Figure 3: Simple Parallel System Reliability

Other very good quantitative reliability/risk models exist for rating pipelines such as C-FER Technology's Pyramid software (Stephens 1996) and (Nessim 1998). The software model considers a host of variables, some are qualitative and others quantitative, to rate pipeline risks by segments and evaluate the consequences. From this effort, Pareto distributions are established to rank the evaluation effort and risks for priority use of smart pigs and other evaluation tools. Pipeline risk pictures are sometimes practiced using a practical methodology of point count systems. (Muhlbauer 1996)

An area of poor reliability lies in problems associated with humans for rapid response when monitoring, controlling, and maintaining systems. The roots of failures, when broken into a Pareto distribution, are: 38% for humans, 34% for procedures/processes, and 28% for equipment. Human error probabilities = (number of errors)/(number of opportunities for error) and human error rates = (number of errors)/(total task duration). Table 2 shows the human probability of failure in a control room to correctly diagnose an abnormal event—reliabilities are obtained by taking the complement of probabilities of failure (AIChE 2000). This infers that automation of control room functions is very important for improving system reliability. The popular, but erroneous, concept is humans are reliable and equipment is unreliable which leads to overemphasizing hardware faults and underemphasizes human faults. Human unreliability is often the dominate factor in unreliability issues.

Table 2
Time Available For Diagnosis Of An Abnormal Event After Control Room Annuciation

Time (minutes)	Probability Of Failure (%)
1	~100
10	50
20	10
30	1
60	0.1
1500	0.01

To an engineer, most issues concerning reliability are related to things (not people)—things that happen and things that mitigate failures. To managers, most issues concerning reliability are related to costs. This requires converting things into money, which drives the need for alternatives. Seldom is the "best" engineering idea implemented because in the real world money is scarce and the first cost is rarely the last cost as things need constant attention and maintenance which ties all issues to life cycle costs and net present value calculations for the time value of money.

Life Cycle Costs

Life cycle costs (LCC) refer to all costs associated with acquisition and sustaining costs for ownership of a product or system over its full life (Fabrycky 1991), (SAE 1999). The usual figure of merit is net present value (NPV).

NPV is a financial tool for evaluating economic value added. It is the present value of an investment's future net cash flows, minus the initial investment for a given discount rate hurdle. The present values for each year of the project are summed for the net present value. Net cash flows are a measure of a company's financial health. Discount rates are the interest rates used in discounting future cash flows. The discount rates include the cost of money, bank and company administration costs, and risk costs for the lender—they are always larger than Federal Bank rates. For an entire project, the life cycle cost number requires a positive NPV. Bigger positive NPVs are better.

Project elements cannot easily show profits/savings for each equipment component, and decisions are made in selecting equipment based on the **least negative** NPV, where smaller negative NPV is better criteria. Many improvement projects will have positive NPV along with internal rates of return (IRR) as a second criteria insisting on higher rates of returns on many small projects that must jump a very high hurdle to hold down the expenditure for capital money—particularly if the company lacks access to financial money for improvements.

All LCC tasks require comparisons of alternative**s**—note the word alternatives is plural. In every LCC task, conflicting issues are obvious:

- Project engineers want to minimize capital expenditures
- Accounting wants to maximize NPV
- Shareholders want to maximize dividends/share price
- Production wants to maximize uptime hours
- Maintenance engineers want to minimize repair hours
- Reliability engineers want to avoid failures

All parties want someone else to put the numbers together to justify their love affair with the project or equipment, which justifies their decisions.

Business is about time, money, and alternatives. Time and money are both in short supply. A single alternative is without choice and unwise because the default position is to do nothing. The LCC concept merges time and money together to arrive at a single indicator called NPV for each alternative. NPV numbers prioritize the projects to select the winner from the alternatives so you buy right rather than only buying cheap.

Techniques used for finding LCC are available in training formats (Barringer 2001d). Technical papers are available for download from the Internet as PDF files (Barringer2001e).

Making the life cycle cost calculations is easy when you have the data. Refer to the safety device example shown above converted into NPV in Table 3 justifying quadruple redundancy as most affordable (perhaps other alternatives will be preferred). The difficult effort is how to resolve the chicken or egg dilemma for finding failure data, maintenance data, and other details involved in the sustaining cost as the acquisition cost is usually the only accurate number you have as it is a quotation. You need reliability engineering details to find when things die. Failure data and repair time data can be converted into statistical format using WinSMITH Weibull software for use in reliability calculations. (Fulton 2001)

Table 3
Device Reliability = 0.95 for 1 year mission, Failure Consequence = $20,000,000, Device Costs = $10,000/each

Number of Instruments	Reliability (%)	$Risk/yr	Capital Cost	NPV
1	0.95	$1,000,000	$10,000	-$4,639,636
2	0.9975	$50,000	$20,000	-$248,714
3	0.999875	$2,500	$30,000	-$37,320
4	**0.99999375**	**$125**	**$40,000**	**-$34,902**
5	0.999999688	$6	$50,000	-$42,932
6	0.999999984	$0.31	$60,000	-$51,485

Few individuals claim knowledge of sustaining cost facts until someone else puts numbers on the table—then the critics are numerous for "correcting" the proposed numbers. Follow the scientific method: build a hypothesis for failures and their cost and then test the hypothesis. When in doubt about the failure data or cost, make an estimate and test the estimate for validity.

Much data needed for LCC comes from operating costs (including electricity, etc.) and maintenance records which show times between failure and repair times. These details are often associated with the field of reliability and maintainability with a direct relationship for finding lower life cycle costs. The cost details should also include costs for lost gross margin for outages of systems when it is appropriate. Some of the failure data is from simple arithmetic calculations and other data follows the preferred method from Weibull databases.

Conditions for installation, operation, and maintenance influence both failures and failure costs, which are susceptible to equipment grades for changing the financial performance. Often Monte Carlo computer simulations, using random numbers, are required to find cost variability for different equipment grades.

Your can build simple, low cost Monte Carlo reliability models using software available from the Internet which is useful for driving life cycle cost decisions. (Barringer 2000e) The reason for building reliability models is to find where failure cost is occurring and to search for the lowest long-term cost of ownership where system details, when priced-out, provide a clear leading alternative for solving the problems. The reliability models show what's affordable and the less desirable alternatives.

Reliability models, using actual failure data and repair times, give system availability, reliability, maintainability, and other operating system details which allows construction of costs and tradeoffs. A clear definition of failure is important for reliability decisions and the data acquired.

If you do not have data collection systems for your failures, you will seldom make substantial improvements in the reliability of your systems.

Reliability models provide evidence for tradeoff boxes. Engineers need graphics for understanding what's happening to their systems. The tradeoff box has life cycle cost on the vertical axis and effectiveness on the horizontal axis. Effectiveness is the product of availability, reliability, maintainability, and capability of the system to perform. Complex items become simple when you see the results shown in Figure 4. The left hand of Figure 4 symbolizes too many failures and the right hand of Figure 4 symbolizes too much equipment. The sweet spot lies between the extremes.

What most companies need is the money and control of risk—they rarely need perfect solutions! Life cycle cost helps provide the answers when driven by the tools of reliability engineering. When you have concepts and features on a product or process that generate value, the value must be quantified for inclusion in the life cycle cost model. .

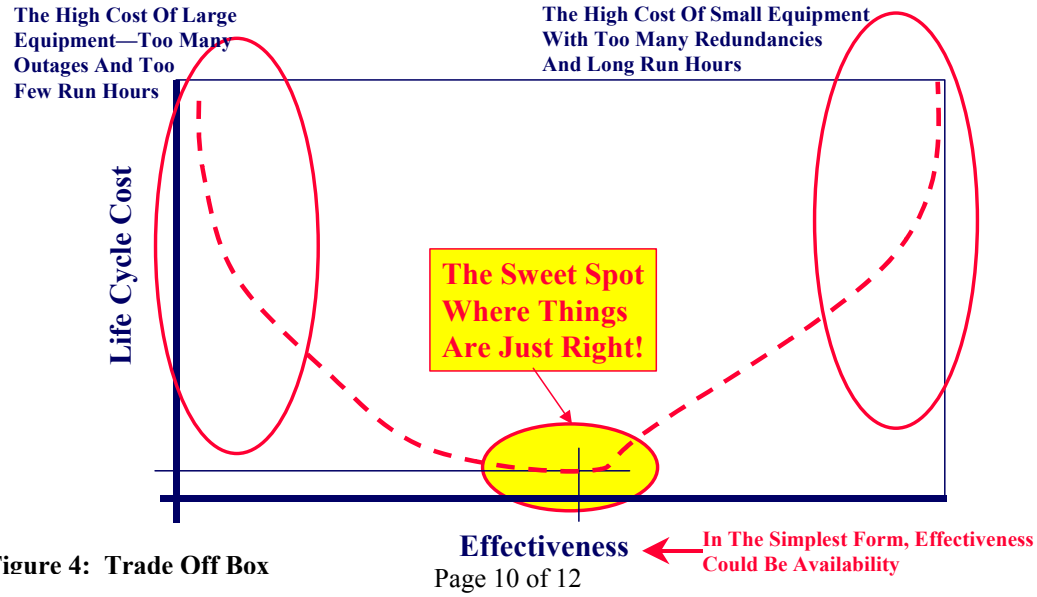

Figure 4: Trade Off Box

Summary

A reliability policy focuses the organization toward a failure free environment to meet management objectives for the business. Reliability engineering tools predict failures and risks associated with certain actions. Details from the reliability analysis go into life cycle costs models for merging engineering details into a format considering the time value of money. Life cycle concepts rely heavily on reliability and maintainability technology issues to convert ideas into hard, engineering facts which convert issues into a monetary values for making trade-off decisions about $Risks.

The first cost for procurement is not the last cost. Procurement cost may represent only a small fraction of the total cost during the life of an item, and in other cases, it may be a large portion of the total life cycle costs—general rules of thumb have much variance.

The engineering facts must be converted into financial details of NPV and IRR with a selection of the best alternative from several courses of action. The decisions you make up front will be with you for many years so it's important to justify risks and improvements using the best tools available.

Without reliability details about failures, NPV are difficult to calculate for making correct business decisions about tradeoffs with failure avoidance for reliability as a business focus.

If your customers or the general public are unhappy about reliability of your systems, improvements must be made—that is a call for change and to get change, you must make a change. If improvements are not voluntary and community outrage is high, trailing legislation will surely follow in ways seldom to your advantage. Unreliability must be quantified and resolved quickly for business purposes. Occasionally reliability begins at low levels in the organization with long incubation times before recognizable progress is recorded; however in private enterprise, high system reliability is best-achieved top down with policy statements to quickly put the organization to work for reaching a target in reasonable time frames.

References

1. Abernethy, Robert B., **The New Weibull Handbook**, fourth edition, Dr. Robert B. Abernethy author and publisher, 536 Oyster Road, North Palm Beach, FL 33408-4328, Phone/FAX: 561-842-4082, e-mail: **Weibull@worldnet.att.net**, ISBN 0-9653062-1-6, 2000.
2. AIChE, **Guidelines For Chemical Process Quantitative Risk Analysis**, 2nd edition, American Institute of chemical Engineers, New York, ISBN 0-8169-0720-X, 2000
3. Barringer, H. Paul, **Reliability Engineering Principles**, author and publisher, Barringer & Associates, Inc., P.O. Box 3985, Humble, TX, 2001 –the reading list is also available on the Internet at **http://www.barringer1.com/read.htm**
4. Barringer, H. Paul, **http://www.barringer1.com/raptor.htm**, **RAPTOR** software for no cost downloads, 2001.
5. Barringer, H. Paul, **Weibull Database**, **http://www.barringer1.com/wdbase.htm**, 2001
6. Barringer, H. Paul, **Life Cycle Cost**, author and publisher, Barringer & Associates, Inc., P.O. Box 3985, Humble, TX, 2001
7. Barringer, H. Paul, **Download Papers**, **http://www.barringer1.com/Papers.htm**, 2001
8. CCPS Staff, **Guidelines for Improving Plant Reliability through Data Collection and Analysis**, Center For Chemical Process Safety of the American Institute Of Chemical Engineers, AIChE, New York, ISBN 0-8169-0751-X, 1998
9. Fabrycky, Wolter J. and Benjamin S. Blanchard, **Life-Cycle Cost and Economic Analysis**, Prentice Hall, Englewood Cliffs, New Jersey, ISBN 0-13-538323-4, 1991
10. Fulton, Wes, **WinSMITH Weibull** probability plotting software, **http://www.weibullnews.com**, 2001
11. Gruhn, Paul and Harry Cheddie, **Safety Shutdown Systems: Design, Analysis, and Justification**, Instrument Society of America, ISBN 1-55617-665-1, 1998
12. Modarres, Mohammad, Mark Kaminskiy, Vasiliy Krivtsov, **Reliability Engineering and Risk Analysis**, Marcel Decker, New York, ISBN 0-8247-2000-8, 1999

13. Muhlbauer, W. Kent, **Pipeline Risk Management Manual**, 2nd edition, Gulf Publishing Company, ISBN 0-88415-668-0, 1996
14. Nessim, Maher A. and Mark J. Stephens, **Managing The Operating Risk Posed By Metal Loss Corrosion And Mechanical Interference**, International Pipeline Conference, Calgary, Alberta, (PDF files available from Mark Stephens at mstephens@cfertech.com), June 7-11, 1998.
15. SAE M-110.2, **Reliability and Maintainability Guideline for Manufacturing Machinery and Equipment—Second Edition**, Society of Automotive Engineers, Warrendale, PA, ISBN 0-7680-0473-X, 1999
16. Stephens, M. J., and M. A. Nessim, **Pipeline Maintenance Planning Based On Quantitative Risk Analysis**, International Pipeline Conference, Calgary, Alberta, (PDF files available from Mark Stephens at mstephens@cfertech.com), June 9-13, 1996.
17. Taylor, J.R., **Risk Analysis for Process Plant, Pipelines and Transport**, E & FN Spon, New York, ISBN 0-419-19090-2, 1994

Biography

Paul Barringer, P.E. is a manufacturing, engineering, and reliability consultant with more than thirty-five years of engineering and manufacturing experience in design, production, quality, maintenance, and reliability of technical products. Experienced in both the technical and bottom-line aspects of operating a business with management experience in manufacturing and engineering for an ISO 9001 facility. Industrial experience includes the oil and gas services business for high pressure and deep holes, super alloy manufacturing, and isotope separation using ultra high speed rotating devices.

He is author of training courses: **Reliability Engineering Principles** for calculating the life of equipment and predicting the failure free interval**, Process Reliability** for finding the reliability of processes and quantifying production losses, and **Life Cycle Cost** for finding the most cost effective alternative from many equipment scenarios using reliability concepts.

Barringer is a Registered Professional Engineer, Texas. Inventor named in six U.S.A. Patents and numerous foreign patents. He is a contributor to **The New Weibull Handbook**, a reliability handbook, published by Dr. Robert B. Abernethy.

His education includes a MS and BS in Mechanical Engineering from North Carolina State University. He participated in Harvard University's three-week Manufacturing Strategy conference.

Other reliability and life cycle costs details are available at **http://www.barringer1.com**

April 16, 2001