Chapter 3

Designing with Reliability

Features

Introduction
Reliability Engineering
System and Subsystem Engineering
Reliability Testing
Environmental Testing
Reliability Reporting

Introduction

During the design process, many engineers overlook the *long-term* failure mode. The probability that a given design will function over a period of time considered acceptable by the customer, is generally not given by the customer, nor is it solicited by the designer. What this means, is an eventual tradeoff between low capital expenditure and high maintenance or downtime costs.

Reliability can involve any of the following, and more . . .

- **Probability of the system performing over a prescribed period of time . . .**
  What is the probability that the system will operate when called on to do so, and for how long? The required duty cycle, environment, maintenance, operator capability, product handling, and other factors all contribute to the ability of the system to reach the desired reliability goal.

- **Analysis of probable strength against probable stress . . .**
  What factors need to be considered to balance these two variables in design calculations? When stress exceeds strength, a failure is imminent. Stress can result from under-design, unknowns in the operating environment, and unknown internal equipment operation. Vibration, electrical noise, temperature, and other factors must be considered to ensure that the given reliability is met.

- **Trading off reliability for other qualities . . .**
  What will you have to compromise to balance reliability with other required design qualities? The ability to achieve the required reliability may be affected by certain operating conditions or options. It is necessary to weigh function and performance against reliability goals to figure out what compromises, if any, may be necessary.

- **Cost to achieve the desired reliability . . .**
  What factors need to be included to calculate the cost of the desired system reliability? Design improvements, *creeping feature-isms*, and other system modifications all place a burden on the reliability requirement. System cost, schedules, labor, and other elements place limits on the ability to reach given goals.

- **Produce-ability of the desired reliability . . .**
  What type of restrictions are there on the ability of the designed system to produce the desired reliability? Mass production can place other types of restrictions on the ability to achieve the requested reliability performance. Construction of one or hundreds of systems may require changes in quality control methods,

part procurement procedures, in-house construction equipment, and other factors all affecting the reliability outcome.

- **Actual use of the product after delivery . . .**
  After delivery, a new set of problems comes into play. The arbitrary increase of product throughput, system maintenance, operator skill, ability to diagnose problems, and spare parts, among other things, all contribute to downtime. System reliability as noted by its ability to *last* over the defined period of time (mean time between failures), and the ability to minimize its time off-line due to problems encountered can make or break the project and perhaps even your reputation.

Since everything done to produce the best reliability relates in some manner to the money invested, the question becomes: *How much reliability is economical?* Figure 3.1 shows a relationship between achieving a reliability goal and the related expense. Good design efforts can allow you to achieve an optimum reliability value for the life expectancy of the product (system, . . .) within the allotted design schedule without exceeding the design budget.

Reliability Engineering

Reliability engineering is the technology of prediction, control, measurement, reporting, and analysis of failure occurrence and failure rate.

What this means, is good design practices allow for worst case situations, along with general operating criteria, to develop a system that will perform the desired goals.

Even with very good practices in place, design oversights and/or lack of communication between design and production departments can hasten failures. Generally, these oversights can be detected with reliability assurance methods designed to reduce such self-imposed failures. Design documentation, production reports, inspection, quality control, and other methods, all help to increase product reliability.

The knowledge that tradeoffs between performance and schedules curb 100-percent reliability is very important. Therefore, the objective is to achieve a realistic reliability goal (see Figure 3.1) and a mutually acceptable level to both the producers of the system and the customer.

Since most companies do not employ reliability engineers, it is up to the designer or design team to put into place failure-control measures. You must plan for and achieve the level of reliability that represents the maximum cost-effectiveness for the complete system within the given boundary conditions. These boundary conditions consist of such variables as system specification, restrictions, and schedule.

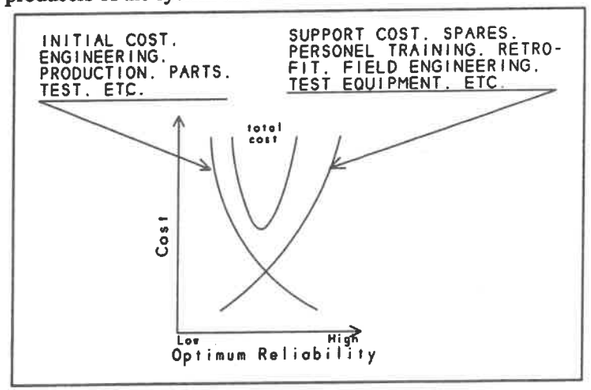

Figure 3.1 Reliability versus Cost.

A quantitative discussion of probability and statistical analysis calculations is beyond the scope of this book. However, it doesn't take a rocket scientist to realize that if you cheat, cut corners or fail to analyze your designs, premature failure is inevitable!

System and Subsystem Reliability

The word *system* has no finite definition but can be thought of as an ordered set of interrelationships. Using this broad definition, it becomes apparent that a system design should be reduced to a series of smaller systems called *subsystems* to make the design task easier and to increase the overall effectiveness of the design from a reliability standpoint.

The following are methods that can be used to figure out reliability design guidelines. The given list is by no means fixed. It can and should be groomed for specific system applications. Of course, the bottom line is that each designer will figure out his or her own direction as the project progresses—adding to or deleting items from the reliability checklist as necessary.

Defining Reliability

Define reliability in terms of the system operational requirements. For example, setting a downtime goal of one 8-hour *down* period in 2080 operational hours might place too heavy a burden on the mechanics, but it could be totally acceptable for the electronics. However, if the system requirement is to only operate on a three-shift five-day basis but not on weekends or holidays, a complete mechanical preventative maintenance program could be instituted on the weekends allowing the specification to be met.

By shifting the reliability burden from high cost mechanics to weekend maintenance, a significant reduction in system cost could possibly be gained.

Developing a Reliability Index

Develop an index for system reliability effectiveness. Below are seven reliability indices that can be used in the design procedure. Any equations shown are simply to supplement the presented ideas. There are many excellent reliability handbooks available to cover in-depth application of reliability calculations.

- **Reliability:** Reliability is the probability that a system will operate without degradation or failure over a period of time. It can be described by:

$$\textit{Reliability} = \frac{\textit{Number of equipment operating after the time interval}}{\textit{Total number of equipment}}$$

- **Mean life:** Mean life, or mean-time-between-failures (MTBF), is the total operating time of the entire system of equipment divided by the total number of equipment failures.

- **Mean-Time-to-Failure:** The MTTF is the expected time until all equipment has failed in a non-maintained system. In a maintained system, the MTTF is a measure of the expected time the system is in an operable state while allowing individual repairs to be made.

- **Instantaneous availability:** This is the probability that the system will be available at any random time. At the time the equipment is needed, will it be in functional order? This index allows you to determine the probability that when the switch is thrown, the system will produce.

$$IA\ (t) = \frac{R_r}{R_r + F_r} + \frac{F_r \exp^{-(R_r + F_r)t}}{F_r + R_r}$$

where: R_r = equipment repair rate (time)
F_r = equipment failure rate (time)
t = random time @ t=0, IA(t) = 1

- **System availability:** This is the portion of time in an interval that the system is available for use.

$$SA(t) = \frac{1}{t_E - t_S} \int_{t_S}^{t_E} IA(t)\ dt$$

where: t_S = start of time interval
t_E = end of time interval
IA(t) = Instantaneous Availability

- **Steady-state-availability:** This is the portion of time that the system is available for operation when the given time interval is very great.

$$SSA\ (\infty) = \lim_{t \to \infty} \frac{1}{t} \int_0^t IA(t)\ dt$$

where: t = time interval
IA(t) = Instantaneous Availability

The choice of which measure to use is determined by the system requirement, duty cycle, and system availability for repair, among other things.

- **Duration of a single downtime:** For some systems and for high-production plants, the cost of a single downtime can be significant. During the preliminary design phase, consideration should be given to repair time (i.e., spares). It can be shown that the average duration of a single downtime (t) for a number of different equipment units operating in parallel, where at least one piece of equipment must be available is:

$$t = \frac{1}{(N_t)\ (R_r)}$$

where: R_r = equipment repair rate
N_t = number of functions or pieces of equipment.

If the time-to-repair an individual piece of equipment, and the system is each exponentially distributed, the probability (P) that a single downtime duration will exceed (T) hours can be found from

$$P(t>T) = 1 - e^{T/s}$$

where: s = average single downtime duration

- **Probability of system success:** In figuring out the probability that a system will be able to fulfill its operational requirements, the occurrence of a single part failure may, in some cases, rarely be enough to cause complete system breakdown. Also, depending upon the structure of the equipment and the location of the parts that fail, more than one failure might occur without causing total system breakdown. The basic equation for determining system success could be given as:

$$P_s = \left(\prod_{i=1}^{N_t} P_i\right)\left[\sum_{i=1}^{N_t} w_i \left(\prod_{i=1}^{N_t} P_i\right) \frac{Q_i}{P_i}\right]$$

where: P_s = Probability of complete success.
P_i = Probability of failure free operation of the *i*th equipment or function.
Q_i = Probability of a failed operation of the *i*th equipment or function, such that: $Q_i = 1 - P_i$
w_i = probability of success with the *i*th function or equipment failed.
N_t = number of functions or pieces of equipment.

- **System readiness:** The relationship between the measure of mean-failure-rate and the probability that a system will be ready to operate at any time is:

$$P_{OR} = \frac{N_T - N_A}{N_T}$$

Where: N_T = Total number of systems
N_A = Average number of systems waiting for or currently in service at a given time.

and:

$$N_A = \sum_{N=0}^{N_T} N\ p_N$$

where: N = number of functions or pieces of equipment.
P_N = State probability of n pieces of equipment.
N_T = Total number of systems

Rearrange the System

Rearrange the system into non-interacting subsystems. To develop the most effective system breakdown, use system timing charts, diagrams, and software flowcharts. By doing this, you achieve several things. First, timing diagrams will allow the designer to parse the system into small subsystem modules generally yielding a higher degree of reliability. Second, software flowcharts will show the *real-time* requirements of the control, and from this you can decide the simplest means of control (i.e., using a switch, a relay, a PLC I/O, or computer). Generally, the simplest approach is the most reliable.

Once the system has been reduced to its subsystem form, the preliminary equipment can be chosen. Initiate a reliability check to find out if the desired reliability factor of the system and subsystems has been met. The subsystem mechanics can be scrutinized simultaneously with control development to give the designer reliability information about the system on a larger scale.

Preliminary system tradeoffs will occur here as well.

Evaluate Configurations

Evaluate various configurations in terms of reliability and cost. Alternative configurations imply nothing more than ensuring the best value for the dollar. It is possible to design the perfect machine the first time around, but this is not very likely. Considering the possibility of using a PLC in place of a computer might save considerable cost unless servo motion is required. Scan times and *real-time* requirements generally dictate what type of control device will be the most cost effective.

Also, if *off-the-shelf* hardware can be obtained in place of in-house construction, you can avoid much, if not all, of the learning curve for this process and still provide the needed system reliability. Increasing the capital construction budget to provide equipment that is proven reliable can usually be offset in the course of one downtime occurrence. No doubt you have heard the phrase,

"Pay me now, or pay me later."

Evaluate Consequences

Evaluate the consequences of each alternative configuration. The point is that if an alternative configuration is brought into the game-plan, check it out! Do not assume one method is necessarily better because it is cheaper, more expensive, or is a *brand* name. If the system fails, your vendor can't be fired, but you can. The only one who loses is you.

It is the responsibility of the system engineer to establish the ground rules. Therefore, when approaching a system design, the designer can . . .

- Use existing equipment, and decide the best configuration.
- Improve upon existing equipment, and interface methods to improve reliability.
- Completely design new equipment to meet the reliability goals.
- Use redundancy (parallel operation) with presently existing equipment.
- Use any combination of these approaches.

Establish Specifications

Specify a configuration, a maintenance philosophy, and a relationship with other environmental and handling factors. As the system design plan develops, note the requirements for general maintenance, adjustments, and such, which **must** be done once the system is on-line. As tradeoffs are made to maintain the budget, make note of any implication to the reliability goal(s) and how, through the control of environmental factors such as ambient temperature, humidity, operator involvement and so on, the goal(s) can possibly be reestablished.

Evaluate Specifications

Evaluate the specifications in terms of failure rate, and/or repair rate to the equipment within the system. Inventory the equipment detected to be failure prone. A *black-box* change-out is most often the best method to maintain the shortest downtime, but it is usually the most expensive. Mechanical parts such as limit switches are rated in contact closures. Can the mechanical devices be replaced with electronic devices, thus eliminating moving parts?

Predict the Reliability

Predict the reliability for each subsystem using available data from previous designs or published data. Nearly all equipment on the market today has specification sheets; if not, each of the equipment components should. Does the device have a UL[1] rating? There is always a means of figuring out the MTBF[2] of a system module. As a *last recourse*, use the unit that you have decided to be the best for the application— whatever the rating. Also, as a contingency, have an alternate device ready to install if your initial choice falls short of the desired goal.

In many cases, knowledge of construction, internal components, workmanship, and the company you are buying from can give you that warm-fuzzy feeling necessary to yield a high degree of confidence in the equipment. In any case, be sure you have at least attempted to obtain product reliability information.

---

[1]Underwriter's Laboratory

[2]Mean Time Between Failures

Compare Desired Reliability Goals

Compare the desired reliability goals with the predicted values to determine the next course of action. Obviously, if the reliability goal(s) and budget have been met, completion is around the corner. Use common sense, and stop engineering short of the point of diminished returns. Failure to do so will cost your customer more money.

Update Your Reliability Predictions

Update your reliability predictions as the system is altered or expanded, and choose the next course of action on a system level. *Creeping feature-isms*, on-line modifications, changing the operation method, and other factors can alter the actual reliability. Before installing or changing some aspect of the design, ensure that you and the customer understand the implications of such a change. Rework the required documents as necessary to learn how the change will influence the reliability.

Whether you use availability, reliability, downtime, or combinations of any indices is really secondary to the problem at hand. The idea is to recognize that some form of meaningful system reliability representation must be carried out to verify customer and long term operation requirements.

Reliability Testing

Regardless of the design techniques and controls used, adequate system and equipment testing is still necessary to:

- Detect and correct unforeseen failure modes.
- Verify and revise part failure rates and date used, to estimate reliability in the drawing board phase of development.
- Determine hardware conformance to specified reliability requirements.
- Determine if the reliability will change over time as the system equipment *wears in*.
- Monitor reliability trends, and evaluate the changes.

The reliability test is used to determine satisfactory product performance for a specified period of time under specified (usually the expected) environmental conditions.

There are three basic product types:

- One-shot products such as fuses that cannot be tested before use
- Products that operate continuously or periodically such as power generating equipment
- Single-use products that can be tested extensively before use such as robot arms and computer controls.

The three main types of reliability tests are:

- Failure terminated tests.
- Time terminated tests.
- Truncated sequential tests, which accept, reject, or continue testing based on the cumulative failures versus test time.

In addition, each of these tests can be classified as with or without a replacement procedure; in other words, failed components will or will not be replaced.

The value of any of these tests in terms of their ability to discriminate between reliable and unreliable product can be described by:

- Acceptable mean life.
- Unacceptable mean life.
- Producer's risk.
- Customer's risk.

These parameters and the derived solutions can be found in any book dealing with reliability testing.

Environmental Testing

Studying the environment in which the system will reside can play a major role in enhancing the reliability of any system. Checking out and testing all of the environmental conditions and influences that will affect the operation of the system is of paramount importance. Not only should the system perform as specified over its life expectancy, it should not require expensive modifications or extensive field engineering due to unforeseen environmental factors.

Systems can be tested under conditions that simulate the real thing, but the requirement is to develop a test plan to ensure that tests being done are realistic. A great amount of time and money can be wasted on cold-testing a product headed for the Western Sahara, Africa.

An example procedure for an environmental test program is . . .

1) Determine the schedule and dates.
2) Determine the available budget.
3) Determine the emphasis necessary at each stage of the hardware.
4) Determine the best tests to fit the specific areas.
5) Evaluate the importance of each type of environmental test.
6) Outline the test program in terms of environmental parameters and design requirements.

Factors to consider when testing are . . .

1) Exactness of the environment simulation.
2) Timeliness of the data.
3) The application of the environmental situation.
4) Extent of the test program required.

The first question to answer is whether complete simulation is necessary, and if so, does it require a combination of **all** environmental conditions? Should they be combined simultaneously, individually, in specific groups, or in some other specific order? Your test philosophy must also consider the use of extremes versus the average levels of environment and the characteristics of the environment. Conditions to consider include:

- temperature
- vibration
- fungus
- rain
- noise
- acceleration
- power and maintenance availability
- operator capability
- the explosive nature of the atmosphere.

Reliability Reporting

The purpose of field reliability data is to:

- Reflect the operation reliability level.
- Provide specific failure information for product improvement.
- Provide customer visibility and management control.
- Provide failure data retention for future design efforts.

Learn as much as possible about reliability and how to design it into your system so you can accomplish nothing less than increasing your awareness of problems that are outside your control. By understanding the environmental processes involved, designing for the unknown becomes simply a design procedure, not a never-ending list of fixes.

Notes: