ComSysDes

COMMUNICATION SYSTEMS DESIGN LLC

http://www.comsysdes.com
Voice & fax 510-792-1760

66 Santos Court
Fremont, CA 94536 - USA

Demystifying Redundant Systems

Practical Knowledge and Formulas

Jose Alvarellos

August 30, 2001

ComSysDes COMMUNICATION SYSTEMS DESIGN LLC
http://www.comsysdes.com 66 Santos Court
Voice & fax 510-792-1760 Fremont, CA 94536 - USA

Table of Contents

Table of Figures

http://www.comsysdes.com
Voice & fax 510-792-1760

66 Santos Court
Fremont, CA 94536 - USA

Scope of this Report

This report covers a number of subjects of the Reliability discipline focusing in the product useful life in the field, as opposed to the Manufacturing processes that may affect that product reliability.

The paper attempts to provide the theoretical basis of the fundamental concepts but at the same time also providing a summary at the end of each chapter for the readers interested in the conclusions and practical applications.

The reader without time to spend in the derivation of the formulas might want ***to read first the last chapter ("Reliability Models and Application Example") and turn back to the "Summary" sections at the end of the other chapters as needed***.

As a word of caution to the optimistic reader, the author wants to emphasize that the Reliability discipline contains an endless number of complications that should not be underestimated by the lecture of a simple introductory paper.

Reader's feedback is encouraged and appreciated. Please address your suggestions and comments by e-mail at Mktg@comsysdes.com.

Introduction

Audience and Purpose

This report is dedicated to the Design Engineering professionals needing a quick introduction to the fundamentals of Reliability Engineering. It is the result of the need expressed by many ComSysDes customers for a handy reference to reliability and similar issues, especially in the telecom field.

This paper does not attempt to replace the Reliability specialist. It is hoped however, that it will help the non-specialists in formulating the problems to be solved by the Reliability professional.

The "Bathtub" Function

It has been observed that the typical distribution of failures along the time follows approximately this shape (with logarithmic scale in the time axis):

.

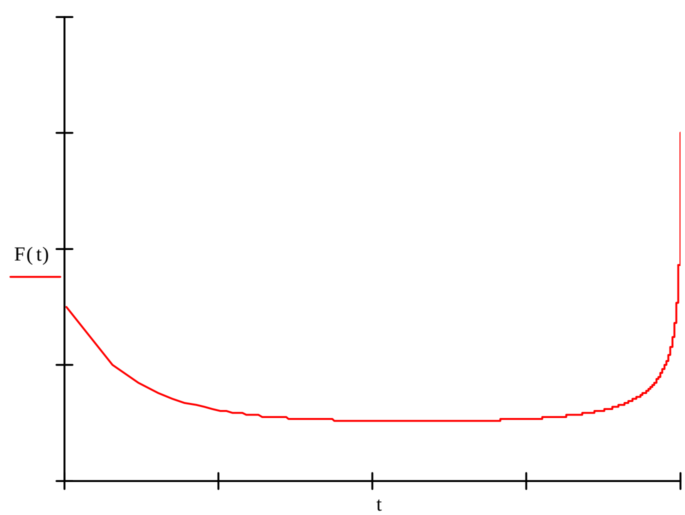

Figure 1: The "bathtub" function

We can distinguish three parts in this plot, each one with a different timeframe and with different failure mechanisms. These are:

1) "Infant Mortality" period: This period is of short duration (from a few hours to a few weeks) and the failures this early in the product life are usually due to defects or errors in the component manufacture.
2) "Useful Product Life": The failures during this period are randomly distributed but at approximately constant rate. This period typically measures in years.
3) "Wear Out": Over longer periods of time other non-random, slow degradation mechanisms become more and more important. This period marks the end of the product useful life and sometimes is not clearly defined in time. For example, renewing a few worn-out components might prolong the product life for years, until other wear out mechanisms take place.

The "Infant Mortality" phenomena are a main subject of study in the disciplines of Manufacturing, Testing and Quality Control, which strive to prevent the products suffering from this problem ever to reach the market. An important tool in this effort is to "burn in" the products for a short period of time (for example, one full day) at high temperature and other stress conditions to force potential problems to show up before the products leaving the factory. The "Wear Out" phenomenon is a subject of the Material Science, among others. Even though these two periods in the life of a product are of significant interest in the industry, we will discuss the period when the product is out in the field, performing its intended function. *The rest of this paper will focus on the random failures that happen during the product "Useful Life"*.

Some of the Jargon and Background

MTBF: Mean Time Between Failures.

MTTR: Mean Time To Repair. This time is measured from the instant that the failure occurs until the original functionality is restored (including the redundancy if applicable). From this definition, it includes the time to detect the failure.

Poisson Distribution: Continuous probability distribution applicable to many Reliability problems, it is characterized by a constant probability of failure in small equal time intervals. It was originally studied by the great French mathematician Simeon Denis Poisson (1781-1840), well known also for his work in potential theory. The general form of Poisson Distribution also deals with multiple events in a given time.

Binomial Distribution: Discrete probability distribution that describes the odds of a certain event to occur exactly 'n' times. Under certain circumstances (discrete events, small number of trials) this distribution may be applicable instead of Poisson's. It is not covered or used in this paper.

Infant Mortality: Set of phenomena that results in probability of failure of a product in much larger numbers during the early part of its operation. This phenomenon is usually the result of problems in the manufacturing process.

Wear-out: Process that results in increased probability of failure late in the life of a product. It is usually the result of aging phenomena, not covered in this paper.

Single Component Failures in Time

Derivation of the Fundamental Formulas

The objective of this section to derive the probability of failure in a given time, as a function of more common parameters usually published by the manufacturers, like the Mean Time Between Failures (MTBF) or the Failures in Time (FIT).

The probability of *no-failure* as function of the probability of *failure* in any interval of time, for any element is obviously:

$$\mathrm{PNfail}(\mathrm{Pfail}) := 1 - \mathrm{Pfail}$$

And for no-failure within *any* of 'n' consecutive intervals 'T':

$$\mathrm{PNfail}(T) := (1 - \mathrm{Pfail}(T))^{n}$$

At this point we can not tell much more about the Probability of Failure in a finite, non negligible interval of time "T". It may not be clear in our mind what are the complications arising from the fact that a failure happening somewhere within the interval may affect the possible failures in another part or the interval. For example, can the device fail again if it has already failed? We can overcome this issue by making the interval under consideration sufficiently small so that no more than one failure can happen within this period. In that case, we can safely say:

$$\mathrm{Pfail}(\Delta T, \mathrm{MTBF}) := \lim_{\Delta T \to 0} \frac{\Delta T}{\mathrm{MTBF}}$$

And again, of course:

$$\mathrm{PNfail}(n, T, \mathrm{MTBF}) := (1 - \mathrm{Pfail}(T, \mathrm{MTBF}))^{n}$$

where: $\Delta T := \frac{T}{n}$

Going back to the formula derived above

$$\mathrm{PNfail}(n, T, \mathrm{MTBF}) := \lim_{n \to \infty} \left(1 - \frac{\frac{T}{n}}{\mathrm{MTBF}}\right)^{n}$$

This is an indetermination of the type "1^{∞}". This does not help in any way. A more deterministic result can be reached by manipulating the equations. First we remove the exponential expression by taking logarithms:

The new expression is:

$$\ln\left[\lim_{n\to\infty}\left(1-\frac{\frac{T}{n}}{MTBF}\right)^{n}\right]$$

re-writing it as:

$$\lim_{n\to\infty} n\cdot\ln\left(1-\frac{\frac{T}{n}}{MTBF}\right)$$

although we are getting closer, it is still an indetermination, but this time is of the type "∞ x 0". By re-writing it again as:

$$\lim_{n\to\infty}\frac{\ln\left(1-\frac{\frac{T}{n}}{MTBF}\right)}{\frac{1}{n}}$$

Still an indetermination but this time it is of the form "0 / 0" so we can apply L'Opital's rule. The rule states that the indeterminate expression will be equivalent (and the indetermination *might* be removed) if we substitute the numerator and denominator by their respective derivatives:

$$\lim_{n\to\infty}\frac{\left(\frac{1}{1-\frac{\frac{T}{n}}{MTBF}}\right)\cdot\left(\frac{T}{MTBF}\right)\cdot\left(\frac{1}{n^{2}}\right)}{\left(\frac{-1}{n^{2}}\right)}$$

Which is finally no longer an indetermination. So we now can simplify the $(1/n^2)$ expressions and remove the big parenthesis expression in the numerator (because its limit tend to approach '1'). Recall that in a previous step, this expression was the *natural logar*ithm of the Probability of no Failure. We then arrive at the final expression that we were pursuing, this time without the artificially introduced variable "n".

$$PNfail(T, MTBF) := e^{\frac{-T}{MTBF}}$$

The inverse of the MTBF is represented in the technical literature by the letter λ, so we also have an equivalent expression for the Probability of No-Failure (survival) for a finite, non negligibly small interval T:

$$PNfail(T,\lambda) := e^{-\lambda \cdot T}$$

This is a form of the Poisson distribution. It applies for constant probability of failure for a single element without redundancy.

This means that it applies when the probability of failure is *not* a function of the elapsed time in the product's life. In other words, it applies when there are no aging or settling phenomena that could increase or decrease the failure rate with time. This is a fundamental formula, which applies to most electronic components and appears very often in the Reliability literature.

Instead of its MTBF, another common way of stating the reliability of a component is its "FIT" (for "Failures In Time"). It is the number of failures experienced by a component in a pre-determined number of hours of operation, conventionally 10^9 hours. For counting the number of failures of a component, the theory assumes that the failed component gets instantaneously back in function, ready to perform (and to fail) again after a failure event. Based on these definitions we can then state:

$$\lambda := \frac{1}{MTBF} \qquad \text{and also} \qquad MTBF := \frac{10^9}{FIT}$$

The FIT number for electronic components are usually published by the component manufacturers and also tabulated for generic technologies (i.e. carbon resistors, aluminum electrolytic capacitors, etc.) and as a function of typical operational environments by certain entities (i.e.: Bellcore and Military Handbook #217). When available, manufacturer's data are usually more up to date with the technology. The data from the above mentioned agencies tend to be more conservative, and sometimes not updated frequently enough.

Summary

1) The component manufacturers and certain agencies publish the FIT and/or MTBF data of electronic products. The product reliability of reputable manufacturers is usually preferred for more up to date calculations.
2) The MTBF and FIT are related by the formula:

$$MTBF := \frac{10^9}{FIT}$$

3) The parameter "lambda" appears frequently in the Reliability formulas and literature and it is defined as:

$$\lambda := \frac{1}{MTBF}$$

4) The probability of no-failure of certain component in a certain given time interval is:

$$PNfail(T, MTBF) := e^{-\lambda \cdot T}$$

5) The hypothesis of constant failure applies to most electronic components. Notable exceptions include cases in which the wear out can not be neglected (CRT's, vacuum tubes, fans and blowers, etc.)

http://www.comsysdes.com
Voice & fax 510-792-1760
66 Santos Court
Fremont, CA 94536 - USA

Failures on Equipment with Multiple Components

Derivation of the Fundamental Formulas

Let us consider the following definition that applies to systems without redundancy, without loss of generality: "*A system is in failed state when any of its components is in failed state*".

The above simple statement implies that every component of the system has been designed to perform an essential function, that is none of the elements can fail without making the entire system to be in failure. In a non-redundant system, this is indeed generally the case. It is possible to conceive component failure modes that do not necessarily result in catastrophic failures of the system, ex. a resistor value changes such that it exceeds its tolerance specification. For this discussion however, we do not distinguish between "failure" and "almost failure". In both cases, we assume that the system performance was affected, resulted in some equipment down time and somebody had to take the time to repair or replace the failed component.

From the above discussion it is then clear that the probability of no-failure of a system with three components, for example, all necessary for the operation of the system is:

$$PNfailSysN := PNfailC1 \cdot PNfailC2 \cdot PNfailC3$$

Where "PnfailSysN" denotes the probability of no-failure of the system and "PnfailCx" denotes the probability of no failure of each of its components. Generalizing for the case of N

$$PNfailSys(N) := \prod_{i=1}^{N} PNfailC(i)$$

components, it becomes:

Where the symbol means "product of the “i” elements, with “i” from 1 to N".

Applying logarithms to the above expression, we convert the product into a summation:

$$\sum_{i=1}^{N} \ln(PNfailC(i))$$

Now, replacing in the formula that we found before about the probability of no failure of each component expressed in its MTBF

$$PNfail(T,\lambda) := e^{-\lambda \cdot T}$$

http://www.comsysdes.com
Voice & fax 510-792-1760
66 Santos Court
Fremont, CA 94536 - USA

form:

The new expression of the probability of no-failure of the system with N components becomes:

$$\sum_{i=1}^{N} \ln\left(e^{-\lambda_i \cdot T}\right)$$

Which is equivalent to:

$$\sum_{i=1}^{N} -\lambda_i \cdot T$$

Or also equivalent to:

$$-\left(\sum_{i=1}^{N} \lambda_i\right) \cdot T$$

Since the expression was the logarithm of the probability of no-failure, so we can say that:

$$\lambda sys\,(N, \lambda i) := \sum_{i=1}^{N} \lambda_i$$

This gives us the value of λ for the system given the λ values of each of its components. Keeping in mind that λ was equal to 1/MTBF we can apply the formulas that we derived before for the case of a single component.

Summary

1) The inverse of the MTBF of the system (all the components working together) is the sum of the inverse of the MTBF's of all the individual components.
2) Another way of stating the same conclusion in a more intuitive form is that the FIT's of the system is the sum of the FIT's of its individual components.

Redundancy with Perfect Switching

Derivation of the Fundamental Formulas

We will consider a system consisting of just one redundant element and will find out what is its probability of its failure given the probability of failure of the single element. To simplify our reasoning, we will assume that once a failure of the working element occurs, it is detected instantly and the standby element assumes the original function instantly. As described by the title of this section and also for simplicity, we will assume that the switch that swaps the active and standby elements is itself, not susceptible of failures. Another assumption that we make in here is that if a failure happens to the standby element, it will also be similarly detected.

When the active element fails, the full system functionality is recovered by switching to the stand-by element. The new functionality after switching does not include of course, the original redundancy feature itself. This is because the element that was originally active has now failed and cannot be used as the new stand-by. The probability of failure of the now non-redundant system is therefore a function of the time that it takes to make it redundant again. We now define a new parameter called Medium Time to Repair (MTTR). The MTTR is the time elapsed between the occurrence of the failure until the failure has been repaired and a new standby element is again available. As it follows from this description, the MTTR is not just a parameter of the element itself but depends also from the service policy and technical organization performing the repair. Depending on equipment accessibility, typical MTTR numbers are two hours, one day, two days, etc.

Since a redundant system essentially "heals" itself of a single failure, the service is normally not interrupted. The only case in which the service will suffer an interruption is *therefore if the second element, originally in standby, also fails before the MTTR*. The probability of failure of this *redundant system* is then the compound probability of failure of the first element *and* the second one *during* MTTR.

It is possible to identify an easy to conceptualize parameter for the redundant system, similar to the MTBF of non-redundant systems.

During a long period T, the stand-by system will need to be switched into service N times, that is:

$$N := \frac{T}{MTBFe}$$

Each time that a switch to the standby element occurs, the system will be operating without a standby element for MTTR hours. *In this condition, and only in this condition, the failure of the standby element would result in the failure of the entire system*.

In a long period T, the probability of the stand-by element to fail while it became active will be:

$$PfailR(T) := Pfail\left(\frac{MTTR}{MTBFe} \cdot T\right)$$

Where "PfailR" refers to the redundant system and Pfail is for a single element, as derived before. Replacing terms in the formula found before for the case on non-redundant systems we can quantify the results of adding redundancy.

$$PnfR(T) := e^{-\left(\frac{MTTR}{MTBFe}\right) \cdot T}$$

One way of describing this equation, is to say that the time variable used for calculating the probability of failure in a redundant system, is equivalent to the actual time, multiplied by a factor (typically very small) that represents the ratio of MTTR to MTBF. Thus, the probability of no failure of a redundant system as a function of time is:

$$PnfR(T) := e^{-\left(\frac{MTTR}{MTBFe}\right) \cdot T}$$

Calling MTBFR the Mean Time Between Failures for a Redundant system, it is:

$$MTBFR(MTBFe, MTTR) := \frac{MTBFe^2}{MTTR}$$

Defining λR similarly to the non-redundant case we will be able to use the formulas derived for non redundant systems.

$$\lambda R := \frac{MTTR}{MTBFe^2}$$

Notice that there is a subtle a change in the implications of a failure in a redundant system. It is still defined as the "inability to perform its function", only now, the number of elements that can fail in the field, has doubled. So even though there may not be any service disruption, the maintenance organization still has to visit the site to perform the replacement of the failed elements. Furthermore, it needs to do so *twice as often* as in the non-redundant case.

It is also possible to use the highly enhanced MTBF to optimize the technician visits, instead of rushing to restore service. The following plot shows the MTBF of the redundant system as function of the MTBF of the same system without redundancy and MTTR of 2 hours, one day and one week.

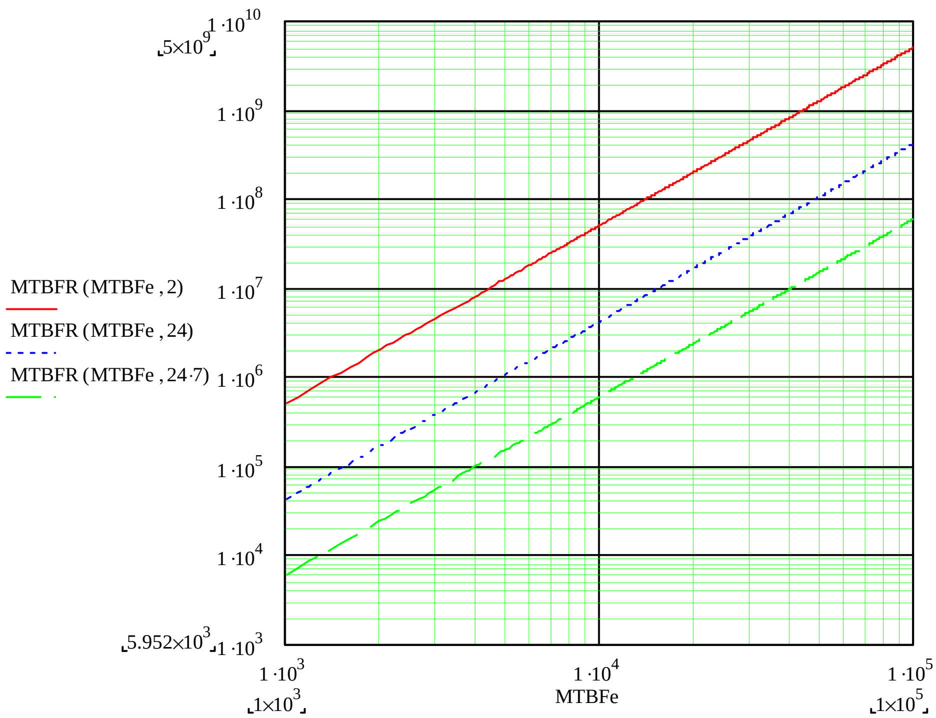

Figure 2: MTBFR as function of MTBF and MTTR

An interesting example from the plot above is providing redundancy to a system with an MTBF of 20,000 hours (a little over two years), which results in a redundant MTBFR of about 1,900 years if the MTTR is two hours. Extending the MTTR to one full day shortens the MTBFR to "only" 471 years. The service organization may find it useful to be able to choose between rapid service or a slower one, (for example, perform repairs only during a daily maintenance routine), especially if the slower response is still results in MTBFR of almost five centuries!

Summary

1) Redundancy multiplies the MTBF of a non-redundant system by a factor equal to the ratio between the MTBF of the non-redundant system to the MTTR, which is usually several orders of magnitude.
2) The enhanced MTBFR compared with the plain MTBF can be used to better schedule the maintenance and repairs.
3) The number of events (non service-affecting visits or repairs) might double when compared with the non-redundant case, assuming that the likelihood of failure is the same for 'active' and 'standby' elements (even though this is not always the case).
4) Even if the system has self-healed as result of its redundancy, the MTTR starts counting *from the time that the failure occurred, not from the time that the self-healed condition is detected* (which might happen much later in a routine inspection).

http://www.comsysdes.com
Voice & fax 510-792-1760

66 Santos Court
Fremont, CA 94536 - USA

Redundancy with Non-perfect Switching

Derivation of the Fundamental Formulas

In real life, the switching function between the failed element and the standby element, is itself, subject to failure. In the previous case, we assumed that the switch was perfect (FIT=0, or MTBFS= ∞). In the general case of non-perfect switching, we can state that *the probability of* *failure of the redundant system is the probability that either a) both redundant elements fail simultaneously OR b) the switching element fails*. (Note: Sometimes the switching element is designed such that it has failure modes that revert to a "pass-through" operation. We leave those cases out of this discussion. The interested reader can pursue those cases by splitting the failure cases in two, and considering each case separately).

Calling PnfRs(T) the probability of no failure of a redundant system with a fallible switch, MTBFs to the MTBF of the switch itself and combining the formulas that we derived in the previous sections.

Putting these words as an equation:

$$PnfRs(T) := e^{-\left(\frac{MTTR}{MTBR}\right)\cdot T} \cdot e^{-\left(\frac{T}{MTBFs}\right)}$$

Which is equivalent to:

$$PnfRs(T) := e^{-\left(\frac{MTTR}{MTBR}+\frac{1}{MTBFs}\right)\cdot T}$$

And also:

$$PnfRs(T) := e^{-(\lambda R+\lambda S)\cdot T}$$

We saw before that λR was orders of magnitude better than the non-redundant λ. Keep in mind that both λR and λ are just two different ways of expressing FIT's. From the formula derived above, which shows FIT's of the switch adding to the FIT's of the redundant system, we can conclude that in order to realize the advantages brought up by the use of redundancy, *the reliability of the switching element must be orders of magnitude better than the elements that it protects*.

http://www.comsysdes.com 66 Santos Court
Voice & fax 510-792-1760 Fremont, CA 94536 - USA

Operating on the above expression, we can use the general expressions derived before.

$$MTBFrs := \frac{MTBF^2 \cdot MTBFs}{MTTR \cdot MTBFs + MTBF^2}$$

ComSysDes

http://www.comsysdes.com
Voice & fax 510-792-1760

COMMUNICATION SYSTEMS DESIGN LLC

66 Santos Court
Fremont, CA 94536 - USA

MTBF plots for Redundant System with imperfect Switch

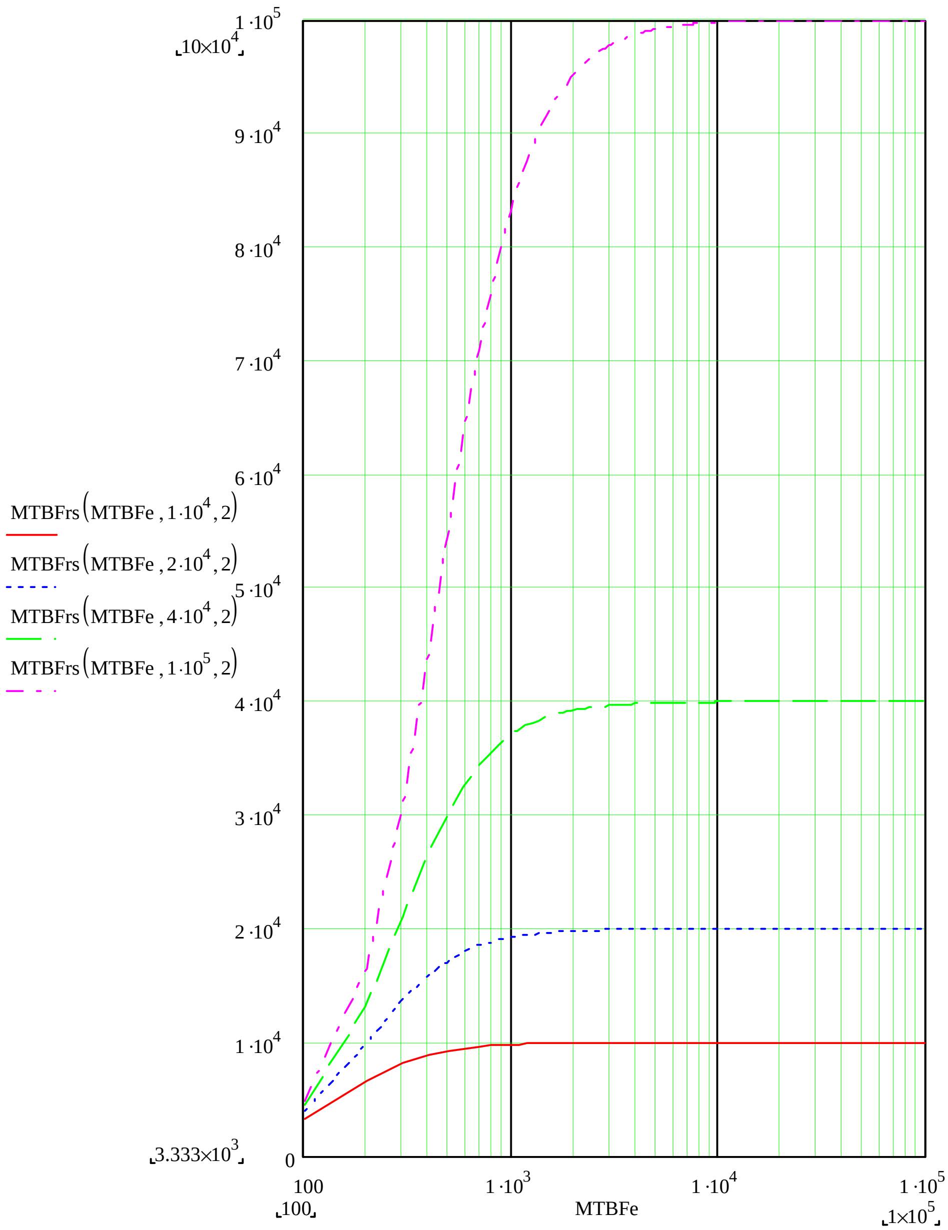

Figure 3: MTBF of redundant elements with imperfect switch (a)

The above graph shows MTBFrs as a function of MTBFe varying from 100 to 100,000 hours, MTTR of 2 hours and MTBFs as parameter, varying from 10,000 to 100,000 hours. Notice how quickly the switch begins to dominate the overall MTBFrs.

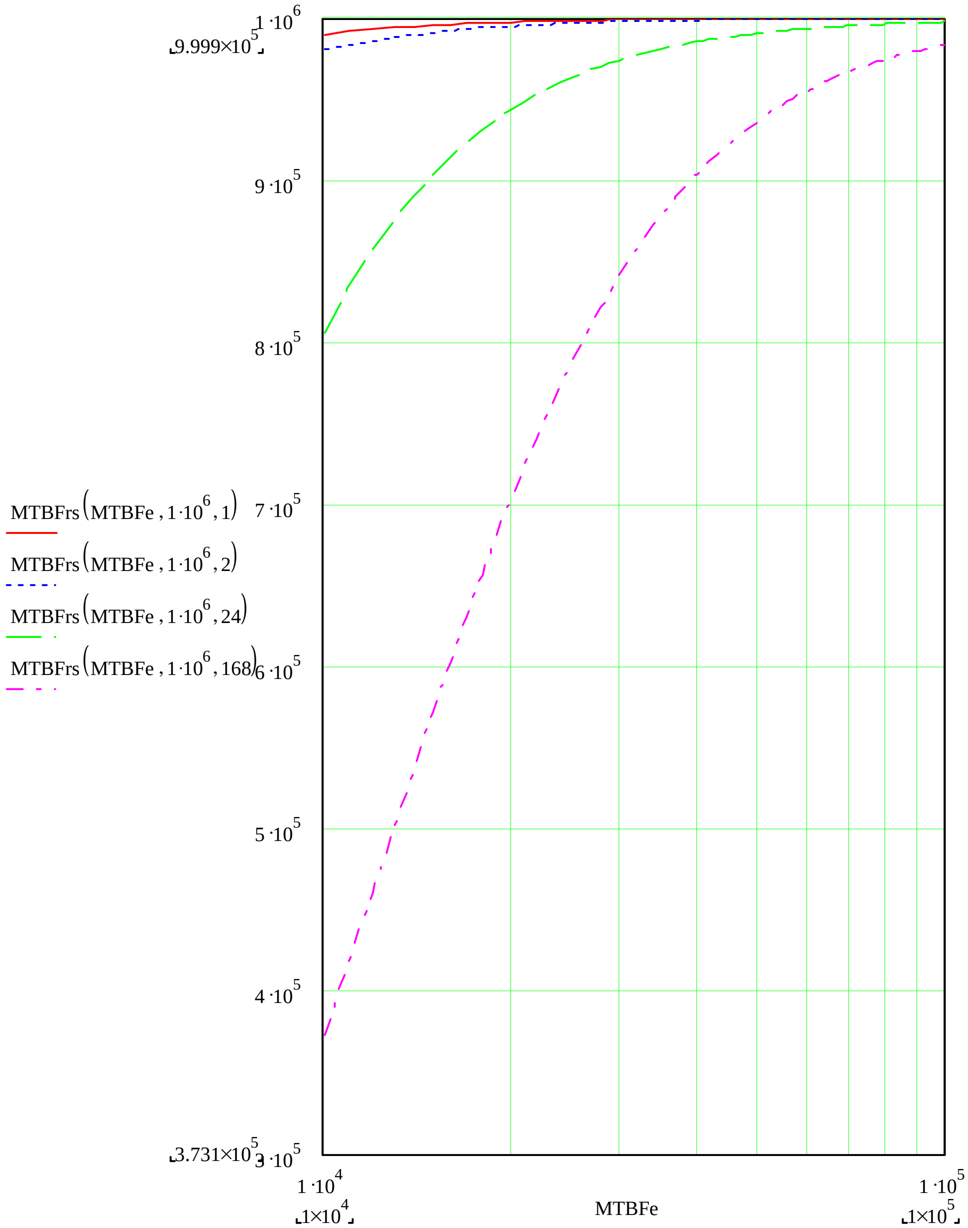

Figure 4: MTBF of redundant elements with imperfect switch (b)

This graph shows MTBFrs as a function of MTBFe varying from 10,000 to 100,000 hours, but with MTBFs fixed in 10,000,000 hours and different values of MTTR (one and two hours, one day and one week). Notice that for MTTR's as long as one week, the overall reliability increased in the order of 100 to 1,000-fold for reasonable MTBFe's

http://www.comsysdes.com
Voice & fax 510-792-1760
66 Santos Court
Fremont, CA 94536 - USA

Summary

1) The reliability of the redundancy switching element must be assessed separately from the functional elements. This is very important because the section that switches the functional elements from standby to active *might be embedded into the same substrate or PCB* as the functional elements (example: OR'ing diodes of two power supplies).
2) The fallible nature of an actual switch implementation is typically the determining factor of a redundant system or subsystem. The switching element should be designed such as its reliability is several orders of magnitude better than the elements under its protection.

Reliability Models & Calculation Example

In this chapter we introduce the concept of Reliability Models and will apply what we learned in the previous chapters by running some calculation examples. We will use the formulas to calculate some simple cases and illustrate the procedures. The purpose of presenting the basic formulas was to establish a foundation on which the interested reader could follow on.

Reliability Models

In Reliability discussions, it is convenient to use models that capture the essence of the matter, without being cluttered with elements not relevant to the topic. These models need to capture the following information:

1) Functional blocks
2) System operation dependencies
3) Redundancy features
4) MTBF or FIT of each block

These concepts will be introduced in the following example.

Example - Telecom Shelf, Partially Redundant

The problem consists of calculating the MTBF of a system given the MTBF of its parts and their functional relationships. This is a hypothetical product consisting of a chassis with one line card connecting from/to the public switched telephone network, two redundant cards that process the traffic, and two cards working together to covert the TDM traffic to/from IP traffic (a CAM card and an Ethernet card). This hypothetical system also consists of a single power supply to provide power to all cards.

The MTBF figures are known for all the cards, chassis, etc. in the system. The MTTR is assumed to be two hours. The figure illustrates the functional block diagram using some conventions that are typical in electrical and systems design:

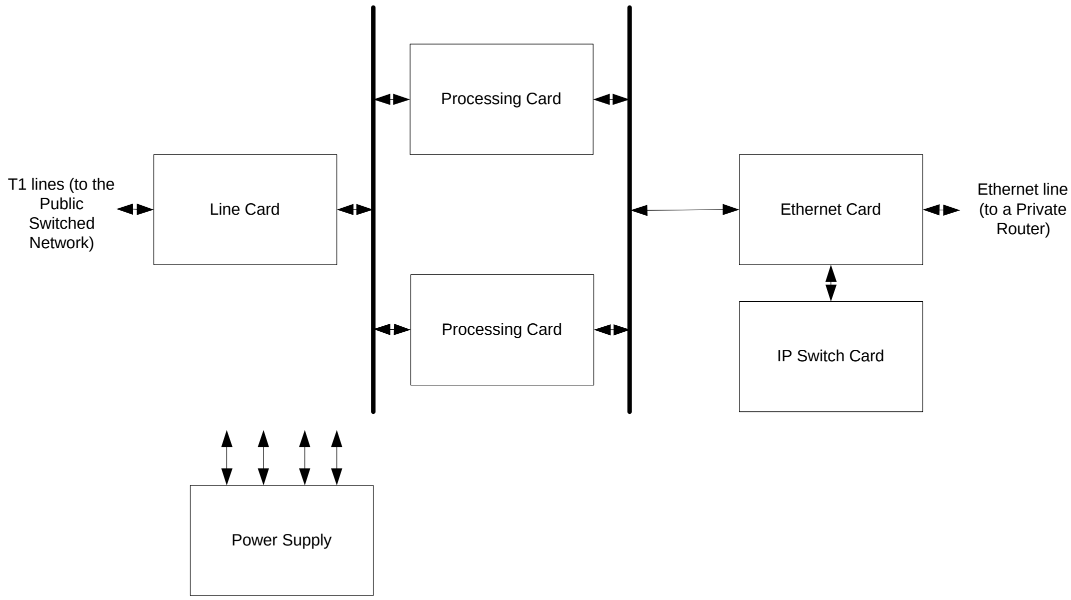

Figure 5: Telecom/datacom Shelf Block Diagram

We will now redraw it to shows the relationships and parameters for Reliability purposes:

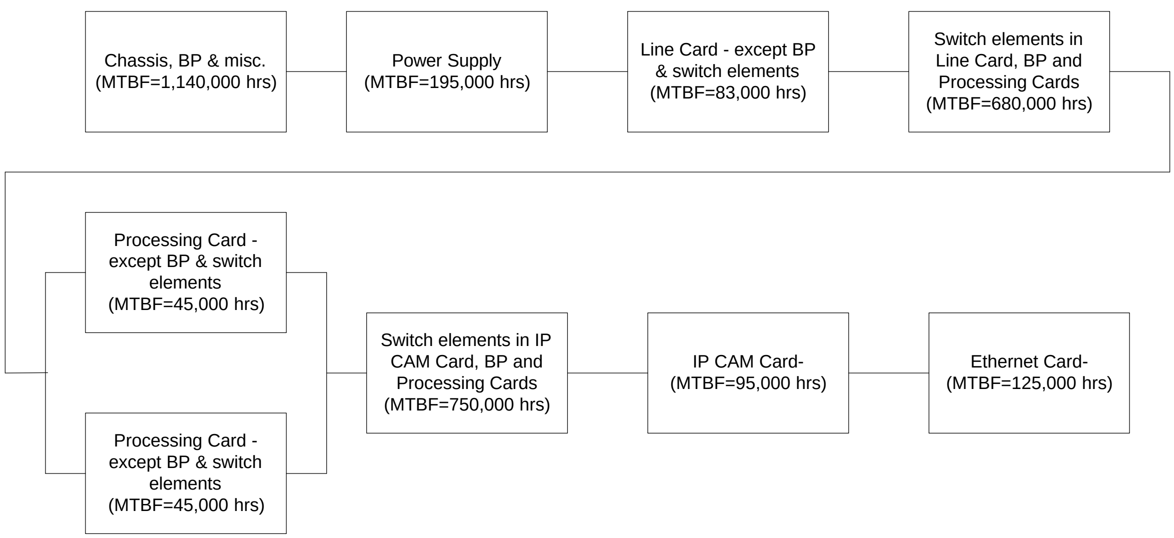

Figure 6: Reliability Block Diagram

Notice the following changes:

1) We placed the Power Supply "in series" with the rest of the blocks to explicitly show the dependency of the equipment on its operation (if it does not work, the system does not work).
2) Elements like the chassis, or most of the backplane, usually have a relatively high but not infinite MTBF. Therefore, we also show them in an explicit manner.
3) We assume that the components that provide the failure detection and switching to the standby elements are *embedded within the cards being switched*, as this is a typical implementation. Therefore, we have to segregate those components and show them explicitly because the influence of its MTBF in the resulting system MTBF will be very different.

Procedure:

1) Let us tackle the redundant cards first. We separated the elements that effect the switching from the active to the standby card, so we can use what we learned about perfect switching. We found before (see Summary of "Redundancy with Perfect Switching") that:

$$\text{MTBFR} \qquad , \text{MTTR}) := \frac{\text{MTBFe}}{\text{MTTR}} \qquad (45000\ 2) = \qquad 10^{9}$$

We also found before that the MTBF of the system is the inverse of the sum of the inverses of the each individual MTBF:

$$\frac{}{\frac{1}{1140000} + \frac{}{195000} + \frac{}{83000} + \frac{}{680000} + \frac{}{1.012\,10} + \frac{}{750000} + \frac{}{95000} + \frac{}{125000}} = \qquad 10^{4}$$

This is approximately 2 years and 11 months.

An alternate, and perhaps more intuitive approach for this step is to add the FIT figures. Based on the relationship between FIT an MTBF:

$\frac{1E+9}{1140000} = 877.193$ $\frac{1E+9}{195000} = 5.128\times 10^3$ $\frac{1E+9}{83000} = 1.205\times 10^4$ $\frac{1E+9}{680000} = 1.471\times 10^3$

$\frac{1E+9}{1.012\cdot 10^9} = 0.988$ $\frac{1E+9}{750000} = 1.333\times 10^3$ $\frac{1E+9}{95000} = 1.053\times 10^4$ $\frac{1E+9}{125000} = 8\times 10^3$

Adding the FIT figures gives 39380 equipment failures in 10^9 hours of service that result in service interruptions of up to MTTR (two hours) periods. It sounds like many failures, but this is the equipment FIT number, and they are distributed over 114,100 years (10^9 hours). By converting the equipment FIT to equipment MTBF we arrive at the same result as before, two years and 11 months.

