Design and Modeling Of A Dependable Network

Applying Dependability Attributes Models To Enhance Network's Performance

By

Muawia Mohamed Ahmed Mahmoud

A thesis submitted for Ph.D Degree

Sudan University Of Science and Technology
Graduate College
Electronic Engineering Department

Supervisor: Dr. Sid Ahmed Ibrahim
Co-supervisor: Dr. Osama Rayis

2006

CHAPTER ONE

Introduction

1.1 Problem definition:

The problem of the thesis concerns on how engineers can setup and study the main dependability attributes (Reliability, Availability, and Maintainability) of a network from failure data, how to use these models to evaluate the network, and how to use the results of the modeling to improve the network dependability. This is based on the fact that without these models, engineers and network's manager will not be able to measure and improve the dependability of the network.

1.2 Objectives of the thesis

The main objective of the thesis is to encourage network's engineers to take the dependability issues as an integral part of the network design.

One of the objectives is to draw the attention of network's designers and managers to the five nines number (0.99999) in reliability and availability as the main target when designing and managing the network.

Also it is necessary to stress that without the five nines, the network cannot be described as a highly dependable network (HDN), thus the thesis aims to have almost non-stop network service.

1.3 Hypotheses

1. Dependability models can be set using the network failure data.
2. The high dependability network cannot be achieved without modeling its reliability, availability, and maintainability.
3. Dependability models are the main guides to improve the network performance.
4. The five nines availability is considered as the standard for the high dependability network, which provide a high level of network's services.
5. As items connected in series increase, the network system dependability decreases, on the other hand, redundant items enhance system dependability.

1.4 Thesis methodology

The thesis follows the analytical and descriptive methods. Failure data was described, analyzed, and used to calculate the reliability and availability values. The maintainability issues were described to show their effects in increasing the network dependability.

1.5 Thesis overview

Chapter one describes the problem definition, which can be summarized in how to set the dependability attributes models, and how to use them in improving the network dependability. The objective of the thesis, the hypothesis, and the methodology of the thesis were explained in this chapter.

Chapter two describes failures, network's dependability attributes, and the relationship between failure rate and dependability attributes of the network.

Chapter three describes the techniques used when dealing with failures, including FMEA, FTA, and RCFA.

In chapter four the network's failure data collection and analysis are discussed in details. The SUST network failure data, which was taken as a case study, was organized in tables to be used in dependability models.

Chapter five explains the methods used in modeling the reliability of the network, and the SUST network reliability was measured using the field data collected. The effect of redundancy on reliability enhancement was discussed, together with various types of redundant configurations.

Chapter six describes the methods used to model the availability and explains the way the SUST network availability was modeled, and its deviation from the five nines standard was shown.

In chapter seven the maintainability issues were discussed including the levels of maintenance, corrective, preventive, and conditional maintenance. The maintainability function was measured. The effect of maintainability engineering on increasing the network dependability was discussed, and methods of choosing the appropriate maintenance policy for networks were explained in order to improve the network's dependability.

Chapter eight describes the dependability of wireless networks. The techniques used in defining the availability of wireless networks were discussed. User mobility, location, and fault propagation make dependability a challenging task in wireless networks. The main contribution of this chapter is to propose the fault tolerant design for wireless networks. The results show that the increased user mobility, can be compensated by deploying multi level redundancy, and the performance of wireless link is not critical in the overall availability as long as the link availability stays above a certain threshold.

Chapter nine discusses the results, and the main guidelines for network's engineers to have a dependable network. The relationship between the reliability and availability was explained.

1.6 Related work

The dependability as an inclusive term consists of many subsets. The three main subsets discussed in this thesis are the most important, which directly affect the network dependability level. The American Department of Defense (DoD), has along history of research into increasing the network dependability, but were limited to military applications. More recently, service web providers focus on network dependability researches aiming to increase the availability of their servers.

What distinguishes this thesis from past work, is that previous engineering researches did not take these three subsets together in one thesis as measures for network's dependability, instead, they concentrate almost on one of network dependability attributes, especially network security issues. For example David T. Smith in his book titled Reliability, Maintainability, and Risk, concentrated on Reliability and maintainability but he did not include the availability. Also Way Kuo focused on Reliability Issue only in his book Optimal Reliability Design Fundamental and applications, although it is consider as the latest book in this field. Network's security is considered as one of the dependability attributes that does not cause downtime since it focuses on blocking unauthorized people from accessing the network, unless a virus attack caused a service cut, besides, network security issue has its own techniques used to evaluate it. For this reason network security is taken as a related work, and there exist many researches in network's security.

Researches in Risk and system safety deal with some dependability topics, because system safety could not be achieved with poor system dependability. Procedures used in analyzing and modeling safety issues by someway touch the models of dependability.

The studies on the COTS (Commercial-On-The Shelf) as a modern approach in installing and operating networks can be one of the related work.

COTS levels of reliability and availability need further studies.

CHAPTER TWO

Failures, and Dependability Attributes

2.1 The dependability of networks

We are likely to meet a future where we rely on an increasingly wider range of information and communication services in our private, social and professional life. In addition to what we are familiar with today, some services will be invisible and provided by an ambient intelligent network. A part of the services will not be critical, while a continuous functioning of others will be mandatory for our productivity and well being. All of these services are intending to be provided by one integrated communication infrastructure. This requires that attention should be paid to availability, continuity of service, reliability, i.e. dependability issues, in its design and operation. The objective of this thesis is to identify some challenges and indicate tentative developments to cope with these dependability issues. One major class of challenges is posed by the steadily increasing complexity and heterogeneity with respect to services as well as service requirements, the technical installations, and the broad specter of parties providing these services. A foreseen development to deal with this is towards autonomy in (re)configuration, interaction between network entities and fault management. Another major class of challenges is posed by the necessity to have a well constructed model for the network to trace its behavior in order to notice any deviation of its intended reliability and availability.

The span of issues related to dependability is wide. The thesis concentrates on the system and service levels of the network, particularly, how to convert the failure field data to a form that is easily use this data in the models set for the network performance.

A high dependability (or synonymously robustness, reliability, availability or fault-tolerance) is in the current systems typically ensured by a high usage of dedicated spare resources and special designs. We have a trend toward more dynamic and flexible use of spare capacity, less special design, and at least, for the network, a less complicated redundancy structure and fault management.

Dependability of a network is the ability of the network to deliver service that can justifiably be trusted.

Dependability is defined as trustworthiness of the system, A systematic exposition of the concept of dependability consists of three parts: the attributes, the threats, and the means by which dependability is attained.

2.1.1 **The dependability attributes**:

Dependability is defined in terms of the following main attributes:

●**Reliability:**

It is the aspect of dependability referring to the continuity of a system correct service without failure for an intended period of time.

It is the probability that an item will perform a required function, under stated conditions, for a stated period of time. Since quality is defined as conformance to specification, reliability is therefore the extension of quality into the time domain. Reliability may be paraphrased as the probability of non-failure in a given period.

● **Availability:**

Refers to, system readiness for usage.

●**Maintainability:**

It is a measure of the ease and rapidity with which a system can be restored to operational status after a failure.

The probability that a failed item will be restored to operational effectiveness within a given period of time when the repair action is performed with accordance of prescribed procedure can be paraphrased as the probability of repair in a given time. There may be other attributes like safety, survivability, and confidence, but the attention is paid to the three main attributes reliability, availability, and maintainability taking into account that they lead automatically to the other attributes.

2.2 The threats: Faults, Errors, and Failures

Correct service is delivered when the service implements the system function.

A system failure is an event that occurs when the delivered service deviates from correct service. A system may fail either because it does not comply with the specifications, or because the specifications did not adequately describe its function. A failure is a transition from correct service to incorrect service.

A transition from incorrect service to correct service is service restoration.

The time interval during which incorrect service is delivered is a service outage.

An error is that part of the system state that may cause a subsequent failure.

A failure occurs when an error reaches the service interface and alters the service.

A fault is the adjudged or hypothesized cause of an error. A fault is active when it produces an error otherwise it is dormant.

An error is detected if it is indicated by an error message or error signal that originates within the system. Errors that are present but not detected are latent errors.

A system does not always fail in the same way. The ways a system can fail are its failure modes.

2.3 The means to attain dependability

The development of a dependable computing system and networks calls for the combined utilization of a set of four techniques:

1. Fault prevention, which means how to prevent the occurrence or introduction of faults.
2. Fault tolerance: how to deliver correct service in the presence of faults.
3. Fault removal: how to reduce the number or severity of faults.
4. Fault forecasting how to estimate or predict the present number, the future incidence, and the likely consequences of faults.

These four points can be measured and achieved only if appropriate models are set for the main dependability attributes, reliability, availability, and maintainability.

2.4 Failure rate:

Failure rate is the number of failures per unit time, and is expressed with the constant lambda (λ) with the unit of failures per hour, usually expressed in failure per million hours (FPMH).

2.4.1 Bathtub:

The bathtub shows typical values for failure rate.

Failure rate λ for an item or system is often not constant over its lifetime. It varies with time. Figure 2.1 shows the typical form of the graph showing how the failure rate varies with time. The graph because of its shape is referred to as the bathtub curve.

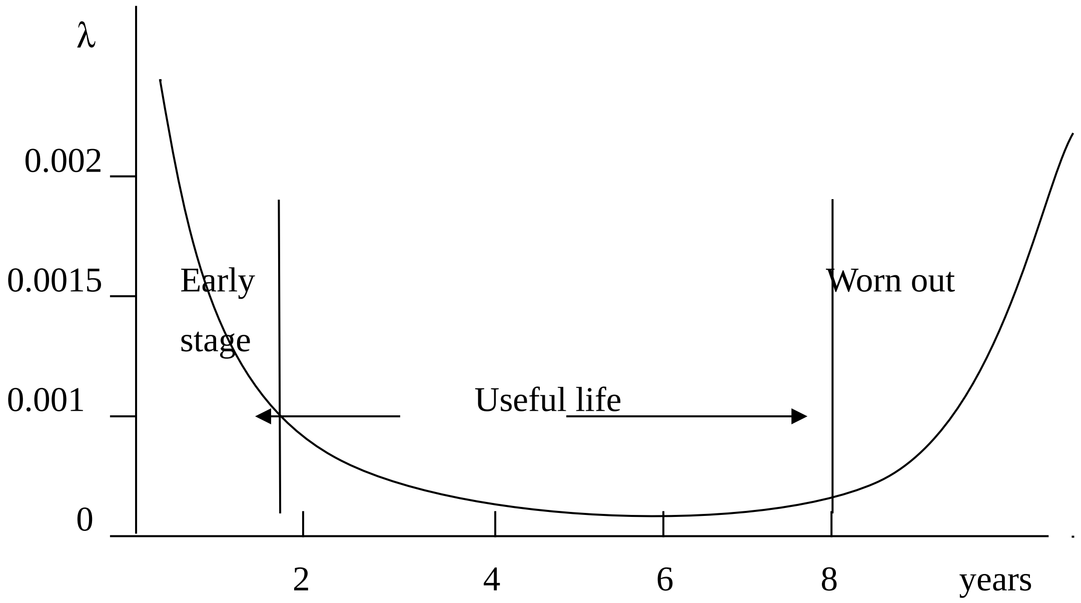


Fig 2.1 Bathtub

The graph shows three distinct phases: early failure, normal working life, and wear-out.

1. Early failure phase

During the early failure phase the failure rate decreases with time and a lot of failure occur. This is a result of manufacturing faults, sub-standard components, material imperfection, bad connections etc, which quickly result in failure following manufacture of the item. To overcome this, manufacturers may use a burn-in period, i.e. run the items for a period of time so that any such faults manifest themselves before the item is sold.

2. Normal working life

During this phase, all the items with manufacturing faults have been eliminated and there is an almost constant failure rate, the failures being due to random causes. This phase represents the useful working life period of use for an item or system.

3.Wear out

With this phase the failure rate increases due to the wearing out of components.

2.4.2 Realistic failure rates

In calculating dependability attributes, failure rate must be calculated first.

Failure rate can be divided into three levels:

A/ Level: Component failure rate.

B/ Level 2: Device failure rate.

C/ Level 3: System failure rate.

The most important fact is that component failure rate leads to device failure rate, since a device unit composed of may be tens or hundreds of components. Similarly, device failure rate leads to system failure rate.

There are many collections of failure rate for components collected by some organizations. Some collections are published data handbooks such as US MIL HANDBOOK 217. Some are in-house data collections, which are not generally available. These occur in large industrial manufactures.

It is important to read carefully any covering notes since, for a given temperature and environment, a component may exhibit a wide range of failure rates owing to:

1. Component source – the degree of screening (quality assurance).

2. Circuit tolerancing – the degree of design effort affects the proportion of failures attributable to parametric drift.

3. Reliability growth – the amount of field experience fed back affects the failure rate data.

Failure rate values can span one or two orders of magnitude as a result of different combinations of factors. The documented failure rates are useful in prediction calculations. Failure data is usually presented in a tabulated form. In electrical and electronic engineering fields component failure rates data is called microelectronics data.

In practice, failure rate is a system level effect. It is closely related to but not entirely explained by component failure. A significant proportion of failures encountered with modern electronic systems are not the direct result of parts failures but of more complex interactions within the system.

For this reason, network dependability calculation is taken at system level. The reason for this arises from such effects as human factors, software, environmental interference, and network system design.

Although empirical relationships have been established relating certain device failure rates to specific stresses, such as temperature, no precise formula exists which link specific environments to failure rates. General adjustment (multiplying) factors have been evolved and these are often used to scale up basic failure rates to particular environmental conditions. The resulting Mean Time Between Failures (MTBF), availability, and reliability values are general guides to design dependability.

2.4.3 Microelectronics data

There are many sources for this data. The most common sources used by engineers for estimating failure rates are US Military Handbook 217 F, British Telecom HRD4, and French PTT, CNET data bank

Table 1.1 presents a sample of the data range from the above-mentioned sources for four temperature values of the most common used microelectronics devices.

		Up to 30^0 c	Approx. 50^0 c	Approx. 75^0 c	Approx. 100^0 c
Bipolar					
Linear	5 trans	0.04 - .07	.05- .08	0.05 - 0.15	0.10 – 0.30
	25 trans.	0.04 - 0.1	.05 - .08	0.05 - 0.15	0.10 – 0.30
	100 trans.	0.04 – 0.2	.05 - 0.2	0.05 - 0.25	0.15 - 0.50
Digital	50 gates	0.02 - 0.1	.02 - 0.2	0.03 – 0.6	0.05 – 1.5
	500 gates	0.03 - .20	.03 – 0.3	0.03 – 1.0	0.07 – 3.0
	1k gates	.05 – 0.30	.05 - .50	0.07 – 1.2	0.15 – 3.0
MOS					
Analog	5 trans	0.04 - .07	.05 – 0.1	.05 – 0.2	0.1 - 0.30
	25 trans.	0.04 - 0.1	.04 – 0.1	.05 – 0.2	0.1 - 0.35
	100 trans.	0.04 – 0.2	.05 – 0.2	.05 – 0.4	0.1 – 0.40

Digital				
NMOS 2k	.15 – 0.4	.15 – 0.7	0.2 – 2.0	0.5 – 6.0
CMOS 2000	.15 – 0.6	.15 – 2.0	0.2 – 10.0	0.5 – 40.0

Table 2.1 Ranges of failure rate (per million hours)

In general, this data represent the maximum and minimum failure rates indicated for these devices in the original data.

To estimate a value from the range given in the data sheets, the arithmetic mean can be used, but most of engineer use geometric mean since it is a more desirable parameter for describing the range.

2.5 Overall data

The previous section concentrated on the particular case of microelectronics failure rate data for some components there is fairly close agreement between different data banks and in other cases there is a wide range of failure rates due to a number of reasons as, for example:

1. Some failure rates include items replaced during preventive maintenance whereas others do not. This can affect rates by an order of magnitude.

2. Failure rates are affected by the tolerance of a design and this will cause a variation in the values.

3. Although nominal environmental and quality levels described in some data, the range of parameters covered by these broad descriptions is large. They represent, therefore, another source of variability.

4. Components parts are often only described by reference to their broad type. Data are therefore combined for a range of similar devices rather than being grouped, thus widening the range of values.

There are many software packages consist of database summary of all electronic components and devices. They show for each component, the range of failure rate values that is to be found from them. Failure mode percentages are also included in this database.

2.5.1 Field data

In all cases, site-specific data or even that acquired from identical or similar equipment, and being used under the same operating conditions and environment, should be used in place of any published data. Field data must be collected by an specialist engineer. Such data may contain a range for each item. The ranges can contain:

1. A single value: the value can be used without need for judgment unless the specific circumstances of the assessment indicate a reason for more optimistic or pessimistic failure rate estimate.
2. Two or three values: in the absence of any specific reason to favor the extreme values the predominating value (center column) is the most credible choice.

2.6 Failure severity

For any dependability assessment to be meaningful it must address a specific system failure mode. The failure rates, mean time between failures, or availabilities must be assessed for defined failure types (modes), and also the severity of this failure. The impacts of failures on the operation differ according to the nature of failure. Therefore classification is much better done by severity and come up with the failure intensity for each classification.

At least three classifications are in common use:

- Cost impact
- Human life impact
- Service impact.

Cost impact is particularly applicable to any system that is operating in the business world. What does the failure cost in term of repair and recovery.

The repair cost depends basically on the Mean Time To Repair (MTTR) service cost in addition to the cost of running the system with the reserved backup system.

Human life impact is appropriate for any kind of system where safety is important.

Service impact might be appropriate for any network, since it affects the providing of the intended service for customers. In practice severity classification of failure are often made by more than one person. There are many principle approaches to handle severity classification in estimating the dependability of the network or any other system. Severity of failure can be classified by using a class code as:

I For tolerant or minor failures

II For basic service degradation failure

III For failures that cause service interruption, or major failures.

To explain these classes assume the telephone network:

An example for class I minor failures such as mistimed ringing.

An example for class II is excessive wait for response.

And the example of class III would be the inability of the telephone network switching system to process calls.

It is useful to work with classes of failures to focus attention on particular aspects of dependability. Failure classification makes it possible for the dependability goals of the network to be achieved at costs that are economic and with schedules that are reasonable.

2.7 Failure Ratio (FR) for repetitive Failures

A careful consideration must be given to failure repetition that is how to count and handle identical failures. Identical means that when the same run is made, the same deviations of behavior from requirements occur, at the same site or different site. Failure ratio can be used to notice the repetitive failures, and can be calculated as follows:

Let T be the operation time of the network system

m number of a certain failure occurrence

N the total number of failures occurred

n any failure

Fr the failure ratio,

Then $Fr = m/N$

Since $N = \sum_{I=1}^{n} n_i$ so

$$Fr = m/\sum^{n} n_i \quad \text{for a period of T.}$$

I=1

T may be a day, a month, or a year. In normal operation T is taken as a year.
When T changed, the value of Fr will be changed also. Failure occurrence can be plotted for a certain period of time for all failure as shown in figure 2.2.

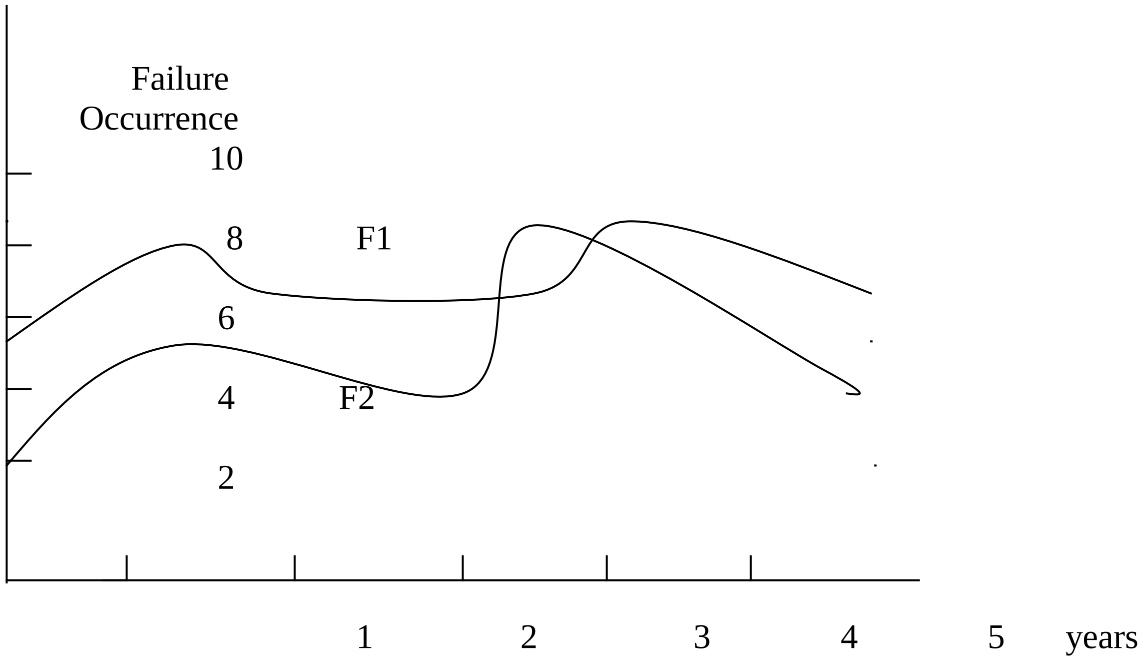


Figure 2.2 Failure Occurrence for a long period of time

2.7.1 The network item failure ratio

Since the network consists of many items, like servers, cables, and connectivity devices, the item failure ratio gives a clear idea about the weakness in these items. It can be calculated as follows:

Let T be the period of the given item

n number of failures in a given item

N total number of failures for all items

Fr_{item} the failure ratio

Then:

$Fr_{item} = n/N$ for a given period of time.

2.8 Life cycle process:

Life cycle begins at the moment when the idea of a new system is born and finishes at the moment when the system is safely disposed. Thus the main processes through which any human-created system goes are:

Specifications

Design

Production

Utilization, and Retirement

2.8.1 The specification process

The specification process is a set of tasks performed in order to identify the needs and requirements for the new system and transform them into a technically meaningful definition.

In the first phase of the life cycle of a system, the needs and requirements, which the future system should satisfy, have to be clearly specified. The mean reason for a new system could be:

a/ A new need for a new function to be performed; or b/ Deficiency of a present used system due to:

Functional deficiency

Inadequate performance

Extremely high maintenance cost

Low demand from the market, Low profit provided to the company

The input characteristics of the specification process are the needs for new system, and the output characteristics are the fully described functionality of the system.

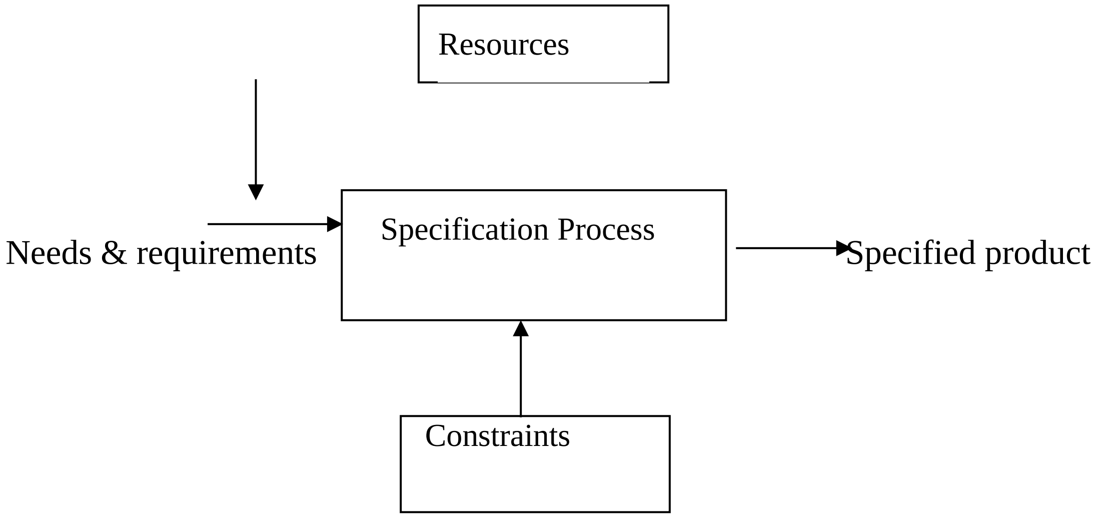


Figure 2.3 The specification process

2.8.2 The design process:

The design process is a set of tasks performed in order to transform the specification for a new system into full technical definition.

The main tasks performed during the design process are:

Management

Planning

Thesis

Engineering design

Documentation

Design of software

Building a prototype

Test and evaluation

Thus the main objective of the design process is to determine and define all items of which a future system consists and to define their attributes as well as relationships in order for the system to meet the needed function according to the specified requirements.

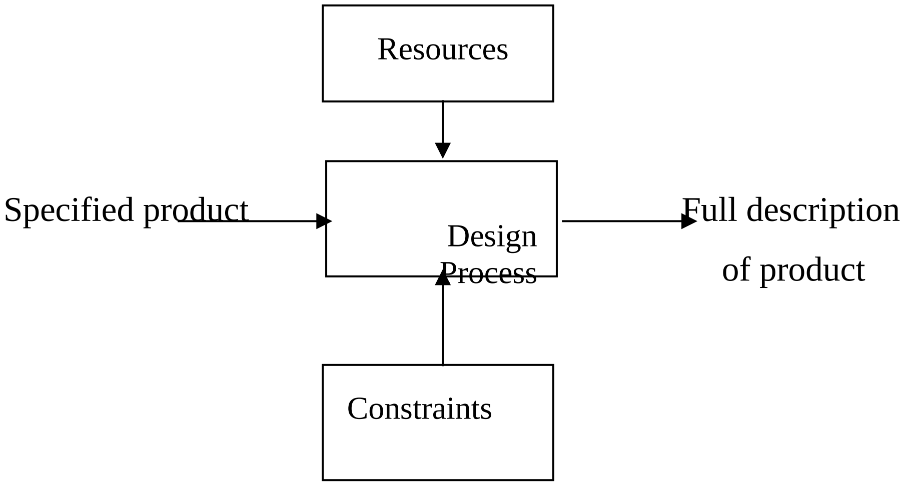


Figure 2.4 The design process

2.8.2.1 Effect of design stage on dependability

Very few integrated design teams deliberately skimp on provisions for attaining the full maintainability requirements in their creations. However some of the following dangers are always present: [2]

Oversight

Lack of specific knowledge

Rationalization.

This type of obstacles occurs in cases when the design team fails to take care of one of those innumerable details, which make up the completed design. For example, a design team may fail to indicate an important item on the drawing. Thus if this oversight is not caught, a substantial delay in completion of a corresponding maintenance task might occur.

It is fair to say that members of design teams cannot know all there is to be known about everything connected with every design, nor do they have the time to verify every detail. Consequently, all design teams do what they can to check where they believe it necessary. For instance, the design team may specify the use of specific test equipment or a tool which was the best available for the purpose the last time there was a need for it. However, a new technology that function better may have become available.

2.8.3 The production/construction process

The production/construction process is a set of tasks performed in order to transform the full technical definition of the new system into its physical existence.

The main tasks performed during this process are:

Management

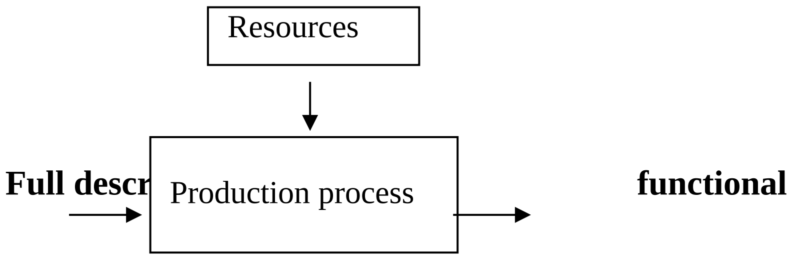
Operation analysis

Manufacturing

Assembling/construction

Testing

Delivery .



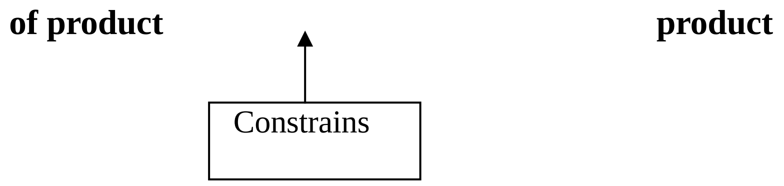


Figure 2.5 The production process

During this process the system is physically created in accordance with the design definition. At the end of this process a system physically exist which fully satisfies all needs and requirements and is ready to be utilized.

2.8.4 The utilization process

The utilization product is a set of tasks performed with objectives to utilize the inherent functionality of a new system in order to satisfy an identified need.

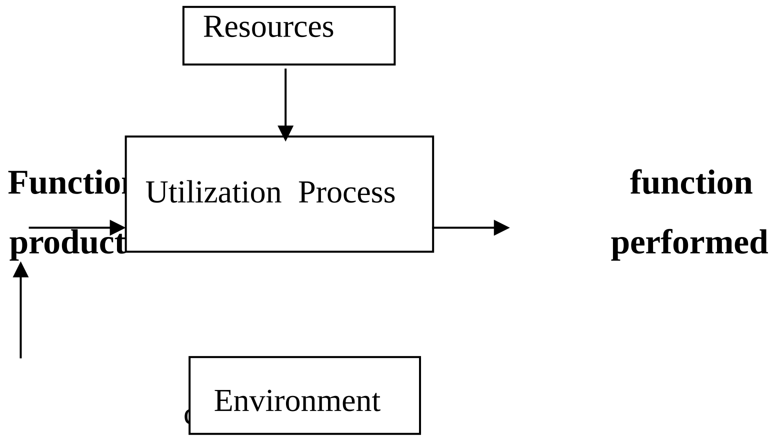


Figure 2.6 The utilization process

The main tasks performed during this process are:

Management

Distribution

Operation

Maintenance

Support

Modification

2.8.5 The retirement process:

The retirement process is a set of tasks performed in order to phase a system out at the end of its useful life.

The main tasks performed in this process are:

Management

Phase-out

Documentation

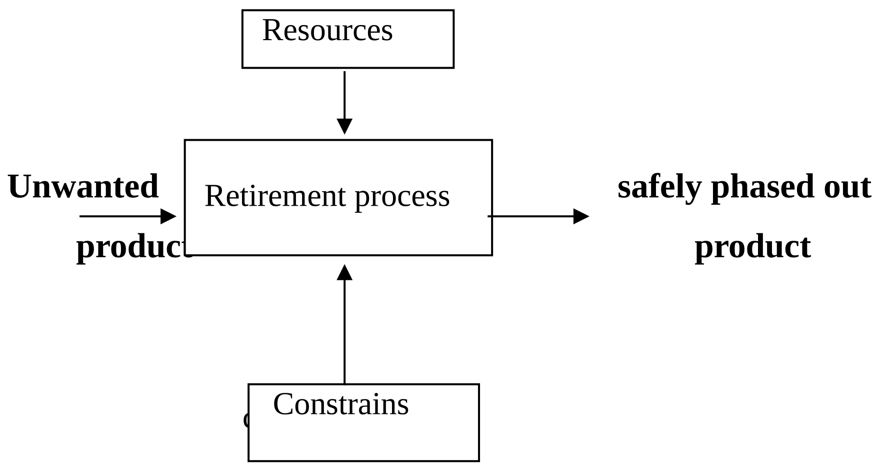


Figure 2.7 The retirement process

Withdrawal from the operation is the last process in the life cycle of the system. This means the actual end of its operational life due to loss of its functionality or to any other reason like lack of maintenance management or destruction due to disaster.

The lack of maintenance almost represents the main reason of this process, which means that well-established maintenance management increases the utilization period, thus more dependability.

2.9 The exponential law of failure:

Consider there to be a constant failure rate λ and a situation where at time t = 0 there are N_0 items and no items are repaired but just eliminated from this number when failure occur. As a result of failures, after a further interval of time δt, the number has decreased by δN. thus the change in number is -δN and so the failure rate is[4]

$$\text{Failure rate } \lambda = -\delta N / N\delta t$$

In the limit when $\delta t \longrightarrow 0$, we can write

$$\lambda = (-1/N)\, dN/dt$$

We can solve this differential equation by the separation of the variables method.

Thus if we have N items left at time t, we can write

$$\int_{N_0}^{N} (1/N)\, dN = -\int_{0}^{t} \lambda dt$$

And so

$$\ln N - \ln N_0 = -\lambda t$$

This can be rewritten as:

$$N = N_0\, e^{-\lambda t}$$

This exponential equation describes how the number of usable items changes with time due to a constant failure rate.

The above equation can be rewritten as:

$$N/N_0 = e^{-\lambda t}$$

Where N/N_0 expresses the reliability because it describe the probability that the system will run without failure, so:

$$\text{Reliability } R(t) = e^{-\lambda t} \qquad (2.1)$$

The unreliability is the [(number of failure)/N_0] and so:

$$\text{The Unreliability} = 1 - e^{-\lambda t} \qquad (2.2)$$

Figure 2 shows how reliability and unreliability change with time.

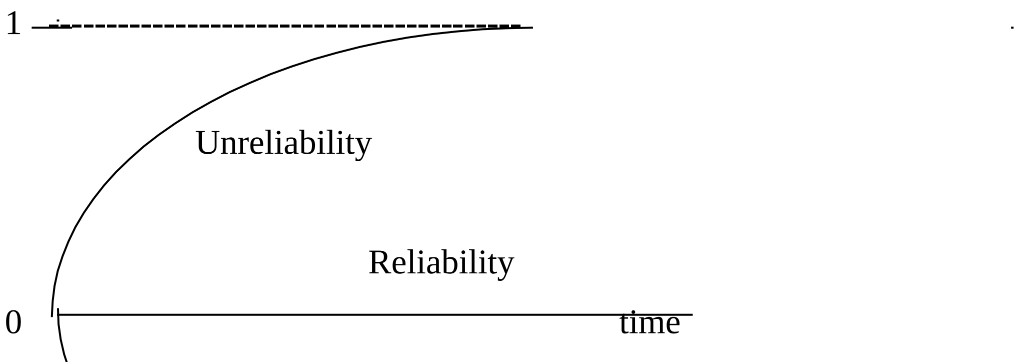


Figure 2.7 Reliability and Unreliability plotting

2.10 The Weibull distribution

The Bathtub curve showed that, as well as random failures, there are distributions of increasing and decreasing failure rate. From the exponential law of failure we saw that:

$$R(t) = \exp\left[-\int_{0}^{t} \lambda(t)\, dt \right]$$

Since the relationship between failure rate and time takes many forms, and depends on the device in question, the integral cannot be evaluated for general case.

In practice it is found that the relationship can usually be described by the following three-parameter distribution:

$$R(t) = \exp\left[- \frac{(t - \gamma)}{\eta}^{\beta} \right] \qquad (2.3)$$

β is the shape parameter

γ is the location parameter, and η is the scale parameter.

β describes the rate of change of failure rate. Increasing, or decreasing.

If $\beta = 1$, then constant failure rate can be assumed.

If $\beta > 1$ then failure rate is increasing (see the bathtub).

If $\beta < 1$ then the failure rate is decreasing.

in many cases a two parameter model is sufficient to describe the data. [1]
Hence:

$$R(t) = \exp\left[- (t/\eta)^{\beta} \right]$$

In this case $\gamma = 0$ which mean that the time origin at $t = 0$.
If $\gamma = 0$, and $\beta = 1$, the expression reduces to the exponential case with η giving the MTBF, thus $1/\eta = \lambda$ (failure rate).
$f(t) = \lambda e^{-\lambda t}$ is the probability density function (pdf) of the exponential distribution. (Appendix 4 shows the effect of λ on the pdf of the exponential distribution).
If the time does not start at t=0, the location parameter γ will be the start point at time domain, so the exponential distribution is shifted to the right of the graph by a distant equal to γ. This case occurs when the mean time between failures (MTBF) is considered starts after t= γ from the system operation time. (Appendix 5 explains the effect of γ on the exponential reliability function).
Failures are generally classified as:
Byzantine failure = system returns wrong values.
Stopping failure = no service being delivered at all.

2.11 Downtime and repair time

It is necessary to introduce Mean Down Time and Mean Time To Repair (MDT, MTTR). There is frequently confusion between the two and it is important to understand the difference. Down time, or outage is the period during which equipment is in the failed state. It is necessary to define down time as required for each system under given operating conditions and maintenance arrangements. MDT and MTTR, although overlapping are not identical. Down time may commence before repair.

A system not in continuous use may develop a fault while it is idle. The fault condition may not become evident until the system is required for operation. Is down time to be measured from the incidence of the fault, from the start of the alarm condition, or from the time when the system would have been required?

Repair may have been completed but it may not be safe to restore the system to its operating condition immediately. Repair often involves an element of checkout or alignment, which may extend beyond the outage.

The definition and use of these terms will depend on whether availability or the maintenance resources are being considered.

Figure 2.8 shows the elements of down time and repair time.

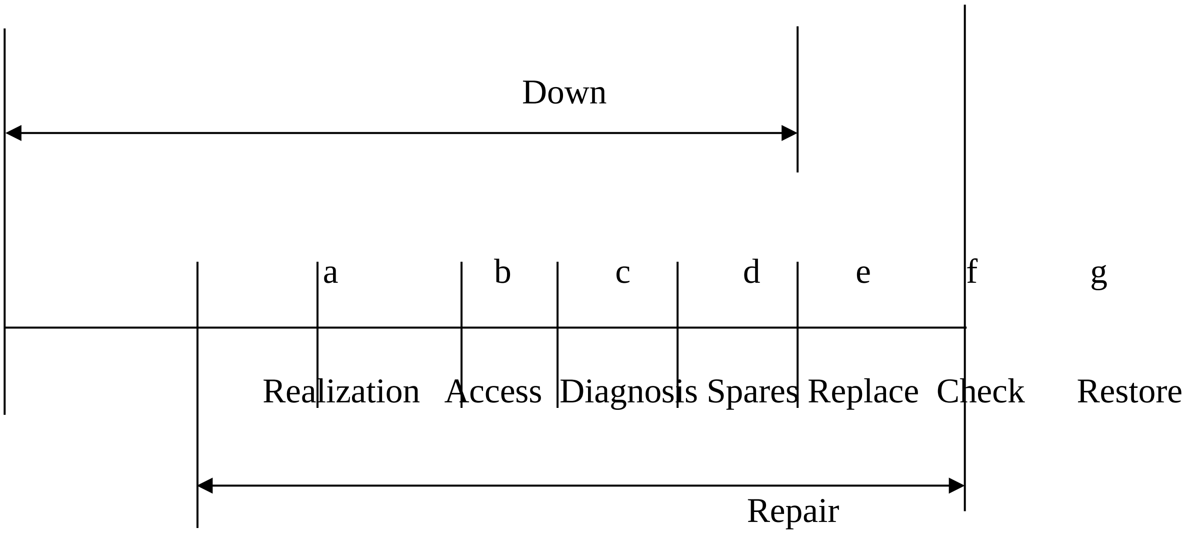


Figure 2.8 Elements of down time and repair time

a. Realization time: this is the time, which elapses before the fault condition becomes apparent. This element is pertinent to availability but it does not constitute part of the repair time.

b. Access time: this involves the time from realization that a fault exists, to make contact with displays and test points and so commence fault finding. This does not include travel but the removal of covers and shields and the connection of test equipment. This is determined largely by mechanical design.

c. Diagnosis time: this is referred to as fault finding and includes adjustment of test equipment, carrying out checks, interpretation of information gained, verifying the conclusions drawn and deciding upon the corrective action.

d. Spare part procurement: part procurement can be from the tool box by taking a redundant assembly. The time taken to move parts from the store to the system is not included, being part of the logistic time.

e. Replacement time: this involves removal of the fault followed by connection and wiring , as appropriate of a replacement. Replacement time is largely dependent on choice of assembly and on mechanical design features such as the choice of connectors.

f. Checkout time: this involves verifying that the fault condition no longer exist and that the system is operational. It may be possible to restore the system to operation before completing the checkout.

g. Restore time: as a result of inserting a new module into the system adjustment may be required. As in the case of checkout, some or all of the alignment to restore the system may fall outside the down time. [1]

Activities (b) to (e) are called Active Repair Elements (ARE) and (f) and (g) are called Passive Repair Elements (PRE). Realization time is not a repair activity but may be included in the MTTR where down time is the consideration. Checkout and alignment for restoration, although utilizing manpower, can fall outside the down time. The active repair elements are determined by design, maintenance arrangements, environment, manpower, instructions, tools and test equipment.

Another parameter related to outage is Repair Rate (μ). It is simply the down time expressed as a rate, therefore:

$$\mu = 1/\text{MTTR}$$

2.12 Hazard and risk

Hazard is usually used to describe a situation with the potential for injury or fatality whereas failure is the actual event, be it hazardous or otherwise.

Risk is a term, which actually covers two parameters. The first is the probability of a particular event. The second is the scale of consequence perhaps expressed in term of fatalities.

2.13 Quantifying failure

The failure may be critical in that there is a total loss of the function of the system and it can no longer be used or just that the item has gone out of its specification limits but can still be used.

For an item, which is tested for a time t and repaired each time it fails, then if it fails N times, the mean time between failures (MTBF) is:

$$\text{MTBF} = t/N$$

If over a time t there are N failures, then:

$$\text{Failure rate } \lambda = N/t = 1/\text{MTBF}$$

To illustrate the above, consider a unit is used in a network. The time interval in days between successive failures of that unit is recorded as:

12, 20, 15, 26, 32, 17, 16, 31, 22, 19 days (look at (t) in figure 1.9)

The MTBF for this unit is thus:

$$(12+ 20+ 15+ 26+ 32+ 17+ 16+ 31+ 22+ 19)/10 \quad = 21 \text{ days.}$$

The failure rate $\lambda = 1/21 = 0.048$ failure per day.

The MTBF and λ are terms used for repairable systems and elements. When items are not repairable, the measure is the mean time to failure (MTTF). It is the average time before failure occurs.

Failure rate, which has the unit of t^{-1}, is commonly expressed as per 10^6 hours. MTTF (Mean Time To Failure) is applied to items that are not repaired, and MTBF to items, which are repaired. The time between failures excludes the down time. MTBF therefore means up time between failure as illustrated in Figure 2.9 and it is the average of the values of (t).

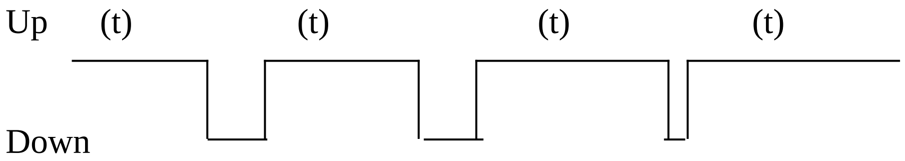


Figure 2.9 Up and down Time

2.14 Dependability planning of networks

This is concerned with models and methods for dependability planning, operation, and maintenance of networks, and the application of these methods to the various services in the network taking into account the following:

(a) That economy is often an important aspect of dependability Planning.

(b) That the ability of achieving a certain level of dependability Differs between network providers.

(c) That network providers often operate in a competitive environment.

(d) That there exists no unambiguous way of implementing these objectives in planning.

(e) That there is a need of establishing a method for dimensioning and allocating dependability in networks.

2.14.1 Dependability planning methods

Dependability planning may be accomplished by using essentially two different methods.

2.14.1.1 Intuitive method

The level of dependability is determined by making a synthesis of objectives and procedures presently used. It is a pragmatic method in absence of an analytical method or in the case when necessary data for a thorough analysis is not available.

This method reflects the present status, but is inconsistent in achieving what administration actually wants to attain the most economic level of dependability taking into account customer needs.

2.14.1.2 Analytical method

This method is based on principles defining the object of dependability planning. The principles are realized through a quantitative model. The level of dependability is deduced by applying the model, taking into account all relevant factors in each planning case.

2.14.2 Basic principles

The main object of dependability planning is to find a balance between the customers needs for dependability and their demands for low costs.

Fault consequences are expressed in terms of money and are included as additional cost factors in planning and cost optimization. The cost factor reflects the customer’s experience of failures in the network, quantified in terms of money.

2.14.3 Application

The administration is provided with a method to integrate the dependability as a natural part of planning. This method enables the preparation of simplified planning rules.

The application of the analytical method using dependability modeling gives the best level of dependability. This reduces the customer complaints and loss of business.

It is therefore considered as the best general way of planning dependability for the administration as well as for the customers.

2.15 Models used for dependability

2.15.1 Modeling

Models can be divided into many types. One can distinguish physical, symbolic, and mental models.

Symbolic models are less problematic to manipulate and build than others. They can further be divided into mathematical or non-mathematical models. The latter may be either linguistic such as verbal or written descriptions of events, graphic models such as pictures, graphs, or drawings, or schematic like flow charts, maps, or network diagrams. They have the common property that it is often very problematic to obtain precise information from them.

For many reasons mathematical models are the most important and the widely used category of models. They are concise and uniquely interpretable, while their manipulation and the evaluating of alternatives are relatively inexpensive.

A mathematical model can be defined as the mapping of the relationships between the physical variables of the system to be modeled into corresponding mathematical structures.

When such relationships are given for the steady state only, the model has static character and is described with algebraic equations. On the other hand dynamic mathematical models include the transient as well as the steady state behavior of a system and are described by a system of differential equations and by a set of boundary conditions.

The dependability is described by measures defining the availability , the reliability, and the maintainability performance of the network, which are achieved by modeling these dependability attributes. The recommended measures are:

(a) Availability modeling

Describes the mean accumulated down time. The model used is the mathematical model that measures the availability. That is

Availability (A) = Uptime/(Uptime + Downtime), or

$$A = MTBF/(MTBF+MTTR)$$

(b) Reliability modeling

Describes the probability of a network to run without a failure. The models used are:

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

(ii) $R(t) = \exp\left[- (t/\eta)^{\beta} \right]$ (weibull law)

(c) Maintainability modeling

Describes the mean administrative delay, the mean active repair time, and methods used to analyze and isolate failures.

Models used are Failure Mode Effect Analysis (FMEA), Fault Tree Analysis (FTA), Root Cause Failure Analysis (RCFA), and maintainability function M(t).

2.16 The cost of dependability

The practice of identifying dependability costs needs to collect and analyze the highly significant data for this purpose. Attempts to set budget levels for the various elements of dependability costs are even rarer. This is unfortunate, since the contribution of any activity to a business is measured ultimately in financial terms and the activities of dependability are not exception. If the costs of failure and repair were more fully reported and compared with the costs of improvement then greater strides would be made in this branch of engineering management.

Dependability analysis entails extracting various items from the account and grouping them under three headings:

Prevention Costs – costs of preventing failures.

Appraisal Costs – costs related to measurement.

Failure costs – costs incurred as a result of scrap, rework, and failure.

2.16.1 Prevention costs

Design review – review of new designs prior to the release.

Reliability training cost of the staff.

Audits – audits of system products and processes.

1.16.2 Appraisal costs

Test and inspection – all line test and inspection activities . if the inspectors or test engineers are direct employees then the costs should be suitably loaded.

Maintenance and calibration – the cost of labor and subcontract charges for the calibration, overhaul, upkeep and repair of test and inspection equipment.

Installation testing – test during installation.

1.16.3 Failure costs

Design changes – all costs associated with engineering changes due to defects.

Rework – loaded cost of rework.

Scrap cost.

Warranty – labor and parts as applicable. And,

Fault finding cost.

CHAPTER THREE

Failure Analysis and Human Factors

3.1 Fault Tree Analysis

A fault Tree is a graphical method of describing the combinations of events leading to a defined system failure. In fault tree terminology the system failure is known as the top event. The fault tree involves essentially logical possibilities and hence two main symbols. These involve gates such that the input below gates represent failure. Outputs at the top of gates represent a result of failure depending on the nature of the gate. The gates used are:

The OR gate whereby any input causes the output to occur.

The AND gate whereby all inputs need to occur for the output to occur.

In some fault tree analysis a third gate called the majority gate is used in which two or more inputs are needed for the output to occur.

Figure 3.1 shows the symbols for the AND and OR gates and also draws attention to their equivalence to reliability block diagram (RBD).

The AND gate models the redundant case and is thus equivalent to the parallel block diagram. The OR gate models the series case whereby any failure causes the top event.

In fault tree diagram, the rectangular box serves as a place for the description of the gate below it. Circles represent the basic events, which serve as the enabling inputs to tree.

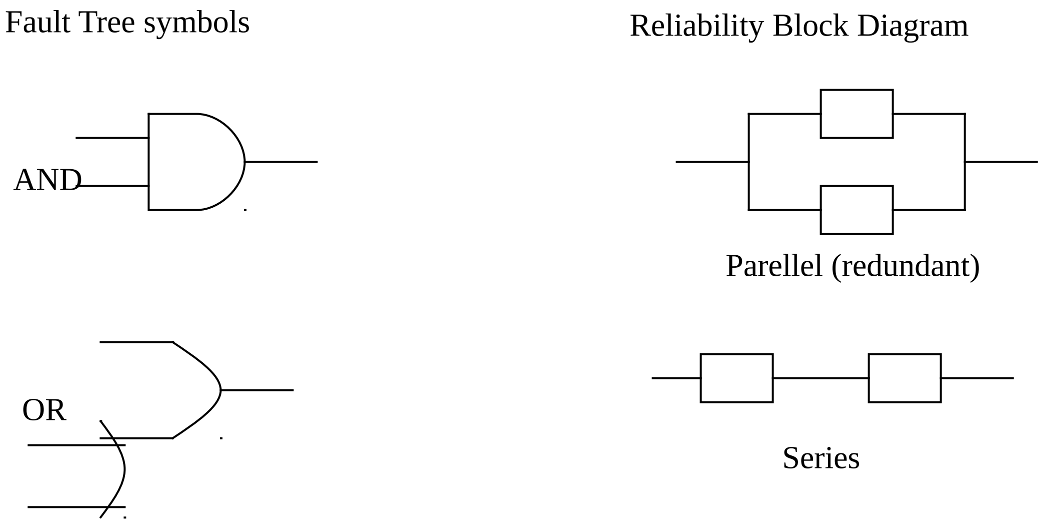


Figure 3.1 fault Tree gates and the equivalent reliability block diagram

Other symbols used in fault tree are shown in figure 3.2 below.

Primary event	FTA symbol	Description

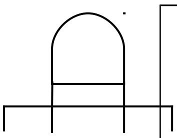
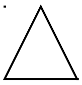
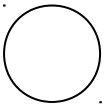
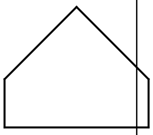
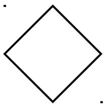
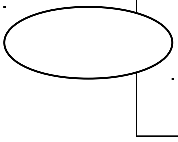
Priority AND		The output event occurs if all input events occur in a specific sequence
Transfer		Used to indicate the transfer to another tree
Basic event		A basic initiating fault event.
External event		An event that is expected to occur or not to occur. Has probability of 0 or 1.
Undeveloped event		A basic event that does not need further resolution
Conditioning event		A specific condition that can apply to any gate.

Figure 3.2 Fault Tree event symbols

The most fundamental difference between fault tree diagram FTD and reliability block diagram RBD is that you work in the success space in RBD while you work in failure space in a FTD. In other words, the RBD looks at success combinations while the FTD looks at failure combinations.

Fault tree analysis can be applied as a model for networks, which will be a powerful tool in modeling maintainability of networks.

3.1.1 Fault Tree calculations

Having the values of failure rates for all items in the network system, and modeled the failure logic as a fault tree, the next step is to evaluate the frequency of the top event.

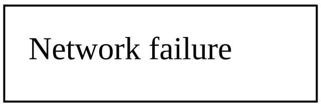
Assume the following basic event data for a network:

Item	**Failure rate (FPMH)**
Mains power supply	10
Standby power supply	10
Server H/W	8
Server S/W	15
Hub	5
Main data cable	20

FPMH describes Failures Per Million Hours, which is used to measure the number of failures that occur during one million of operational hours.

The first step is to model the failure logic as a fault tree.

Figure 3.3 shows the fault tree diagram for this network.



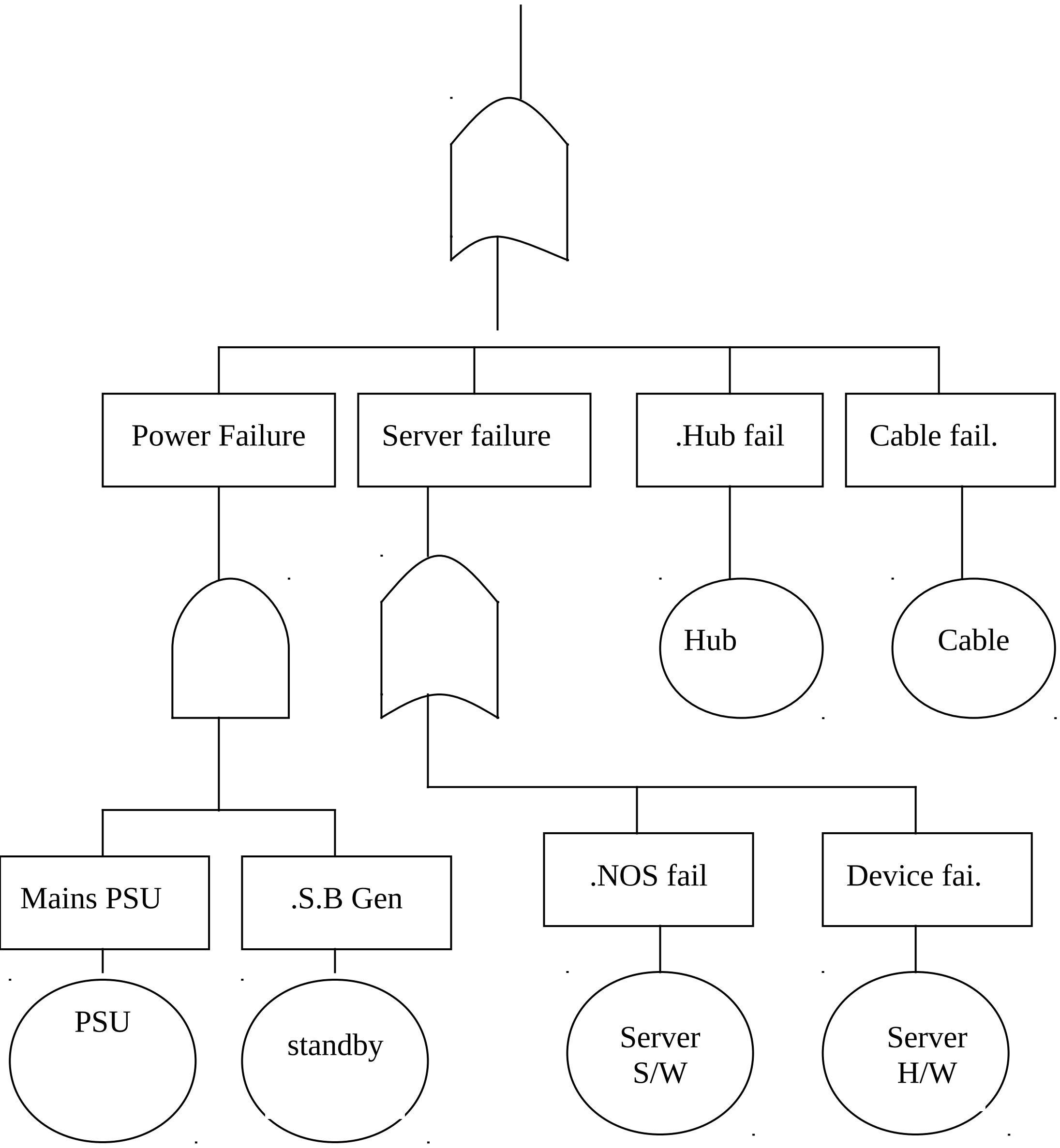


Figure 3.3 Fault Tree Analysis for the network

Total failure rate of the network can be calculated according to the values of each item and the resultant of each gate.

For AND gate which appear only when there is a redundancy, the failure rate of the redundant unit is equal to the failure rate of the operating unit since they are identical. In some rare cases the standby unit may have a different failure rate, and this should be taken into account.

The resultant failure rate at the output of the and gate could be calculated from the rule of the overall reliability of redundant system, in which the overall reliability (R_t) of two parallel units is calculated as:

$$R_t = R_1 + R_2 - R_1 R_2 \qquad (3.1)$$

Hence for the values given the main supply and the standby generator are in parallel. The reliability over one year (8760 hours) can be found and then the overall failure rate can be calculated fro the equation:

$$\lambda_t = (-1/t) \ln R_t \qquad (3.2)$$

R_1 (mains) = Exp(-λt) exp[-(10/1000000).(8760) = 0.91666

R_2(standby) = 0.91666 the same value since they are identical

$R_{12} = R_1 + R_2 – R_1R_2 = (0.91666)+(0.91666) - (0.91666).(0.91666)$

$R_{12} = 0.993$ then,

$\lambda_{12} = -1/8760 \ln 0.993 = 8.02$ failure/hour = 0.000008 FPMH

Notice that in the case of redundancy a less failure rate is produced.

At the output of the OR gate in the fault tree analysis, the input failure rates are summed because it represent a series construction. Hence,

$$\lambda_{(network)} = \lambda_{(power)} + \lambda_{(server)} + \lambda_{(hub)} + \lambda_{(cable)} \qquad (3.3)$$

$$\lambda(server) = \lambda(s/w) + \lambda(h/w) = 8 + 15 = 23 \text{ FPMH}$$

λ(network) = 8.02 + 23 + 5 + 20 = 56.02 FPMH

Which represent the overall failure rate of the network.

3.2 Failure Mode and Effect Analysis (FMEA)

The FMEA discipline was developed in the United States military. Military procedure, MIL-P, titled procedure for performing a failure mode, effect, and analysis. It was used as a dependability evaluation technique to determine the effect of system and equipment failures. Failures were classified to their impact on mission success and personnel/equipment safety. The term equipment/safety is taken directly from an abstract of military standard MIL – STD. The concept that personnel and equipment are interchangeable does not apply in the modern manufacturing context of producing consumer goods. Advanced product quality planning standards provide a structured method of defining and establishing the steps necessary to assure that a product satisfies the customer's requirements, with conjunction with the ISO quality standards QS 9000. An emphasis is placed on minimizing process and product variation. A control plan provides a structured approach for design, selection, and implementation of value added control methods for the total system. QS 9000 compliant suppliers must utilize Failure Mode and Effect Analysis (FMEA) in the advanced quality planning process and in the development of their control plans.

The FMEA is commonly defined as "a systematic process for identifying potential design and process failures before they occur, with the intent to eliminate them or minimize the risk associated with them".

FMEA is used to identify potential failure modes, determine their effect on the operating of the product a crucial step is anticipating what might go wrong with a product. A list of potential failure modes should be formulated.

3.2.1 Types of FMEAs

There are several types of FMEAs, some are used much more often than others. FMEA should always be done whenever failures would mean potential harm to the user of the end item being designed. The main types of FMEA are:

System – focuses on global system function.

Design – focuses on units and subsystems.

Process – focuses on assembly process.

Software – focuses on software functions.

For networks system, design and software FMEA is used.

Historically, engineers have done good job of evaluating the functions and the form of products and processes in the design phase. Often the engineer uses safety factors as a way of making sure that the design will work and protect the user against product failure, but a large safety failure does not necessarily translate into a reliable product. Instead, it often leads to an over designed product with reliability problems.

FMEA provides the engineers with a tool that can assist in providing a dependable product. They can use it to:

-Develop product requirements that minimize the likelihood of those failures.

-Evaluate the requirements obtained from the customer or other participants in the design process to ensure that those requirements do not introduce potential failures.

-Identify design characteristics that contribute to failure and minimize the resulting effects.

-Develop methods and procedures to test the product to ensure that the failures have been successfully eliminated.

-Track and manage potential risks in the design. Tracking the risk contributes to the development of corporate memory and the success of future products as well.

-Ensure that any failures that could occur will not seriously impact the customer of the product.

3.2.2 Benefits of FMEA for networks

FMEA is designed to assist the engineer improve the dependability of any design. Properly used FMEA for networks provides the engineer several benefits, include:

- Improve network dependability.
- Increase user satisfaction
- Early identification and elimination of potential failure modes.
- Capture engineering/organization knowledge
- Emphasizes problem prevention in the network
- Document risk and actions taken to reduce risk
- Provide focus for improved testing of network.

- Minimize late changes and associated cost
- Catalyst for teamwork and idea exchange between network staff.

3.2.3 FMEA procedure

The process for conducting an FMEA is straightforward. The basic steps are:

1. Describe the network system and its function. An understanding of the network system under consideration is important to have it clearly articulated. It is important to consider both intentional and unintentional uses since network failure often ends in litigation, which can be costly and time consuming.
2. Create a block diagram of the network. A block diagram of the network should be developed. This diagram shows major units and components as blocks connected together by lines that indicate how these units and components are related. The diagram shows the logical relationships of components and establishes a structure around which the FMEA can be developed. Establish a coding system to identify system elements. The block diagram should always be included with the FMEA form.
3. Complete the header on the FMEA form worksheet like network type, subsystems, component, design lead, prepared by, date, and revision date. Modify these heading as needed.
4. Use the diagram prepared to begin listing items and functions. List them in a logical manner based on the block diagram.
5. Identify failure modes. A failure mode is defined as the manner in which an item could potentially fail .
6. A failure mode in one component or a unit can serve as the cause of a failure mode in another component or a unit. Each failure should be listed in technical terms. At this point the failure modes should be identified whether or not the failure is likely to occur. Looking at similar networks and the failures that have been documented for them is a good starting point.
7. Describe the effects of these failure modes. The engineer should determine what the ultimate effect would be. A failure effect is defined as

the result of the failure mode on the function of the network. Examples of failure effects categories include:

- Category I Inoperability of the network (fail),
- Category II Degraded performance (marginal)
- Category III Negligible,

Establish a numerical ranking for the severity of the effect. A common industry standard scale uses IV to represent no effect and I to indicate very sever with failure affecting system operation and safety without warning. The intent of the ranking is to help the analyst determine whether failure would be minor or a catastrophic occurrence to the customer. This enables the engineer to prioritize the failure and address the big issues first.

8. Identify the causes for each failure mode. A failure cause is defined as a design weakness that result in failure. The potential causes for each failure mode should be identified and documented. The causes should be listed in technical terms and not in symptoms. Example of potential causes include:

-	Improper Network Installation	code INI
-	Improper Operating Conditions	code IOC
-	Excessive Loading Especially in software	code EXL
-	Excessive Voltage.	code EXV

9. Identify current controls, which are the mechanisms that prevent the cause of failure mode from occurring or which detect the failure before it reaches the user. The engineer should now identify testing, analysis, monitoring, and other techniques that can or have been used on the same or similar network to detect failures.

10. Review Risk Priority Number (RPN). The risk priority number is a mathematical product of the numerical severity and probability.

$$RPN = (severity).(probability)$$

High severity is given number 3, marginal is given number 2, and low severity is given number 1. for example a sever failure with a probability of occurrence equal t0 20% for one year of time, will give a RPN equal to:

RPN = (3).(0.2) = 0.6

11. Determine recommended actions to address potential failures that have a high RPN. Redesign of the items to avoid failures, monitoring mechanism, performing preventive maintenance, and inclusion of redundancy.

12. Update FMEA as the design changes, the assessment changes or new information becomes known.

The form shown in figure 3.4 illustrates a sample form of FMEA.

Item Name	Item Code	Failure Mode Code	Failure Category	Effect Category	Cause Code

Action:--

Recommendations:---

RPN: ---

By Eng:---

Date ---

Sig. ---

Approved by:---------------------------

Signature ---------------------------

Date ---------------------------

Figure 3.4 FMEA form

FMEA forms should be kept carefully for periodical checks made by network engineers in order to make the required modification to lower the RPN.

3.2.4 FMECA

FMECA is an acronym, for Failure Modes Effect, and Criticality Analysis. FMECA is similar to FMEA, though criticality is usually computed. FMECAs are used extensively in military, aerospace, and medical fields, for both design and process reliability analysis.

3.3 Root Cause Failure Analysis (RCFA)

The maintenance engineer probably spends a lot of time administering quick fixes to small chronic problems. It is just a part of the job. Tending these chronic failures can take eighty percent of the maintenance budget. There is a way to entirely eliminate these problems. It is called Root Cause Failure Analysis (RCFA), and it has the potential to save a lot of money in repair costs and down time.

RCFA is a simple discipline process used to investigate, rectify, and eliminate equipment failure, and it is most effective when directed at chronic breakdowns. It is found that a large portion of down time came from small events that occurred frequently on a very frequent basis, rather than big one-time failures. Chronic items typically ignored by the system of addressing and prioritizing things because they just seem to be inconveniences.

RCFA develop a method that addresses those chronic failures. The power of the process is that it shows you how to find the latent roots responsible for the failure. Root cause failure analysis takes you to latent roots, which are the management system weaknesses. Once you have found these, you have the means to solve many other potential problems that haven’t yet occurred. In most failures there are actually three layers:

- The physical item

- The human error
- The latent root of the failure.

The later is always the true cause of the problem. In any failure, there is always a human error. Either someone did something wrong, or forgot to do something. But when you get into true root cause failure analysis, you get deep into management system. A prime example of these layers can be seen in the network cable failure when installed it did not work. When the RCFA was performed, they found that small cuts in the cable were the cause. Further analysis revealed that the defect was due to store environment, which was full of mice. So

- The small cuts in the cable were the physical failure
- The lack of cleaning the store area was the human error
- The latent root cause was the weakness in the store management.

RCFA should be used for seeking out flaws within management systems, and not for laying blame on an individual. RCFA consists of six steps:

1. A failure mode and effect analysis FMEA
2. Preservation of failure information
3. The organization of an analysis team
4. The actual analysis
5. Sharing the findings and making recommendations
6. Tracking the results.

During the actual analysis, a logic fault tree is used.

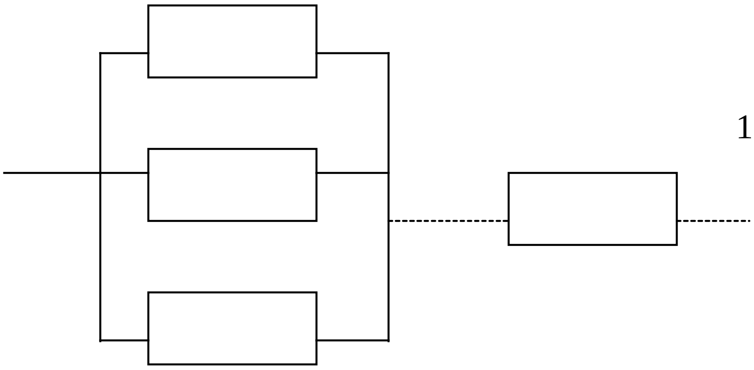
3.4 Common Mode Effects (Dependent Failures) in redundant system

3.4.1 Terms

Consider the redundant system illustrated in figure 3.5 whose configuration requires that two out of the three channels operate. Typical figures of 10^{-4} per hour for failure rate and 10 hours mean down time for each unit are used. Consider that only one failure in 100 is of such a nature as to effect all three channels and thereby defeat the redundancy. It is therefore necessary to add, to the block diagram model, a series element whose failure rate is

1% x 10^{-4} = 10^{-6}

The effect is to swamp the redundant part of the prediction with an element, which is nearly twice as unreliable.



1% x 10^{-4} = 10^{-6}

Figure 3.5 The added series element to the redundant system

The following terms are widely used:

- Dependent Failures (DF): Occurrences which are not independent and whose probability is therefore greater than the multiple of their individual probabilities.
- Common Mode Failure: This is the result of an event, which, because of dependencies, causes a coincidence of failure states of components in two or more separate channels of a redundant system, leading to the defined system failure to perform its intended function.

Typical causes of this type failure arises from:

1. Requirements: Incomplete or conflicting requirements.

2. Design: Software failures affecting all three channels, common power supplies, and noise problems.

3. Maintenance/operating procedure: Human induced failures, faulty, or inappropriate test equipment

4. Environment: Lightning, electrical interference, and temperature cycling.

Typical defenses against CMF are:

1. Operating diversity: Using two or more methods of achieving a particular

   Function, that is to use analogue as well as digital systems.
2. Equipment diversity: Using two or more designs in the redundancy.
3. Segregation of channels: Physical, and electrical segregation.
4. Proof testing: Periodic manual or automatic checks.

The degree to which these failures are likely depends largely on the design. Redundant channels having a high degree of segregation and diversity and with little interconnection will have a low susceptibility to the problem. On the other hand, designs involving closely interconnected units and having shared power supplies may well be dominated by common mode failure CMF.

Clearly any prediction of this phenomenon must be highly subjective since if it were possible to identify the element by means of Failure Mode Effect Analysis, then they would be allowed for in the prediction as series elements in the ordinary way. In essence, a prediction of common mode failures is an attempt to predict the unforeseeable. The BETA method is commonly used.

3.4.2 The BETA method

An estimate is formed of the value (beta) which correspond to the 1% used in figure 3.5 example. Typical figures used are shown in table 3.1.

Design	**Frequently used β**	**Typical β range**	**Assumed min. failure rate F/H**
Redundancy with identical channels	20%	5 – 25%	10^{-3}
Partial diversity (separate H/W or S/W)	2%	0.1 – 10%	10^{-5}
Full functional diversity	0.2%	0.1 – 10%	10^{-5}

Table 3.1 β values of different designs

Although no universally accepted method exists for assessing common mode failure, [1] this Beta method is recognized as having a number of positive features. The main advantage is that the checklist method provides an auditable trial of assessment. A number of checklist methods for the assessment of beta have been proposed. They are intended to estimate random hardware failures and do not include human error related failures. The following checklist is widely used it involves scoring the design against eight criteria:

Separation
Similarity (redundancy/diversity)
Complexity
Analysis
Procedure
Training
Control
Tests

The total score is then converted into a beta value. The methodology is as follows:

Separation is the degree to which redundant units can be affected by a single environmental event depends on their physical separation. It is also the case that most work on safety analysis concentrates on an electronic circuit, with limited attention being paid to physical arrangement of cables and components. Scores for separation are:

(a) Minimal separation in the same enclosure without barriers
(b) Redundant units in the same enclosure with barriers.
(c) Redundant units in separate enclosures, which are adjacent.
(d) Redundant units in separate enclosures in the same room, which are not immediately adjacent.
(e) Redundant units in enclosures, which are in different rooms.

Similarity is The susceptibility of redundant units to a common cause event depends on the degree to which they are alike. While this is obviously true for environmental influences such as high temperature, it should also be noted that diversity is an important safeguard against many forms of failures for both design and operation.

Similarity scores are:

(a) Identical redundant units.

(b) Similar units with only small difference in layout or circuit.

(c) Some functional diversity (different layout to achieve the same purpose)

(d) Units with different function but with common factors (number of identical components).

(e) Diverse units, quite different both in function and construction.

Complexity is the potential for common cause failure will be higher for equipment that is not designed for the particular application. There is less risk attached to well understand designs that have been used before. Much greater risks appear in difficult designs. A major design complexity is introduced by inclusion of software. Complexity scores are:

(a) Equipment of good quality not designed specially for the application. Limited knowledge and experience of design. Software is used.

(b) Equipment of good quality not designed specially for the application. More than 10 equipment years in similar environment.

(c) Equipment designed specially for the application. Limited experience.

(d) Equipment designed specially for the application. Design well understood and documented. More than 10 equipment years in similar environment.

(e) Equipment designed specially for the application. Uses traditional and straightforward design technique. More than 10 equipment years experience in the same environment.

3.5 Fault analysis

The fault analysis or FMEA carried out of system for safety assessment provides an important and independent check on design. This is particularly the case with regard to the detection of failure and the adequacy of testing. Such analysis, by checking the effectiveness of the test and in some cases introducing new types, prevents the common cause failure that would result from the gradual deterioration of a system. Scores for analysis are:

(a) No formal safety analysis or design knowledge of CMF.

(b) Limited analysis some knowledge of CMF.

(c) Detailed fault analysis of the most important circuits in equipment linked with FMEA and some evidence of feedback.

(d) Detailed fault analysis of all circuits in equipment of difficult design.

(e) Detailed fault analysis of well-understood item of equipment with traditional design techniques and evidence of feedback of CMF issues.

3.6 Operating procedures/man-machine interface

There are a number of potential common causes effects that arise from human error in operation, testing, or maintenance. In most cases this would be a consequence of a human error repeated with regard to all n components of a redundant system, for example, misreading of meters. Carefully written procedures, properly observed, greatly reduce human error by optimizing the sequence of actions and preventing errors of omission. For any given system, the probability of human error will depend not only on the detailed understanding of procedures but also on the number and complexity of operator actions.

To assign a value to this sub-factor, two judgments are necessary:

- Written procedures YES/NO/DETAILED
- Operator involvement MINIMAL/NORMAAL

Minimal operator involvement should only be claimed for those systems with automatic trips, with no override or defeat features available to the operator.

The scores are:

(a) No written procedure – normal operator interaction.

(b) No written procedures – minimal operator interaction.

(c) Written procedures – minimal operator interaction.

(d) Detailed procedures – minimal operator interaction

(e) Detailed procedures – minimal operator interaction and more than 10 operating years experience with the system.

3.7 Training/safety culture

The training of staff directly affects the probability of human error. Such training is particularly relevant to unusual or emergency operation.. this must also include the regular training of experienced operators in emergency procedures. The training types are:

(a) On-the-job training.

(b) Systematic regular training.

(c) Simulator training. All personnel involved in operation, testing and maintenance, spend more than 50% of their time on high dependability applications. The particular system has been in use for more than 10 years.

3.8 Environmental control

This factor refers to the control exercised over the environment in which the system is installed. The worst case may be represented by installation in an open place. The potential dangers result from the unlimited access of people with no knowledge of the equipment. The common cause effect may be direct. This sub-factor does not relate to the severity of the environment, which should be taken into account by the designer.

The highest environmental factors can be claimed only if everyone and everything present is controlled. This must include cleaners, drains, and cables [3]. The levels are:

(a) Minimum control, other machines, and processes not related in function are also present.

(b) Separate building limits access – other activities are associated.

(c) Access by authorized personnel only.

(d) Trained personnel only. All equipment and services subject to design control.

(e) AS (d) but on smaller scale with closely related activities.

3.8.1 Environmental testing

It is the intention of the designer that the equipment should be able to stand a number of environmental effects, such as shocks, vibration, temperature, and humidity. Environmental testing is capable of revealing certain common cause susceptibilities [1] .The variety, type, and range of tests should be considered. The scores are:

(a) No environmental tests other than those conducted by component manufacturers.

(b) Limited environmental tests.

(c) All main environmental tests on production standards units, including shock, vibration, temperature, humidity, electrical interface, and water spray.

(d) Comprehensive environmental tests on production standards units including all effects regarded as possible in the particular installation.

(e) As (d) with actual production equipment subject to burn-in of at least one year.

The BETA method can be calibrated by comparing results with one's own field data. Now to find beta value for a network system, the following steps must be taken:

Step 1: From beta table shown in table 3.2 find the total scores for the network.

Step 2: The total of scores is divided by 50 000 to obtain the beta estimate.

Step 3: Convert beta value to a percentage value.

Step 4: Multiply the beta value by the failure rate of the redundant items

Step 5: Add an item in series to the redundant configuration with the calculated failure rate from step 4.

Item	**a**	**b**	**c**	**d**	**e**
Separation	2400	580	140	35	8
Similarity	1750	425	100	25	6
Complexity	1750	425	100	25	6
Analysis	1750	425	100	25	6
Procedures	3000	720	175	40	10
Training	1500	360	90	20	5
Control	1750	425	100	25	6
Test	1200	290	70	15	4

Table 3.2 Scores values of beta method

Example 3.1

	Assessment	Score
Separation	b	580
Similarity	c	100
Complexity	b	425
Analysis	c	100
Procedures	b	720
Training	d	720
Control	e	6
Test	e	4
	Total =	1955

Hence β = 1955/50000 = 0.039 = 3.9%

3.9 Human Factors

For some years there has been an interest in modeling human factors so that quantified reliability and risk assessments can take account of the contribution of human error to the system failure. There was attempts to develop a database of human error rates and these led to models of human error whereby rates could be estimated by assessing relevant factors such as stress, training, complexity, and the like. These human error probabilities include not only simple failure to carry out a simple task but diagnostic tasks where errors in reasoning, as well as action, are involved. There is not a great deal of data available since:

- Low probabilities require large amounts of experience in order for meaningful statistics to emerge.
- Data collection concentrates on recording the event rather than analyzing the cause.
- Many large organizations have not been prepared to commit the necessary resources to collect data.

More recently interest has developed in exploring the underlying reasons, as well as probabilities, of human error. In this way assessments can involve not only quantification of the hazardous event but also an assessment of the changes needed to bring about reduction in error.

3.9.1 Models of human factors

There are currently several models, each developed by separate groups of analysts working in this field. Whenever several models are available, the need arises to compare them and to decide which is the most suitable for the in hand. Factors for comparison should be:

- Accuracy – There are difficulties in the lack of suitable data for comparison and validation.
- Consistency – Between different analysts studying the same scenario.
- Usefulness – In identifying factors to change in order to reduce the human error rate.
- Resources – Needed to implement the study.

The most common approaches used are:

1. Human Error Assessment and Reduction Technique (HEART)
2. Technique to Estimate Operator Errors (TESOE)

3.9.2 Human Error Assessment and Reduction Technique (HEART)

This is a deterministic and fairly straightforward method developed during early eighties in the last century. It involves choosing a human error probability from a table of error rates and modifying it by multiplication factors identified from a table of error-producing conditions. It is considered to be of particular use during design since it identifies error-producing conditions and therefore encourages improvements. It is a quick, and flexible technique requiring few resources. The error rate table contains nine basic error task types, as described in table 3.3. (Appendix 9 shows more human error rates per task).

Task	Probability of error
Totally unfamiliar, perform at speed, no idea of outcome	0.55
Restore system to original state on a single attempt	

without supervision or procedure checks.	0.26
Complex task requiring high level of skill	0.16
Fairly simple task performed rapidly or given scant attention	0.09
Rapid task involving relatively low level of skill.	0.02
Restore system to original state following procedure checks	0.003
Totally familiar task, performed several times, well motivated, highly trained staff	0.0004
There is supervisory system providing interpretation	0.00002
Miscellaneous task – no description available	0.03

Table 3.3 Tasks and human error probabilities

The procedure then describes error-producing conditions to each of which a maximum multiplier is used. Any number of these can be chosen, and then multiplied by the probability of the error. Examples are:

Newly qualified operator	multiply by 3
Using more dangerous procedure	multiply by 2
Unreliable instrumentations	multiply by 1.6
Emotional stress	multiply by 1.3
Low morale	multiply by 1.2

Assume that a newly qualified operator is required to upgrade the operating system.

From the table, restore system to a new state following procedure checks condition is chosen, which has 0.003 probability of error. Now looking for the multipliers, we can choose the most suitable multiplier for this operator. It is clear that newly qualified operator is suitable (multiply by 3)

Here the analyst must see if the chosen error producing condition (EPC) number can be fit totally for this person or not, taking into account the individual differences between operators. Say for this operator, the EPC can be fit by eighty percent (80%). In this case 0.8 is called the proportion effect, and the calculations will be:

$$(EPC-1).(\text{proportion effect} + 1)$$

= (3 – 1).(0.8+1) = 3.6

The final step is to multiply 3.6 by the probability of error from table 2.2

(3.6).(0.003) = 0.0108

Hence error rate for this operator is 0.0108

Not that since the probability of failure cannot exceed 1 , therefore for calculations taking the prediction above 1 will be assumed that the error will almost certainly occur.

3.9.3 Technique to Estimate Operator Errors (TESOE)

It involves an easy applied model whereby live factors are identified for each task and the error probability is obtained by multiplying together the main factors as in table 3.4.

When using such error rates in a fault tree or other quantified method, select the most pessimistic value for task error rate. If in the overall incident probability computed by the fault tree, the contribution from that human event is negligible, then the problem can be considered unimportant.

More recently there is a focus of interest in analyzing the causes of human error and seeking appropriate procedures and defenses to minimize or eliminate them.

Item	Error probability
Activity	
Simple	0.001
Requires attention	0.01
Operator	
Expert	0.5

Average	1
Poorly trained	3
Anxiety	
Emergency	3
Normal	1

Table 3.4 TESOE operator error probabilities

CHAPTER 4
Data collection and Analysis

4.1 General hints in dependability data collection

You need to spend some time thinking about the data you are going to collect. You should have a clear purpose in mind for each piece of data and how the data will be processed to achieve that purpose. A question always arises in data collection, that is, is the data you plan to collect worth the cost of collecting?

The problem with this approach is that it places such a burden on data collectors.

Also there is a definite cost in collecting data and data you collect, the greater the cost as illustrated in figure 4.1.

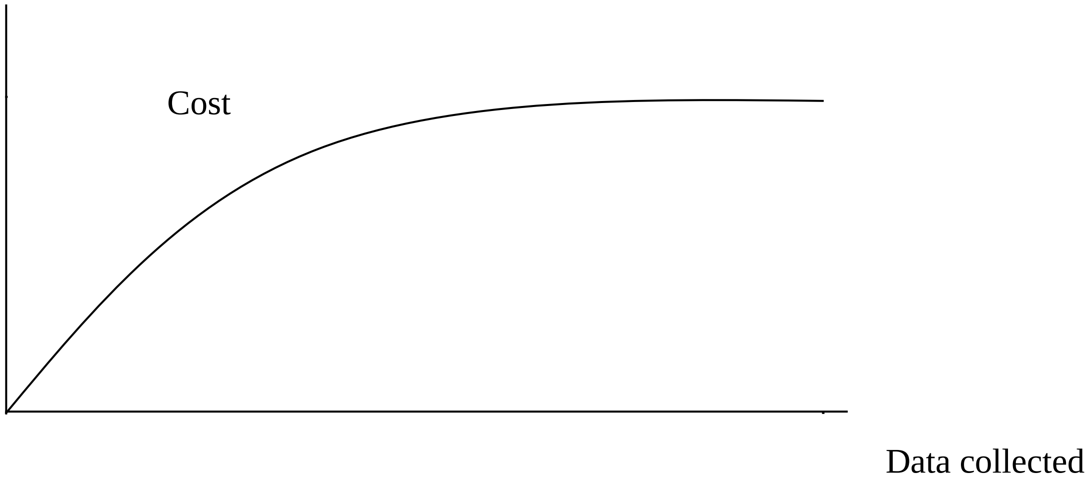


Figure 4.1 Relationship between data collection and cost.

The data may be a multipurpose data that can serve several purposes, and this will reduce the collection burden considerably.

The following approach is generally more effective in collecting data plan:

- Obtain the motivated participation of the data takers.
- Make the collection mechanism as easy as possible.
- Collect data in real time.
- Provide feedback of results obtained fro the data on a regular and timely basis.

4.1.1 Motivating data takers

The most important question is how one can motivate data takers, and your goals can be related to those of the data takers. Most of people realize that if they cooperate in something that benefits the project they are working on, their colleagues and their managers will notice this, and it will be to their credit. However you really have to be honest with them in showing what you are trying to accomplish. Letting the data takers plan the details of the effort, will actually result in concrete benefits.

The best approach in data collection is to start with the first draft of the data collection plan. Generally you will then have a small number of problems to deal with. Once the plan has been established, data takers should be given a clear technical understanding of the purpose of the data collection, if it is not already obvious to them from the planning session. Data takers must be intelligent when confronted with the many special problems that occur in trying to reduce the reality to a box in a form. An oral presentation is usually best for this purpose rather than written materials.

Data collection must be integrated with other data collection activities and with the primary work that is proceeding in parallel. This sometimes requires to combine forms. Collection automation is necessary. It means making human intervention unnecessary if possible. The advantages of automated data collection are the reduced burden and greater accuracy. The disadvantage of automated data collection is that it is unsatisfactory when interpretation is needed in establishing the data values.

The conversational online data collection for the person taking data is appropriate. One of the best alternatives is to have a recording device to which data taker can dictate. If forms are used, they must be simply designed for ease of use. The form should provide enough space to record the information required and should elicit the information in the natural order in which the person would provide it.

4.2 Reasons for dependability data collection

Dependability of networks is built on achieving high levels of its main attributes namely, reliability, availability, and maintainability. Failure data is the most important data to model the three main attributes of dependability. Failure data can be collected from production models or from the field. In either case a formal failure-reporting document is necessary in order to ensure that the feedback is both consistent and adequate. Field information is far more valuable since it concerns failures and repair actions that have taken place under real conditions. Since recording field incidents relies on people, it is subject to errors, omissions, and misinterpretations. It is therefore important to collect all field data using a formal document. Information of this type has a number of uses, the main two being feedback, resulting in modifications to prevent further defects, and the acquisition of statistical reliability and repair data. Field data can:

- Indicate design deficiencies and can be used to support reliability growth programs.
- Provide reliability and availability modeling.
- Identify wear out and decreasing failure rates.
- Contribute statistical data for repair time predictions.
- Enable spares provisioning to be refined.
- Allow routine maintenance intervals to be revised.
- Enable the field element of dependability costs to be identified.
- A failure reporting system should be established for every network.

4.3 Information and difficulties

A failure report form must collect information covering the following:

Repair time – active and passive.

Type of fault – primary or secondary, random or induced.

Nature of fault – open or short circuit, drift condition, wear out, or design deficiency.

Fault location – exact position and details.

Environmental conditions at time of fault.

Action taken – exact nature of replacement or repair.

Personnel involved.

Equipment used.

Spares used.

Unit restoration.

The main problems associated with failure recording are:

1. Inventories: Whilst failure reports identify the numbers and types of failure they rarely provide a source of information as to the total numbers of item in question and its installation dates and running times.
2. Motivation: If the field service engineer can see no purpose in recording information it is likely that items will be either omitted or incorrectly recorded. The purpose of fault recording and the ways in which it can be used to simplify the task need to be explained. If the engineer is frustrated

by un realistic time standards, poor working conditions, and inadequate instructions, then the failure report is the first task which will be skimped or omitted. A regular circulation of field data summaries to the field engineer is the best way of encouraging feedback. It will help him to see the overall field picture and advice on diagnosing the more awkward faults will be appreciated.

3. Verification: once the failure report has left the person who completes it the possibility of subsequent checking is remote. If repair times or diagnoses are suspect then it is likely that they will go undetected or unverified. Where failures data are obtained from customer's staff, the possibility of challenging becomes even more remote.

4. Cost: Failure reporting is costly in terms of both the time to complete failure report forms and the hours of interpretation of the information. For this reason, both supplier and customer are often reluctant to agree to a comprehensive reporting system. If information is correctly interpreted and design or manufacturing action taken to remove failure sources, then the cost of the activity is likely to be offset by the savings and the idea must be sold on this basis.

5. Recording non-failures: The situation arises where a failure is recorded although non-exists. This can occur in two ways. First there is the habit of locating faults by replacing suspect but not necessarily failed components. When the fault disappears the first wrongly removed component is not replaced and is hence recorded as a failure. Failure rate data are therefore artificially inflated and spares depleted. Second there is the interpretation of secondary failures as primary failures. A field component may cause stress condition upon another, which, may as a result fail. Diagnosis may reveal both failures but not always which one occurred first again failure rates become wrongly inflated. More complex maintenance instructions and the use of higher grade personnel will help reduces these problems at a cost.

6. Times to failures: these are necessary in order to establish dependability models. Sometimes they are omitted.

4.4 Spreadsheets

Many data collection schemes arrange for the data to be manually transferred from the written form into a computer. In order to facilitate data sorting and analysis it is very useful if the information can be in a coded form. This requires some forms of code database for the field personnel in order that various entries can be made by means of simple alphanumeric. This has advantage that field reports are more likely to be complete since there is a code available for each box on the form. Furthermore, the codes then provide definitive classifications for subsequent sorting. Headings should include:

Equipment code: Prefer a hierarchical coding scheme which defines the network system, subsystem and an item. For example:

PS1	main power supply
PS2	standby power supply
SVR	Server
CD	connectivity device
CBL	main cable
SCB	branch cable
SW	switching item

The failure Mode codes:

Examples are:

0	No fault found
1	Short circuit
2	Open circuit
3	Leak
4	Bad contact
5	Disconnect
6	S/W error

Action taken:

Examples are:

1	item replaced
2	Adjusted
3	Item repaired

4.5 Free text

In addition to the coded report there needs to be some provision for free text in order to amplify the data.

Each of the above fields may run to several dozen codes, which would be issued to the field maintenance personnel as a handbook. The suitable package for analysis of the data is the spreadsheet. Spreadsheets allow the data including text to be placed in cells arranged in rows and columns. Sorting is available as well as mathematical manipulation of the data.

Figure 4.2 shows an example of a well-designed failure recording form. This simple form strikes a balance between the need for detailed failure information and the requirement for simple reporting format.

Appendix 7 shows the failure reporting form of European companies of the International Telephone and Telegraph Corporation. A feature of the EITT is that the information is accurately recorded with minimum effort.

It is unfortunate that few forms give adequate breakdown of maintenance times separated into the various passive and active elements. Identifying and recording this level of information increases the maintenance cost and time. It has to be justified if a special investigation is required. Such an analysis can result in improved maintenance procedures, in which case it may be pay for itself by reducing long-term costs.

Failure Report and Action Form

Report number: --

Report date: ---

Completed by: ---

Company: ---

Failure:
Item code : ----------
Location : ----------
Failure code: ----------
Failure mode: ----------
Down time: ----------
Effect of failure: major degradation minor

Action taken:
Replace ---------------------------------------
Repair Repair date -------------------Repair time------------
Modification Date----------------------------- Time ---------------
Program reload Date -----------------------------Time ---------
Others --------------------------------------

Notes: ____________________________________

____

____

Approved by

Eng. ------------------------

Signature -----------------

Date ------------------------

Figure 4.2 failure reporting form

4.6 SUST Network field data

The Sudan University of Science and Technology network was taken as the case study to set up the dependability models, first to evaluate this network, second to focus on the points and areas that need more attention, and finally which steps should be taken to increase its reliability and availability of this network.

The field data points to the operational data collected for the network under study.

The SUST network generally can be divided into two phases:

1. The local phase (campus)
2. The PSTN phase

The two phases work together to achieve the network service required. This means that these two phases can be considered as a series system. This is illustrated in figure 4.3.

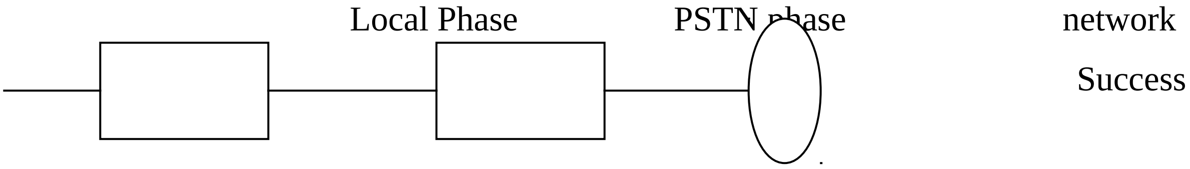


Figure 4.3 The SUST network series configuration

The block diagram of SUST is illustrated in figure 4.3.

The local phase (the campus) consists of the following main items:

1. Power supply
2. Interconnectivity device (Router and DTU)
3. Connectivity device (switch)

4. Server system
5. Transmission media, and converters (if any)

The local phase is the university campus phase. It taken as a separate phase because it is under the direct management of network and maintenance group within the staff of the university. On the other hand, phase II is managed by the PSTN company outside the university.

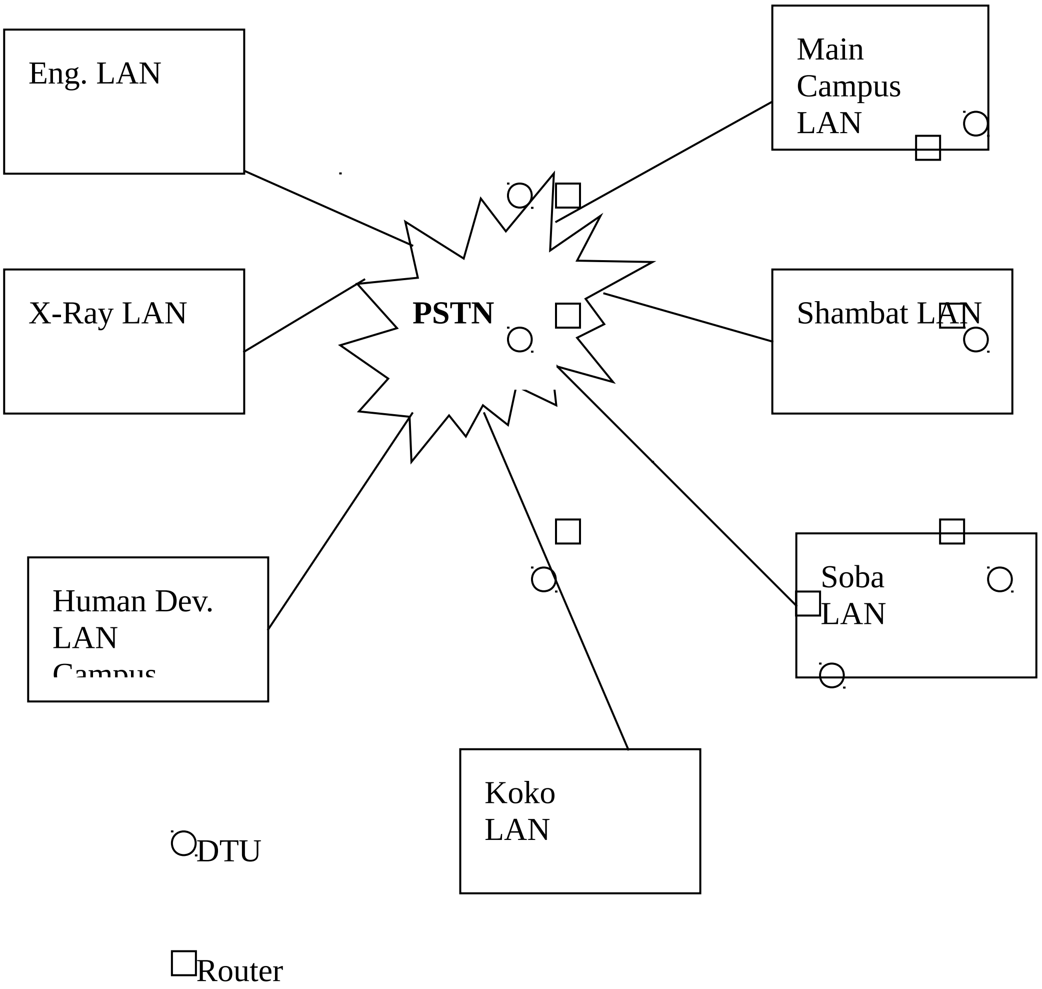


Figure 4.4 The SUST WAN block diagram

For the purpose of measuring the campus dependability attributes, each LAN failure data must be collected and analyzed. For phase II, the number of outages caused by the PSTN failures should be counted over a year to find the

Annual Failure Rate of the PSTN for the campus under consideration. It is very important to stress here that the distance of the campus LAN from the main campus affects the number of outages occurrence at that campus. This is because long distance means more exchanges and long transmission medium must be traveled. This can be explained as:

$AFR \propto d$

Where AFR is the Annual Failure Rate, and d is the distance from the main campus.

The AFR of PSTN part that connected with each campus could be found.

To find the overall AFR for each LAN, the formula of series failure rate is used.

$$AFR_{campus} = AFR_{Local} + AFR_{PSTN}$$

To measure reliability and availability for colleges outside the main campus, the series configuration of the Reliability Block Diagram (RBD) could be used. It represents the backbone of measuring the dependability attributes for each campus. This series configuration is shown in figure 4.5.

Note that for any campus to be reliably connected to the SUST network and uses its service, all items in the series connection shown in figure 4.5 must function properly.

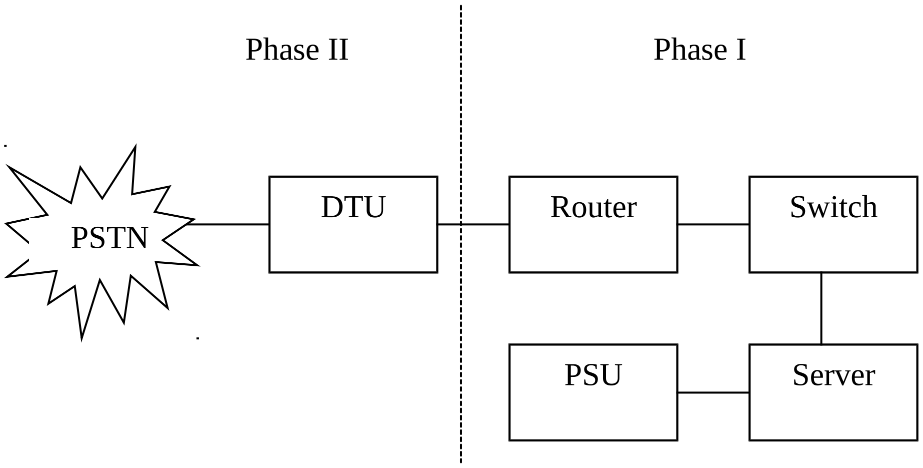


Figure 4.5 The series connection of a campus

The failures data for the items shown in figure 4.5 should be collected for each campus to assess its dependability. Any campus data can be a sample for the rest of the campuses in order to calculate the dependability attributes.

4.6.1 Main campus failure data

The main campus consists of only one phase since the PSTN phase is connected to the outside colleges.

The data shown in table 4.1 was collected from main campus as one of the main locations of SUST WAN. The main campus LAN consists of the following college and offices:

- Computer science college (Ethernet)
- Science college (Ethernet)
- College of Art (connected by fiber optic cable)
- Communication science college, (Ethernet cable), and education.
- Administration offices (Vice chancellor, principal and administrative Affairs) connected by fiber optic cable.
- Routers and DTUs for other sites.

The aim is to use this data to find the reliability and availability of the network taking into account that the data may differ from a year to another, but the most important thing is that to use this data to set up the required models for dependability assessment which can be applied to all parts of the SUST network.

Item	**No. of Failures Per 1 year**	**Down time**	**AFR λ AFR**
PSU	4	Failure 1 = 10 minutes Failure 2 = 5 minutes Failure 3 = 5 minutes Failure 4 = 10 minutes	0.00046 (The UPS period was not included in downtime)
Server (S/W)	2	Failure 1 = 1.5 hours Failure 2 = 0.5 hour	0.00023
Main Switch	0.50 (1 fail. per 2	3	5.7E-5

	years)		
Cables (UTPCAT5, Fiber)	0.25	4	2.86E-5
Routers Rack (for outside colleges)	0.25(1 failure in 4 years)	24	2.86E-5
DTUs (for other sites)	0	0	0

Table 4.1 Failures data of Main campus

For the items shown in table 4.1 (phase one), the main campus LAN items are sequentially connected. The last two items (Routers and DTUs) are connected with PSTN for outside colleges. The PSTN is considered as the second phase of the network.

4.6.2 Data Analysis

The approach of the thesis towards the analysis of the field data has three analysis methods:

a) Data classification: Classify the data as left, right, interval or complete censored data.

b) Failure Tree Analysis: another method, used is to draw the FTA to show the relationship between failures.

c) Data Conversion: This method converts the failure data into dependability data to be ready for dependability measurement.

IN field data analysis the research attempts to make predictions by fitting a statistical distribution to the field data from a representative sample of units. The parameterized distribution for the data set can then be used to estimate important operation characteristics of the item such as reliability or probability of failure at a specific time, the mean life of the item and failure rate.

Field data analysis requires:

- Gather the required field data for the item
- Select a lifetime distribution that will fit the data and model the performance of the item.
- Estimate the parameters that will fit the distribution to the data.

- Generate plots and results that estimate the item characteristics, like reliability, or mean life of the item.

Item running time can be measured in hours or any metric that applies to the period of successful operation. Since time is a common measure of life, life data points are often called time to failure (TTF), especially in unrepairable items. There are different types of data and because each type provides different information about the performance of the item, the analysis method will vary depending of the data type.

4.6.2.1 Data classification

Data of an item or a system can be classified into four categories:

1. Complete data.
2. Right censored data.
3. Interval censored data.
4. Left censored data.

1/ Complete data

Complete data as shown in figure 3.6, indicates that all of the units under test failed and the time-to-failure for each unit is known. Therefore, complete information is known regarding the entire unit.

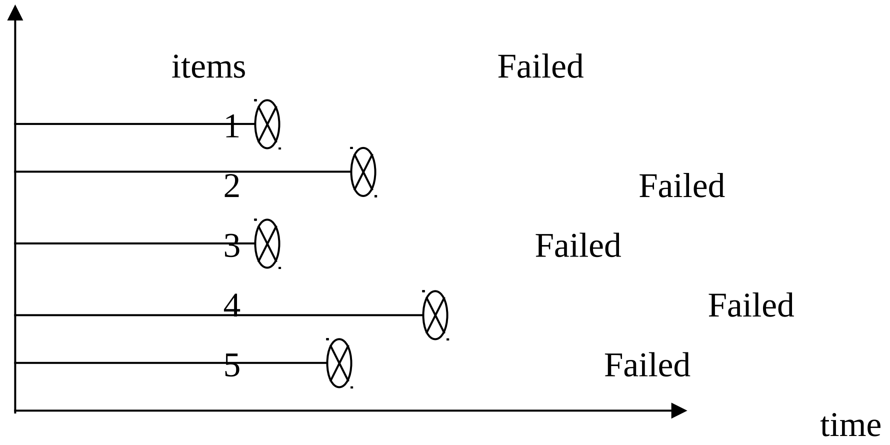


Figure 4.6 Complete data

2/ Right censored data

Also called suspended data, is composed of units that did not fail during the test. Suppose that five items shown in figure 3.6 are put under test. Three units fail and their observed time-to failure in hours are 65, 76, and 84. The last two units are still operating when the test is stopped at 85 and 100 hours respectively. Therefore the last two units are considered to be suspended or right censored.

3/ Interval censored data

Another type of censored data is called interval data. It contains uncertainty as to when the units actually failed. For example if five units under test are inspected every 100 hours, then status of each unit failed or still running is known only at the time of each inspection. If a unit fails, it is known only that it failed between inspections and the exact time of failure is not known. This will affect the calculations of down time and MTTR. Instead of exact time-to failure, an interval time between 100 and 200 hours would be recorded.

4/ Left censored data

Left censored data is a special case of interval censored data in which the time-to-failure for a particular unit is known to occur between time zero and some inspection time. For example, if the inspection occurs at 100 hours, a failed unit could have failed at any time between 0 and 100 hours.

4.6.3 Fault Tree Analysis (FTA)

This method of analysis is used to describe the behavior of the system when a failure occurs. As explained in chapter two, the logical gates are used to describe the system failure as follows:

1. The top of the gate describes the system failure. This the reverse of the RBD which the output describes the system success.
2. The OR gate is used when any item failure causes a system failure. This corresponds to a series items configuration.

3. The AND gate is used to describe the system failure in the only case that all items must fail to have a system failure. This illustrates the redundant case of items.

4.6.4 Data conversion

In this method the Annual Failure Rate should be found using the failure data.

The Mean Time Between Failure (MTBF), and Mean Downtime (or MTTR), also should be calculated in order to use this data in dependability attributes measurements.

4.6.5 The Main campus data analysis

The SUST network was taken as a case study to show how the failure data can be classified and converted to dependability data. The three methods of data analysis, data classification, data conversion, and FTA were applied to SUST network to explain the procedure of field data analysis, taking into consideration that the failure data could be changed from a year to another.

4.6.5.1 Failure data to dependability data conversion

This data was collected from the main campus.

1/ Power supply unit:

1. The failure rate for the power supply unit can be calculated as:

$$\lambda = \text{(number of failure)/(operation period)} \qquad (4.1)$$

The operation period = 1 year , and number of failures = 4 then:

$$\text{AFR} \quad \lambda = 4 \text{ failure/year} = 0.00046 \quad \text{AFR} \qquad (4.2)$$

AFR = Failures per Year Hours (Failure per 8760 hours)

2. Mean time between failure (MTBF) = 8760/4 2190 hours. (Annual MTBF)

Also can be found from :

$$\text{MTBF} = 1/\lambda = 1/(0.0004566) = 2190 \text{ hours.} \qquad (4.3)$$

3. Mean time to restore (MTTR)

The four failures down time were :

Failure 1 = 10 minutes

Failure 2 = 5 minutes

Failure 3 = 5 minutes

Failure 4 = 10 minutes

Total down time = 0.5 hours.

Mean Downtime (MDT) = 30/4 = 7.5 minutes = 0.125 hours

Here the mean time to restore is used instead of mean time to repair because it is a power cut from the source and it does not need a local repair to be done.

2/ The server

Two failures occurred in a year period of time.

1. Annual Failure rate λ for this item is equal to 2/8760 = 0.00023 AFR
2. Mean Time Between Failures can be determined as:
   a. MTBF = 8760/2 = 4380 hours (4.4)
3. Mean Time To Repair is the mean of 1.5 hours and 0.5 hour

= (1.5 + 0.5)/2 = 1 hour.

3/ The switch

One failure occurred in a period of two years.

1. Failure rate λ is equal to 0.5/8760 = 5.7E-5 F/H (4.5)

2. Mean Time Between Failures (MTBF) = 8760/0.5 = 17520 hours. (4.6)

3. For Mean Time To Repair (MTTR), since there was 1 failure the MTTR in this case is equal to the down time, which is equal to 3 hours.

4/ The Router

1. A complete failure occurred once during a period of 4 years, which means that the Annual failure rate λ is equal to 2.86E-5.
2. The MTBF is equal to 35040 hours.
3. The MTTR for this failure is equal to the down time because it is only one failure, which was 24 hours.

5/ The DTU

1. NO failure occur in the operation period which means the failure rate λ = 0
2. The MTBF is equal to full operation period.
3. The MTTR is considered as Zero

6. The cables:

1. Failure rate = 0.25/8760 =2.86E-5 (4.7)

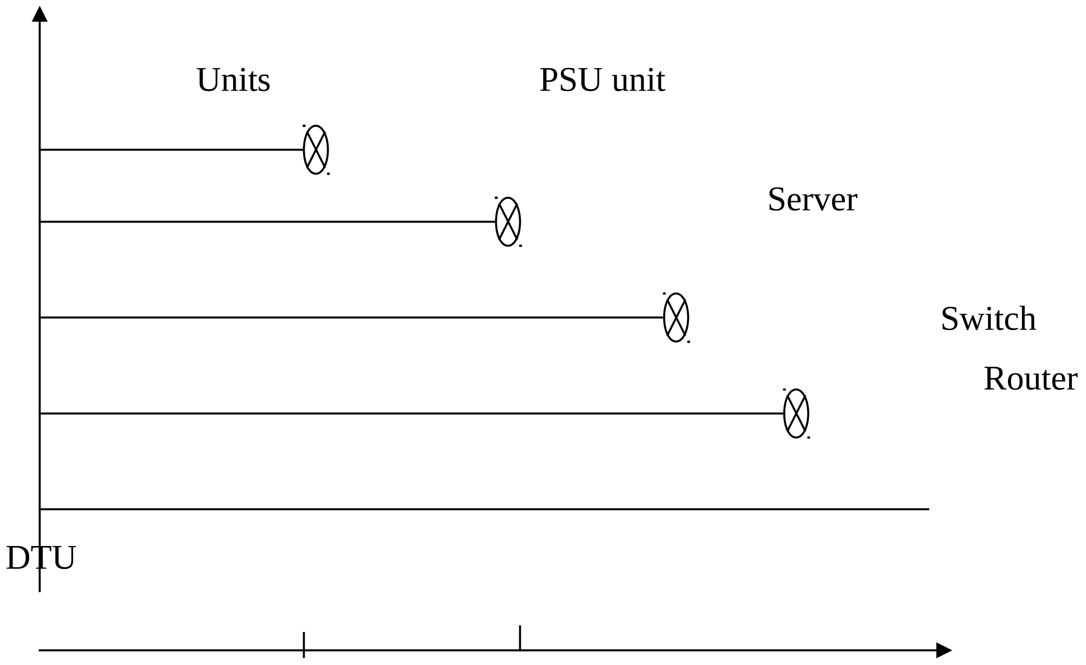
2. MTBF = 8760/.25 = 35040 (4.8)

4.6.5.2 Main campus data classification

From the data collected for phase one which consists of three units we can classify the data for this phase as follows:

1. Since the PSU failure arises first, then its data is classified as left censored data, because the time of failure lies between the time of zero and the moment it failed.
2. The server unit data is considered as right censored data because when PSU failure appeared, this unit was still running.
3. The class of any unit's failure helps practitioners to pay an additional attention for the unit that has an interval censored data class, because the time of failure is a range may be sometimes a long range. This can be solved by narrowing the inspection gab time say, for example, from every 72 hours or every 24 hours.
4. The switch item data is considered as right-censored data.
5. The router item data is a right-censored data.
6. The DTU item is the most right censored data because it did not fail during the operation period.

The data classification of Main campus is shown in figure 4.7.



2190 4380

hours

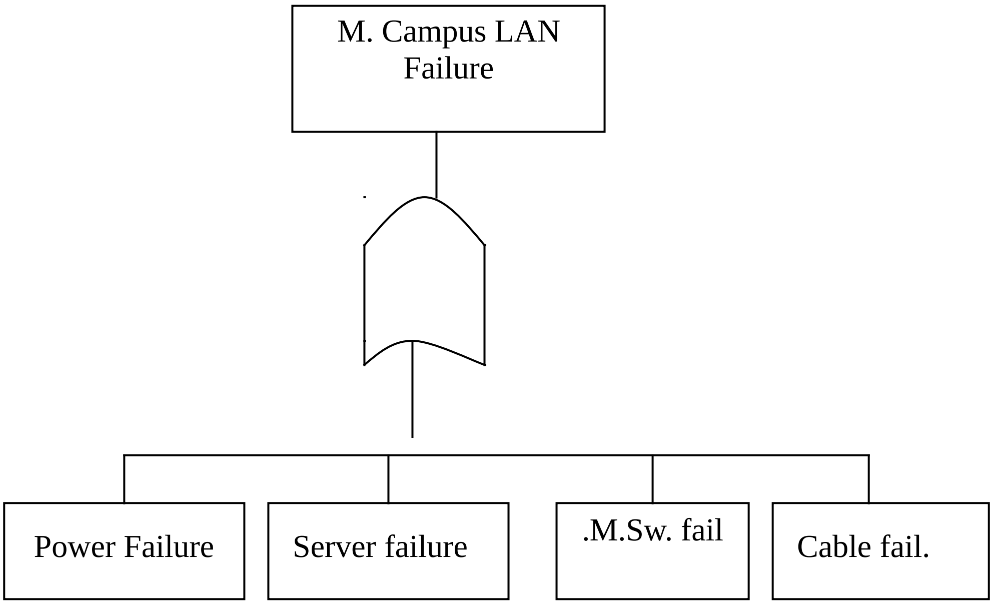
Figure 4.7 Main campus data classification

4.6.5.3 FTA for main campus

FTA could be applies to the failure data of the main campus to show the relationship between these failures, and their effects on the complete network system failure.

From table 4.1, the LAN failure occurs when one of the main switch, server, main cable, or power supply failure occurs. So these four items are considered as a series configuration, and any failure occurs at any one of these items, stops the LAN. Hence, the FTA for the main campus will be as shown in figure 4.8. For simplification, the FTA is usually simplified in a Boolean FTA using AND-OR gates to show the occurrence of failure and if the failure is produced from a combination of another item's failure or not.

Using the switches instead of the logical gates as used in Boolean diagram is another approach in FTA. One can see that the FTA is considered as the opposite of RBD because in FTA the AND gate is used in parallel combination of items showing that the failure will occur only when the two items fail.



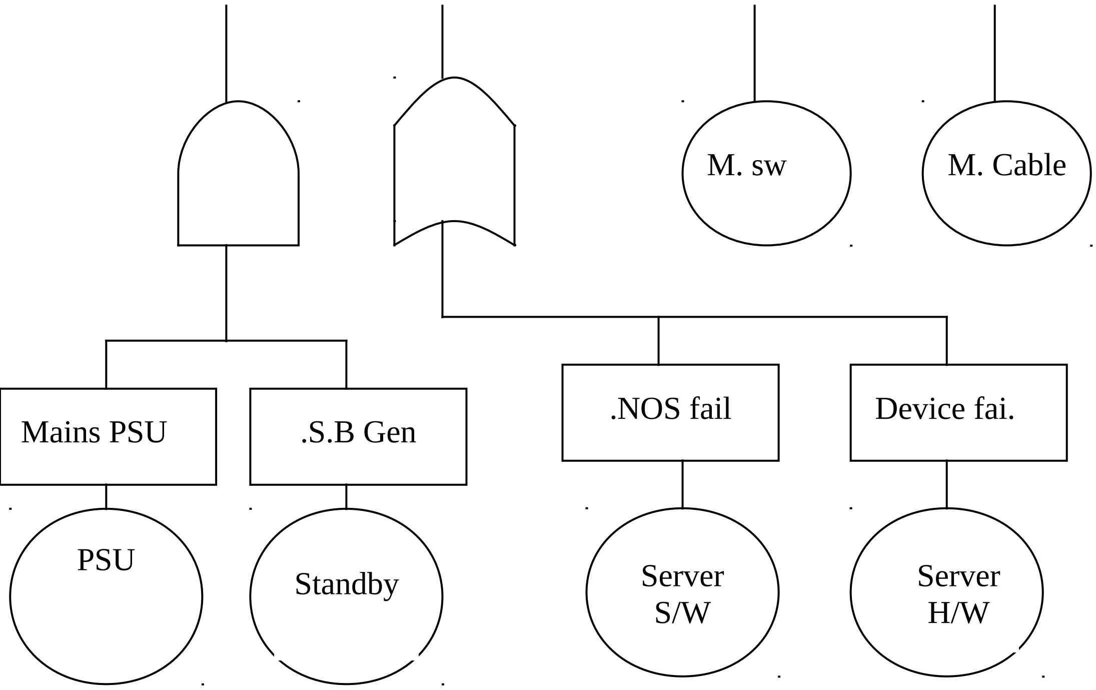
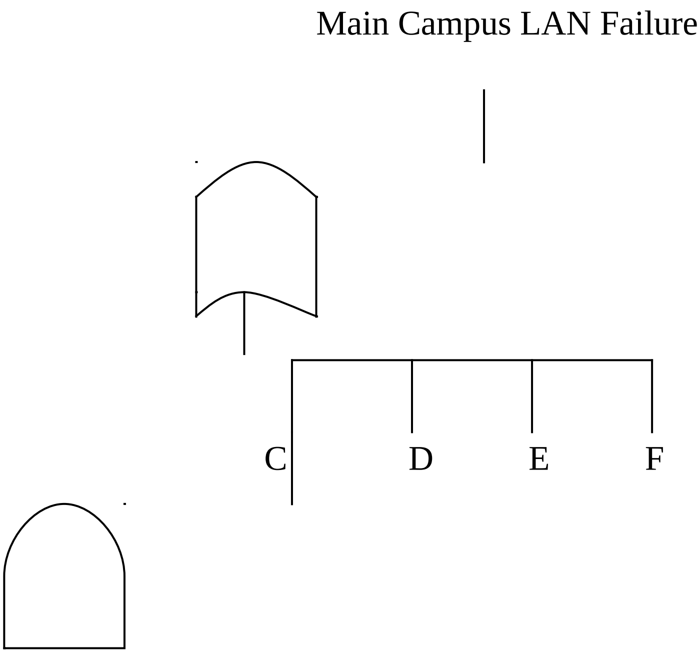


Figure 4.8 Fault Tree Analysis for Main campus LAN.

Figure 4.8 can be simplified in Boolean analysis as shown in figure 4.9. Note that items in series are combined in OR gate because any failure occurrence in any one of the items connected in series will cause a network failure.



A = Main Power Supply B = Standby Power Supply

C = Power Supply Failure D = Hub/Switch Failure

E = Server Failure F = Main Cable Failure.

Figure 4.9 The Main Campus LAN Boolean Analysis

4.7 PSTN data (Exchange Data Method)

As explained in the failure form, the item code clarifies one of the items that construct the network. The research concentrated on the public switched telephone network for many reasons. First, this network represent one of the two phases of SUST network for outside colleges, which is taken as a case study in this research. Second, its service affects a lot of people. Third, it consists of many items that are not available in small networks, like the large cabling system in addition of its switching system which consists of a number of subscribers in each board in the racks of the switching room.

The failure data of PSTN could be gathered by dividing the PSTN network into many items in order to simplify the data collection method. This will also be very helpful in calculating the reliability and availability of the PSTN
The failure data of PSTN network can be arranged as shown in table 4.2.

Item	**Code**	**Failures per year**
Part I		
Power supply unit	PS1	14
Digital line unit	DLU	2
Central processing unit	CPU	1
Part II		
Primary cable and manhole	PCB	4
Secondary cable unit and	SCB	18

cabinet		
Drop cable and subscriber pole box unit	DCB	3

Table 4.2 Failure data for one of the PSTN exchanges

In failure and dependability calculation the approach is to deals with each network exchange alone, because PSTN consist of many exchanges each has its own network. All exchanges are linked together using fiber optic cables through the whole country.(The data in table 4.2 was collected from Shambat Exchange)

The reason of dividing the network into many units is that for calculation of the dependability attributes it is more reasonable to deal with each unit separately and then the overall attribute value can be computed.

The first three units represent the switching part (part I) of the network.

The primary cable unit, the cabinet and the secondary cable unit, and the drop cable unit represent the outside part (part II) of the network. This illustrated in figure 4.10

The two parts work together for system success. For simplicity, each item in the two parts is focused and the failure data is collected for this item. The items found in each part are connected in series because for system success each item should be working properly. For this reason the Reliability Block Diagram (RBD) is configured as series configuration.

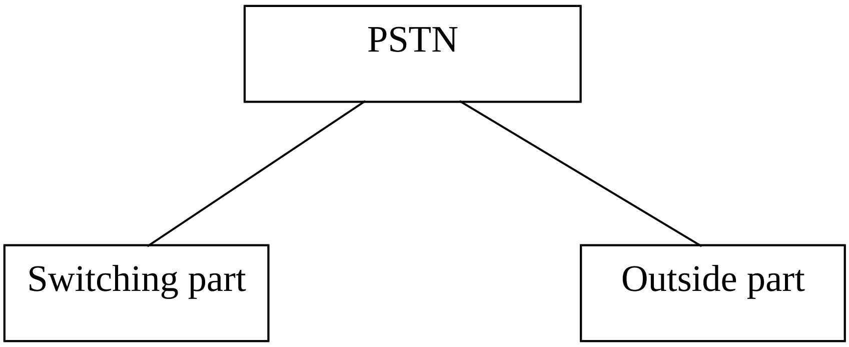


Figure 4.10 PSTN main parts

a) Part I :

This part consists of three units as shown in figure 4.11 below.

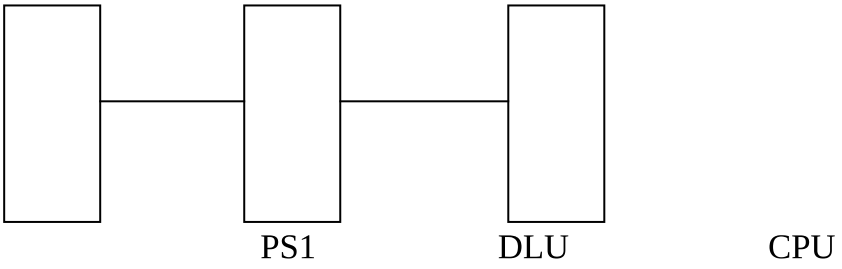


Figure 4.11 PSTN part I items

The following data was collected from Shambat exchange as an example for the PSTN exchanges used in SUST network.

Appendix 2 shows PSTN failure categories and sources.

1. PS1 unit failure report summary

The failure data collected for this unit showed that 1 failure has occurred in a period of five years. The summary taken from the failure report was:

Item code PS1

Failure code I sever

Failure mode 02 open circuit

Failure occurrence over a year = 14 failures

Down time 5 minutes for each failure

2. Digital Line Unit (DLU) failure report summary

Item code DLU

Failure code I sever

Failure mode 02 open circuit

Failure occurrence over a year = 2 failures

Down time 2 hours , 1.5hour, respectively

3. CPU (central processing unit) failure summary:

Item code	CPU	
Failure code	I	sever
Failure mode	06	(disk read error)
Failure occurrence	over a year	= 1 failure
Down time	2 hours .	

b) Part II

This is the outside unit. The goal is to show how the failure data can be treated. The best way to do that is to assign one exchange of the PSTN and record its failures. This was the way followed in the research. The number of customers per exchange varies from an exchange to another, but the average number of customers per one exchange is 20000 customers.

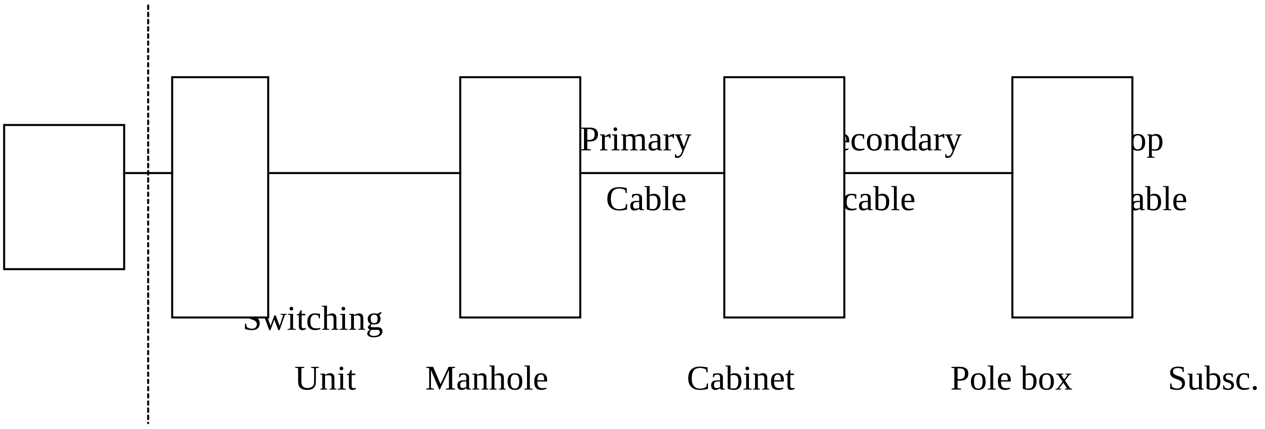


Figure 4.12 The outside part items

This unit is responsible of carrying the voice and other data for the various places of customers. The block diagram of this unit is shown in figure 4.12. Since this outside part consist of only cabling system, the failure modes are limited in the following codes:

04   Short circuit

05   Leak

06   Bad contact

07 Disconnect

Most of the failures in all exchanges occur in the rain season.

The primary cable and manhole (2400 line):

Item code PCB

Failure code II marginal

Failure mode codes 01, 03, 04, 05

Failure occurrence = 4 failures.

Down time 7 hours.

Note:

It is not necessary that all primary failures should affect all users of the exchange.

4.7.1 Number of Users Affected Factor (NUAF)

Here the effect factor should be taken into consideration, because the failure of the primary cable affects a large number of users. How many lines were stopped due the failure is very important. The number of user's lines affected varies from a failure to another. This must be considered when measuring any dependability attribute, because when you measure the availability or reliability in another area out of the failure zone you find a different value. Assuming that the PSTN is one network and should run without failures, any failure must be considered giving a very poor reliability and availability values.

For example in the year 2005 in Shambat exchange there were 120 failures in the primary cable, but the SUST network will be affected only by failures that cause some outages in SUST network for the campus that is connected to the exchange under consideration, (total of 14 outages) mentioned in table 4.4. For this reason in calculating the reliability or availability of the SUST network, only the 14 failures should be taken for this item. The reasonable method of calculating the dependability values for the whole PSTN, the end- to- end method is preferable. This is done by taking the number of the service cuts from a large number of customers (say 2000 in different areas) who use the PSTN over a year in order to measure the reliability and availability of the whole PSTN.

The secondary cable and cabinet:

The failures that affected the dependability of the exchange in this item over a year (2005) are shown below:

Item code SCB

Failure occurrence over a year = 18 failures

Failure codes I and II

Failure mode codes 01 for 3 failures, 03 for 5 failures, 04 for 1 failure, 05 for 9 failures.

Failure down time 3 hours for each failure.

The pole box and drop cable:

Item code DCB

Failure occurrence over a year = 3 failures

Failure codes I

Failure mode codes 03, 05, 05 respectively

Failure down time 3 hours each

Month of august was a remarkable month during the whole year because of the number of failures that occur in this month. This is due to the rainy whether in this period of the year.

4.7.2 PSTN data analysis

Phase two data can be converted into dependability data as follows:

1.Power supply unit data conversion:

1. The failure rate for the power supply unit can be calculated as:

$$\lambda = \text{(number of failure)/(operation period)}$$

For annual failure rate, AFR, the operation period = 1 year , and number of failures = 14 then:

$$\lambda = 14 \text{ failure/year} = 14/8760 = 0.00159$$

2. Mean time between failure (MTBF) can be found from :

$$\text{MTBF} = 1/\lambda = 1/(0.00159) = 625 \text{ hours.} \qquad (4.9)$$

3. Mean time to repair (MTTR) = 5 minutes = 0.0833 hours.

2. Digital Line Unit (DLU) conversion

1. The annual failure rate, AFR, λ:

$$\lambda = 2/8760 \text{ hours} \quad 0.00023 \quad \text{F/H} \qquad (4.10)$$

2. MTBF $= 1/\lambda = 1/0.00023 = 4380$ hours. (4.11)

3. MTTR $= (2 + 1.5)/2$ hours $= 1.75$ hours (4.12)

3. CPU unit data conversion

1. The annual failure rate, AFR, λ for this unit can be found as:

$$\lambda = \text{(number of failures)/(period time)} \qquad (4.13)$$

$$= 1/8760 = 1.142\text{E-}4 \ \text{F/H}$$

2. MTBF = 8760 hours

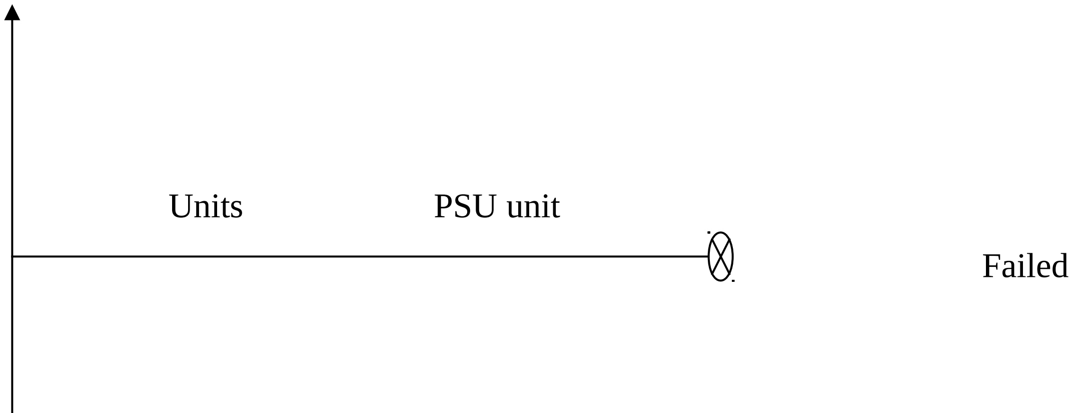
3. MTTR = 3 hours

4.7.3 Part I data classification

From the data collected for part I which consists of three units we can classify the data for Part I as:

1. Since the DLU unit arises a failure first, then its data is classified as interval censored data, because the time of failure lies between the time of complain and the moment it failed .
2. The PSU and CPU units data is considered as right censored data because when DLU failure appeared, CPU and PSU were still running. So they were suspending when DLU failure appeared.

The class of any unit's failure helps practitioners to pay an additional attention for the unit that has an interval censored data class, because the time of failure is a range may be sometimes a long range. This can be solved by narrowing the inspection gab time, say for example from every 72 hours to every 24 hours. The data of part I of phase two (PSTN) is shown in figure 4.13.



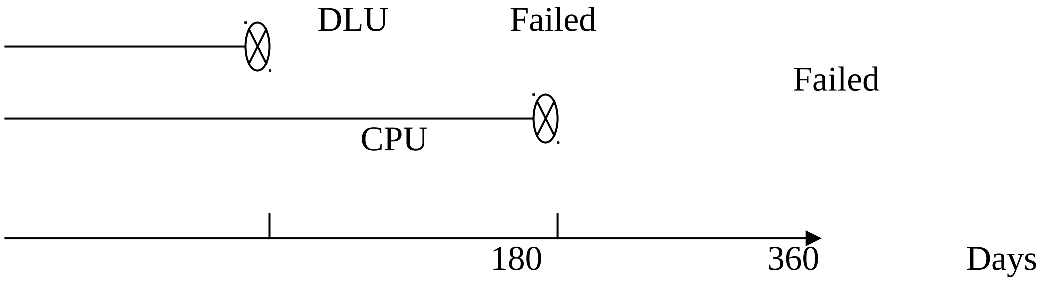


Figure 4.13 Part I data classification

4.7.4 Overall failure rate for part I:

Since the three units of this part are in series configuration, in other words, if any of the three units failed then the system will fail, and the network service is cut.

For serial system (AND configuration) of this part with three units, the overall reliability $R_{system} = \exp^{-\lambda st} = \exp(-\lambda_1 t).\exp(-\lambda_2 t).\exp(-\lambda_3 t)$ (4.14)

$$= \text{Exp}\,[-(\lambda_1+\lambda_2+\lambda_3)t]$$

Hence, $\lambda_s = \lambda_1+\lambda_2+\lambda_3$ (4.15)

so the overall annual failure rate (AFR) for this part = $(\lambda ps+\lambda_{DLU}+\lambda_{cpu})$

= 0.00159 + 0.00023 + 1.142E-4 AFR

= 0.0019342 AFR

4.7.5 PSTN outages for a campus

Another approach can be followed, that is to find the number of outages occurred in each college network because of the PSTN in a year and thus the AFR of the PSTN for that college could be found. For example, if the PSTN outages that affect any campus occurred 10 times during a year, then AFR will be equal to 10/8760 = 0.001142 AFR.

Using this method for Shambat Agricultural campus, 17 outages occurred in part I, so the AFR for this part is 17/8760 = 0.001934 AFR, which is the same value calculated by using individual method.

4.7.6 Overall MTBF for part I

The easiest way to find the overall MTBF is to calculate it from:

$MTBF_{PI}$ = $1/\lambda_{PI}$ (assuming that λ is constant) (4.16)

= 1/0.0019342 = 517 hours

4.7.7 Part II analysis

(a) Primary cable unit (PCB):

1. The annual failure rate, AFR, λ for this unit is equal to:

λ = 4/8760 = 0.000456 F/H (4.17)

2. The MTBF can be calculated as the average of the time between failures for all failures appeared in this unit. MTBF can be calculated using three methods:

Method 1:

$MTBF_{pcb}$ = [(time from the beginning of the year to failure one) +(time between failure one and failure two)+(time between failure two and failure three)+(time between failure three and failure four)+(rest of the year)]/4. OR

= [(206 days)(12 days) + (22 days) + (26 days)+(100)]/4 =

= (366days)/4 (4.18)

= 91.5 days = 2196 hours.

Method 2:

The MTBF can be calculated directly from :

MTBF = $1/\lambda$ = 1/0.000456 = 2190 hours (4.19)

(The difference in hours from method 1 is due to calculation digits)

Method 3:

Also the MTBF can be calculated from:

MTBF = $\frac{\text{Time period}}{\text{No. of failures}}$ = 8760/4 = 2190 hours = 92.1 days (4.20)

This method is the reciprocal of method 2.

3. The MTTR for this unit can be calculated as:

[(Time to repair failure 1) + (Time to repair failure 2)+(Time to repair failure 3)+(Time to repair failure 4)]/4

$$= (5 + 4 + 4 + 3)/4 = 16/4 = 4 \text{ hours.}$$

(b) The secondary cable unit (SCB):

1. The annual failure rate, AFR, λ for this unit can be calculated as:

$$\lambda = \text{number of failures/ time period}$$

= 18 failures per year

= 18/8760 per hour = 0.00205 AFR

This is the annual failure rate, AFR.

2. The MTBF of this unit follows the same basis of finding the time between failures divided by the number of time periods between these failures.. First the time between failure 1 and failure 2, failure 2 and failure 3, failure 3 and failure 4, and so forth up to the end of the table. At the end the sum of these periods must be divides by the number of the periods calculated.

To find time between failure 1 and failure 2, find the time gab between these two failures. This is the time between the time and date of the first failure and the time and date of the second failure.. Hence the same calculation will be done for the rest of failures.

The annual MTBF for this unit = 1/0.00205 = 487 hours.

3. As shown in table 4.3 the MTTR is calculated by dividing the sum of the time spent to repair each failure by the total number of failures.

$$\text{MTTR} = \frac{\sum_{i=1}^{n} (\text{TTR}_i)}{n} . \qquad (4.21)$$

Where n equals the number of items repaired, and TTR is the time spent to repair the item.

This is shown in table 4.3.

Failure	TTR	MTTR

1	4	
2	2.5	
3	4.33	
4	1.5	
5	1.5	
6	4	
7	3	
8	1.5	
9	2	
10	2.5	
11	3.75	
12	3	
13	2	
14	3	
15	2.5	
16	1.5	
17	3	
18	2	2.532

Table 4.3 TTR and MTTR for SCB unit

(c) The drop cable (DCB) unit:

1. Annual failure rate calculation:
2. The number of the total failures for this unit was eight failures per year, so, the annual failure rate, AFR, λ for this unit is equal to 2/8760 per hour

$$= 0.00023 \quad \text{AFR}$$

3. The MTBF will be calculated as the same as calculation done for the primary cable unit which is equal to 8760/2 = 4380 hours.
4. The MTTR for DCB unit is also found by dividing the time to repair each failure by the total number of failures. The time to repair failure 1 was 3 hours, and the time to repair failure 2 was 4 hours. Thus MTTR is equal to:

$$\text{MTTR} = (3+4)/2 = 3.5 \text{ hours.} \qquad (4.22)$$

4.7.8 Overall failure rate for part II

Since the three units of part II are in series, then the overall annual failure rate λ_{PII} will be calculated as :

$$\lambda_{PII} = \lambda_{PCB} + \lambda_{SCB} + \lambda_{DCB} \qquad (4.23)$$

$$= 0.000456 + 0.00205 + 0.00023 \quad F/H$$

$$= 0.00684 \quad F/H$$

4.7.9 Overall MTBF for part II:

$$MTBF = 1/(\lambda_1 + \lambda_2 + \ldots\ldots\ldots\lambda_n) \qquad (4.24)$$

$$= 1/[(1/MTF_1) + (1/MTBF_2) + \ldots\ldots\ldots(1/MTBF_n)]$$

and assuming that λ is constant, the overall MTBF can also be calculated from the overall failure rate as:

$$MTBF_{PII} = 1/\lambda_{PII} \qquad (4.25)$$

$$= 1/0.00684 = 146.2 \text{ hours}$$

4.7.10 The Average MTTR for part II:

$$= (MTTR_{PCB} + MTTR_{SCB} + MTTR_{DCB})/3 \qquad (4.26)$$

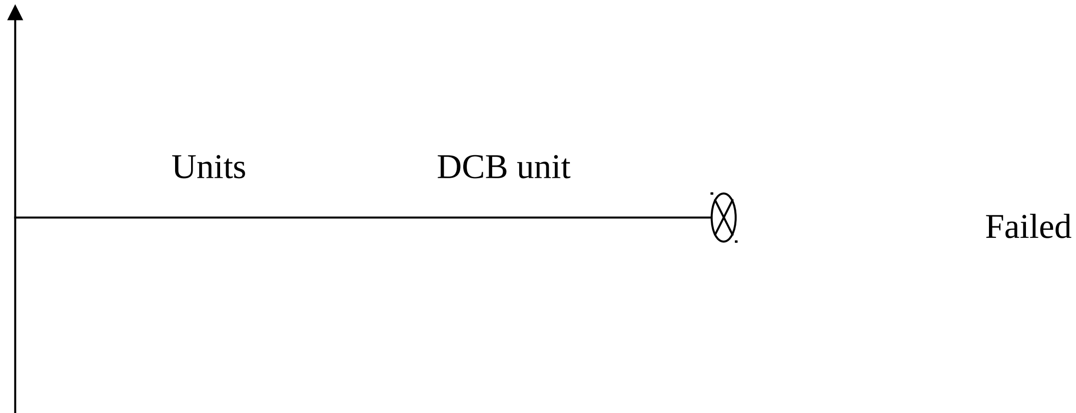
$$= (4 + 2.532 + 3.5)/3 = 3.344 \text{ hours}$$

4.7.11 Part II data classification

The data collected for part I which, also consists of three units can classified as:

1. The PCB unit arises a failure first, and then its data is classified as interval censored data, because the time of failure lies between the time of complain of affected customer or from the time of inspection by the technical persons and the moment it actually failed.

3. The SCB and DCB units data is considered as right censored data because when PCB failure appeared, SCB and DCB were still running. So they were suspending when PCB failure appeared. This is shown in figure 4.14.



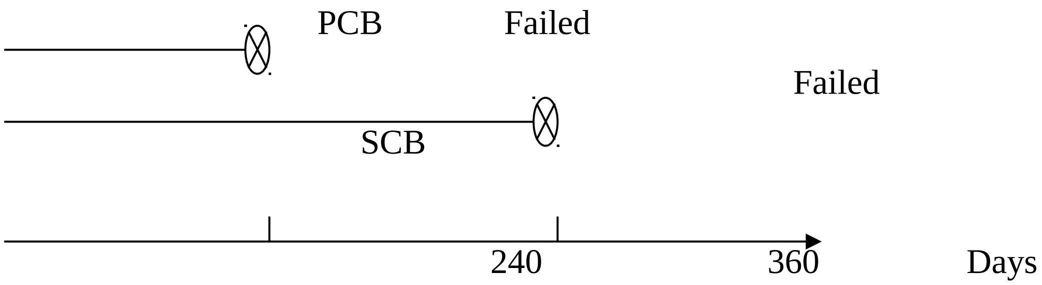


Figure 4.14 Part II data classification

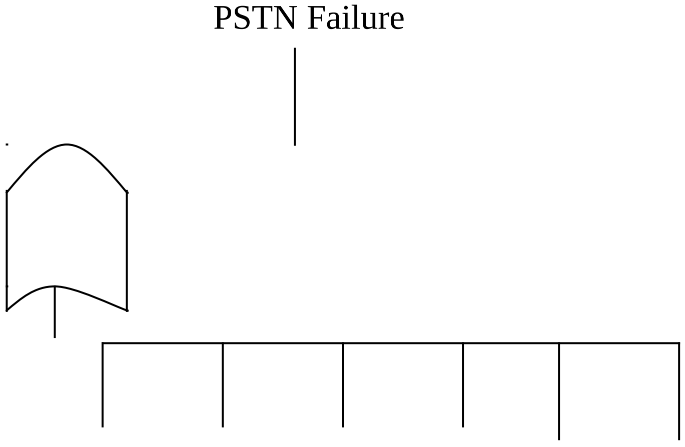
4.7.12 PSTN FTA

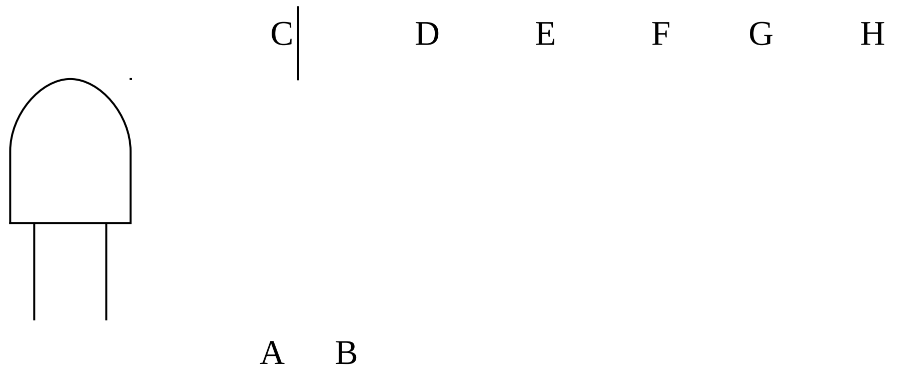
The Boolean failure analysis can be used to show the PSTN failure as dependent on its items failures. This is shown in figure 4.15.

Part I has PS, DLU, and CPU in OR gate since any failure of them will cause network failure. The standby PS of this part will be in AND gate because to have a PS failure, both of main PS, and standby PS must fail.

Part II three items (PCB,SCB, and DCB) are connected through OR gate because any failure of the three cuts the network service.

Note that the output of any logical gate in the Boolean analysis represents the state of failure occurrence. For example if two items inputs are connected to the inputs of an OR gate, it means that any one of these two items fails, the output is high and that means a failure will occur, and no system success will appear.





A = Main PS	B= Standby PS	C= PS failure	D= DLU
E = CPU	F= PCB	G= SCB	H= DCB

Figure 4.15 Boolean Analysis for PSTN

4.8 FTA for SUST network Sites

For any site outside the main campus, the RBD and Boolean FTA could be described. Figure 4.16 illustrates the block diagram for the site. It clear that for any college site to work, both phase I, and phase II must be working.

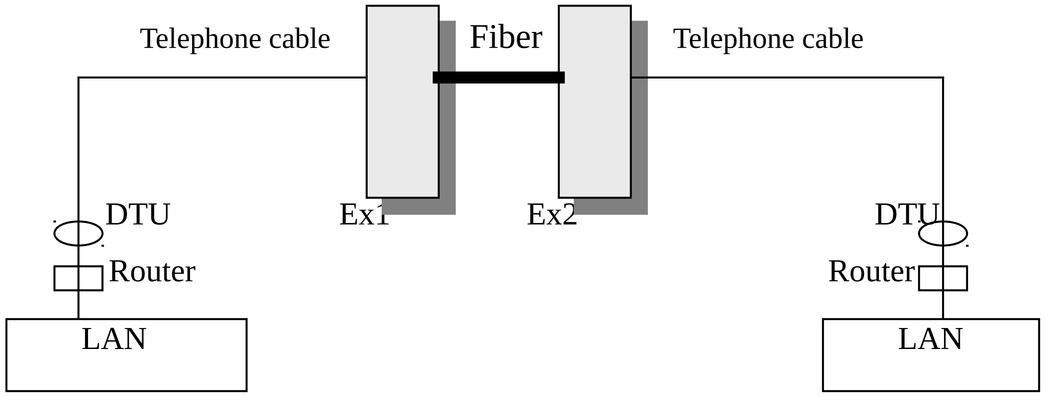


Figure 4.16 College site connection block diagram

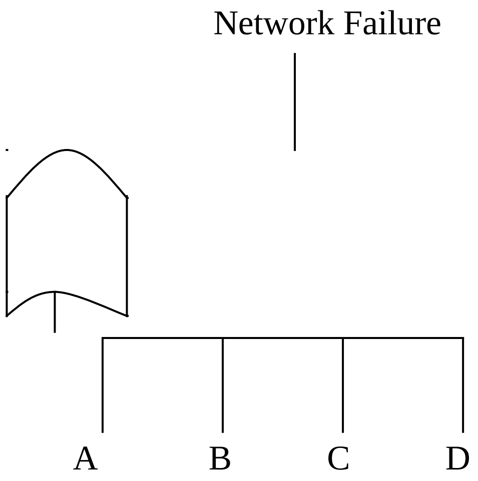
Ex1 and Ex2 are the PSTN exchanges, which are connected by fiber.

The items that should be working to have a network services for any site are:

1. DTUs at LAN1 and LAN2.
2. Routers at LAN1 and LAN2
3. The LAN switch
4. The PSTN

The first three items are involved in phase I, and the fourth item represents phase II.

Thus, the Boolean Failure analysis would be like the one shown in figure 4.17.



A = DTU$_{12}$ B= Router$_{12}$

C= Switch D= PSTN

Figure 4.17 The Boolean FTA for a college site

Note: DTU$_{12}$ means the two DTUs, one at each end as illustrated in figure 4.13

Router$_{12}$ are the two routers, one at each end of the LANs.

4.8.1 Repair Ratio (μ)

The mean time to repair MTTR for any unit can be measured as:

$$\frac{\text{Time period for all repairs}}{\text{Number of repairs}}$$

But the repair rate is sometimes may be needed to give an idea about the repair action done associated with the time spent in these repairs. So the repair ratio can be calculated also from any field data as:

Repair ratio μ = 1/MTTR repair per time R/T.

Part I:

1. PS1 repair ratio = 1/5 = 0.2

2. DLU repair ratio = 1/1.75 = 0.57

3. CPU repair ratio = 1/3 = 0.333

Part II:

1. PCB repair ratio = 1/4. = 0.25

2. SCB repair ratio = 1/2.532 = 0.4

3. DCB repair ratio = 1/3.5 = 0.286

4.9 Summary table

Table 4.4 summarizes the failure data for SUST network including all colleges divided as phase I, and phase II outages. This table will be used in measuring the dependability of SUST network. It is important to stress here that occurrence of any failure causes a service cut. Each outage has a downtime measured in minutes or hours.

Site	Phase I failures per year	Phase II (PSTN) failures per year	Phase I D.T per year Hrs	Phase II D.T per year Hrs	Phase I (AFR)	Phase II (AFR)
Main	6.75	-	3	-	7.7E-4	-
Engineering	1	16	1	7	1.141E-4	0.00183
Human Dev	-	8	-	5	-	9.13E-4
X-Ray	1	15	2	8	1.141E-4	0.00171
Agr.College	2	14	2	7	0.000223	0.00160
An. Recs	2	18	3	9	0.000223	0.0021
Forstry Col.	1	23	2	8	1.141E-4	0.00263

Table 4.4 Summary of SUST WAN failure data

CHAPTER 5

Network Reliability Modeling and Measurement

5. Network Reliability modeling

5.1 Reliability Modeling

Reliability modeling is the process of calculating the anticipated system Reliability from assumed item failure rate. It provides a quantitative measure of how close a design comes to meeting the design objectives and allows comparisons to be made between different design proposals. It is a valuable :exercise for the following reasons

1. It provides an early indication of the network's potentials to meet the network design requirements.
2. It enables an assessment of life cycle costs to be carried out.
3. It enables one to establish which item or area in the design contributes to the major portion of the unreliability.
4. It enables a comparison to be made between reliability, maintainability, and availability.
5. Its use is increasingly called in invitations to tender, and contracts reports.

Reliability engineering is the function of analyzing the expected or actual reliability of a product, or services, and identifying actions to reduce failures or mitigate their effects. The overall goals of reliability engineering is to make the product or service more reliable in order to reduce repairs, and to lower costs

A system's overall reliability can be determined by the development of reliability models. The complexity of these reliability models is dependent upon various factors such as mission profiles, function criticality, and redundancy characteristics. The general approach is to capture the modeling effort with the use of Reliability Block Diagrams (RBD).

For each system the mission profile or usage profile varies. For example a combat aircraft's mission profile may be expressed in maximum mission duration of six hours, with a required probability of mission success (reliability) of 98%. Whereas, a financial institution data processing system must provide a continuous operation, twenty-four hours a day, every day of the year, and it may be expressed in achieving a target operational availability.

The model could be concerned with just showing the critical functions and the associated failures modes, as derived in the FMEA. This information may further be used in the FTA .

Redundancy or back-up mechanisms will enhance the reliability of a system, but augment the Life Cycle Support (LCC). Questions that would need to be considered, is whether the system should employ "active redundancy or standby redundancy ". The actual decision for the system redundancy could also be dictated by other engineering constraints, for example the safety requirements might mandate a 2 out of 3 voting redundancy for critical system components.

5.2 Redundancy

There are numbers of ways in which redundancy can be applied. These are shown in figure 5.1. The full redundancy is widely used, while others are rarely used. The standby redundancy is widely used in power supplies plants like standby generators.

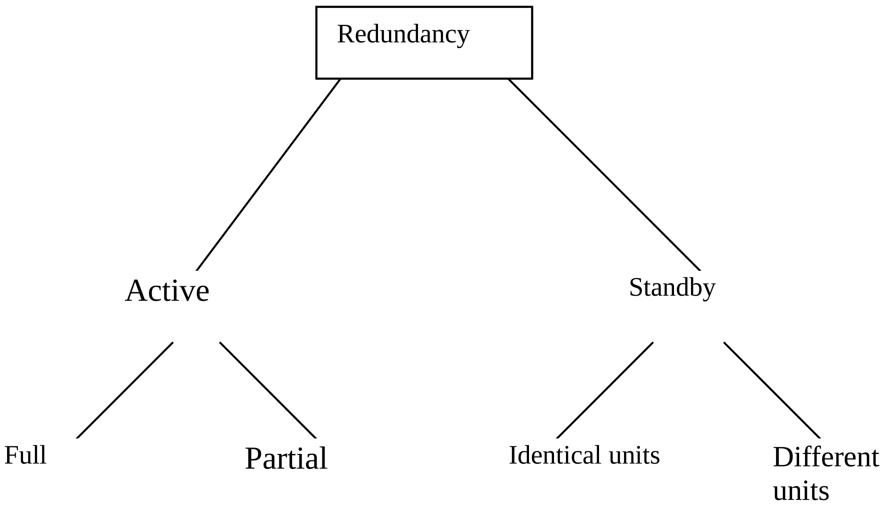
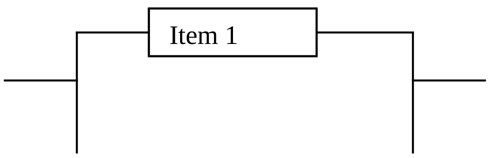


Figure 5.1 Redundancy types

5.2.1 Full active redundancy

Full active redundancy does not need a switch to change from item one to item two. This is illustrated in figure 5.2. Both items need to fail in order for the system success to fail. This is a parallel reliability block diagram.



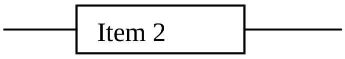


Figure 5.2 Full redundant system

Since the two items are in parallel, the system reliability for two items is:

Rsystem = $1 - (1 - R_1)(1 - R_2)$ (5.1)

= $R_1 + R_2 - R_1R_2$ where R1 is the Reliability of item 1

R2 is the Reliability of item 2.

If both items have the same failure rate λ, say for example $3\text{x}10^{-6}$ per hour, then:

$R1=R2 = e^{-\lambda t}$

$\lambda t = 3\text{x}10^{-6}\ \text{x}8760 = 0.026$ (Annual Failure Rate, AFR)

$R1=R2= e^{-0.026} = 0.974$

$R_{system} = 2R1 - R_1^2 = 2(0.974) - (0.974)^2 = 0.999$

Using the system AFR, $AFR_{system} = (AFR_1)\ (AFR_2)$ (5.2)

$R_{system} = 1 - (0.026)^2 = 0.999$

This means that the system failure rate is equal to the product of the failure rates of the two items. Appendix 8 explains the probability addition and subtraction, together with Binomial and Bays theorems.

5.2.2 Partial active redundancy

Consider a system with three items with reliability R. If two of the items are required for system success, and the third is redundant, then it is a partial redundancy. So, only one of the three is allowed to fail. This is illustrated in figure 5.3 in which two items out of three is required for system success.

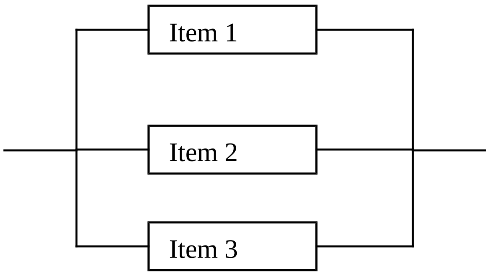


Figure 5.3 Partial redundancy

Once again the reliability can be obtained from the binomial expression since it is the probability of 0 or 1 failures, which is given by the sum of the first two terms. Hence:

$$R_{system} = R^3 + 3R^2(1 - R) \qquad (5.3)$$

$$= 3R^2 - 2R^3$$

5.2.3 Standby Redundancy

Standby redundancy involves additional units, which are activated only when the operating unit fails. This means that the standby unit operates for less time. Figure 5.4 shows two identical units, one is active, and the other is standby.

Standby redundancy differs from active redundancy in that standby needs a switch which is turned over when the operating unit fails.

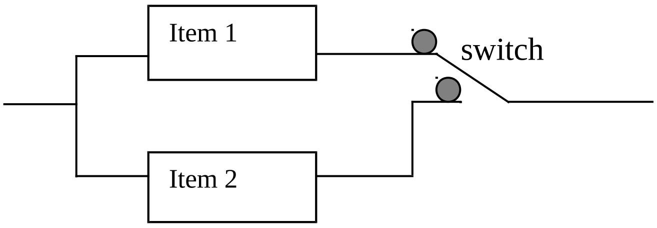


Figure 5.4 Item 2 is standby for item 1

The switch is always considered as ideal switch, where the time of changing from item 1 to item 2 is neglected. The standby item is assumed not to fail when idle.

When calculating the reliability, one approach is to consider the system as if it consists of one item. If the two items are identical, the same failure rate and thus the same reliability is assumed. If they are different, different failure rate and reliability are taken.

The approach here would have redundant elements that would support a fault tolerant architecture. In this case, the active redundancy, all of the redundant elements are utilized by the system, (they are powered up). However, in the event that one (or more) element fails, the system is capable of performing its required function and operation. The redundant elements incorporated into a design could be a simple affair or consist of very complex elements. With a more complex configuration the architecture could consist of a combination of elements having no redundancy, a couple of elements having dual redundant, to several elements in parallel.

The final system configuration would be influenced by the actual required reliability and availability requirements, which takes into consideration whether the system is repairable or non repairable. For example a system is required to operate for a given operating time period, and maintenance is not possible. Such as a commercial airliner making a transatlantic crossings, its redundant architecture would have take into consideration the fact that a repair could not be implemented for the several hour flight duration,. In the case of a satellite or space probe, it is required to operate for several years and during this time no maintenance would be feasible.

Another example might be a data processing system which is required to have a high operational availability, and must provide a continuous service of 24 hours a day, seven days a week, 365 days a year. This type of system could be an air traffic control system or a financial banking network system. To support the operational availability requirement, a maintenance philosophy may be developed, that would ensure that all repair actions (corrective maintenance tasks) are completed with one or two hours of a failure.

There might be instances where a system must achieve an operational availability and itself cannot afford an extend downtime. With repair actions of a failed unit being possible, but the implementation of an active

redundant configuration not considered feasible, due to economic or operational reasons. It maybe more appropriate to utilize a standby redundant configuration. An example of this could be a field power generation plant. The power distribution configuration would consist of two diesel generators. One would be online (running) continuously and the other would be in a standby state (not running). In the event that the operational generator experiences a failure (or where the need to perform preventative maintenance exists), the standby generator would be brought on-line. This would then permit a repair action to be implemented on the failed generator set without downtime.

5.3 Reliability Measurement

There are many methods available for determining the reliability of an item (this could be a piece part to a complete system). They are:

5.3.1 Reliability Prediction

This is the process used to determine the MTBF of an item. This is achieved by performing a prediction analysis.

Similarly this method is used to determine what the reliability of a new product will be based upon the "known" reliability of an existing product with similar attributes. These attributes can be the type of technology used, digital circuitry, complexity of components and also comparable operating environments and scenarios.

5.3.2 Operational Reliability

This is the result of determining the reliability of a product based upon its operational performance in the field. Normally an organization would establish a process designed to collect fielded data. The MTBF will be determined by dividing the total cumulative operation hours for all fielded products by the number of failure occurrences.

In the design and development of a new product, the design and reliability engineers, may not have available field data (reliability performance data), due to the simple fact that the system has not been fielded. In this case the reliability engineer must use alternative methods to determine the reliability of the proposed system. Early in the concept phase, with a minimum depth of knowledge of the proposed system, a high level understanding of the system could be determined.

Example: A local area network LAN, the basic system will consist of a computer server, a hub, a cable, and Data processing equipment and possible some data communications equipment. From these Function groups of equipment we can estimate that there will be Power supplies, Digital Circuit Card assemblies, computers, etc. With this we can start the preliminary process of estimating the systems MTBF.

For preliminary estimation the MTBF may be determined by similarity, in other words, the MTBF of a known system (previously developed and fielded) is available, and therefore this data will be used until more information becomes available.

Important to most people is the numeric performance value for an equipment or system. It may be a figure such as the Mean Time Between Failure (MTBF) for a piece of communication equipment or the Mean Distance Between Failures (MDBF) for a transmission medium. Whatever the numeric value, what is important is how it is derived for the equipment or systems.

A good method is to put "x " number of systems in the operational field and wait to see how many items fail and are returned for repair. However this reliability information is required long before the fielding of an equipment or system.

5.3.3 Apportionment Reliability

The purpose of the apportionment method is to assign a reliability figure to an item. This is particularly useful in the early conceptual and design phase. The apportionment allocates the reliability figure to the item in question, allowing the overall budgetary control of a system's end reliability. This will also allow the development of reliability figures that could be introduced into the performance specifications for sub-systems. The apportioned reliability will be reviewed, as the design of the equipment becomes more solid.

5.3.4 Similarity Reliability

The similarity method is employed when there is enough design clarity of an item. Basically it utilizes known predicted or fielded data from other components similar in nature, in terms of technologies and complexity.

This method should also take into consideration the operational environment and quality of the product, of the new item and that to which it is been compared. For instance an electronic computer module has an Input Buffer Module (12 discrete inputs) and, is being designed for a new application. A previous module was developed for another application, using the same component quality and density. As this item was previously developed for another project there is some reliability prediction data available. This data can be utilized for the new design, when it has been modified by a factor to take into account the differences between the two operating environments.

5.4 Microelectronic Basic Data Reliability

This method, considered by some to be controversial, is used in the design of equipment to permit a predictive assessment of its reliability. Predictions of electronic components can be achieved by using MIL-HDBK-217 or Bellcore. There are several standards (handbooks) widely used by the reliability engineering world, these include military and commercial. They concentrate on the application of Military Handbook MIL-HDBK-217. This particular handbook has been constantly revised over the years. This handbook is focused on the electronic parts reliability predictions. The fundamental approach of this document is to commence the development of a reliability prediction from the discrete component upwards, using specific algorithms for generic electronic components.

In the case of MIL-HDBK-217, there are two methods, a part count and a full stress. To implement either of these two methods requires certain knowledge with respect to the electronic components and the maturity of the product design. The Parts count is performed when for example, a Printed circuit board's design is such as to be able to determine the main component type, quality and quantity. This method makes general assumptions on the applied stresses for each electronic component.

The full stress method is invoked when the design of a printed circuit board is nearly complete and subject to possibly only minor changes. This particular method evaluates the thermal and electrical stresses that are applied to a component under given environment conditions (operational environment and ambient temperature). This method will afford an analyst to assess if specific design practices are been adhered to such as stress dreading. Therefore it is possible identify if a component is been operated outside allowable stresses.
A mechanical system or component may be subjected to stress/ strength interference modeling. Also generic reliability figure can be sourced from documents. The user should also be aware of the actual design margins of a mechanical component. Implementing stress analyses is used to determine the margin of safety and the safety factor of a particular item.

5.4.1 Parts Count

The parts count method is utilized in the bid phase or early design phase when there is insufficient information available, thus not enabling a full stress method to be conducted. There is sufficient information or data available to allow for a preliminary reliability prediction to be conducted. MIL-HDBK-217 provides a set of default tables that provides a generic failure rate (λ_g) for each component type and is based upon the intended operational environment. This component generic failure rate is also modified by a quality factor (π_Q), which represents the quality of the component(s) in question. The component is manufactured and tested to a full military standard or to a lesser commercial standard. In addition for micro-electronic circuits a learning factor (π_L) is used and represents the number of years that a component has been in production. Using a components generic failure for a given environment and modifying it to give consideration for its quality and in the case of microelectronics the learning factor, its final failure rate is established and given by:

$$\lambda_p = \lambda_G \cdot \pi_Q \cdot \pi_L \qquad (5.4)$$

λ_p is the part failure rate

λ_G is the device generic failure rate

π_Q is the device quality factor

π_L is the learning factor.

The summation of the individual component's failure rates will yield the overall failure for the circuit card assembly they populate. With this and the summation of other circuit card assembly failure rates, the failure rate of a line replaceable unit will be established. This process will provide an overall failure rate for a system

5.4.2 Full Stress

The full stress method, like the parts count method, provides a failure rate for an electronic component. The summation of the failure rates for all components on a circuit card, and all the circuit cards within a black box, and all the black boxes, within a system will yield the overall failure rate for any system. To enable a full stress analysis to be conducted there must be sufficient details on the systems design available to the reliability engineer. In essence the design of the system must be such that the electronic and electrical design of the hardware is to the components level. There will be detailed parts lists and circuit schematics available. This is required because the stress analysis takes into consideration the electrical and thermal stress that will be experienced by each component.

The full stress analysis is completed by the reliability engineer who knows the detailed knowledge of the electrical and electronic design. In addition he/ she will require specific data pertaining to each component type used within the design. Component information, or data sheets, are supplied by the manufacturer. In the case of a full stress analysis, the mathematical models are detailed in MIL-HDBK-217 for each component type (micro electronics, resistors, capacitors and electro/ mechanical devices).

The general approach used by MIL-HBK-217, is each generic component type is assigned a base failure rate (λ_b) and is modified by influential factors. These factors, as listed below are used when modifying the base failure rate. Some of the factors will result in a linear degradation of the base failure while others will cause an exponential degradation, in particular factors associated with temperature. These factors are:

π_E = Use Environment.

This factor is set based upon the intended operating environment for the equipment/ System

π_Q = Quality Factor.

This is a general look up factor that represents the quality of the component in question. Generally the base failure rate is modified by the multiplication of this factor.

Depending on the type of component under analysis the base failure rate will be subject to additional modification by various factors

5.4.3 Microelectronic mathematical models

Mathematical Model: Microcircuits, Gate/ Logic Arrays and Microprocessors

The following algorithm is a general model used by MIL-HDBK-217 for microcircuits that include Bipolar and MOS devices, digital and linear gate/ logic arrays, Field Programmable Logic Arrays (PLA) and Programmable Arrays Logic (PAL) and Microprocessors.

$\lambda_P = (C_1\pi_T\pi_A + C_2\pi_E)\,\pi_Q\pi_L$ Failures Per Million Hours (FPMH)

Where:

C_1 = The die complexity (number of gates or transistors): A look-up table provides a figure depending on the number gates/ transistors of the device under analysis, plus if it is linear, digital (or PLA/ PAL) or in the case of a microprocessor the bit word complexity, e.g. up to 8, 16 or 32 bit word. The temperature factor is derived from a formula. Given below is the formula for silicon devices. A look up table provides a figure for specific devices, based upon its junction temperature. This is calculated based upon the case and ambient temperatures, taken into consideration the junction to case and case to

π_T is the ambient thermal resistances.

C_2 Is the package Failure Rate factor used for microcircuits, this takes into consideration how the device is packaged in a flat pack, can, hermetic sealed etc.

π_E Is the environmental factor, depending on the intended operational environment. For example the factor applied to a device used in a Ground

Benign would use 0.5, whereas for the Naval Sheltered a factor of 4.0 would be used and in the case of a sever environment such as the cannon launch Environment a factor of 220 would be applied.

$\pi_A =$ Application factor is applied to for the intended use of the device, for MMIC devices used in a high power application a factor of 3 would be applied, where as a digital device would use an applied factor of one

$\pi_Q =$ The Quality Factor is applied to the quality standard that the devices has be manufactured to, whether commercials to Mil-Spec Quality levels

$\pi_L =$ Learning Factor. This factor is applied to represent the number of years that a device has been in production.

A deployed (or fielded) system will after a given period of time reveal its actual reliability performance. Only when a system is fielded can its performance be readily measured to determine its design adequacies or in some cases inadequacies. The reliability performance is derived from observing the failures that have occurred in the field. For the system/ product user/ provider to determine actual reliability performance, a data collection system needs to be established and put into place.

An existing mature system maybe proposed as a hardware solution for another project, which itself has been operating in an operational environment for sometime. In assessment of this field data, it must be clearly understood how this system was operated and in which environment, under what conditions, and what the total system fleet cumulative operating hours are. In addition the quality of the data needs to be established. Was the data collected and obtained in a realistic way, or were some data elements obtained by making assumptions. For example, were all reported failures actually caused by the inherent reliability characteristics of the equipment or were failures induced through poor management and maintenance practices, such as poor preventive maintenance, operator and/ or maintainer induced failures etc. Further to this was the data accurately collected and reported.

Data presented and furnished by suppliers cannot always be taken at face value. Some suppliers might have made assumptions about the equipment and its utilization For example, a supplier of equipment, such as commercial computer equipment, may only have visibility on how their equipment is performing by those items returned to them under warranty or as part of a service contract. In deriving their actual reliability they may have factored in a duty cycle with respect to the total number of hours that the equipment (on average) is used or powered up. If one was to use this data, and decide to apply an operating duty cycle for their own intended environment, then a clear case of double dipping will occur.

The ramifications of not fully understanding how field data was derived could have a profound impact on the conclusion of a system/ equipment reliability performance assessment, which would directly influence spare parts holding, warranty and life cycle cost.

5.5 Software Reliability

Software's increasing role creates both requirements for being able to trust it than before, and for more people to know how much they can trust their software. A sound engineering approach requires both techniques for producing reliability and sound assessment of the achieved results.

There are some difficulties in applying engineering approach to software reliability because of its diversity in industry. It is commonplace that software is increasingly important for society. The Y2K bug has just brought this to the attention of the public, not only was a huge expense incurred for assurance against its possible effects, but this effort affected all kinds of organizations and systems. Various dimensions of software dependence include:

- Software-based systems replace old technologies in critical applications. Software has found its way into aircraft engine control, nuclear plant protection, as well as networks. New critical applications are developed, like automating aspects of surgery. Some of these applications imply ultra-high dependability requirements.
- Software moves from an auxiliary to primary role in providing critical services. Air traffic control networks are being modernized to handle more traffic transactions. Network's software failure leads to network failure which may affects thousands of people services.

The major difference between software and other engineering artifacts is that software is pure design. Its unreliability is always the result of design faults. The unreliability of hardware systems, in the other hand, has tended until recently to be dominated by random physical failures of components.

Software in networks is either system software or application software, and in both cases the number of faults should be recorded. The software item is configured as series with other item when finding the network reliability.

5.6 Reliability Modeling Concepts

To model the reliability, two important issues should be considered. These are the relationship between the items in the system under consideration (system configuration), and the method to describe the model, which is usually the mathematical expression of the model.

5.6.1 System Configuration

One of the most important concepts in reliability modeling is to gain a full description and understanding of the system to be studied. The system should be divided into a set of items, each of whose reliability is easy to measure. Then there appear a relationship between the items and components and the reliability of the whole system.

There are two basic types of system relationships considered in the combinatorial analysis of reliability:

1. Sequential system
2. Redundant or concurrent system

For all networks or other systems, the sequential or series configuration is the basic configuration since it describes the passage of required service from an item to another till it reaches the output to the end user of the system. In sequential system, all items of the system must function successfully for system success. It called AND configuration because the failure of any of the items in series will cause system failure.

This is illustrated in figure 5.5.

Q1 Q2

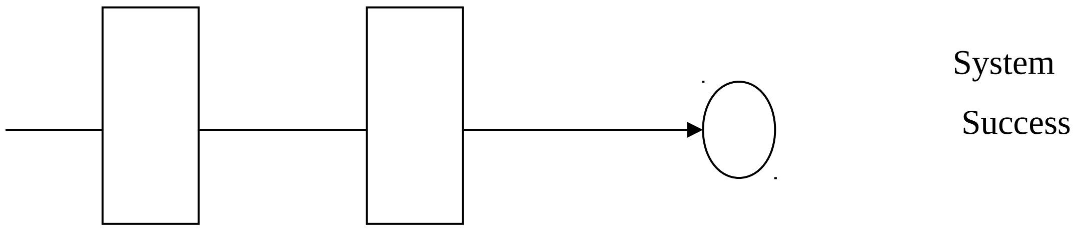


Figure 5.5 Series system configuration

The system success of the series (or sequential) system is expressed as:

System success = (Q1).(Q2) .

The concurrent or redundant system consists of items Q1, Q2 that connected in parallel and function at the same time (both are active) as explained in the event diagram in figure 5.6.

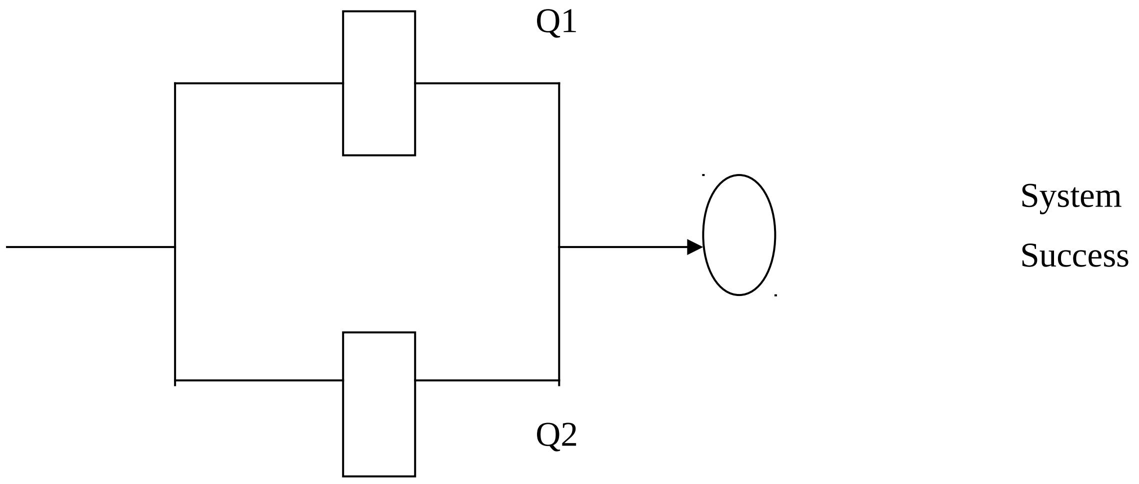


Figure 5.6 Concurrent system block diagram

The system success of the concurrent or redundant system is expressed logically as:

System success = (Q1) OR (Q2).

The events diagrams explained in figure 4.3 and figure 4.4 can be used as a Reliability Block Diagram (RBD) for modeling and measurements purposes. A system may consist of a series and redundant items in which case the configuration of the system is called AND-OR configuration.

For different operational modes, one must determine what kind of network system he has from combinatorial viewpoints, especially the two principal kinds, the serial and concurrent functioning systems.

5.6.2 Reliability Measurement

After the system configuration was set, which reliability rule should be used to find the system reliability depends on the system configuration itself. There is a rule for series system, and another rule for parallel or redundant systems.

5.6.2.1 Series Items Reliability Rules:

(a) If all items must function successfully for the system success, the failure of any of the item will cause the system failure. Thus the overall system reliability, R_{system} is given by:

$$R_s = \prod_{i=1}^{k} R_i = R_1.R_2.R_3........R_k. \qquad (5.5)$$

where R_i = item reliability.

(b) The unreliability UR represents the probability of failure F(t). so

$$F(t) = 1 - R(t) \qquad (5.6)$$

This can be rewritten as:

$$R(t) = 1 - F(t) \qquad (5.7)$$

As you add more items in series, you lessen the overall reliability.

Appendix 3 shows how added items in series affect the overall system reliability.

5.6.2.2 Reliability of Redundant System

If successful functioning of any of the items will result in system success, or the failure of all items is required for system failure, the system reliability is given by:

$$R_s = 1 - \prod_{i=1}^{k} (1 - R_i) \qquad (5.8)$$

The equation is derived from the fact that the overall probability for concurrent system F_s is equal to:

$$F_s = F_1.F_2.F_3\ldots\ldots\ldots..F_k. \qquad (5.9)$$

Where F_k is the last item failure probability.

$$\text{Since } R_s = 1 - F_s = 1 – (F_1.F_2.F_3\ldots\ldots F_k) \qquad (5.10)$$

Substituting for $F = 1 – R$ gives

$$R_s = 1 - [(1 – R_1).(1 – R_2).(1 – R_3)\ldots\ldots\ldots(R_k)]$$

$$R_s = 1 - \prod_{i=1}^{k} (1 - R_i) \qquad (5.11)$$

For two concurrent items system, the overall reliability Rs can be calculated as:

$$R_s = 1- (1 – R_1).(1 – R_2)$$

$$= 1 - (1 – R_2 – R_1 + R_1R_2)$$

$$= 1 – 1 + R_2 + R_1 – R_1R_2$$

$$= R_1 + R_2 – R_1R_2 \qquad (5.12)$$

The reliability R of any system can be calculated from the equation:

$$R = \exp(-\lambda t)$$

And the failure rate is equal to:

$$\lambda = (-1/t)\ln R \qquad (5.13)$$

For sequential system each item has a failure rate, then the system failure rate λ_s is equal to the summation of the items failure rates.

$$\lambda_s = \sum_{i=1}^{k} \lambda_i \qquad (5.14)$$

$$= \lambda_1 + \lambda_2 + \lambda_3 + \ldots\ldots\ldots\ldots\lambda_k$$

Some examples will give more explanation.

Example 5.1:

For a series system of two items, if R1 = 0.67 and we seek an overall reliability R_s of 0.6 for 24 hours of operation, what must be R_2 to obtain the required reliability? Find the system failure rate λ_s for the operation period given.

Solution :

We have

$$Rs = R_1R_2$$

$$0.6 = (0.67).R2 \qquad \text{then}$$

$$R2 = 0.6/.67 = =0.895$$

$$\lambda_s = (-1/t)\ln R_s$$

$$= (-1/24) \ln (0.719) \text{ failure per 24 hours}$$

$$= 5.7E\text{-}4 \text{ failure/hour} \qquad F/H$$

Example 5.2:

What is the overall reliability R_s of the following system? Calculate the overall failure rate for a month of operation.

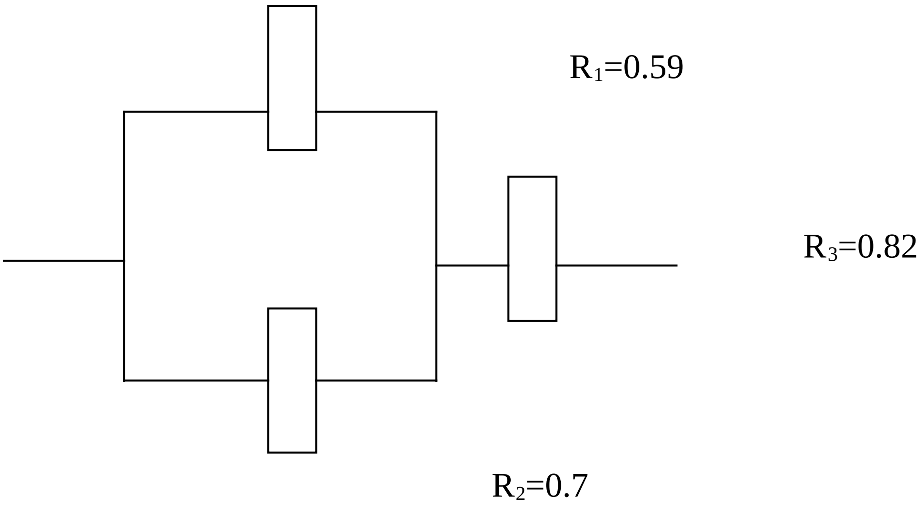


Figure 5.7 The AND-OR RBD of example 5.2

Solution

For R_1R_2 parallel configuration

$$R_p = R_{12} = R_1 + R_2 - R_1R_2$$

$$= 0.7 + 0.59 - (0.7).(0.59)$$

$$= 0.877$$

R_1R_2 are in series with R_3 then

$$R_s = (R_P).(R_3)$$

$$= (0.877).(0.82) = 0.719$$

failure rate $\lambda_s = (-1/t) \ln (0.719)$

$$= (-1/720) \ln (0.719)$$

$= 4.6E{-4}$ failure per hour (F/H).

Example 5.3

Suppose a data communication company wants to set up a network system. They set a reliability objective of 0.9 (90% reliability) for eight hours of operation shift. The network has the following configuration shown in figure 5.8.

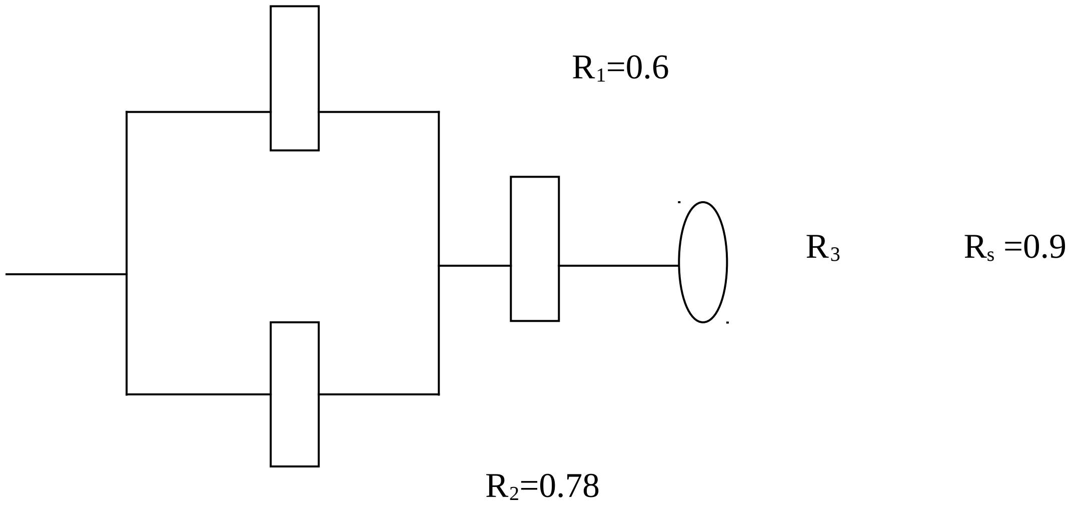


Figure 5.8 The RBD of the network of example 5.3

What is the maximum failure rate for R_3 so as to obtain the required reliability?

Solution:

To find R_3 failure rate, we have to find the reliability of R_3 first.

The reliability of R_1 and R_2 items is concurrent and given by:

$$R_{12} = R_1 + R_2 - R_1R_2$$

$$= (0.6) + (0.78) - (0.6).(0.78)$$

$$= 0.912$$

Now the overall reliability is given by:

$$Rs = (R_{12}).(R_3)$$

$$0.9 = (0.912).R_3$$

Then,

$$R3 = 0.9/0.912 = 0.987$$

The failure rate of R3 is equal to

$$\lambda_3 = -(1/8) \ln (0.987) \quad = \quad 0.00164 \quad F/H$$

5.7 Reliability Measurement Using Annual Failure Rate, AFR

The calculation of any item reliability starts with the MTBF. From this fact the Annual Failure Rate, AFR, can be determined which is used to determine the annual reliability value. The MTBF represents the average time it takes for a failure to occur.

$$AFR = 8760/MTBF = (8760).\ \lambda$$

$$R = (1 - AFR)$$

For an item with MTBF of 100000 hours, the following reliability value is determined:

$$AFR = 8760/100000 = 0.0876$$

$$R = (1 - 0.0876) = 0.9124 \quad \text{(or 91.24\%)}$$

5.8 The SUST Network Reliability Measurement

One method of improving the network system performance is to find its reliability as a system and as individual item. Without doing so, you can never evaluate the performance of the network and no engineering aspects could be done regarding its operation.

The Sudan University of Science and Technology network is a good case study to measure dependability main attributes to find out the weakness areas and to show the importance of measuring reliability and availability for the network, and their roll in improving the network performance. The reason of choosing this network as a case study is that it consists of various media connections including the use of the PSTN as essential part of the network. In addition, it uses the Frame Relay technology for communicating packets.

The Reliability Block Diagram (RBD) for the SUST network for any college is simplified in figure 5.9.

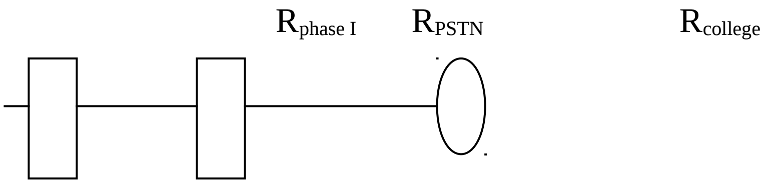


Figure 5.9 The overall RBD of any SUST college network.

To measure the reliability of the SUST the following were taken:

1. The network was divided into two parts, the campus part, and the PSTN part.
2. Each part was divided into main units, and each unit was divided into main items.
3. The reliability of each item was measured individually and the reliability of each unit was found, thus the reliability of the part was measured.
4. The PSTN failure per year was found for each college.
5. The overall reliability is achieved as a series combination of the two main parts illustrated in figure 5.9. (College part and PSTN part)

5.8.1 The Reliability Modeling of Main Campus

To measure the reliability of the Main campus, the dependability data mentioned in table 4.4 in chapter 4 can be used. The dependability data for the main campus is summarized in table 5.1

Site	Failures/yearλ	**Downtime/year**	**AFR**
Main	6.75	3	7.7E-4

Table 5.1 Main campus failure data

1/Using the formula:

R(t) = exp(-λt) then the annual Reliability will be:

R = exp[(-6.75)/8760] = exp(7.7E-4)

= 0.99923

2/ Using AFR:

Annual Reliability R = (1 – AFR)

= (1 – 7.7E-4) = 0.99923 (Same Value of method one)

5.8.2 Reliability Using Individual Items

The main campus network reliability can be computed using individual components configured in series to have the network system success. The items in table 5.2 reside in the main campus, and directly affect the main campus LAN.

Item	AFR λ	MTBF hrs	MTTR hrs
PSU	0.00046	2174	0.125
Server	0.00023	4348	1
Switch	5.7E-5	17520	3

Table 5.2 dependability data for Main campus LAN

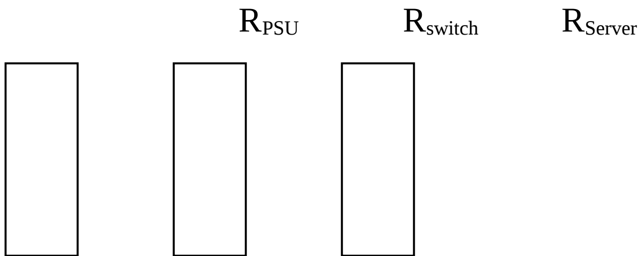
To model the operational reliability for the Main campus LAN, the following steps should be taken:

1. The time period, in which the reliability will be measured, must be assigned. Usually one year.
2. The RBD of the campus should be prepared, and must include all items, sequential items, and redundant items if any.
3. The value of each item reliability must be calculated using the formula:

$$R(t) \;=\; \exp(-\lambda t)$$

4. The overall reliability of LAN can be calculated according to Individual reliability of each item, with regard to the network system configuration. Multiply reliabilities of items in series, and use the redundancy formula for redundant items. The overall reliability also can be found from the overall failure rate.

The Reliability Block Diagram RBD is shown in figure 5.10



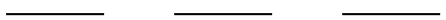


Figure 5.10 Main campus LAN RBD

1. R_{PSU} Measurement:

λ_{PSU} = 0.00046

R = exp(-λt)

R_{PSU} = exp(-0.00046)(1) = 0.99954 for one year.

Using AFR formula:

R_{PSU} = (1 – AFR) = (1 – 0.00046) = 0.99954 (the same value)

This means that the probability of the PSU to run without a failure for a year is equal to 99.994%

2. R_{switch} :

λ_{switch} = 5.7E-5 F/H

R_{switch} = exp(-5.7E-5)(1) = 0.99994

Using AFR formula:

R_{switch} = (1 – 5.7E-5) = 0.99994 (the same value)

This means that the probability of the switch to run for a year without a failure for a year is equal to 99.994%

3. R_{server} :

AFR, λ_{server} = 0.00023 F/H

R_{server} = exp(-0.00023)(1) = 0.99977

Using AFR formula:

R_{server} = (1 – 0.00023) = 0.99977

This means that the probability of the server to run without a failure for a year is equal to 99.977%.

Then the overall reliability R_{MAIN} of the main campus LAN can be calculated using
two methods:

Method I:

By using the overall annual failure rate, AFR, as follows:

$\lambda_{phaseI} = \lambda_{PSU} + \lambda_{switch} + \lambda_{server}$

$= 0.00046 + 5.7E\text{-}5 + 0.00023 + \quad = 0.00075$

$R_{MAIN} = \exp(-0.00075)(1) = 0.99925$ for a year.

Method II:

By using the individual reliability of each item connected in series.

$R_{phaseI} = (R_{PSU}).(R_{switch}).(R_{server})$

$= (0.99954)(0.99994).(0.99977).$

$= 0.99925$ (the same value of method I)

Thus, the reliability of every college outside the main campus could be found using the data in table 4.4. It is important to stress here that the PSTN phase Affects the reliabilities of these colleges because it is the main transmission media used to connect these LANs together. The approach is to count number of outages caused by both the local phase, and PSTN phase.

5.9 Engineering Campus Reliability

The failure data for this campus, recorded in table 4.4 in chapter 4 were:

Phase I outages =1 per year, with AFR =1.141E-4

Phase II (PSTN) outages = 6 per year, with AFR = 6.85E-4

Total downtime = 1+7 = 8 hours

The RBD for Engineering campus could be illustrated as shown in figure 5.11

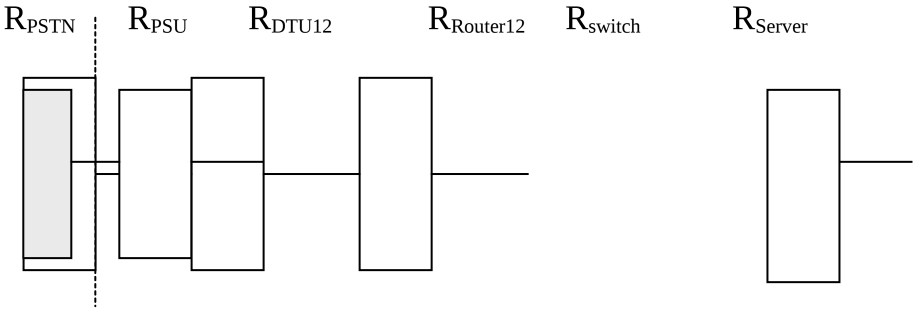


Figure 5.11 RBD for Engineering site (and other sites)

The R_{Eng}. could be found from phase I, and phase II reliabilities as:

$$R_{Eng} = (R_{phase\ I})(R_{PSTN})$$

R_{phase} = (1 – $AFR_{phase\ I}$) = (1 - 1.41E-4) = 0.99985

R_{PSTN} = (1 – AFR_{PSTN}) = (1 – 0.00183) = 0.99817

Hence $R_{Eng.}$ = (0.99985)(0.99817) = 0.99080

Look at the difference in reliability between phase I, and phase II (PSTN)

5.10 Human Dev. College Reliability.

The failures data for this college were:

Phase I outages =0, with AFR =0

Phase II (PSTN) outages = 8 per year, with AFR = 9.13E-4

Total downtime = 5 hours.

Thus,

$$R_{H.D} = (R_{phase\ I})(R_{PSTN})$$

$R_{phase\ I}$ = (1 – 0) = 1 = 100%

R_{PSTN} = (1 – AFR_{PSTN}) = (1 – 9.13E-4) = 0.99908

Hence $R_{H.D.}$ = (1.0)(0.99908) = 0.99908

5.11 X-Ray college Reliability

From table 4.4 the failures data for this college were:

Phase I outages =1, with AFR = 1.141E-4

Phase II (PSTN) outages = 15 per year, with AFR = 0.00171

Total downtime = 2+8=10 hours.

Thus,

R_X = ($R_{phase\ I}$)(R_{PSTN})

$R_{phase\ I}$ = (1 – 1.141E-4) = 0.99985

R_{PSTN} = (1 – AFR_{PSTN}) = (1 – 0.00171) = 0.99829

Hence $R_{x.}$ = (0.99985)(0.99829) = 0.99814

5.12 Agricultural Studies campus Reliability

The failure data from table 4.4:

Phase I outages =2, with AFR = 0.000223

Phase II (PSTN) outages = 14 per year, with AFR = 0.00160

Total downtime = 2+7=9 hours.

Thus,

$$R_{Sh} = (R_{phase\ I})(R_{PSTN})$$

$$R_{phase\ I} = (1 – 0.000223) = 0.99977$$

$$R_{PSTN} = (1 – AFR_{PSTN}) = (1 – 0.00160) = 0.99840$$

$$\text{Hence } R_{Sh.} = (0.99977)(0.99840) = 0.99817$$

5.13 Animal production campus Reliability

From table 4.4, the failure data:

Phase I outages =2, with AFR = 0.000223

Phase II (PSTN) outages = 18 per year, with AFR = 0.0021

Total downtime = 3+9= 12 hours.

Thus,

$$R_K = (R_{phase\ I})(R_{PSTN})$$

$$R_{phase\ I} = (1 – 0.000223) = 0.99977$$

$$R_{PSTN} = (1 – AFR_{PSTN}) = (1 – 0.0021) = 0.9979$$

Hence $R_{K.}$ = (0.99977)(0.9979) = 0.9976

5.14 Forestry studies campus Reliability

The failure data:

Phase I outages =1, with AFR = 1.141E-4

Phase II (PSTN) outages = 23 per year, with AFR = 0.00263

Total downtime = 2+8=10 hours.

Thus,

R_{FR} = ($R_{phase\ I}$)(R_{PSTN})

$R_{phase\ I}$ = (1 – 1.41E-4) = 0.99985

R_{PSTN} = (1 – AFR$_{PSTN}$) = (1 – 0.00263) = 0.99737

Hence R_{FR} = (0.99985)(0.99737) = 0.99722

The Reliability values for SUST WAN different sites can be summarized as described in table 5.3.

The goal of this table summary is to show the reliability of both phases side by side in order to compare between them. This is very useful because it shows which phase could be described as the weakest phase, and hence many decisions could be taken to make some modifications or redesign in some areas.

This is considered as one of the most important objectives of reliability measurement. A reliability team should study carefully the results of reliability measurement, and then a well-established decision could be held.

Site	Phase I Reliability	Phase II Reliability	Overall Reliability
Main campus	**0.99925**	**-**	**0.99925**
Eng. campus	**0.99985**	**0.99817**	**0.99802**
H. Dev. Campus	**1.0**	**0.99908**	**0.99908**
X-Ray campus	**0.99985**	**0.99829**	**0.99814**
Agricultural studies	**0.99977**	**0.99840**	**0.99817**
Animal	**0.99977**	**0.9979**	**0.99767**

Product campus			
Forestry studies campus	**0.99985**	**0.99737**	**0.99722**

Table 5.3 SUST WAN sites Reliability summary

5.14 General approach for Reliability Modeling of PSTN

To measure the operational reliability for the PSTN, the following steps should be taken:

-The failure rate for this period for each item of the PSTN must be calculated. It can be calculated from the value of the MTBF of the each item, or from the number of failure occurrence divided by the operation period.

-The RBD of the network should be prepared, and must include all items, sequential items, and redundant items if any.

-The value of each item's reliability could be calculated using the formula:

$$R(t) = \exp(-\lambda t)$$

Or the formula $R = 1 - AFR$

-The overall reliability of the PSTN can be calculated according to

Individual reliability of each item, with regard to the network system configuration. Multiply reliabilities of items in series.

To find the reliability of the PSTN the correct method is to find the reliability of part I, and part II then the overall reliability can be calculated for both parts in series configuration as (R_{PI}).(RP_{II}).

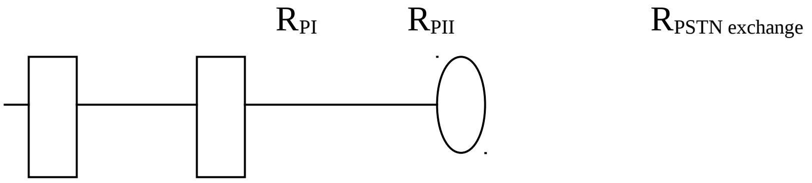


Figure 5.12 The overall RBD of the PSTN exchange.

For the PSTN discussed in chapter three, the field data was collected and analyzed. Now each item data of part I is summarized in table 5.4. The same table should be set for part II, and this is shown in table 5.5

Item	AFR λ	MTBF hours	MTTR hours
PS	0.00159	641	0.0833
DLU	0.00023	4348	1.75
CPU	1.142E-4	8760	3
Part I	**0.0019342**	**517**	**1.6111**

Table 5.4 PSTN Part I summary

The MTBF for each part is calculated as :

MTBF (part I) = $1/\lambda_{\text{part I}}$ = 1/0.0019342 = 517 hours, provided that the failure rate is considered as constant failure rate.

For variable failure rate, the MTBF is obtained from the integral of reliability assuming that the reliability characteristics are variable. Hence, in this case:

$$\text{MTBF} = \int_{0}^{\infty} R(t)\, dt \qquad (5.15)$$

The data used in table 5.4 and table 5.5 is considered as a field data because it was collected from Agricultural studies exchange. For this reason the reliability calculated from this data is the actual reliability, taking into account that we can never say that this reliability value is constant for all life cycle of this network. An annual reliability calculation should be made because it reflects the behavior of the network for a long period of time. In normal situation the reliability is supposed to increase a year after a year due to the experience gained for the personnel responsible of the network providing that

items of the network have not yet been weaired out.

Item	AFR λ	MTBF Hours	MTTR Hours
PCB	0.00456	2175	4
SCB	0.00205	730	2.532
DCB	0.0023	435	3.5
Part II	**0.00684**	**146.2**	**3.177**

Table 5.5 PSTN Part II data summary

(a) Overall Reliability of PSTN

The annual overall reliability of PSTN = $(R_{PI}).(RP_{II})$

$$R_{PI} = \exp[(-0.001934)(1)] = 0.99804$$

Or, $R_{PI} = 1 – 0.001934 = 0.9980$ (using AFR)

$$R_{PII} = \exp[(-0.00684).(1)] = 0.99352$$

Or, $R_{PII} = 1 – 0.00648) = 0.99352$

$$R_{PSTN} = (R_{PI}). (R_{PII}) = (0.99804).(0.99352)$$

$$= 0.99157$$ (classified as two nines)

This means that the probability for PSTN to run for a year without failure is equal to 99.157%.

To find the probability for PSTN to run for one day (24 hours) without any failure the following calculation can be done:

$$R_{PI} = \exp[(-0.0019342)(24)/8760] = 0.999995$$

$$R_{PII} = \exp[(-0.00684).(24)/8760] = 0.99998$$

Then the PSTN reliability for 24 hours = (0.999995)(0.99998) = 0.99998.

Here one sees that part I has reached the five nines for one day reliability , but the goal is to have this value for one year.

Hence one can find the reliability for any required period of time.

(b) Overall failure rate λ_{PSTN}

Can be calculated as:

$$\lambda_{PSTN} = \lambda_{PI} + \lambda_{PII} =(0.0019342) + (0.00684)$$

$$= 0.0087742 \quad \text{AFR}$$

The overall reliability of PSTN for a year can also found using the overall failure rate as:

$$R_{PSTN} = \exp[(-0.0087742).(1)] = 0.99157$$

Which is the same value calculated from the series connection of the two parts.

5.15 Estimating PSTN exchange reliability from customer data

The reliability as mentioned before is the probability of running a system or a service for an intended period of time without failure. To estimate the reliability of the PSTN one way is to collect sample data from customer's side. For example if 1000 customers from 21000 customers connected to the Agricultural studies PSTN exchange showed that only one failure was observed during one year of service time, excluding the programmed service cut due to the payment system, then annual failure rate, AFR, is equal to 1/8760.

This method is known as End-to-End method because it looks for the subject from the two ends of the service view, the service provider and the customer.

From this data:

$$\text{Failure rate } \lambda = 1 \text{ failure per year} = 1/8760 = 1.142\text{E-4}$$

$$\text{MTBF} = 8760 \text{ hours.}$$

Then :

$$R = \text{Exp}(-1.142\text{E-4})$$

$$= 0.99988 \qquad \text{(three nines)}$$

This means that the probability that the service will run for a year without a failure is equal to 99.988%.

5.16 The overall reliability of the PSTN of the country

The most acceptable method to find the overall reliability of the PSTN for the whole country is to find the reliabilities of all exchanges utilized, then the average reliability can be calculated as a series system with the average reliability of the fiber optic system that connects the exchanges together. PSTN can be illustrated as shown in figure 5.13.

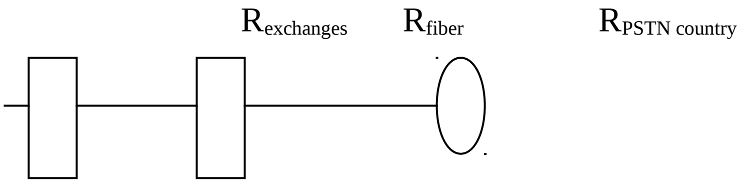


Figure 5.13 The overall RBD of the whole country PSTN .

5.17 Overall SUST Network Average Reliability

The Reliability of the SUST WAN as a whole can be divided into two divisions:

1/ The university division, which consists of all LANs of the various colleges. This division is distinguished based on the fact that the full administration of this division belongs to the university.

2/ PSTN division, which describes the part that belongs to the telephone company, and the university, has to accept its reliability as offered by the company. This means that, the University cannot take the decisions of enhancement for this division.

Thus, the overall average Reliability of the SUST WAN is the average of overall reliabilities of different colleges.

$$R_{SUST} = [(R_{All\ colleges})/\text{number of colleges}]$$

$$R_{SUST} = (0.99925+0.99802+0.99908+0.99814+0.99817+0.99767+0.99722)/7$$

$$= 0.99822$$

5.18 Reliability Growth Modeling

This concerns the improvement in reliability during use, which comes from field data feedback resulting in modifications, improvements depend on ensuring that field data actually lead to design modifications. Reliability growth then is the process of eliminating design related failures. It must not be confused with the decreasing failure rate described by the Bathtub curve. Figure 5.14 illustrates this point by showing two Bathtub curves for the same item of equipment. Both show an early decreasing failure rate, whereas the later model, owing to reliability growth, shows higher reliability in the random failures part of the curve.

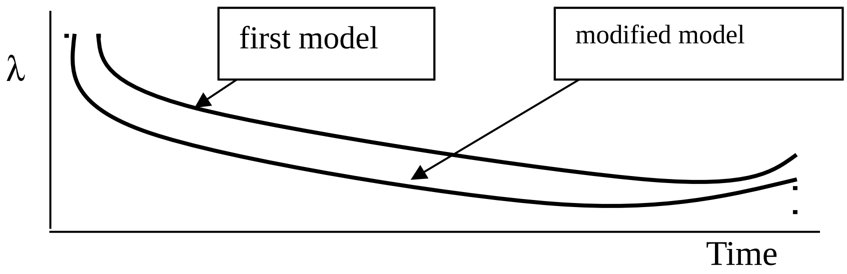


Figure 5.14 Effect of reliability growth on Bathtub curve

CHAPTER SIX

Network Availability

6. Availability

Network availability is considered as one of the most important dependability subsets, which, obviously points out to the dependability level of the network.

6.1 Understanding Availability

What does it mean when we say availability and how does this understanding impact the engineering of practical systems? Existing measurements and models do not capture the complex time-varying nature of availability in today's network environments. Further, unforeseen methodological shortcomings have dramatically biased previous analyses of this phenomenon.

Inevitably, real systems stop working at some point, disks fail, hosts crash,

networks partition, software miscalculates, administrators misconfigure or users misuse. Consequently, the principal challenge in designing highly available systems is to tolerate each failure as it occurs and recover from its effects. However, engineering such systems efficiently requires the designer to make informed decisions about the availability of individual system components.

Availability is defined as “the quality of being present or ready for immediate use”. However, this seemingly simple definition can conceal tremendous complexity. In traditional data storage systems, the components of interest are devices like disks, interfaces, and buffers, each of which have well-understood statistical failure properties that are usually assumed fail-stop and independent (e.g., redundant disk arrays). In network systems, however, all network equipment are of interest.

While the failure of individual hardware components can still compromise the availability of any network device, a network system designer must also anticipate transient software failures, partial or total communication interruption, and users.

6.2. Availability modeling

The definition of availability is somewhat flexible, depending on what types of downtimes are

considered in the analysis. Availability in the simplest form, is:

$$A = \text{Uptime}/(\text{Uptime} + \text{Downtime}) \qquad (6.1)$$

When the results are studied for annual time frame, the equation can be rewritten as:

$$A_a = (\text{Uptime hours})/8760 \qquad (6.2)$$

If we look at the availability from a design perspective, it can be calculated as:

$$A_i = \text{MTBF}/(\text{MTBF}+\text{MTTR}) \qquad (6.3)$$

Availability calculated from this equation is called the mean or instantaneous availability.

If mean time between failures (MTBF) (or mean time to failure MTTF) is very large compared to the mean time to repair (MTTR) or mean time to replace in case of unrepairable systems, then a high availability can be seen. As reliability decreases (MTBF becomes smaller), better maintainability (shorter MTTR) is needed achieve the same availability. Of course as reliability increases then maintainability is not so important to achieve the same availability. Thus tradeoffs can be made between reliability and maintainability to achieve the same reliability, and thus the two disciplines must work hand-in-hand to achieve the objectives.

Operational availability looks at availability by collecting all of the abuses in a practical system.

$$A_o = \text{MTBM}/(\text{MTBM}+\text{MDT}) \qquad (6.4)$$

This is called the operational availability.

The mean time between maintenance (MTBM) includes all corrective and preventive actions, compared with the MTBF, which only accounts for failures. The mean down time (MDT) includes all times associated with the system being down for corrective maintenance (CM) including delays, and self-imposed down time for preventive maintenance (PM) compared with

MTTR which only addresses repair time. A_o is smaller than A_i because of considering the preventive maintenance time as a downtime.

Like reliability, availability is a probability. Thus one might assume that the same technique of multiplying probabilities could be applied to estimate system availability. Consider a series system with two items. the point or instantaneous availabilities at time t for item 1 and item 2 are 80% and 90% respectively. The system availability at time t would be:

$$A_s = A_1.A_2 = (0.80).(0.9) = 0.72 \quad \text{or} \ 72\%.$$

This method can be justified from a probabilistic perspective because both items need to be available when called upon in order for the system to be available. However, the method does not take into account the effect of item availability when the items are operating together in a system configuration. The availability of one item will be different within the system than when calculated individually. This is because when the system is down due to the failure of the second item, the first item is running.

This effect of system operation is not taken into account in the estimation of the availability for the individual component and yet it quite relevant to the availability of the system.

6.3 Effect of system operation on item availability

Figure 6.1 demonstrates the effect of system operation on item availability. Consider a system with two units configured in series. As shown in figure 6.1, and figure 6.2, where unit 1 fails every 100 hours and takes 20 hours to restore and unit 2 fails every 75 hours and take 25 hours to restore.

The individual availabilities of the unit for 300 hours are 86.6% and 75% respectively.

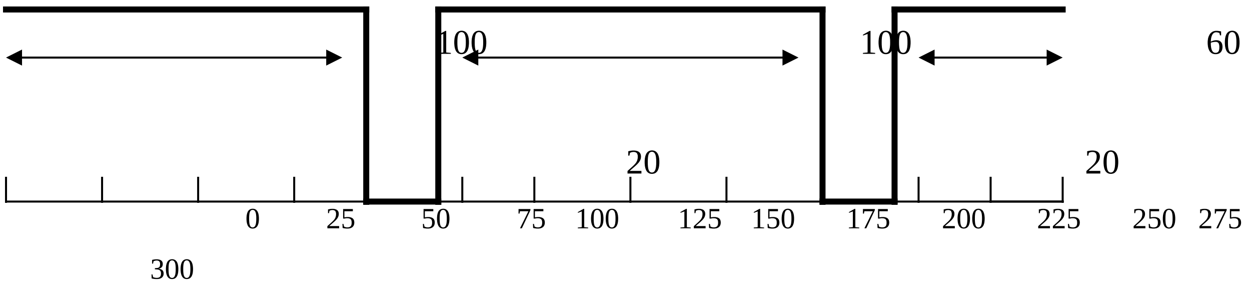


Figure 6.1 Up and downtimes for unit 1

Unit 1 availability = 260/300 =86.666%.

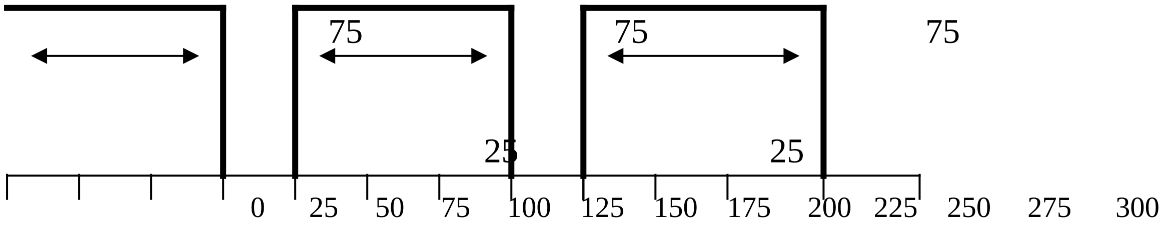


Figure 6.2 Up and downtimes for unit 2

Unit 2 availability =225/300 =75%.

However when we analyze the items units operating together in a system, we see that unit 2 will fail first at 75 hours, causing the system to fail. The system will then be undergoing maintenance for 25 hours and will be operational again at 100 hours. At 125 hours the system will fail again, this time due to unit 1. this is because unit 1 fails after 100 hours of operation and it had accumulated 75 hours before system fail and another 25 hours after the system was restored. The same process can be repeated yielding the system results shown in figure 6.3.

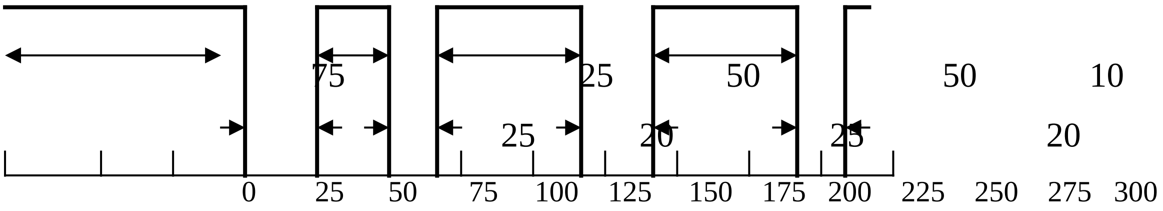


Figure 6.3 Up and downtimes for the system

The system availability =210/300 =70%.

6.4 Network availability

For example, a peer-to-peer network system may replicate some files on machines at a certain time. However, after some time, some machines may be turned off as their owners go to do another job, returning at some later time. The availability of the hosts is therefore dependent on time of day, and hence, the availability of the file is a function of time. Another issue is whether the availability of a host is dependent on the availability of another host, or, whether two host availabilities are interdependent. This issue is important since many peer-to- peer systems are designed on the assumption that a random selection of hosts in a P2P network does not all fail together at the same time.

Consequently, host availability is not well modeled as a single stationary

distribution, but instead is a combination of a number of time-varying functions, ranging from the most transient (e.g., packet loss) to the most permanent (e.g., disk crash). Traditionally, distributed systems have assumed that transient failures are short enough to be transparently masked and only the long-term components of availability require explicit system engineering. In peer-to-peer systems, though, this abstraction is grossly insufficient. Users periodically leaving and joining the system again at a later time introduce a new intermittent component of availability. Moreover, the set of hosts that comprise the system is continuously changing, as new hosts arrive the system and existing hosts depart it permanently on a daily basis.

A peer-to-peer system designed on this substrate will need to incorporate arriving hosts into it without much overhead, while being able to provide all the functionality it promises to provide in the face of regular departures.

Engineers are motivated to study peer-to-peer host availability in part to shape the design and evaluation of a highly available, wide-area peer-to-peer storage system. A primary goal of the system is to provide efficient, highly available file storage even when the system is comprised of hosts with relatively poor and highly variable availability. Even so, results can apply to any peer-to-peer system constructed from a similar collection of hosts.

Availability can be examined empirically by characterizing host availability in a large deployed peer-to-peer file sharing system over a seven days period.

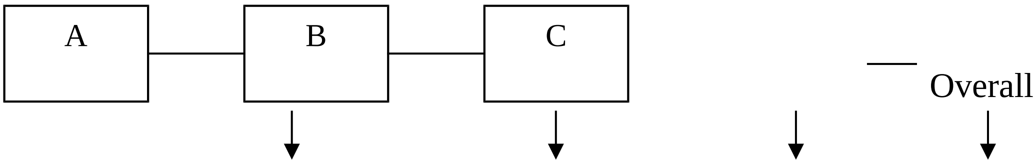
To describe and measure other networks rather than P2P network, the following five steps should be taken:

1. The block diagram of the network must be drawn including all units.
2. Any redundant items must be shown.
3. The network software should be considered as a series unit with other units.
4. The availability of each unit must be found individually.
5. The overall availability of the network then should be found.

6.5 Availability using downtime

The availability can be measured using the lost time compared with useful time of a complete cycle of operation time. Consider the availability block diagram (ABD) shown in figure 6.4 with the values given.

Block C fails every two years, and its down time is a long time. Thus block C has a maintainability problem.



Failure Rate	22.8E-6		114.2E-6		57.1E-6	=194.1E-6/hr
Fail./year	0.2	+	1	+	0.5	=1.7
fail./year						
Repair time/fail	18		24		83	= 41.6 MTTR

Downtime/year 3.6 + 24 + 41.5 = 69.1 hrs/year

Figure 6.4 ABD of three items

Using downtime, the availability of the system in figure 5.4 is:

$$A = \text{Uptime}/(\text{Uptime} + \text{Downtime})$$

The average availability for one year is equal to:

$$A = \text{Uptime}/(8760)$$

$$A = (8760-69.1)/8760 = 99.2\%$$

Using the mean rule for availability in equation (6.3) gives:

$$A = \text{MTBF}/(\text{MTBF} + \text{MTTR})$$

MTBF = 1/(Failure Rate) = 1/1.7 =0.58823529 year

MTTR = 41.6/8760 year = 0.00474886 year

Then average availability is equal to:

$$A = 0.58823529/(0.58823529 + 0.00474886)$$

$$= 0.992 = 99.2\%$$

Thus the same value of the average availability is obtained.

6.6 SUST network availability calculation

The approach used in the research to measure the availability of SUST network follows the same method of measuring the reliability. In calculating availability of SUST network, the network is divided into two phases:

-The local or campus phase

- The PSTN phase.

The overall availability is then found as a series configuration of the two phase and thus it is equal to the product of the two availabilities as shown in figure 5.4.

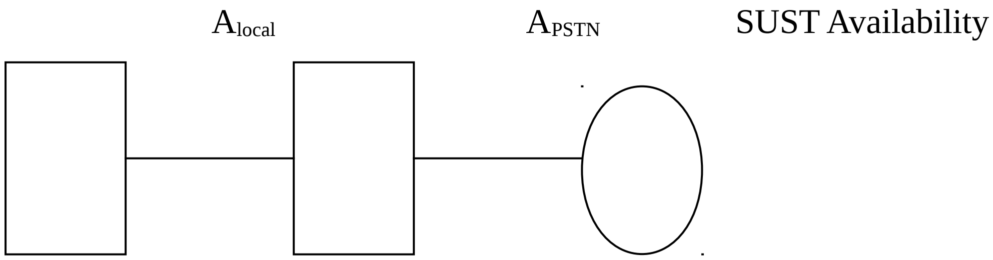


Figure 6.5 SUST network availability

The overall availability of SUST network A_t can be calculated as:

$$A_t \quad = \quad (A_{local}).(A_{PSTN})$$

Each phase of the two phases includes many items that conclude its availability.

6.6.1 Main campus availability

Figure 6.6 illustrates the availability block diagram (ABD) of from which the availability can be found.

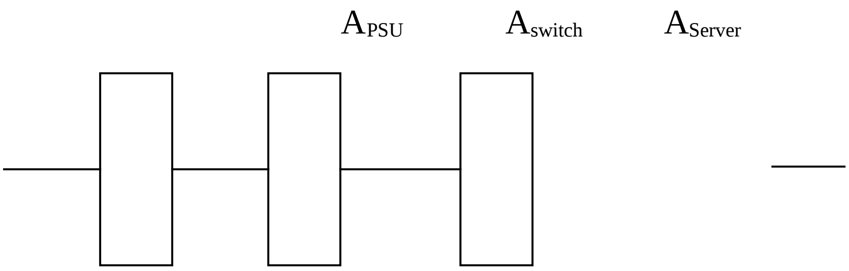


Figure 6.6 Phase I ABD

Notes:

1/In the ABD, the transmission medium is ignored since its outage is almost zero.

2/ The Routers and DTUs found in the main campus are used to connect other sites of the WAN, thus, their failures data are included in other sites.

The ABD diagram of figure 6.6 can be applied to every college campus of the SUST WAN. This configuration is connected in series with the PSTN in order to find the overall availability of any college.

The failure data used to calculate the availability of this phase is summarized in table 6.1 below, which is extracted from table 4.4 in chapter 4.

Item	MTBF hrs	MTTR hrs
PSU	2190	0.125
Server	4380	1
Switch	17520	3
Fiber cable	35040	4

Table 6.1 The availability data

6.6.1.1 PSU availability

The most suitable way to calculate the availability is to use the mean availability rule.

A_i = MTBF/(MTBF + MTTR) so

A_{PSU} = 2190/(2190 + 0.125) = 0.99994

This is equal to 99.994% availability.

Also the availability can be determined from Uptime/(Uptime+Downtime) as:

A_a = 8759.5/8760 = 0.99994

6.6.1.2 The server availability

From table 6.1 the server availability can be found as:

A_{server} = 4380/4381 = 0.99977
This is equal to 99.977% availability.

6.6.1.3 The switch availability

Can be found as:

A_{switch} = 17520/(17520+3) = 0.99983

This is equal to 99.983% availability.

6.6.1.4 The cable availability

From table 6.1 the cable availability can be calculated as:

A_{cable} = 35036/(35040) = 0.99988

This is equal to 99.932% availability.

From the values of availabilities calculated for all items of phase I, the overall availability of this phase is equal to the product of these availabilities.

A_{Main} = (A_{PSU}).(A_{server}).(A_{switch}).(A_{cable})

= (0.99994).(0.99977).(0.99983).(0.99988)

=0.99889

The overall availability of the main campus can also be determined from:

A_{Main} = Uptime/(8760)

Uptime = 8760-downtime = 8760 – 9.5 = 8750.5

A_{Main} = 8750.5/8760 = 0.9988

6.7 Engineering campus Availability

The failures data for this site were:

Total annual downtime = 8 hours (see table 4.4)

A = (operation period – downtime)/operation period

A_{Eng} = (8760 – 8)/8760 = 0.99908

6.8 Human Dev. Site Availability

from table 4.4 the down time of this site is 5 hours.

The availability of this site is equal to 8755/8760

= 0.99942

6.8.1 X-Rays site Availability

From table 4.4 in chapter four, the annual down time is equal to 10 hours.

Thus, the availability is determined as:

A_X = 8750/8760 = 0.9988

6.9 Agricultural studies site Availability

The total down time per year is equal to 9 hours.

Then,

A_{sh} = 8751/8760 = 0.99897

6.10 Animal production site Availability

From table 4.4, the total down time per year is equal to 12 hours.

A_K = 8748/8760 = 0.99863

6.11 Forestry Studies site Availability

The total downtime per year for this site as found in table 4.4 is equal to 10 hours. Then,

A_s = 8750/8760 = 0.99885

Table 6.2, below summarize the availability values for both phase I, and phase II (PSTN) for all sites.

Site	Phase I Availability	Phase II Availability	Overall site Availability
Main campus	99.88%	-	99.88
Eng. Campus	99.998%	99.92%	99.908%
Human Dev.	100%	99.942%	99.942%
X-Ray campus	99.97%	99.9%	99.88%
Agricultural studies campus	99.97%	99.92	99.897%
Animal production	99.965%	99.897%	99.863%

campus			
Forestry Studies campus	99.97%	99.9%	99.885%
Average	**99.965**	**99.913**	**99.878**

Table 6.2 Availability summary table for all sites

From the table, it is clear that:

1. **No site has five nines,**
2. **The PSTN availability is always less than the local phase availability.**

6.12 PSTN availability (general approach)

This is the PSTN availability that can also be determined by calculating the availability of each item in this phase and then the overall availability of the PSTN can be found as the product of all items availabilities. The approach is to divide the PSTN into its exchanges, and then each exchange is divided into its main parts. Then each part could be divided into its main items. Availability Block Diagram (ABD) then could be set to show the relationships between these items. Usually system success results from series connected items in the ABD unless there are some redundant items. It is very important to stress here that the availability of the PSTN could be estimated from calculating the availability of one of its exchange, taking into account the differences in operational environment between various exchanges.

The PSTN generally could be divided into two parts as shown in figure 6.7.

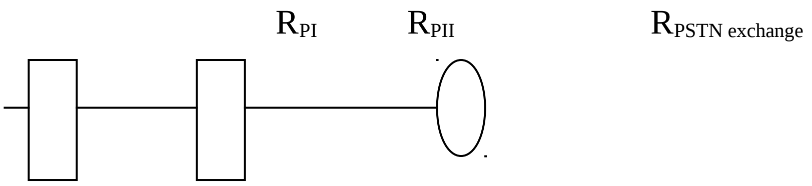


Figure 6.7 The overall ABD of the PSTN.

$A_{PSTN} = (A_{part\ I}).(A_{part\ II})$

As shown in figure 6.7 the availability block diagram (ABD) of the PSTN exchange that was taken as an example for the PSTN, consist of two parts. Part I represents the switching part, and part II represents the outside part.

Part I includes three main items, the Power supply unit (PS), the digital line unit (DLU), and the central processing unit (CPU).

The data collected for this part is shown in table 6.3. The availability of this part is equal to the product of the three availabilities of the three items of this part. This is illustrated in figure 6.8.

Item	MTBF hours	MTTR hours
PS	641	0.0833
DLU	4348	1.75
CPU	8760	3
Part I	**507.6**	**1.6111**

Table 6.3 Part I availability data summary

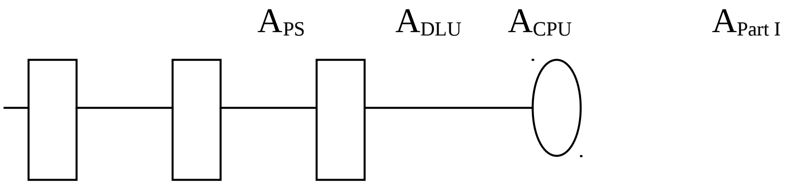


Figure 6.8 The ABD of part I of the PSTN exchange.

6.12.1 The PS availability

The availability of the first item of part I (PS) can be calculated from table 5.2 as:

$$A_{PS} = MTBF/(MTBF+MTTR)$$
$$= \quad 641/(641+0.0833) \quad =0.99987 \quad =99.987\%$$

6.12.2 The DLU availability

The second item in part I is the DLU. The availability of this item can be determined as:

$$A_{DLU} = MTBF/(MTBF+MTTR)$$
$$= \quad 4348/(4348+1.75) \quad =0.99959 \quad =99.959\%$$

6.12.3 The CPU availability

This is the third item of part I of the PSTN. Its availability can be found as:

$$A_{CPU} = MTBF/(MTBF+MTTR)$$
$$= \quad 8760/(8760+3) \quad =0.99966 \quad =99.966\%$$

Now the overall availability of this part will be:

$$A_{\text{part I}} = (A_{PS}).(A_{DLU}).(A_{CPU})$$
$$= (0.99987).(0.99959).(0.99966)$$
$$= 0.99912 \qquad = 99.912\%$$

Note the deviation in the availability number from the five nines number.

6.12.4 Part II availability

The availability of part two is determined as the product of the availabilities of the items that included in this phase. This is illustrated in figure 6.9 that shows the three items of the availability block diagram (ABD).

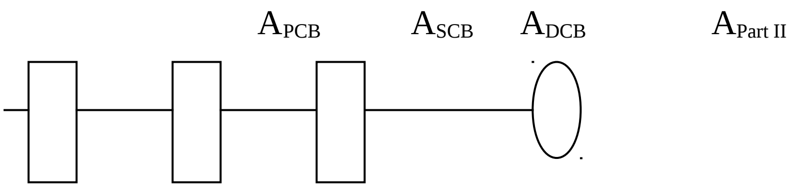


Figure 6.9 The ABD of part II of the PSTN phase.

PCB = Primary Cable item

SCB = Secondary Cable item

DCB = Drop cable item

Item	**MTBF hours**	**MTTR hours**
PCB	2175	4
SCB	730	2.532
DCB	435	3.5
Part II	**146.2**	**3.177**

Table 6.4 Part II failure data summary

6.12.5 The PCB availability

The availability of the PCB that represents the first item in part II can be found from the data in table 5.3 as:

$$A_{PCB} = MTBF/(MTBF+MTTR)$$

$$= 2175/(2175+4)$$

$$=0.99816 \qquad =99.816\%$$

6.12.6 The SCB availability

The second item in part II is the secondary cable (SCB). The availability of this item can be calculated as:

$$A_{PCB} = MTBF/(MTBF+MTTR)$$

$$=730/(730+2.532)$$

$$=0.99654 \quad =99.654\%$$

6.12.7 The DCB availability

This the third item in part II. From the data in table 5.3 the availability of this item can be found as:

$$A_{DCB} = MTBF/(MTBF+MTTR)$$

$$=435/(435+3.5)$$

$$=0.99202$$

Part II availability now can be calculated as the product of the availabilities of the three items as follows:

$$A_{part\ II} = (A_{PCB}).(A_{SCB}).(A_{DCB})$$

$$= (0.99816).(0.99654).(0.99202)$$

$$= 0.98677 \qquad = 98.677\%$$

Now phase II availability will be equal to the product of the availabilities of its two parts as follows:

$$A_{phase\ II} = (A_{part\ I}).(A_{part\ II})$$

$$= (0.99912).(0.98677)$$

$$=0.98590 \qquad =98.59\%$$

One can see that the availability of the PSTN is categorized as one nine availability.

This means that the probability readiness for the PSTN service is equal to 98.59%. Here one can notice that the availability of the second phase (PSTN phase) is less than the availability of the first phase (local phase) of the SUST network. This fact indicates that the weakest area of the SUST network is the PSTN phase.

6.13 The SUST network average overall availability

The SUST network overall availability will be equal to the product of the average the two phases for all sites of this network as illustrated in table 6.2 , and can be found as:

$$A_{SUST}\text{ (average)} = \text{(average of }A_{\text{phase I}}).(\text{average of }A_{\text{phase II}})$$

$$= (0.99965).(0.99913)$$

$$= 0.99878 \qquad = 99.878\%$$

6.14 The network availability assumed nines

For highly redundant network, outages should rarely occur. Most networks will experience outages over a given interval of time. Since the availability can be computed from MTBF and MTTR, this means that the failure rate λ has sensitivity to system availability because the failure rate λ is equal to 1/MTBF. Table 6.5 illustrates the sensitivity of λ to network system availability and MTTR. Assume that a goal of 99 percent (two nines) has been established for the SUST network. Referring to the first three columns of table 6.5, the network system availability is assumed to be constant while the MTTR assumes values of 3.5, 4, and 4.5 respectively. For each combination of availability and MTTR, the system MTBF is calculated to be 346.5, 396, and 445.5 hours respectively. The corresponding values of λ are shown in the fourth column. They are 25.30, 22.14, and 19.68 failures per year respectively.

SUST network system			
Availability	MTTR (hr)	MTBF (hr)	λ (Failures/year)
0.99	3.5	346.5	25.30
0.99	4	396	22.14
0.99	4.5	445.5	19.68

Table 6.5 The 99 goal and MTTR, MTBF values

The main objective of this table is to show that to sustain a required level of availability, you should do the following:

1. If the failure rate increases (low reliability) for any reasons, you should decrease the repair time for each failure occurrence.
2. if you have a chronic problem in maintenance, then you should lower the failure rate (increase the reliability) to maintain the same required level of availability.

6.15 Effect of the two phases on SUST network availability

If the PSTN and local phase encounter the same number of failures (50% each phase) and the MTTR is 3.5 hours, the local and PSTN portions of the SUST network will both achieve an availability of 0.99495. If the PSTN is responsible for 65 percent of failures, then the local phase of the network must achieve an availability of 0.993434. This is illustrated in table 6.6.

SUST	**Local Phase**					**PSTN Phase**				
Avail.	**Fail. %**	**λ /year**	**MTBF (Hrs)**	**MTTR (Hrs)**	**Avail.**	**Fail. %**	**λ per year**	**MTBF (Hrs)**	**MTTR (Hrs)**	**Avail.**
0.99	50%	12.65	689.50	3.5	0.99495	50%	12.65	689.50	3.5	0.99495
0.99	45%	11.38	766.50	3.5	0.99545	55%	13.91	626.50	3.5	0.99444
0.99	40%	10.12	862.75	3.5	0.99596	60%	15.18	574.00	3.5	0.99394
0.99	35%	8.85	986.50	3.5	0.99646	65%	16.44	529.58	3.5	0.99343
0.99	50%	11.07	788.00	4	0.99495	50%	11.07	788.00	4	0.99495
0.99	45%	9.96	876.00	4	0.99545	55%	12.18	716.00	4	0.99444
0.99	40%	8.85	986.00	4	0.99596	60%	13.28	656.00	4	0.99394
0.99	35%	7.75	1127.4	4	0.99646	65%	14.39	605.23	4	0.99343
0.99	50%	9.84	886.50	4.5	0.99495	50%	9.84	886.50	4.5	0.99495
0.99	45%	8.85	985.50	4.5	0.99545	55%	10.82	805.50	4.5	0.99444
0.99	40%	7.87	1109.3	4.5	0.99596	60%	11.81	738.00	4.5	0.99394
0.99	35%	6.89	1268.4	4.5	0.99646	65%	12.79	680.88	4.5	0.99343

Table 6.6 Local and PSTN phases MTTR and MTBF for two nines availability

CHAPTER SEVEN

Network Maintainability

7. Maintainability

The maintainability engineering effort in the conception and design phase is critical to ensure that high system availability is obtained at optimum life cycle support cost. Key in the availability calculation of a system is its down time, the time required to bring a failed system back to its operational state or capability. This down time is normally attributed to maintenance activities. An effective way to increase a system's availability is to minimize the downtime. This minimized downtime does not happen at random, it is made to happen by actively ensuring that full consideration is given during the conceptual and design phase. Therefore the inherent maintainability characteristics of a system must be assured. This can be achieved by the implementation of specific design practices and validated through a maintainability assessment process, utilizing both analyses and testing. The following subtopics cover some of these assurance activities.

- Maintainability Programs
- Maintainability Assessment
- Maintainability Modeling
- Maintainability Demonstration
- Design for Maintainability
- Defect Reporting and Corrective Action System (DRACAS)

The maintainability program would normally be effectively implemented by a

well defined program strategy and captured in a maintainability program plan. The responsibilities differ significantly from those of a system integrator to those of a sub component/ assembly supplier [2]. The responsibilities of the system integrator would include the assessment of potential supplier products and eventually the allocation and flow down of the maintainability product design requirements and maintainability validation documentation.

7.1 Maintainability subsets

Maintainability is described as: The relative ease and economy of time and resources with which an

item can be retained in, or restored to, a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources.

In this context, it is a function of design.

Experience tells us that maintainability suggests roughly 40% of the life cycle cost. Design for maintainability requires a product that is serviceable (must be easily repaired) and supportable (must be cost-effectively kept in or restored to a usable condition) better yet if the design includes a durability feature (reliability*)* then you can have the best of all worlds.

Supportability has a design subset involving testability (a design characteristic that allows verification of the status to be determined and faults within the item to be isolated in a timely and effective manner such

as can occur with build-in-test equipment (BIT) so the new item can demonstrate it’s status (operable, inoperable, or degraded) and similar conditions for routine trouble shooting and verification that the equipment has been restored to useful condition following maintenance.

Maintainability is primarily a design parameter. The design for maintainability defines how long equipment will be down and unavailable. You can reduce the amount of time spent by having a highly trained workforce and a responsive supply system, which paces the speed of maintenance to achieve minimum downtimes. Unavailability occurs when the equipment is down for periodic maintenance and for repairs. Unreliability is associated with failures of the system. The failures can be associated with planned outages or unplanned outages.

Maintainability has true design characteristic. Attempts to improve the inherent maintainability of a product/item after the design is frozen is usually expensive, inefficient, and ineffective as demonstrated so often in manufacturing plants when the first maintenance effort requires the use of a cutting torch to access the item requiring replacement.

Poor maintainability results in equipment, which is unavailable, expensive for the cost of unreliability, and results in an irritable state of conditions for all parties who touch the equipment or have responsibility for the equipment.

Reliability and maintainability are considered complementary disciplines from the inherent availability equation. Inherent availability looks at availability from a design :perspective

(A_i = MTBF/(MTBF+MTTR

If mean time between failure or mean time to failure is very large compared to the mean time to repair or mean time to replace, then you will see high availability. Likewise if mean time to repair or replace is very small, then availability will be high. As reliability decreases (i.e., MTBF becomes smaller), better maintainability (i.e., shorter MTTR) is needed to achieve the same availability. Of course as reliability increases then maintainability is not so important to achieve the same availability. Thus tradeoffs can be made between reliability and maintainability to achieve the same availability and thus the two disciplines must work hand-in-hand to achieve the objectives. A_i is the largest availability value you can observe if you never had any .system abuses

The administration delay is an important issue because the down time is often results from the actual time to repair plus the administration delay which, sometime :represents eighty percent of the down time. Thus down time can be described as

Down time = Repair time + Administration delay

The administration delay usually includes proving spare order, financial procedure .and time spent in getting the spare part from the store

In the operational world we talk of the operational availability equation. Operational availability looks at availability by collecting all of the abuses in a practical system.

$$A_o = MTBM/(MTBM+MDT).$$

The mean time between maintenance (MTBM) includes all corrective and preventive actions (compared to MTBF which only accounts for failures). The mean down time includes all time associated with the system being down for corrective maintenance (CM) including delays (compared to MTTR which only addresses repair time) including self imposed downtime for preventive maintenance (PM) although it is preferred to perform most PM actions while the equipment is operating. A_o is a smaller availability number than A_i because of naturally occurring abuses.

Operational availability includes issues associated with: inherent design, availability of maintenance personnel, availability of spare parts, maintenance policy. Testability, the subset of maintainability/supportability, enters strongly into the MDT portion of the equation to clearly identify the status of an item so as to know if a fault exists and to determine if the item is dead, alive, or deteriorated, these issues always affect affordability issues. Operational availability depends upon operational maintainability, which includes factors totally outside of the design environment such as:

1. Insufficient number of spare parts
2. Slow procurement of equipment
3. Poorly trained maintenance personnel
4. Lack of proper tools and procedures to perform the maintenance actions.

Achieving excellent operational maintainability requires sound planning, engineering, design, test, excellent manufacturing conformance, adequate support system (logistics) for spare parts, people, training, etc to incorporate lessons learned from previous or similar equipment.

Critical to the remove and replace times is the accessibility to the failed unit required by the maintainer. This would include the ability to use the necessary hand tools and or test equipment and the actual physical removal of the unit. Therefore, the design phase consideration must be given to the layout of the components and avoid the prospect of having to remove other components to access a failed unit. A good example of this would be the restricted engine compartment of an automobile, where many mechanics have been faced with the prospect of having to strip out half the engine to gain access to a particular item.

Another critical consideration when determining the overall MTTR calculation is the time it takes to isolate the fault. For some systems this could be relatively straight forward, while for others it could be a more complex affair. To ensure that the fault detection and isolation components and capabilities of a system are obtained, a careful testability analysis must be performed.

7.2 Maintenance task

Maintenance is a set of activities, which need to be performed, in specified manner, in order to maintain the functionability of the item or the system. Figure 7.1 illustrates the maintenance task.

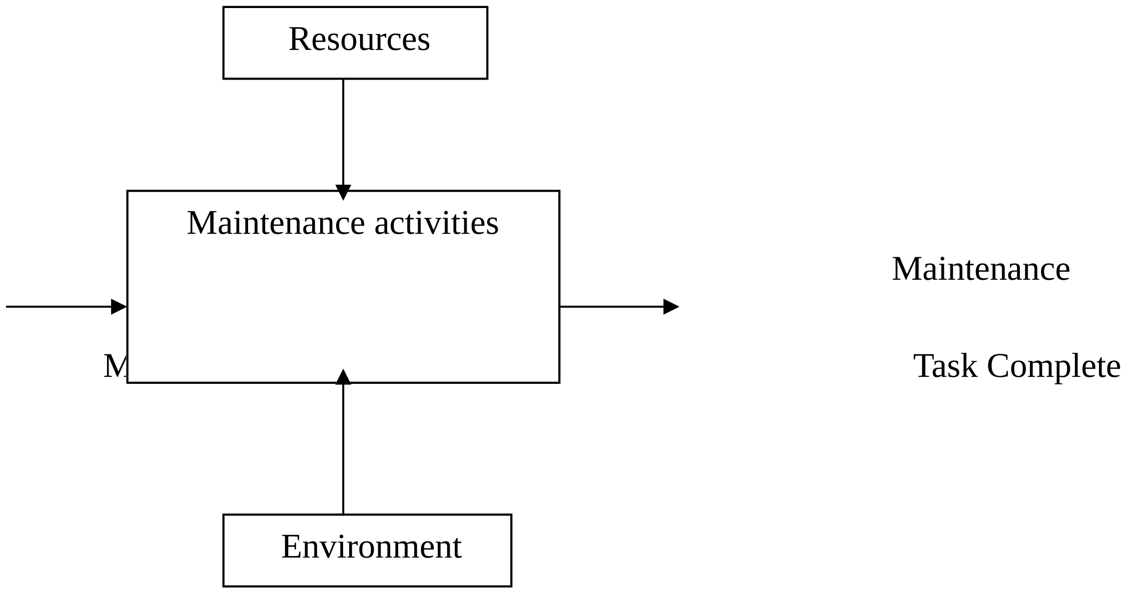


Figure 7.1 Maintenance task items

It is necessary to stress that the number of activities, their sequence, and the type of resources mainly depend on the decisions taken during the design phase of the item or the system. In a sense, the magnitude of the elapsed time required for the restoration of functionability 5 minutes, 5 hours, or 2 days could only be taken at a very early stage of the design process through decisions related to the complexity of the maintenance task, accessibility of the items, safety of the restoration, and physical location of the item, as well as decisions related to requirements for the maintenance support resources.

Maintenance resources needed for the successful completion of every maintenance task could be grouped into the following categories:

1. Maintenance supply support, MSS: A generic name that, include all spares, consumable, special supplies and inventories needed to support the maintenance process.
2. Maintenance test equipment, MTE: Includes all tools, monitoring equipment, diagnostic equipment, servicing and handling equipment required to support maintenance tasks.

3. Maintenance personnel, MP: Required for the check-out, handling and sustaining maintenance of the item or the system. Formal training for maintenance personnel should be considered.

4. Maintenance Facilities, MFC: Refers to all special facilities needed for completion of maintenance task. Physical plant, cooperative administration, maintenance shops, laboratories, and special repair facilities must be considered related to each maintenance task.

5. Maintenance Technical Data, MTD: Necessary for check out procedures, maintenance instruction, and inspection.

6. Maintenance Computer Resources, MCR: All computer equipment and software programmes, databases necessary to perform maintenance functions. This include both condition monitoring and diagnostics.

7.3 Maintenance task classification

According to the objective of performing a maintenance task, all of them could be classified into three categories:

(a) Corrective maintenance task
(b) Preventive maintenance task

(c) Conditional maintenance task.

7.3.1 Corrective maintenance tasks (CRTs)

Are the tasks which are performed with the intention of restoring the functionability of the item or system, after the loss of the function. A typical corrective maintenance task consist of the following activities:

- Failure detection
- Failure location
- Disassembly
- Replacement or adjustment
- Assembly
- Test/check
- Verification

The elapsed time needed for the successful completion of the corrective maintenance task is denoted as DMT^c

7.3.2 Preventive maintenance tasks:

A preventive maintenance task, PRT, is a task, which is performed in order to reduce probability of failure of the item/system. Atypical preventive maintenance task consist of the following maintenance activities:

- Disassembly
- Required maintenance activity
- Assembly
- Test/check
- Verification.

The elapsed time needed for the successful completion of the preventive maintenance task is denoted as DMT^p.

It is necessary to stress that the preventive tasks are performed at a fixed intervals regardless of the real condition of the items/systems.

7.3.3 Conditional maintenance tasks

Traditionally, corrective and preventive maintenance tasks have been favorite among maintenance managers. However, the disadvantages of these approaches have been recognized by many organizations. Therefore the need for the provision of safety and reduction of maintenance cost have led to an increasing interest in development of an alternative maintenance tasks. Consequently, the approach, which seems to be the most attractive for minimizing the limitations of existing maintenance tasks is the conditional maintenance task, COT. This maintenance task recognizes that a change in condition or performance is the principle reason for carrying out maintenance, and execution of preventive maintenance task should be based on the actual condition of the system. Thus through monitoring some parameters it should be possible to identify the most suitable instant of time at which preventive tasks should be placed.

Consequently, a conditional maintenance task represents a maintenance task which is performed to gain insight into the condition of the item/system or discover hidden failure, in order to determine the further course of actions regarding the maintenance of functionability of the system, from point of view of the user.

The conditional maintenance task is based on condition monitoring activities, which are performed in order to determine the physical state of an item/system. Therefore, the aim of condition monitoring, whatever form it takes, is to monitor those parameters, which provide information about the changes in condition or performance of an item/system. The philosophy of condition monitoring is therefore the assessment of the current condition of an item/system by use of techniques, which can range from human sensing to sophisticated instrumentation, in order to determine the need for performing a preventive maintenance task.

Atypical conditional maintenance consists of the following maintenance activities:

- Condition assessment
- Condition interpretation
- Decision-making.

This means that the preventive maintenance tasks are not performed as long as the condition of the item/system is acceptable.

7.3.4 Condition monitoring parameters

In order to assess the condition of the network item/system, in engineering practice, there are two distinguishable types of conditional parameters used.

(a) Relevant Condition Indicator, RCI

This is the monitorable parameter, which indicates the condition of the network item/system, at the instance of checking. According to the RCI, the condition of the network item/system is satisfactory as long as it maintains a value below its critical level, $\text{RCI}_{\text{cr.}}$ When this level is reached, the required maintenance task must be performed, because the failure will occur as soon as the parameter reaches its limit value, RCI_{lim} as illustrated by figure 7.2. RCI could have identical values at different instances of operating time.

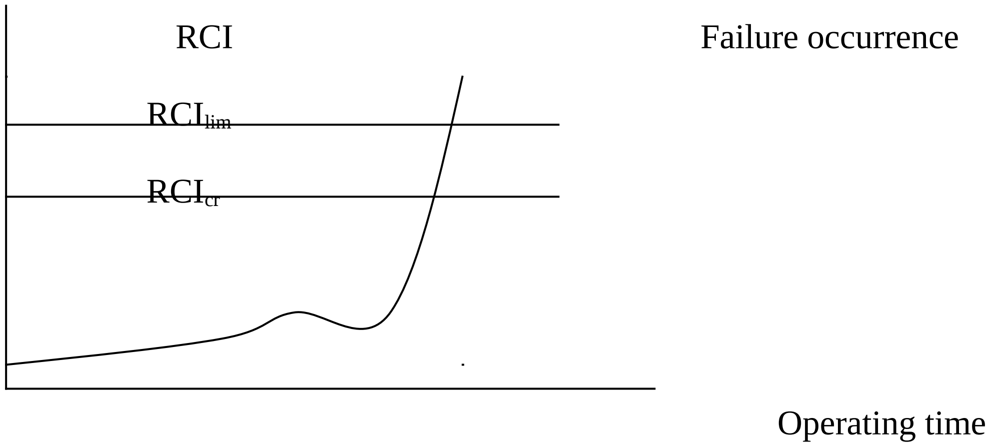
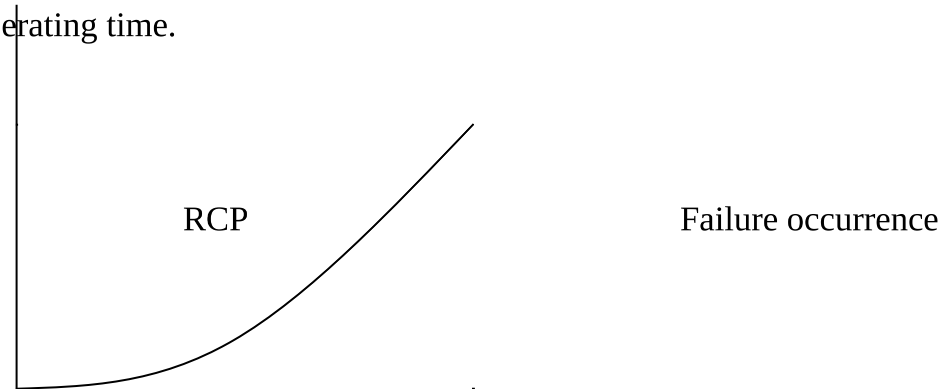


Figure 7.2 Change of RCI during operational time

(b) Relevant Condition Predictor, RCP

This is a monitorable parameter, which describes the condition of the item at every instant of operating time. Usually this parameter is directly related to the shape, geometry, weight, and another characteristics, which describe the condition of the item under consideration. Typical examples of RCP are overheating of the router, reading errors of the storage media. Generally the condition of the item is satisfactory as long as the RCP maintains a value beyond its critical level, RCP_{cr}. At this point the required preventive maintenance task must be performed, because the failure will occur as soon as the parameter reaches its limit value, RCP_{lim}. It is necessary to say that the RCP cannot have identical values at two or more instances of time as illustrated by figure 7.3. This means that the RCP is continuously increasing or decreasing with operating time.



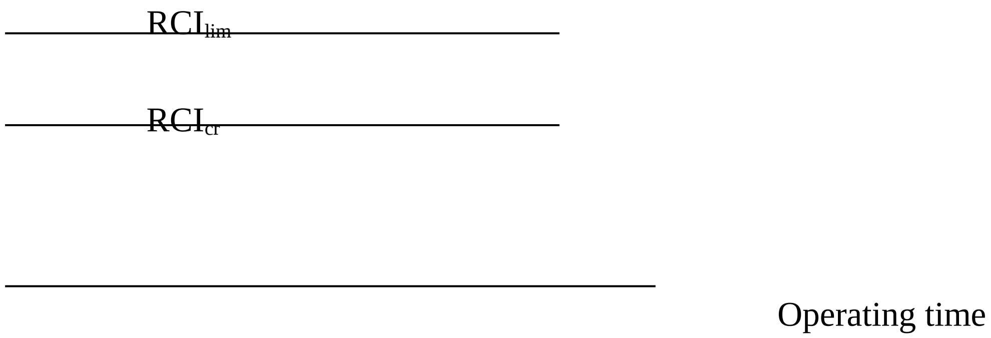


Figure 7.3 Change of RCP during operational time

7.4 Maintainability function

This function, denoted as M(t), represents the probability that the maintenance task considered will be successfully completed before or at the specified maintenance elapsed time t, thus:

$$M(t) = P(DMT <= t) \qquad (6.1)$$

Where, DMT is the Duration of Maintenance Task.

7.4.1 Maintainability function of SUST network

A maintainability function should be set for each item in the network in all cases of maintenance. A corrective maintainability function, and preventive maintainability function should be set.

This is done in the early installation stage of the network. A hypothetical task elapsed time should be assigned for each item in the network, which indicates the duration of the maintenance task for both types of maintenance, preventive and corrective maintenance. The elapsed time assigned is based on the previous experience of similar network items. Table 7.1 shows the MTTR for phase I of the SUST network.

Item	**MTTR hrs**

PSU	0.125
Server	1
Switch	3
Router	24

Table 7.1 MTTR for phase I from the field data

The elapsed time for the duration of maintenance task, DMT, which can be set from the previous experience for each item, is shown in table 7.2.

Item	**MTTR hrs**
PSU	0.125
Server	1
Switch	0.250
Router	3

Table 7.2 The assumed DMT for phase I

The maintainability function M(t) for each item could be found by comparing the assumed DTM with the actual MTTR of this phase. This could be calculated as follows:

$$M(t) = (DTM/MTTR)x100$$

For the PSU item

$$M(t) = (0.125/0.125)x100 = 100\%$$

For the server item

$$M(t) = (1/1)x100 = 100\%$$

For the switch

$$M(t) = (0.250/3)x100 = 8.3\%$$

For the router

$$M(t) = (3/24)x100 = 12.5\%$$

This means that for the PSU and the server the maintainability function is acceptable and the required availability of these items are fair.

For the switch, the M(t) of 8.3% is very poor compared with the 100% required for this item to have the predicted availability based on MTD assigned.

For the router, the 12.5% of M(t) also is poor and hence the predicted availability of this item will be less.

The main benefit of calculating the maintainability function is that it reflects if there is a defect in the maintenance tasks or not. Thus, if:

$M(t) = 100\%$ indicates an optimum maintenance

$100\% > M(t) > 80\%$ indicates good level of maintenance

$80\% > M(t) > 50\%$ indicates fair level of maintenance

$M(t) \leq 50\%$ indicates poor level of maintenance.

The last level (M(t)<50%) is considered as a poor level of maintenance so, it needs a good analysis for the maintenance policy and management in order to improve the maintenance tasks, and hence the availability of the network.

For the switch and the router, the suggested solution includes two options:

1. To decrease the administration delay in spare parts provision
2. To use a redundancy.

7.5 Cost of maintenance tasks

The direct cost associated with each maintenance task should be analyzed. The direct cost of maintenance task, CMT, is related to the cost of maintenance resources, CMR, directly used during execution of the task. Thus it is a function of:

$$CMT = f(C_{MSS}, C_{MTE}, C_{MPS}, C_{MFC}, C_{MTD}, C_{MCR}) \qquad (6.2)$$

Where C_{MSS} is the cost of maintenance supply support

C_{MTE} is cost of test and maintenance support equipment

C_{MPS} represents the cost of maintenance personnel

C_{MFC} represents the cost of maintenance facilities

C_{MTD} is the cost of maintenance technical data, and

C_{MCR} represents the cost of maintenance computer resources.

The type and quantity of all maintenance resources required for successful completion of any maintenance task are inherited from the design of the system and they are fully addressed during the maintainability analysis of the design process. The cost of personnel involved with a specific maintenance task is a function of the following variables:

$$C_{MPS} = f(DMT, HCP) \qquad (6.3)$$

Where DMT represents the duration of elapsed maintenance time, and HCP represents the monetary value of the hourly cost of maintenance personnel used for the execution of specific maintenance task.

Most frequently, in daily practice, engineers deal with the average (mean) value of direct cost of a maintenance task, which could be defined as:

$$MCMT = C_{MSS} + C_{MTE} + C_{MFC} + C_{MTD} + C_{MCR} + (MDMT \times HCP) \qquad (6.4)$$

Under the assumption that, the cost of all maintenance resources, apart from personnel, is constant.

It is necessary to underline that the MCMT could differ considerably between different types of maintenance tasks.

7.5.1 Direct cost of corrective maintenance tasks

The direct cost associated with each corrective maintenance task, CMT^C, is related to the cost of maintenance resources needed for the successful completion of the task, CMR^C. Thus, the general expression for the cost of each corrective maintenance task will have a form as:

$$CMT^C = f(C^C_{MSS}, C^C_{MTE}, C^C_{MFC}, C^C_{MTD}, C^C_{MCR}, MDMT^C x HCP^C)$$

(6.5)

In daily practice, engineers deal with the average (mean) value of corrective cost of a maintenance task, which could be defined as:

$$MCMT^C = C^C_{MSS} + C^C_{MTE} + C^C_{MFC} + C^C_{MTD} + C^C_{MCR} + (MDMT^C x HCP^C)$$

(6.6)

7.5.2 Direct cost of corrective maintenance tasks

This is direct cost associated with each preventive maintenance, CMT^P, is related to the cost of maintenance resource needed for the successful completion of the task. Thus, the general expression for the cost of each preventive maintenance task will have a form as:

$$CMT^P = f(C^P_{MSS}, C^P_{MTE}, C^P_{MFC}, C^P_{MTD}, C^P_{MCR}, MDMT^P x HCP^P)$$

(6.7)

Again, In daily practice, engineers deal with the average (mean) value of preventive maintenance costs, which denoted as $MCMT^P$.

$$MCMT^P = C^P_{MSS} + C^P_{MTE} + C^P_{MFC} + C^P_{MTD} + C^P_{MCR} + (MDMT^P x HCP^P)$$

7.5.3 Direct cost of conditional maintenance tasks

It is the direct cost associated with each preventive maintenance, CMT^{m}, which is related to the cost of maintenance resource needed for the successful completion of the task. Thus, the general expression for the cost of each conditional maintenance task will have a form as:

$$CMT^{m} = f(C^{m}_{MSS}, C^{m}_{MTE}, C^{m}_{MFC}, C^{m}_{MTD}, C^{m}_{MCR}, MDMT^{m}xHCP^{m})$$

The average (mean) value of conditional maintenance cost, denoted as $MCMT^{m}$, could be obtained according to the following expression:

$$MCMT^{m} = C^{m}_{MSS}+ C^{m}_{MTE} +C^{m}_{MFC} + C^{m}_{MTD} + C^{m}_{MCR} + (MDMT^{m}xHCP^{m})$$

7.6 Maintenance levels

The levels of maintenance could be categorized into three types:

1. Organizational level
2. Intermediate level
3. Depot/producer level

7.6.1 Organizational level

This type of maintenance level compromises all maintenance tasks which, are performed at the operational site. Generally it includes work performed by the using organization on its own equipment. Personnel assigned to this level generally do not repair the removed components, but forward them to the intermediate level.

7.6.2 Intermediate level

This type of maintenance level refers to the maintenance tasks performed by mobile, semi mobile, and fixed specialized organizations. At this level, items concerned may be repaired by the removal and replacement of major modules, assemblies or piece parts. Available maintenance personnel are usually more trained/skilled, better equipped than those at the organizational level, and are responsible for performing more detailed maintenance. Mobile units are often assigned to provide close support for dispersed operational equipment. These units may constitute vans, trucks, or portable shelters containing some test and support equipment and spares. The mission is to provide on-site maintenance to facilitate the return of the system to its full operational status on an expedited basis.

Fixed installations (permanent shops) are generally established to support both the organizational level and mobile units. Maintenance works that cannot be performed by the lower levels, due to limited personnel skills, additional test and support equipment, more spares and better facilities often enable equipment repair to the module and piece part level. Fixed shops are usually located within specified geographical areas.

7.6.3 Depot/producer level

This constitutes the highest level of maintenance and supports the accomplishment of maintenance tasks whose complexity is beyond the capabilities available at the intermediate. Physically, the depot may be specialized repair facility supporting a number of systems or types of equipment in the inventory, or it may be the equipment manufacturer's plant. Complex equipment, large quantities of spares, environmental control, are the mean reasons of depot level. The depot facilities are generally remotely located to support specific geographical area needs or designated product lines.

7.7 Selecting the suitable maintenance level for networks

This process is the determination of the most suitable maintenance level for the system under consideration, based on the minimum maintenance cost. Assume that the available data associated with an item are:

- The cost of the network item is 350000 S.D
- The MTBF is 4380 hours (six months)
- The MTTR is 14 hours for organizational and 4 hours for intermediate maintenance level.
- The maintenance task requires one technician at hourly rate of 2500 S.D for organizational level and 5000 S.D for intermediate maintenance level.
- The transportation level is 3000 S.D for intermediate level

From the above data the annual total cost of organization level is equal to:

Repair cost = 2x14x2500 S.D = 70000 S.D

Mean Time Duration = 14 hours

The total annual cost for intermediate maintenance level is:

Repair cost = 2x4x 5000 = 40000 S.D

Transportation cost = 2x 3000 = 6000 S.D

Total cost = 46000 S.D

This means that the intermediate level is better in cost and the MTD .

The low MTD for intermediate levels shows that the personnel are highly skilled in intermediate level.

From the above comparison, it is clear that the decision-making should be based on this analysis.

7.8 COTS systems

In order to reduce development times and resources, NATO countries have encouraged an extensive use of Commercial Off The Shelf items. This new COTS approach has brought an increased dependence of the design/development team on the vendor/supplier environment. Consequently, maintainability issues become more prominent due to the needs for engineering changes initiated by system support related considerations.

This method is suitable for organizations that work in the vender country or in the area of their agents in which, the communication and transportation are easy. Experience tells that this method is more efficient than other level of maintenance.

7.9 Network maintenance policy

The issue here is to discuss the all polices used in maintenance and which policy is suitable to have a dependable network. With respect to the relationship of the instant of occurrence of failure and the instant of performing the maintenance task, the following maintenance polices exist.

(a) Failure-based maintenance policy, FB, where the corrective maintenance tasks are initiated by the occurrence of failure.

(b) Life-based maintenance policy, LB, where preventive maintenance tasks are performed at a predetermined times during operation.

(c) Inspection-based maintenance policy, IB, where conditional maintenance tasks in the form of inspections are performed at fixed intervals of operation, until the performance of a preventive maintenance task is required.

(d) Opportunity-based maintenance policy, OB, where corrective maintenance task is performed on the failed item and preventive maintenance tasks are performed to the remaining items. In another word, to take the opportunity of the down time caused by the failed item to make a preventive maintenance to the rest of the items.

7.9.1 Failure-based maintenance

The main attraction of this maintenance policy is the full utilization of the operating life of the item under consideration. This means that no service cut will appear because of the preventive maintenance. The mean duration of utilized life (MDUL^F) of the item is identical to the mean duration of functional life (MDFL). Hence the coefficient of utilization of items considered, denoted, as CU^F will always have a value of 1, thus:

$$CU^F = MDUL^F/MDFL = 1 \qquad (6.8)$$

The algorithm for failure-based policy is illustrated in figure 7.4.

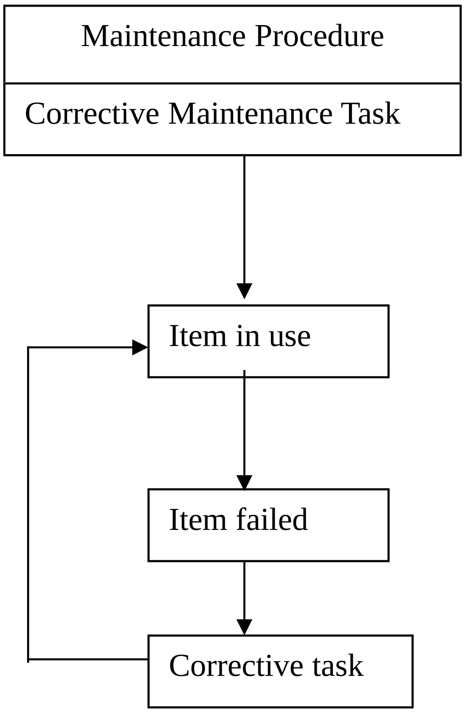


Figure 7.4 Algorithm for failure-based maintenance policy

Despite the monetary advantage offered by this maintenance policy, it has some disadvantages among which, the following are the most important:

- The failure of the item can cause consequential damage to other items in the system
- As the instance of occurrence of failure is uncertain, the maintenance task cannot be planned, hence longer downtimes, due to unavailability of resources should be expected.

Therefore, this policy can be potentially costly, due to direct costs of restoring the functionability of the system caused by failure and the indirect costs incurred as a result of the downtimes.

7.9.2 Life-based maintenance policy

With a life-based policy preventive maintenance tasks are performed at fixed intervals, which are a function of the life distribution of the items considered. The main aim is to prevent failure and its consequences. Another name for this policy is planned maintenance. Figure 7.5 illustrates this maintenance policy. The frequency of maintenance tasks, FMT, is determined even before the item has started functioning. If the item fails between preventive tasks a corrective maintenance task has to be performed.

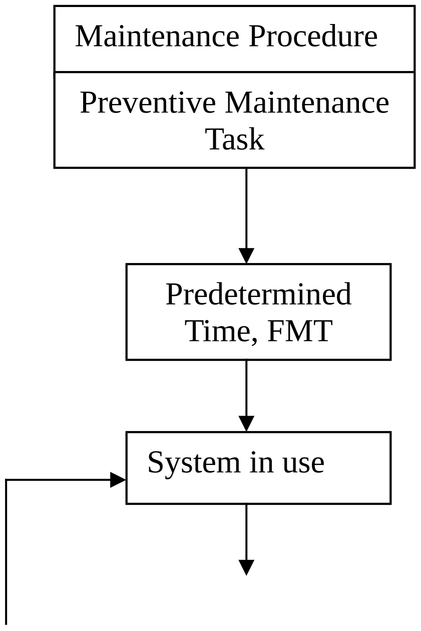


Figure 7.5 Algorithm for life-based maintenance policy

The LB maintenance policy could be effectively applied to items that meet some of the following requirements:

1. Performing this task reduces the probability of occurrence of failure in future.
2. The total costs of applying this policy are substantially lower than that of the FB maintenance policy.
3. Monitoring of the condition of the item is not technically feasible or it is economically unacceptable.

7.9.2.1 Advantages and disadvantages of LF policy

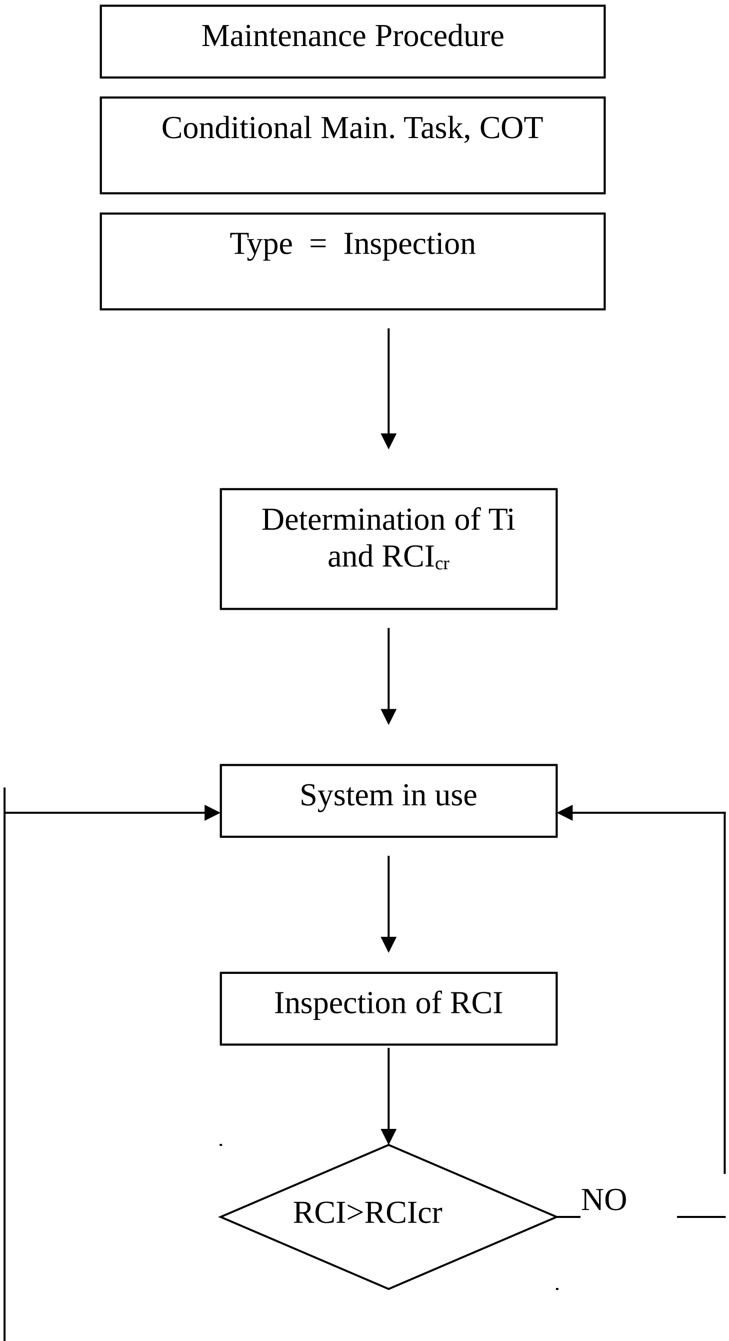
One of the main advantages of this maintenance policy is the fact that preventive maintenance tasks are performed at a predetermined instant of time enabling all maintenance support resources to be provided in advance, and potential costly outages avoided.

Despite the advantages given, the LB maintenance policy has several disadvantages that must be recognized and minimized. For example, it could be uneconomical because the majority of items are prematurely replaced, irrespective of their condition. Hence, the coefficient of utilization of the item considered, CU^L, has a value less than one, and its defined as:

$$CU^L = [(MDUL^L)/(MDFL)] < 1 \qquad (6.9)$$

7.10 Inspection-based maintenance policy

The advantage of this procedure is a provision of better utilization of the item considered than in the case of applying preventive maintenance. Inspection is a conditional maintenance task, the result of which is a statement about the condition of the item, if the condition is satisfactory or unsatisfactory, which is determined according to the Relative Condition Indicator (RCI). Before the item is introduced into service the most suitable frequency of the inspection, FMT^I, has to be determined. Thus, during the operation of the item inspections are performed at specified fixed intervals until the critical level is reached, $RCI > RCI_{cr}$, when prescribed preventive maintenance tasks take place. If the item fails between inspections, corrective maintenance takes place. The algorithm of this policy is shown in figure 7.6, in which the inspection is used as the condition-monitoring task.



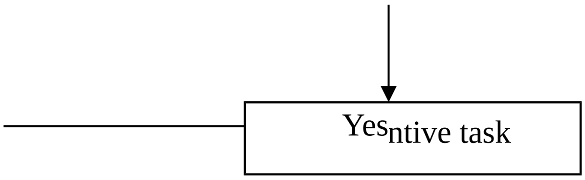


Figure 7.6 Inspection-based maintenance policy

The coefficient of utilization, CU^I, could be determined as:

$$CU^I = MDUL^I/MDFL$$

It is necessary to outline that the CU^I is less than one but the downtime of inspection is less than the downtime of preventive maintenance [5].

7.10.1 Advantages of inspection-based maintenance

The benefits of this policy can be summarized as:

1. Detection at the earliest time possible of deterioration in performance of an item.
2. Reduction of system downtime, since maintenance engineers can determine the optimal maintenance interval through the condition of items in the system. This allows better maintenance planning and more efficient use of resources.

3. Improved safety, since it enables engineers to stop the system before a failure occurs.

4. Increased availability, by reducing the downtime results from complete failure.

The frequency of inspection should be determined very carefully depending on the similar network systems. Sometimes the engineer's experience may be useful in scheduling the inspection timetable. Also, the operational environment affects the inspection scheduling especially when a clear variation of the environment appears according to the season of the year where a wide difference in the heat is noticed. This requires some variation in the inspection timetable, for example in the summer a narrow time intervals may be suitable because of the overheat that could be noticed. On the other hand in the winter season, the inspection timetable might be expanded to have long intervals of inspections.

7.11 Opportunity-based maintenance policy

This policy depends on taking the chance of corrective maintenance to make a preventive maintenance. The main advantage of this policy is that the preventive maintenance downtime is equal to zero. The main disadvantage of this policy is that it is driven by the failure-based policy, so the disadvantages of this policy are the same of the failure-based policy. The algorithm of this policy is shown in figure 7.7.

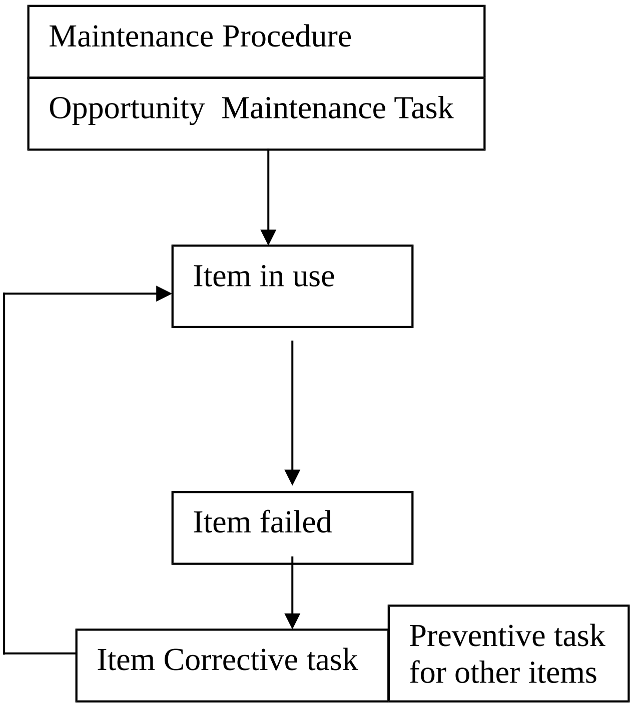


Figure 7.7 opportunity-based maintenance policy

7.12 The suitable policy for networks

Looking for the advantages and disadvantages of the policies discussed, the more suitable policy can be determined by the network's engineers depending on the environment, the need for a high availability, the skilled technicians availability, the testing and inspecting tools, and the provision of the other resources.

For networks, the following points should be considered:

1. The network high availability is needed
2. High reliability should be considered
3. The maintenance cost should be reduced
4. The maintenance facilities must be provided
5. The maintenance skilled personnel should be available, and
6. The utilization coefficient should be high (almost 1)

Calling that:

- Failure-based corrective maintenance is risky since it may increase the down time and cost.
- Life-based preventive maintenance increases the downtime, thus, gives low availability.
- Conditional maintenance is risky since the network's items have a short period of time between RCI and RCI_{cr} .

From the given considerations, the inspection-based policy is better since it provides a less downtime, and low maintenance costs.

CHAPTER EIGHT

Dependability Of Wireless Networks

8. Dependability of wireless networks

8.1 Introduction

As wireless networks are increasingly deployed in the enterprise and other environment and such trends are expected to intensify with emergence of high performance wireless networks, an important and emerging area of research is the dependability of wireless networks. In the last decade or so, the quality of service, QoS, of wireless network was an important issue. Most wireless researches assume that the dependability of wireless network is primarily dependent on the availability of resources and the channel allocation schemes. However the dependability is affected by wireless components and links. More work is necessary before high dependability can be provided in the current and emerging wireless networks. The dependability will be more complex and important in the emerging 3G and beyond networks due to the increased heterogeneity, and interconnectedness of networks leading to increased fault propagation. In addition, these networks would support group-oriented applications, thus the impact of dependability problems would propagate to the current and future locations of wireless users. Many ad hoc wireless networks will be backboned using infrastructure-oriented wireless networks, resulting in an even broader impact of component and link failures.

Since cost considerations would preclude network providers from introducing significant redundancies in their network, a more selective fault-tolerant design would be required to compensate for the impact of failures. A dependable quality of service support would also become a factor in selecting a provider in areas of overlapped coverage from multiple carriers and network.

8.2 Wireless Building Blocks, WBB

A multi-level network design using fault-tolerance techniques could be proposed for enhancing the dependability of wireless networks. The fault-tolerance can be added at component, link, block, and network level. To study the effectiveness, a wireless building block, WBB, can be used where WBBs contain several levels and multiple components, and links are used to model a wireless network of any size and number of users. The components involve transceivers (in wireless local area networks), Mobile Switching Center (MSC) in wide area network, WWAN, user register, UR, base station controllers, BSCs, and base station, BS. Table 8.1 illustrates these items for both WLAN, and mobile networks.

Wireless Building Block	
Mobile network's items	**WLAN items**
MSC	WNIC
UR (S/W)	S/W
BSC	Access points
BS	

Table 8.1 Wireless network items

The main difference between the two types of network is that the mobile network has got a very important parameter that is the user mobility parameter, which is not found in simple fixed location WLAN.

8.3 WLAN reliability

For dependability of WLAN, reliability, availability, and maintainability follows the same procedures in wireline networks. The overall reliability of the WLAN is the product of the three items reliabilities since the three main items are in series configuration as illustrated in figure 8.1.

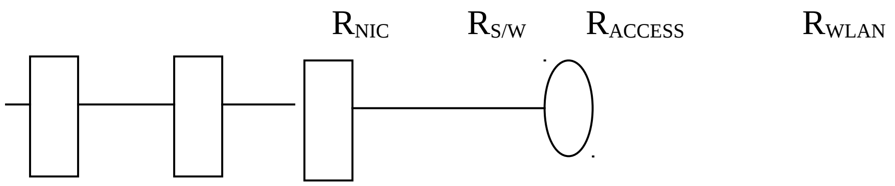


Figure 8.1 The overall RBD of the WLAN.

The WNIC consists of transceivers and antenna system.

The network software, S/W, depends primarily on the storage media. Hence, one can say that the MTBF for this item is equal to the MTBF of the storage media, which is usually a disk.

The three items MTBFs as obtained from the manufacturers, which represent the common values from various manufactures are assumed as:

WNIC MTBF = 800,000 hours
Access point MTBF = 400,000 hours
Disk MTBF = 600,000 hours

The MTBF values were taken from real network storage component statistics. However, such values vary greatly, and these numbers are given here purely for illustration.

Then the Annual Failure Rate, AFR, for each item can be determined as:

WNIC AFR = 8760/MTBF = 8760/800000 = 0.011
Access point AFR = 8760/400000 = 0.022
DISK AFR = 8760/600000 = 0.0146

Using the AFR reliability formula:

R_{NIC} = (1 – AFR) = (1 – 0.011) = 0.989 = 98.9%

R_{Access} = (1 – AFR) = (1 – 0.022) = 0.978 = 97.8%

R_{disk} = (1 – AFR) = (1 - 0.0146) = 0.9854 = 98.54%

Now the overall WLAN reliability R_{WLAN} is equal to:

$$R_{WLAN} = (R_{NIC}).(R_{Access}).(R_{disk})$$
$$= (0.989).\ (0.978).(0.9854) \quad = 0.9531 \quad = 95.31\%$$

8.4 WLAN availability

The availability of the WLAN depends on the mean time to repair or replace, MTTR. The average value taken for MTTR for the three items of the WLAN is 3 hours. Hence the availability of each item can be determined as:

A_{NIC} = (MTBF)/MTBF + MTTR)

= 800000/(800000 + 3) = 0.99999 (five nines values)

A_{Access} = 400000/(400000 + 3) = 0.99999 (five nines value)

A_{disk} = 600000/(600000 + 3) = 0.99999 (five nines value)

The overall availability of the WLAN is:

AWLAN = $(A_{NIC}).(A_{acess}).(A_{disk})$

= (0.99999).(0.99999).(0.99999) = 0.99997 (four nines)

8.5 Mobile network dependability

The wireless building block, WBB, for mobile networks as illustrated in table 8.1 consists of mobile switching center (MSC), user registers (UR), base station controller (BSC), and base stations (BS). The links may involve MSC to BSC, BSC to BS, and BS to wireless subscriber. BSC also performs radio channel management and handoff assistance. The MSC performs switching functions, coordinates location tracking, and perform call delivery. The MSC is also connected to PSTN along with signaling system (SS). The user register (UR), associated with MSC and SS provide information such as the user profile, user location, as well as information concerning subscribers within the MSC coverage area. The WBB is shown in figure 8.2.

Among the components, differences in terms of the maximum number of users, MTBF, MTTR, and hardware/software functionalities are assumed to exist.

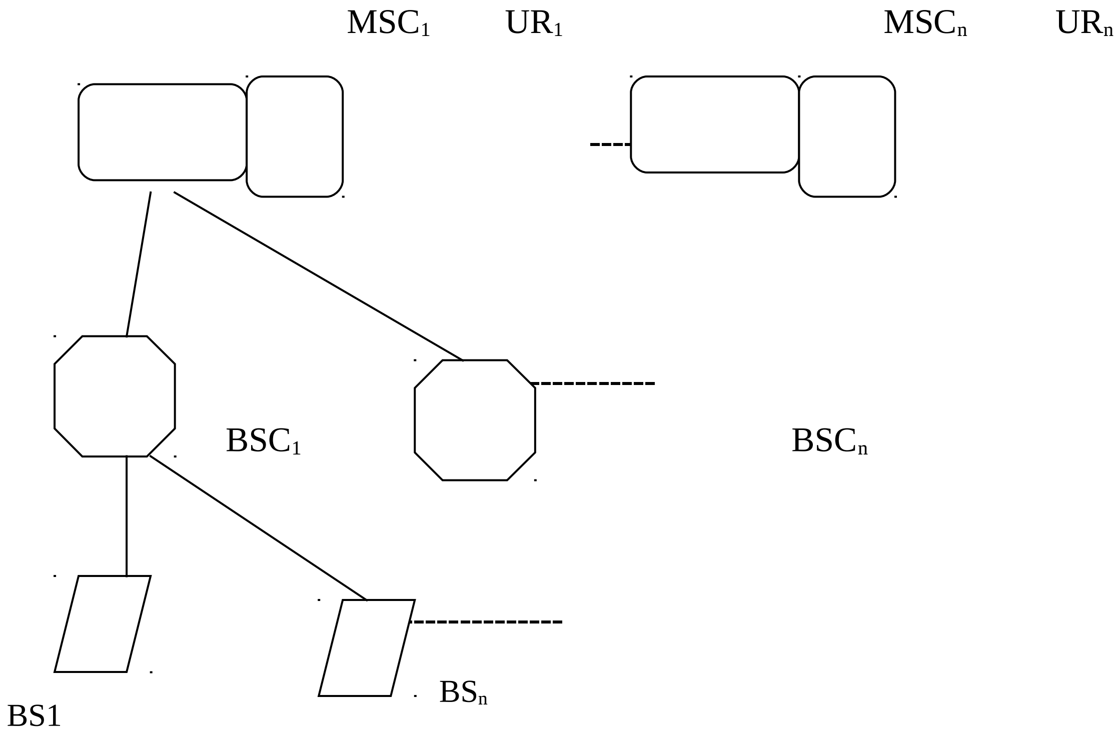


Figure 8.2 A generalized Wireless Building Block (WBB) for mobile network

Using a combination of some parameters, the dependability of wireless network can be optimized or a certain desired level of dependability could be achieved. The important parameters are:

- Number of users
- size and number of building blocks. This is related to number of users.
- Number of different types of components and their characteristics, which affect MTBF and MTTR.
- The number of links and interconnecting among multiple blocks, which is related to availability.

One or more of these parameters could be chosen to derive optimal values of dependability attributes of wireless mobile network under a given number of users. The user density in a block varies according to the level of user mobility and thus the impact of component, link and block failures would be both time and location dependent. Dependability optimization could be performed with a fair accuracy by considering higher level of mobility, which would make such optimization intractable and also very sensitive to small changes in user mobility. If dependability optimization is not desired, then one of several combinations of these system parameters could be selected to provide the required level of dependability in different locations. If needed different levels of dependability performance could also be supported in different locations, as the dependability required in highly congested business area could differ significantly from that required in rural areas. In theory, it is desirable to have the same level of high dependability everywhere in every network, but the cost and complexity considerations may preclude such design and deployment in wireless network. Therefore it is more likely that certain areas or locations would be pre-selected where highest levels of dependability could be provided. Irrespective of cost, due to type of customers and businesses served in these locations.

Besides location-sensitive dependency in network of a single carrier, a large-scale network could be deployed to interconnect multiple wireless networks of diverse dependability levels from several carrier, thus creating significant impact in future wireless networks involving large number of users receiving advanced services. Considerable efforts must be directed towards enhancing dependability attributes on both the local and global scale during the design of such future networks.

In general terms, fault-tolerance could be introduced in wireless networks at multiple levels including device, switching, block, and networking, leading to several configurations for fault-tolerant wireless networks. Fault tolerance at device level, could be supported by using multiple interfaces to the same network (replication). Fault tolerance at cell level could be supported by deploying multiple base stations per cell. Fault tolerance at switch level could be supported by internal redundancy of components. Using partial redundancy could provide fault tolerance at the block level, and fault tolerance at networking level could be achieved by using a fault-tolerant links.

The proposed architecture is shown in figure 8.3

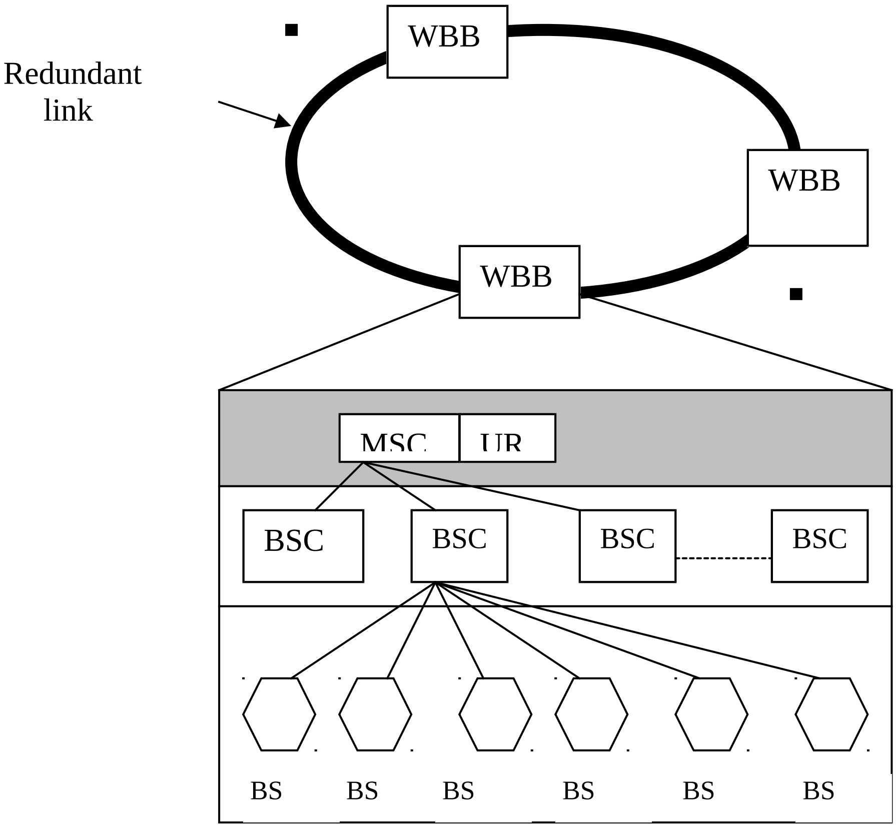


Figure 8.3 An integrated fault-tolerant wireless architecture

As a result, a small amount of redundancy at different levels could enhance the network availability to near optimal values.

8.5.1 Modeling and performance evaluation

Modeling will provide a platform to study the impact of various design changes for enhancing dependability attributes of wireless networks. The input parameters to the model will be:

- Number of users

- Size of building blocks
- Values of MTBF and MTTR of each component, link, and interconnecting architecture along with chosen distribution.
- Levels of redundancy.

Low, medium, and high ranges of MTBF ranges could be used to model the wireless network. The MTBF and MTTR used for the WBB are shown in table 8.2.

Item	MTBF (years)			MTTR
	Low	Medium	High	Hours
MSC	5	7.5	10	6
UR	2	3	4	3
MSC-BSC link	3	4	5	2
BSC	3	4	5	3
BSC-BS link	1	3	5	2
BS	1	2	3	2

Table 8.2 Assumed values of MTBF and MTTR for a WBB

In wireless environment, dependant failures are likely to occur where failures in a WBB can also affect customers in other WBBs.

From table 8.2, the availability for each item can be determined, and the overall availability of wireless network can be achieved. The medium value will be suitable in calculation to have an average availability value.

MSC availability = MTBF/(MTBF+MTTR) = (7.5).(8760)/[(7.5).(8760)+6]

= 0.99999

UR availability = (3).(8760)/[(3).(860)+3] = 0.99988

MSC-BSC link availability = (4).(8760)/[(4).(8760)+2] = 0.99994

BSC availability = 0.99991

BSC-BS link availability = 0.99988

BS availability = 0.99988

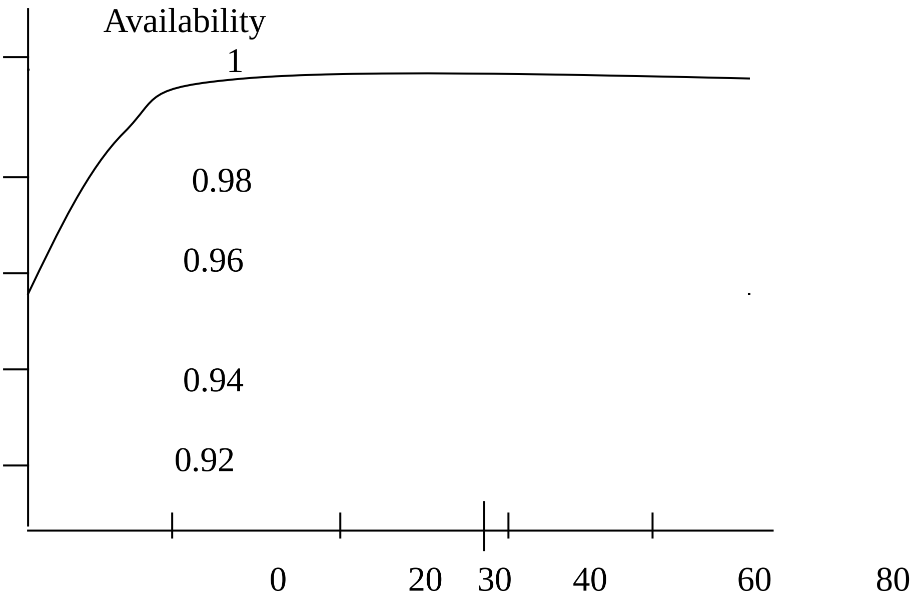
Hence, the overall availability of WBB is equal to:

$$(0.99999)(0.99988)(0.99994)(0.99991)(0.99988)(0.99988)$$

$$= 0.99948 \quad \text{or} \quad 99.948\%$$

8.5.2 Impact of redundancy on wireless network availability

Assuming that the total number of users per each WBB is 100,000, the MTBF and MTTR for all components is the same. The redundancy of components and links enhance the availability of the network strongly. But it should be noted here that the percent of redundancy in WBB enhances the availability of the wireless network for a certain level. Increasing the percentage of redundancy after this level will not give more enhancements. This is illustrated in figure 8.4 in which, redundancy of more than 30% has no effect on the network availability. The explanation of the 30% limit is still under study.



percentage

Figure 8.4 Impact of redundancy percentage on wireless network availability

8.5.3 Impact of mobility on wireless dependability

One important aspect of wireless dependability is the impact of user mobility. Therefore, this should be taken into consideration when determining the dependability attributes values. The term macro-level mobility is used, which is defined as the percentage of users registered in a block but roaming in the neighboring blocks. As the mobility level increased, the network availability reduces and the number of users impacted after failures are increased. This is illustrated in figure 8.5, from which, it can be seen that an increased level of redundancy could compensate mobility. Thus a network with higher mobility requires a higher redundancy to achieve a certain level of dependability. This fact was reached from many researches.[25] The results show that a level of 10% redundancy decreases the number of users affected by 1000 users.

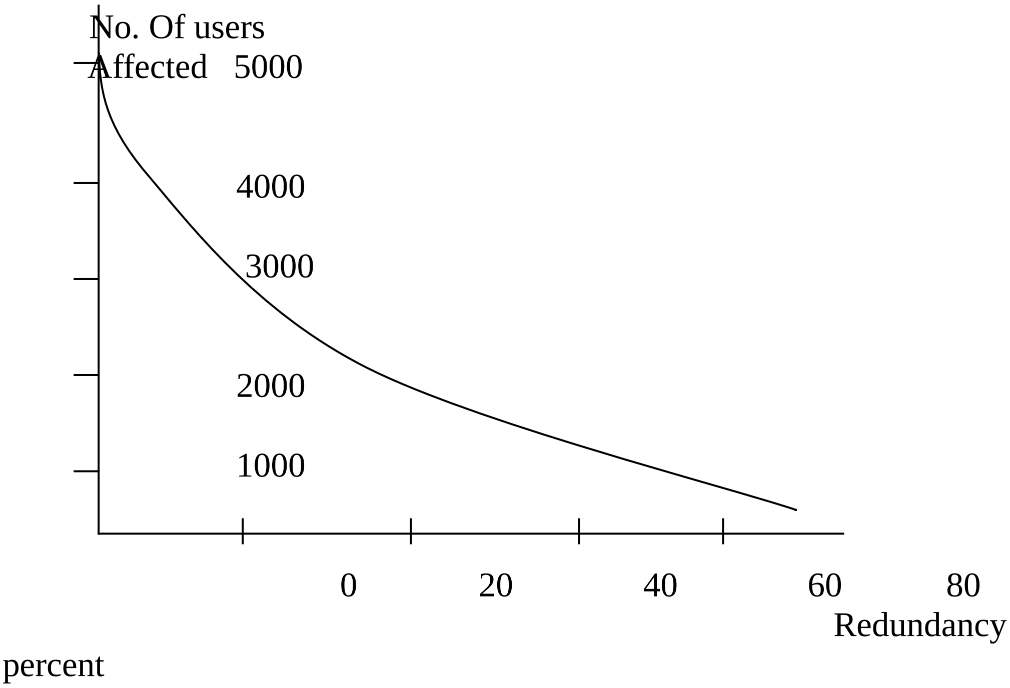


Figure 8.5 Impact of redundancy percentage on number of users affected

If very high level of dependability, redundancy is important. It should be noted here that for implementation purposes, a cost-benefit analysis should be done by comparing the cost of providing redundancy at each level and estimating the improvements of several different combinations.

CHAPTER NINE

Results

9. Results

9.1 Importance of network dependability

Networks have become essential for nearly all the key activities in our life. A dependable network is one that just works. It does what you want, when you want it, to meet your needs. To have a dependable network, dependability attributes should be modeled, analyzed, and improved. The main dependability attributes are reliability, availability, and maintainability. Once these three attributes have been well measured and evaluated, the enhancement of dependability level is possible. Reliable, maintainable, and available networks are achieved through a disciplined systems engineering approach employing the best design and support practice.

9.2 General guidance

In order to achieve reliability, availability, and maintainability requirements, emphasis should be on:

(a) Understanding the network mission performance requirements, physical environment, the resources available to support the mission, the risks associated with these requirements, and translating them into network system requirements that can be implemented in design and operation.

(b) Managing the contributions to network system reliability, availability, and maintainability that are made by hardware, software, and human elements of the network system.

(c) Preventing design deficiencies precluding the selection of unsuitable parts and items, and minimizing the effects of variability in the manufacturing and support process. And

(d) Developing robust network systems, insensitive to environment experienced throughout the network system's life cycle and capable to be repaired under adverse or challenging conditions.

Reliability, availability, and maintainability design analysis should be part of an iterative process continually assessing and improving the design. Reliability, availability, and maintainability objectives should be translated into quantifiable terms and allocated through the network system design hierarchy. The estimated or measured reliability, availability, and maintainability characteristics should be used to evaluate the design.

One of the most important issues is avoiding of single point of failure in designing stage. If a single point of failure cannot be eliminated through the design, the design should be made robust or redundant.

Fault tree analysis (FTA), and failure mode and effect analysis (FMEA) are tools that should be used to help identify where the degradation or failure could compromise the mission.

(e) The design should be based on established items selection practice and guidelines. Past items history, physical and environmental stresses, and item criticality should be considered in the network item selection. Design criteria should specify that maintenance tasks would be performed with a minimum number of common tools.

9.3 Relationship between Reliability, Availability, and Maintainability

Availability is defined as the probability that the system is operating properly when it is requested for use. In other words, availability is the probability that a system is not failed or undergoing a repair action when it needs to be used. At first glance, it might seem that if a system has a high availability then it should also have a high reliability. However, this is not necessarily the case. However, the relationship between availability, reliability, and maintainability is shown in table 9.1

Reliability represents the probability of components, parts and systems to perform their required functions for a desired period of time without failure in specified environments with a desired confidence. Reliability, in itself, does not account for any repair actions that may take place. Reliability accounts for the time that it will take the component, part or system to fail while it is operating. It does not reflect how long it will take to get the unit under repair back into working condition.

As stated earlier, availability represents the probability that the system is capable of conducting its required function when it is called upon, given that it is not failed or undergoing a repair action. Therefore, not only is availability a function of reliability, but it is also a function of maintainability. Table 9.3 below displays the relationship between reliability, maintainability, and availability. Note that in this table, an increase in maintainability implies a decrease in the time it takes to perform maintenance actions.

Reliability	**Maintainability**	**Availability**

Constant	Decreases	Decreases
Constant	Increases	Increases
Increases	Constant	Increases
Decreases	Constant	Decreases
Constant	Constant	Constant
Increases	Decreases	Decreases
Increases	Increases	Increases
Decreases	Decreases	Decreases
Decrease	Increases	Increases

Table 9.1 The relationship between reliability, maintainability and availability

As seen from the table, if the reliability is held constant even at a high value, this does not directly imply a high availability, as the time to repair increases, the availability decreases. Even a system with a low reliability could have a high availability if the time to repair is short. The cases in the table show that the availability is affected by both reliability and maintainability.

9.4 Impact of Redundancy

To explain the importance of redundancy, consider a system with three items configured in series to have a system success as illustrated in figure 9.1.

Each item with an annual failure rate (AFR) equal to 0.0876

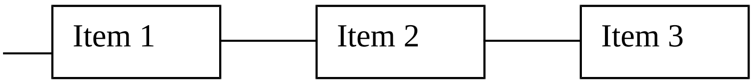


Figure 9.1 Three items in series

The risk of the whole system failure in the first year is equal to the failure of any single item in the system.

A general formula for series system with equal failure rate, AFR, is:

System AFR = x.y (9.1)

For redundant system, the formula is:

System AFR = x^y (9.2)

Where x is the item AFR, and y is the number of items. Thus, for the series system in figure 9.1:

System AFR = $3 \times$ (AFR) $= 3\times 0.0876$ = 0.2628

Hence, system reliability = 1 - 0.2628 = 0.7372 or 73.72%

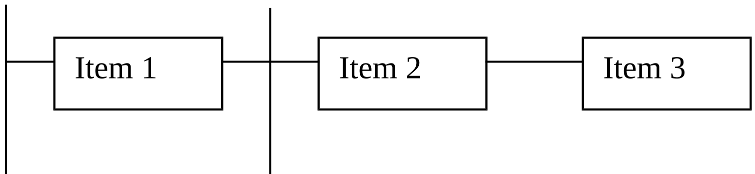
The redundancy may be partial or complete, and usually measured in percentage. Partial redundancy will be less than hundred percent, and which item should be redundant depends on the failure data of that item. Generally an item with a high failure rate is the nearest to be redundant. To see the impact of redundancy on system success, the system illustrated in figure 9.1 can be partially or fully redundant, which in each case the impact will be described.

9.4.1 Case I

If item 1 is redundant as shown in figure 9.2, the system AFR will differ and hence the overall reliability and availability of the system will differ also.

Redundancy percent = (No. of items redundant)/Total No. of items per system

Case I redundancy percent = 1/3 = 33.33%



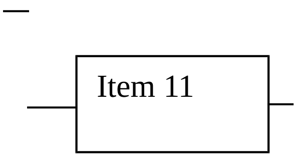


Figure 9.2 Case I, Item 1 redundancy

The system AFR could be calculated as :

$$AFR_s = (AFR_1)^2 + (AFR_2) + (AFR_3) \qquad (9.3)$$

$$= (0.0876)^2 + (0.0876) + (0.0876) = 0.18287$$

Thus, the system reliability is equal to:

$$R = (1 – AFR)$$

$$R_{system} = 1- 0.18287 = 0.81713 \quad \text{or} \quad 81.713\%$$

Note the enhancement of reliability by adding one item redundancy.

9.4.2 Case II

In this case two items are redundant as illustrated in figure 9.3.

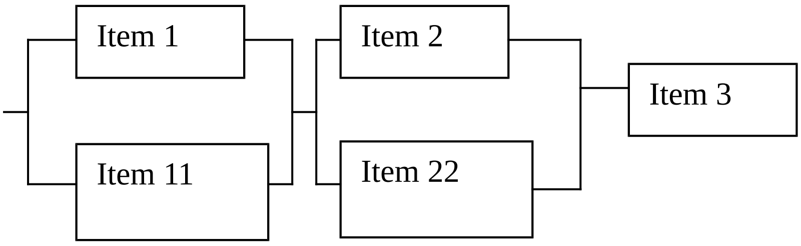


Figure 9.3 Case II, Item 1 and item 2 redundancies

The redundancy percent in this case = 2/3 = 66.66%

The system AFR can be found as:

$$AFR_s = (AFR_1)^2 + (AFR_2)^2 + (AFR_3) \qquad (9.4)$$

$$= (0.0876)^2 + (0.0876)^2 + (0.0876) = 0.10295$$

So, the system reliability in this case is equal to:

$$R_{system} = 1 - 0.10295 = 0.89705 \quad \text{or} \quad 89.705\%$$

9.4.3 Case III

This case represents the full redundancy situation or 100% redundancy with all items redundant, as illustrated in figure 9.4.

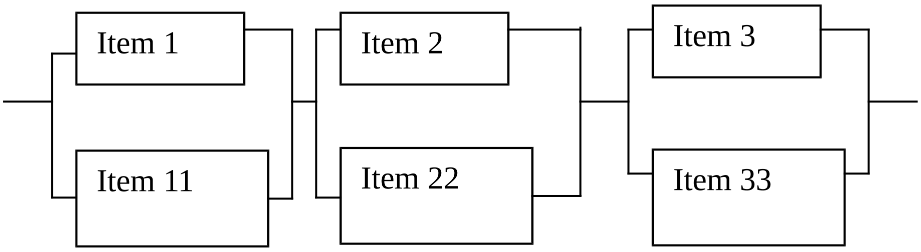


Figure 9.4 Case III, Full item's redundancy

The redundancy percent in this case = 3/3 = 100%

The system AFR can be found as:

$$AFR_s = (AFR_1)^2 + (AFR_2)^2 + (AFR_3)^2 \qquad (9.5)$$

$$= (0.0876)^2 + (0.0876)^2 + (0.0876)^2 = 0.023$$

So, the system reliability in this case is equal to:

$$R_{system} = 1 - 0.023 = 0.977 \quad \text{or} \quad 97.7\%$$

Case II gives the best reliability of the system, but should be balanced with the cost and importance of the redundancy to make the right decision.

9.4.4 Case IV

The three cases discussed fall in which is called one channel redundancy. Another alternative may be used which is called dual channel configuration as illustrated in figure 9.5.

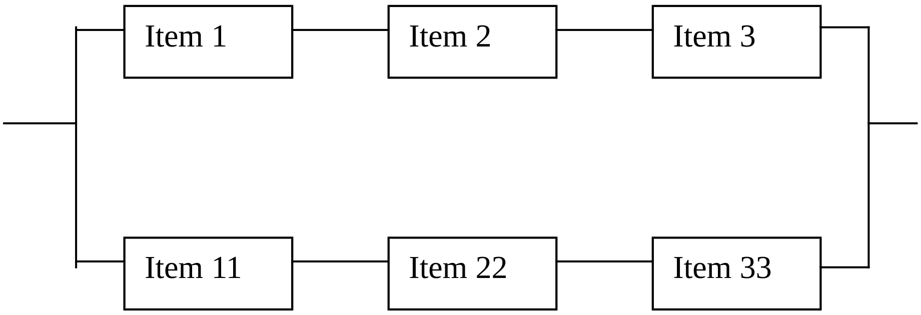


Figure 9.5 Case IV, Dual channel configuration

In dual channel configuration, the system AFR will be:

$$AFR_s = [(AFR_1) + (AFR_2) + (AFR_3)]^2 \qquad (9.6)$$

$$= [(0.0876) + (0.0876) + (0.0876)]^2 = 0.06906$$

The system reliability in this case is:

$$R_{system} = 1 - 0.06906 = 0.93094 \text{ or } 93.1\%$$

9.4.5 Case V

In this case item 1 and item 2 are in a single channel as shown in figure 9.6, in which they make a dual channel. The system AFR and reliability will differ from other configurations. In this case the system AFR will be:

$$AFR_s = [(AFR_1) + (AFR_2)]^2 + (AFR_3)^2 \qquad (9.7)$$

$$= [(0.0876) + (0.0876)]^2 + (0.0876)^2 = 0.03837$$

The system reliability in this case is:

$$R_{system} = 1 - 0.03837 = 0.96162 \quad \text{or} \quad 96.162\%$$

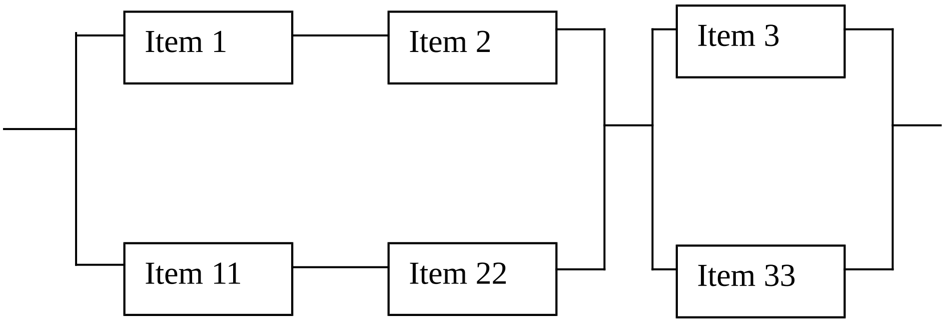


Figure 9.6 Case V, Item 1 and item 2 in a dual channel

This configuration implies that either item 1 or item 2 fails, the second channel (of item 11 and item 22) will be operated instead of channel one.

9.4.6 Case VI

This configuration differs from case IV only in none-redundant item 3.

This is illustrated in figure 9.7.

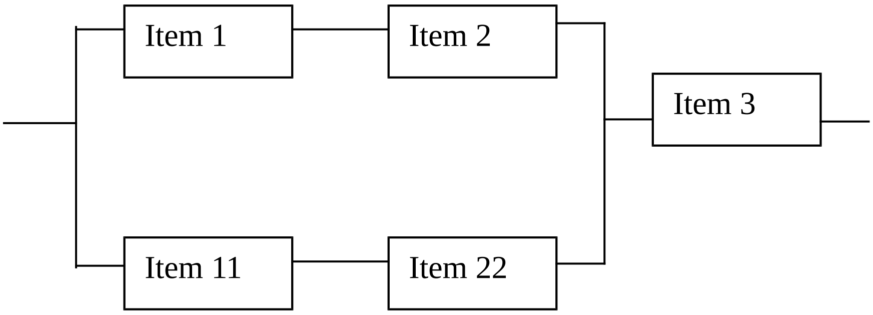


Figure 9.7 Case VI, Only Item 3 with no redundancy

In this case the system AFR will be:

$$AFR_s = [(AFR_1) + (AFR_2)]^2 + (AFR_3) \qquad (9.8)$$

$$= [(0.0876) + (0.0876)]^2 + (0.0876) \quad = 0.11830$$

The system reliability in this case is:

$$R_{system} = 1 - 0.11830 = 0.8817 \quad \text{or} \quad 88.17\%$$

9.4.7 Case VII

Item 1 with no redundancy, and the dual channel is set with item 2 and item 3 as illustrated in figure 9.8.

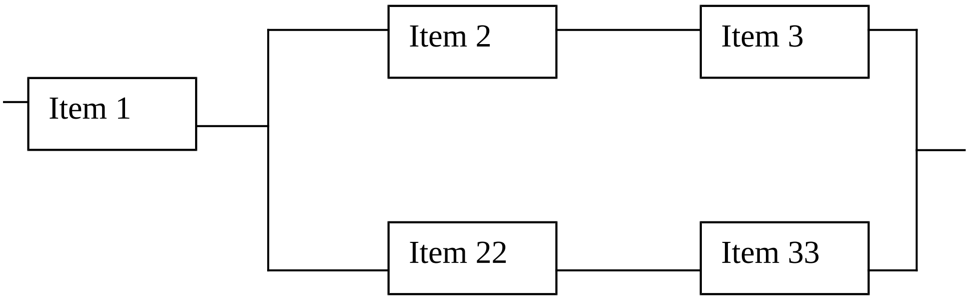


Figure 9.8 Case VII Item 2 and item 3 dual channel

In this case the system AFR will be:

$$AFR_s = (AFR_1) + [(AFR_2)] + (AFR_3)]^2 \qquad (9.9)$$

$$= (0.0876) + [(0.0876)] + (0.0876)]^2 \quad = 0.11830$$

The system reliability in this case is:

$$R_{system} = 1 - 0.11830 = 0.8817 \quad \text{or} \quad 88.17\%$$

Since the AFR of all items is identical, case VI and case VII are the same.

9.4.8 case VIII

In this case, item 1 is redundant with a dual channel between item 2 and item 3 as shown in figure 9.9

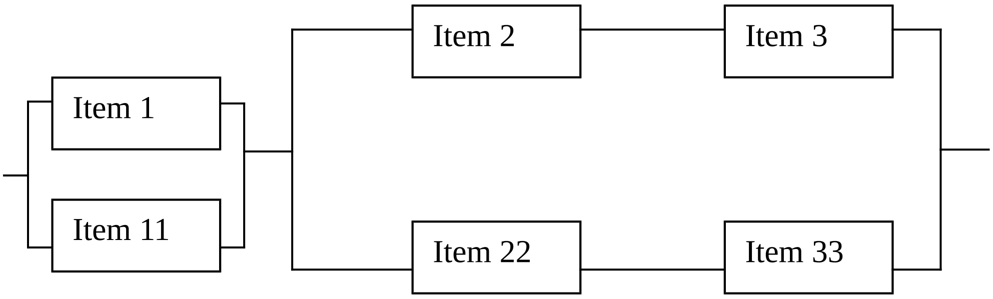


Figure 9.9 Case VIII item 1 full redundant, Item 2 and item 3 in dual channel

In this case the system AFR will be:

$$AFR_s = (AFR_1)^2 + [(AFR_2)] + (AFR_3)]^2 \qquad (9.10)$$

$$= (0.0876)^2 + [(0.0876)] + (0.0876)]^2 = 0.03837$$

The system reliability in this case is:

$$R_{system} = 1 – 0.03837 = 0.96163 \text{ or } 96.163\%$$

9.5 Decision making

To make a decision which redundancy case is the best:

1. A list should be set concerning the operation of the system in all cases as explained in table 9.2.
2. Compare between listed cases looking for system success.

3. In system success cases choose the one with the highest reliability.

4. Consider the cost in each system success case.

5. For critical network application, system success case with the highest reliability should be selected directly.

	System Success Cases							
Failing item	**I**	**II**	**III**	**IV**	**V**	**VI**	**VII**	**VIII**
Item1	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Item 11	Yes	Yes	Yes	Yes	Yes	Yes	Y	Yes
Item 2	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Item 22	Y	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Item 3	No	No	Yes	Yes	Yes	No	Yes	Yes
Item 33	Y	Y	Yes	Yes	Yes	Y	Yes	Yes
R_{sys}	0.881	0.897	0.977	0.931	0.962	0.882	0.882	0.962

Table 9.2 Reliability and system success in all cases

Notes:

Yes = system success, No = No system success

Y = System success, but the corresponding redundancy item does not exist

From table 9.2, the highest reliability is obtained from case III, so if the cost is not a concern, this case is the optimal.

9.6 Availability classes and management

Networks availability values are classified according to the number of nines achieved in availability modeling. One can stress here that availability less than 90 percent, in other words, has no nines, is considered to be poor availability. The network system with no nines in its availability need complete revision and analysis, because it indicates that this network is undependable.

Table 9.3 shows the classes of availability and the corresponding management kind associated with the availability value. This table could be the foundation for engineers and management of the network to specify their availability goal, and thus the required design is set to meet their goal.

Table 9.3 Availability classes and management Roll.

Network type	Unavailable min/year	Availability %
Unmanaged	52560	90
Managed	5256	99
Well-managed	526	99.9
Fault tolerant	53	99.99
High management	5	99.999
Very high management	0.5	99.9999
Ultra high management	0.05	99.99999

9.7 SUST network results

Looking for failure data of this network, one can see that the weakness of this network appear at phase II, especially part II of this phase which consists of the cabling system. Since the PSTN management concerns the PSTN company, it is clear that modifications and enhancements is not available for the customer. Hence, availability, reliability, and maintainability of this phase is out of hand for customers. Phase I of this network is manageable, and many things can be done to enhance the dependability.

9.7.1 Phase I suggestions

A redundancy approach could be followed in this phase to increase the dependability of the network.

(a) The PSU item of this phase I encounters 0.0046 AFR, which is the highest AFR of this phase. If the PSU was redundant by a standby generator assumed to be fully ready, with automatic converter switch, the AFR of this item will be equal to:

$$AFR = (AFR_{psu})^2 = (0.0046)^2 = 0.00002116$$

and hence, the reliability of this item will be:

$$R_{PSU} = (1 – 0.00002116) = 0.9999788$$

This reliability value affects the overall reliability of SUST network. The new SUST network reliability will be:

$$\begin{aligned} R_{phaseI} &= (R_{PSU}).(R_{switch}).(R_{server}).(R_{Router}).(R_{DTU}) \\ &= (0.9999788)(0.99994).(0.99977).(0.99997)(1) \\ &= 0.99966 \quad \text{instead of } 0.99922 \end{aligned}$$

generally it could be said that adding any item redundancy will enhance the overall reliability of SUST network.

9.7.2 Replacing PSTN

Since PSTN used in phase II of the SUST network, using another alternative with less failures will enhance the overall reliability and availability. For example using wireless link instead of PSTN will increase its reliability and availability.

9.7.2.1 Replacing PSTN with Wireless link

The failure data for this link shows that 5000000 hours of MTBF is experienced for this link. The AFR for wireless link will be:

$$AFR = 8760/50000000 = 0.00175, \text{ thus}$$

$$R_{wireless} = (1 – 0.00175) = 0.99825, \text{ (Phase II reliability)}$$

The overall SUST network will be:

R_{SUST} = (Rphase I).(Rphase II)

= (0.99922).(0.99825) = 0.9975 or 99.75%

From a design perspective, this value is better, but a cost analysis should be done to compare the overall network cost.

9.7.2.2 Using VSAT as phase II

This could be another alternative with a very low AFR. The AFR for the Very Small Aperture Terminal (VSAT) could be estimated from manufacturer data. The approximate value of AFR for the VSAT is equal to 0.0008. Thus, the VSAT reliability is:

VSAT reliability = (1 – 0.0008) = 0.9992

The overall reliability of SUST network in this case is:

R_{SUST} = (Rphase I).(Rphase II)

= (0.99922).(0.9992) = 0.99841 or 99.841%

9.8 Benefits of low MTTR

A widely accepted equation for availability is

Availability=MTBF/(MTBF+MTTR)

MTTR is the Mean Time To Repair, which sometimes expressed as Mean Time To Recovery, Mean Time To Replace, or Mean Time To Restore. All expressions imply that MTTR is so important in determining the availability. The equation suggests that to improve availability, 10x decrease in MTTR is just as valuable as 10x increase in MTBF. In networks, a decrease in MTTR is sometimes more valuable than the corresponding increase in MTBF to improve availability by the same amount, because fast recovery could be a part of the network design. A common interpretation of network availability is that it represents the probability that any given request made for the network will be successfully serviced.

Availability of 0.99 means that MTBF is 100x to MTTR.

Availability of 0.999 means that MTBF is 100x to MTTR.

The reasons that lowering MTTR is more valuable than increasing MTBF in availability calculation are:

1. In the case of today's component MTBFs are so high that directly measuring them requires many network system's years of operation. Most customers cannot afford this and must largely rely on vendor claims to assess the impact of MTBF on availability. On the other hand, MTTR can be directly measured for both hardware and software, making MTTR claims independently verifiable.
2. For interactive services such as networking, lowering MTTR can directly affect user experience of an outage.

3. Lowering MTTR draws the attention of the network managers for the importance of maintainability issues, especially planning to prepare skilled personnel to handle failures when occur.

9.9 Network-Critical Physical Infrastructure (NCPI)

The current trends towards higher dependability of computing and networking resources have led to increased focus on the physical infrastructure on which those resources depend. When choosing a management solution for the physical infrastructure of the network, key factors considerations are the cost of deployment and maintenance, adaptability, as business needs change, and functionality.

A manner consistent with an overall management structure is desirable and offer the benefits of providing information on issues affecting network system availability,

lessening the burden of managing the system, lowering the risk of downtime, and increasing the network personnel productivity.

9.9.1 NCPI elements

Network Critical Physical Infrastructure (NCPI) is the foundation upon which network resides. They affect strongly the failure rates of the items of the network. High level of performance of the NCPI results in high dependability of the network. The NCPI include:

- Power
- Cooling
- Racks and physical structure
- Security and fire protection
- Cabling
- Management systems
- Service

At first look, these components seem similar to those in buildings. Almost all traditional buildings have a power, air conditioning, environmental monitoring, and security in place. What distinguishes these systems from NCPI is the focus on availability of network resources. A standardized, adaptable, and integrated NCPI is essential to maintaining highly available and manageable network. The NCPI represents the base for all network's activities and technologies used.

Figure 9.10 illustrates the layers of a dependable network, and the location of NCPI of these layers.

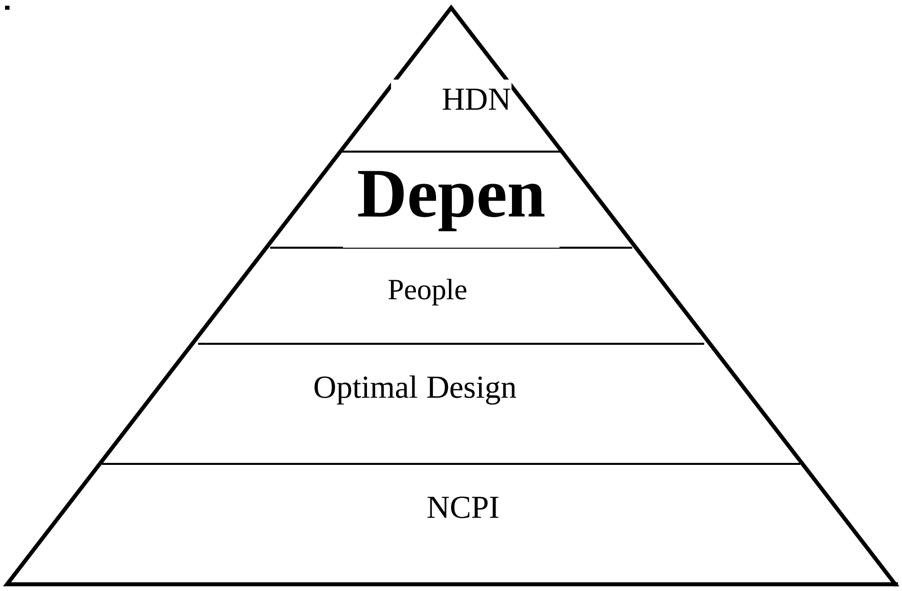


Figure 9.10 Dependable network layers

HDN = Highly Dependable Network

When choosing a management solution for the physical infrastructure of networks, management of individual devices is necessary in order to have reliable operation of critical physical infrastructure. Device management solution offers the optimum approach as it manages a particular type of devices necessary for network dependability.

9.10 Optimum Design Level Determination

With a good grasp of the dependability of network system, it is possible to devise specifications and design that result in the optimum level of dependability. Designing a network with inexpensive and unreliable items will result in a network system with low initial costs, but high support cost. On the other hand, designing a network with costly highly reliable items will result in a final network system with low support costs, but that is prohibitively expensive. The optimum design should balances out both of these factors, resulting in a design dependability that minimizes the overall cost of the network system. Figure 9.11 gives a graphical representation of this concept.

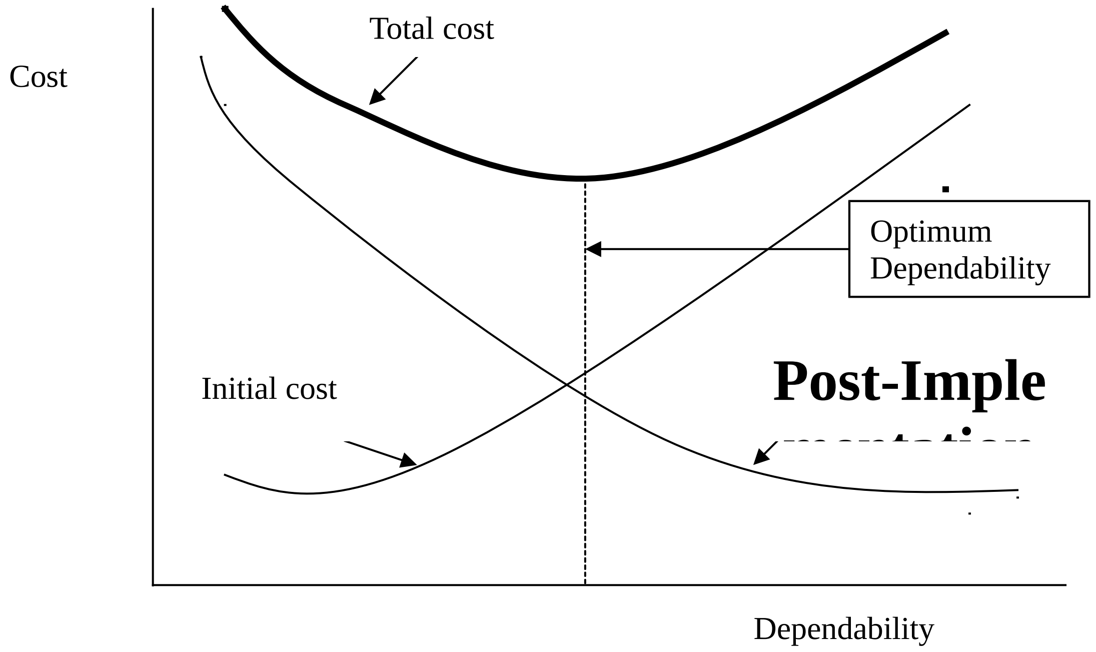


Figure 9.11 Balancing initial and support costs to determine optimum dependability

9.11 Conclusion

The dependability is an important issue in networks. Services and money lost by undependability of networks are very considerable. Improving the dependability of networks should be one of the most important topics in networking. The thesis covered the main attributes of network dependability. The three main attributes studied throughout the thesis were reliability, availability, and maintainability. The models used in measuring and evaluation these attribute were mathematical models.

Reliability was modeled using two formulas:

1. Exponential formula

$R = Exp(-\lambda t)$ where λ is the failure rate (failure/hour).

This formula is suitable for systems with many failure occurrences during a year, which measure the reliability at any given time.

2. The second reliability formula was:

$R = (1 - AFR)$ where AFR is the annual failure rate. This formula is simpler and very appropriate for reliability measurement of network systems that encounter few failures over a long period of time. This formula measure the reliability of a network system through a year, in other words, the probability that the network system will run without a failure for one year time interval. One year is a suitable time period to measure the reliability, because evaluation of the network performance usually done every year to see what modification could be made to improve the network performance. This also excludes the abnormal situation that may occur due to unexpected catastrophic failures.

The availability, which is defined as the readiness of the network when its needed, was measured using the formula:

$A = MTBF/MTBF+MTTR$

This formula measures the availability of the network system at any point of time. The availability should not be less than two nines (0.99) to have an acceptable level of network availability. Improvement should be done to increase the number of nines. This cannot be achieved without an accurate network availability modeling. The target of network engineers should be the five nines (0.99999) of network availability, which is classified as high network availability.

Maintainability, which is defined as the relative and economically ease to repair failed items and restore them to the required operation, aims to lower the MTTR. The main parameter that affects the availability of the networks is its downtime. All maintainability modeling should carry out this fact, and techniques should be directed to lower this downtime. The importance of lowering downtime could be seen from the availability formulas used, as:

A = Uptime/(Uptime+ Downtime)   or,

A = MTBM/(MTBM+MDT) where MTBM is the mean time between maintenance, and MDT is the mean down time. Corrective, preventive, and conditional maintenance levels were discussed. The conditional maintenance was chosen as the best level of maintenance, because it may prevents failure occurrence, and since it is a planned maintenance, the MTTR is manageable to lower its period. Also conditional maintenance avoid the long downtime results from complete failure occurrences.

The thesis suggested a function that can be used to measure the probability of completing the maintenance within the required time. This depends on the availability of the maintenance resources. For example, if all resources are available, this function is equal to one. Hence, it varies according to percentage of the resources availability.

This maintainability function, denoted as M(t), represents the probability that the maintenance task considered will be successfully completed before or at the specified maintenance elapsed time t, thus:

M(t) =P(DMT < = t)

Where, DMT is the Duration of Maintenance Task.

The SUST network was modeled to evaluate its dependability by modeling the reliability and availability as the main dependability attributes. It is important to stress here that the failure data used in SUST network evaluation are not fixed. They vary from a year to another, and hence the main concern was to make a framework for modeling dependability.

One of the methods used to improve the network dependability is adding redundancy. Where you add redundancy, and how was discussed showing that redundancy should be associated with cost analysis. In critical network applications, redundancy must be used since the cost of downtime may sometimes exceeds the cost of the item added as a redundant item. It was clear from the results that many options are available in adding redundant components. Single channel and dual channel methods were explained in order to choose the most suitable way of adding redundant items.

The techniques used with failures were described including Failure Mode and Effect Analysis (FMEA), in which any failure should be analyzed to clarify its mode, or the way failure occurred and what are the consequences of this failure. Root Cause of Failure Analysis (RCFA) was discussed to explain that any failure has a cause, and the cause has a root cause, and so forth. Defining root cause of failure reduces the probability of occurrence of this failure in the future, providing that the root cause was properly maintained.

9.12 Recommendations

From observations, it was clear that the network personnel have a considerable contribution of the network outages. Either by misuse, uncountable accidents made by network users, or their capability of doing fast recovery. Network dependability is a broad subject. One of the most important areas in network dependability is the people training. A reliability team should be set in every critical application network that affects a large number of users. This group must be responsible for network performance monitoring, and suggests the proposed actions that improve the reliability of the network. Some projects regarding network dependability improvement, which represent considerable areas of researches, are:

- Determining the cause of a problem

A software may be developed that determines when problems exist may be able to localize the problem precisely enough to identify the cause of the problem, foe example link failure. However, there will also be times when additional diagnosis is needed to determine the cause of the problem.

- Informative failure report wizard

  The goal is to create software that will allow the network user to know much about the failure occurred in is connectivity, together with some guides for remedial procedures and future avoidance.

- Maintenance Best Practice

Since there are corrective, preventive, and conditional maintenance, a software encyclopedia covering a wide range of network devices used. The software package that provides a complete maintenance policy and plans, according to the type of the network and the devices used. When you enter your network parameters, a list of best practices will be displayed, from which, one can be chosen which meets the network under consideration.

-Since the evaluation of the dependability attributes models depend basically on the real data, this situation requires a very accurate data records. For this reason data takers or observers should be very accurate in taking their data and at least two levels of data approve should be taken.

- The best way for data collection is using automated data. This could be done by using watchdog devices like time counters to count the up time of the device. For example a time counter, which works as the device works will count the uptime of this device. The counter can count also the number of outages of that device.

Thus the number of outages will give an accurate failure rate giving an accurate reliability value for the device.

The uptime will in turn give an accurate value of the availability of the device when a counter is attached to this device.

- Wireless media for networks provide better values of availability and reliability hence it is recommended that cables should be replaced as possible by wireless media. For this reason the PSTN part of the SUST network should be replaced by a wireless media to increase this network performance.

References

1. David T. Smith, *Reliability, Maintainability, and Risk*, Butterworth and Heinman, 1997.
2. DR Jezdimir Knezevic, *Systems Maintainability Analysis, Engineering, and Management*, Chapman and Hall, London, 1997.
3. Paul A. Tobias, David C. Trindade, *Applied Reliability*, *2nd Edition* , Chapman and Hall, New York , 1995.
4. W. Bolton, *Measurement and Instrumentation Systems*, Oxford, 1996.
5. John Moubry, *Reliability Centered Maintenance,* Butterworth – Heinemann, Hordan Hill, Oxford, 1997.
6. Ushakan, Igon A. *Handbook of Reliability Engineering*, New York, John Wiley and Sons, 1994.
7. Tony W. and James A. *Electronic Product Design*, Alden Press, Oxford, 1996.
8. Karl Kummerle, Fouad A. Tobagi, John O. Limb, *Advances in Local Area Networks*, IEEE Press, 1987.
9. John D. Musa, Anthony Iannino, Kazuhira Okumoto, *Software Reliability Measurement, Prediction, and Application*, McGraw-Hill, 1987.
10. Joe Casad, Dan Newland, *MCSE Networking Essentials*, New Riders Publishing, 1997.
11. Van Valkenburg, *Reference Data for Engineering Radio, Electronics, Computer, and Communication*, Butterworth-Heinemann, 1998.
12. Way Kuo, V. Rajenda, Frauk A. Tillman, Ching-Lai Hwang, Optimal *Reliability Design-Fundamental and Applications*, Cambridge University Press, 2001.
13. Doris Lloyd Grosh, *A primer of Reliability Theory*, John Wiley and Sons, 1989.

14. Warner Fleischammer, *Quality by Design for Electronics*, Chapman and Hall, 1996.

15. J . P. Holman, *Experimental Methods for Engineers*, McGraw-Hill, 1978.

16. John A. Pitts, *The Human Factor*, U.S Government Printing Office, Washington DC, 1985.

17. Kivensen, G., *Durability and Reliability in Engineering Design*, Pitman, London, 1972.

18. O. Connor, P. D. T. O., *Practical Reliability Engineering*, 3rd Edition, Wiley, Chichester, 1991.

19. Anderson, R.T and Neri, L., *Reliability-Centered Maintenance Management and Engineering Methods*, Elsevier Science Publishers, London, 1990.

20. Jones P. F., *CAD/CAM Features, Applications, and management*, Macmillan, Hong Kong, 1992.

21. Knezevic J., *Reliability, Maintainability, and Supportability Engineering – Probabilistic Approach*, McGraw-Hill, London, 1993.

22. Blanchard, B. S., Verma, D. and Peterson, E. L., *Maintainability*, John Wiley and Sons, New York, 1995.

23. Sanders M. S., and McCormick, E. J., *Human Factors in Engineering and Design*, 7th Edition, McGraw-Hill, New York, 1993.

24. Drago Matko, Rihard Karba, Borut Zupancic, *Simulation and Modeling of Continuous Systems*, Prentice Hall International, UK Ltd. 1992.

25. Atlanta University, Research Center, USA, 2003.

Web Sites

26. http://www.itl.nist.gov/div898/handbook/apr/section1/apr161.htm

27. http://www.weibull.com/Articles/Re1Intro/Brining_It_All_Together.htm

28. http://www.reliasoft.com/newsletter/3a2002/availabilities.htm

29. http://www.quanterion.com/KnowledgeBase/ReliabilityToolkit.htm.

30. http://www.national.com/quality/8d.html

31. http://www.jisc.ac.uk/index.cfm

32. http://www.maintenanceworld.com/Articles/acq/achieving.htm

33. http://www.acq.osd.mil/io/se/re1_mnt/pratices.html

34. http://www.chinarel.com/hotwire/issue26/relbasics26.htm

35. http://hissa.ncs1.nist.gov/kuhn/pstn.html

36. http://www.isographsoftware.com/ftnover.htm

Appendix 1

ACRONYM

A	Availability
ABD	Availability Block Diagram
AFR	Annual Failure Rate
A_{av}	Average Availability
A_i	Instantaneous Availability
A_o	Operational availability
A_t	Total Availability
BA	Boolean Analysis
BBD	Boolean Block Diagram
CMF	Common Mode Failure
CMT	Cost of Maintenance Task
COT	Conditional Maintenance Task

COTS	Commercial –Off- The Shelf
CPU	Central Processing Unit
CU	Coefficient of Utilization
CU^F	Coefficient of Utilization of Failure based maintenance
CU^L	Coefficient of Utilization of Life based maintenance
CU^I	Coefficient of Utilization of Inspection based maintenance
DCB	Drop Cable
DLU	Digital Line Unit
DoD	Department of Defense
DF	Dormant Failure
DT	Down Time
DTU	Data Terminal Unit

EITT	European International Telephone and Telegraph
EPC	Error Producing Condition
ER	Error Rate
EX	Exchange
EXP	Exponential
FC	Failure Cause
FMEA	Failure Mode and Effect Analysis
FMECA	Failure Mode and Effect Criticality Analysis
FPMH	Failure Per Million Hours
FR	Failure Rate
FS	Failure Severity
FTA	Fault Tree Analysis
HA	Hazard Analysis
HAZOP	Hazard and Operability
HEART	Human Error And Reduction Technique

LAN	Local Area Network
LBM	Life Based Maintenance
MCMT	Mean Cost of Maintenance Task
MDT	Mean Down Time
MTBM	Mean Time Between Maintenance
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
M(t)	Maintainability function
NC	Not Connected
NCPI	Network Critical Physical Infrastructure

NU	Not Used
OBM	Opportunity Based Maintenance
OV	Overall
PCB	Primary Cable
PN	Part Number
PSU	Power Supply Unit
QF	Quality Factor
QoS	Quality Of Service
R	Reliability
R_s	Reliability of the System
R_t	Total Reliability
RCFA	Root Cause of Failure Analysis
RCI	Relevant Condition Indicator
RCM	Reliability Centered Maintenance
RCP	Relevant Condition Parameter
RPN	Risk Priority Number
SVR	Server
S/W	Software

SW	Switch
T	Time
TBF	Time Between Failures
TTR	Time To Repair
UF	Utilization Factor
UPS	Uninterrupted Power Supply

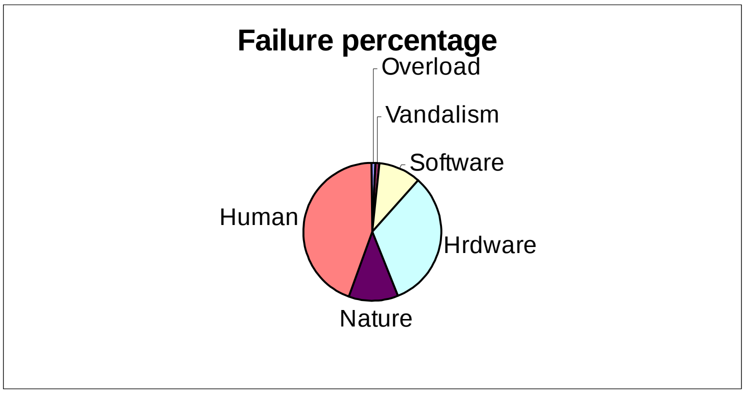
UR	Unreliability
WBB	Wireless Building Block
WLAN	Wireless Local Area Network
λ	Failure Rate
γ	Weibull Location Parameter
η	Weibull Scale Parameter
μ	Repair Ratio (1/MTTR)
π_Q	Quality Factor of the Electronic Device
π_L	Learning Factor of the Electronic Device
π_E	Environmental Factor of the Electronic Device

Appendix 2 PSTN sources of failures

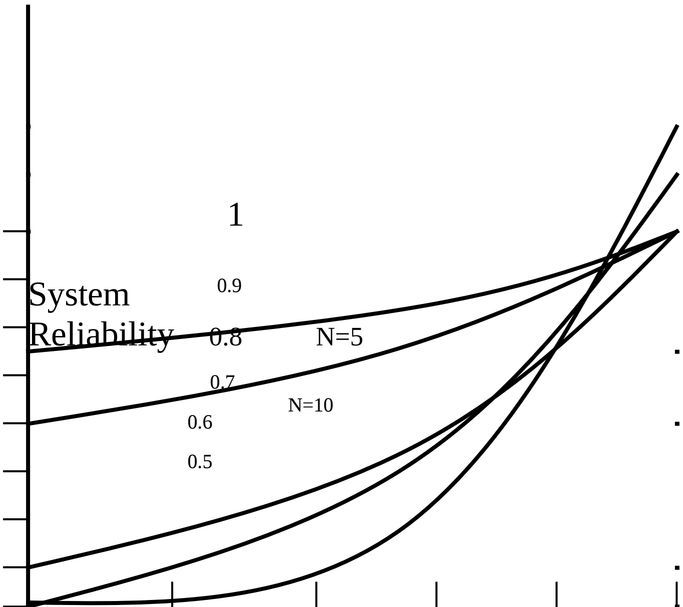
Colleted and organized over two years 2003 – 2005 (Sudatel)

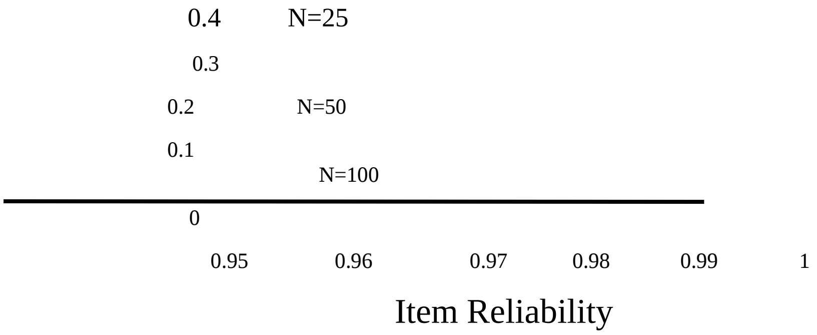
Category	**Source**	**Example**	**Percentage**
Human Error	People	Cable cuttings Car accidents	45

Acts of nature	Rain Wind	Primary cable (In manhole) Drop cable	11
Hardware failures	Power supply DLU Cable /cabinet		32
Software failures	Internal errors in software (in CPU)	Disk R/W errors	10
Vandalism	Intentional damage	Cabinets	1
Overload	Service demand exceeds the designed capacity		1



Appendix 3 Many Items in series destroy system reliability

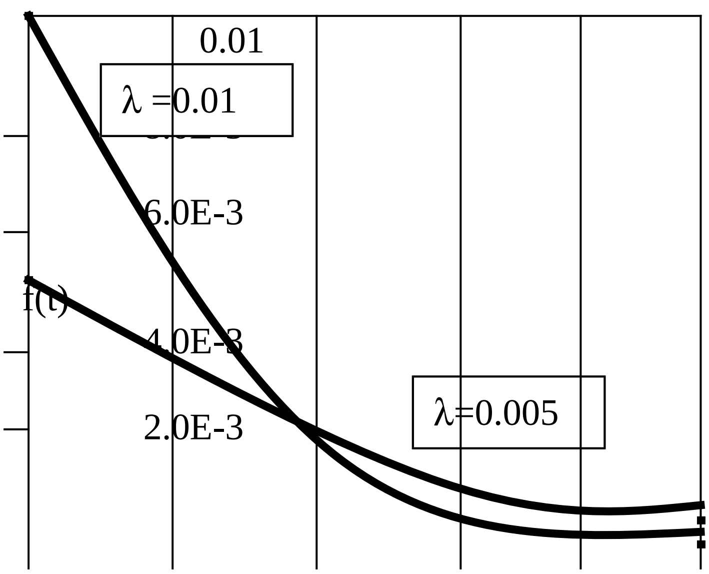


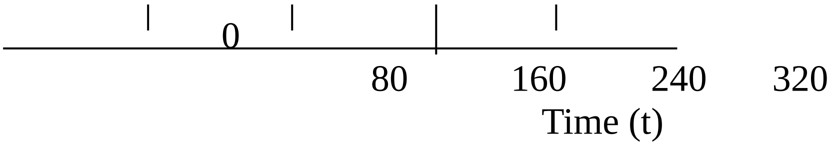


Item Reliability	**System Reliability** **N=5**	**N=10**	**N=25**	**N=50**	**N=100**
0.95	0.77	0.6	0.28	0.08	0.006
0.96	0.82	0.66	0.36	0.13	0.017
0.97	0.86	0.74	0.47	0.22	0.048
0.98	0.9	0.82	0.6	0.36	0.133
0.99	0.95	0.9	0.78	0.61	0.366

N = Number of items in series with the same failure rate

Appendix 4
Effect of λ on Exponential pdf

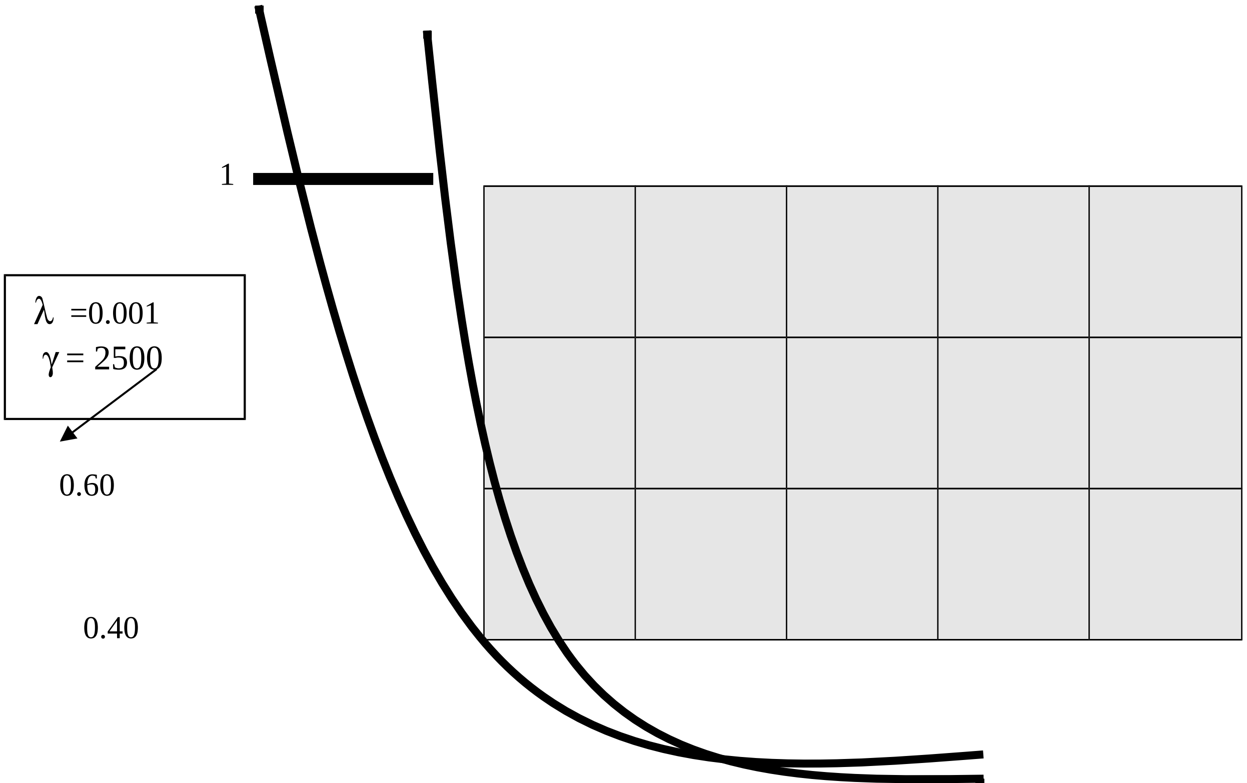


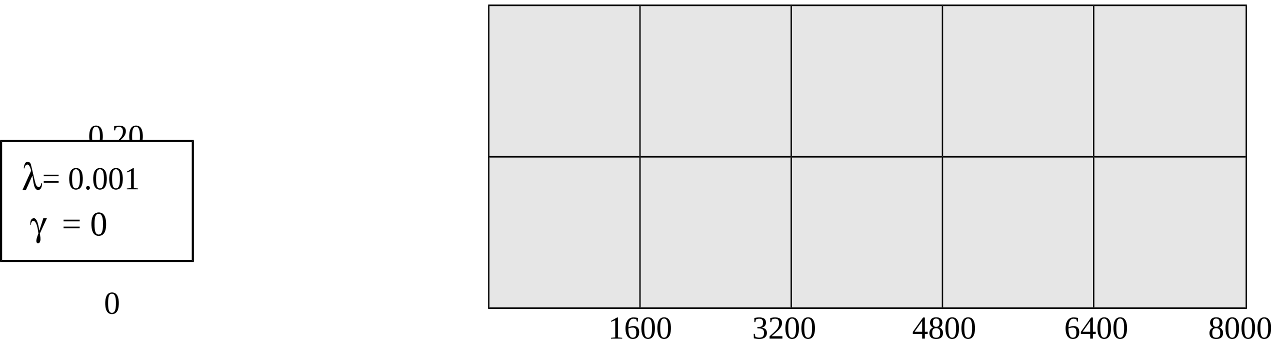


$f(t) = \lambda e^{-\lambda t}$ probability density function (pdf)

- The exponential function has no shape parameter, as it has only one shape.
- The exponential function always convex and stretched to right as λ decreases in value.
- The value of the function is always equal to the value of λ at T= 0 (or T = γ)
- The location parameter, γ, if positive, shift the beginning of the distribution by a distance of γ to the right of the origin, signifying that the chance failures start to occur only after γ hours of operation, and cannot occur before this time.

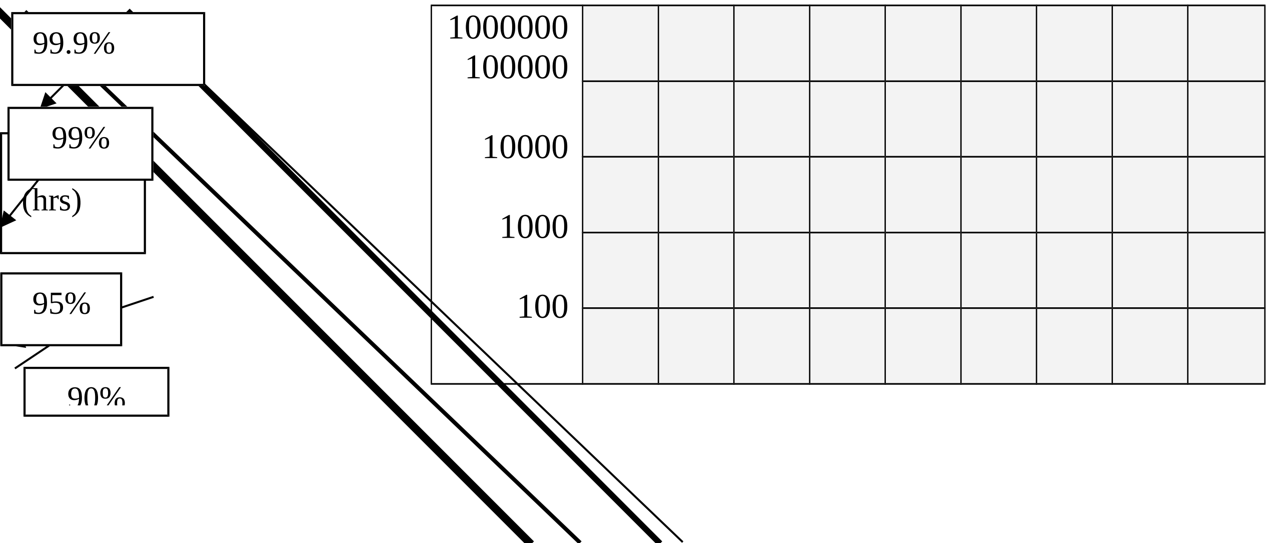
Appendix 5
Effect of γ on exponential Reliability Function

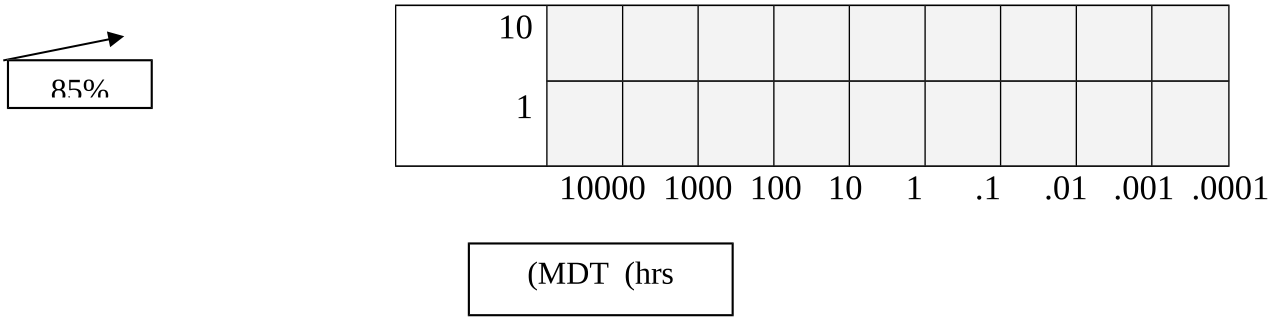




- The one-parameter exponential reliability function starts at T=0, it decreases therefore monotonically and is convex.
- The two-parameter exponential reliability function starts at T=γ.
- AS T approaches infinity, R(T) approaches 0.

Appendix 6
MTBM and MDT Relationship for Fixed Availability





A_o = . MTBM
MTBM+M

Effect of failure on system
Complete sys. Failure
Major Degradation
Minor Degradation
None

Module

On site diagnosis:
No defect found
Part failure
Installation defect
Manufacturing defect
Design defect
Program defect
Human error
Others
Action taken:
Replace module
R
M
P
C

Report No.----
Report date----
Completed by-
Company------

Analysis and action taken: Eng. change no.......date.........
Follow up report Ref. No..... date.....
Name..........................Sig............date................
For information to:

Appen 10/14 8
Probability Rules, Binomial and Bayes theorems

A8.1 The Multiplication Rule

If two or more events can occur simultaneously, and their individual probabilities of occurring are known, then the probability of simultaneous events is the product of the individual probabilities. The shaded area in figure A8.1 represents the probability of event A and B occurring simultaneously. Hence the probability of A and B occurring is:

$$P_{ab} = P_a \times P_b$$

Generally

$$P_{an} = P_a \times P_b \times P_c, \ldots\ldots\ldots\ldots\ldots \times P_n$$

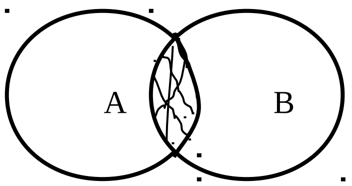


Figure A8.1 Multiplication Rule

A8.2 The Addition Rule

It is also required to calculate the probability of either event A or B occurring. This is the area of the two circles of figure A8.1. This probability is:

P(a OR b) = Pa + Pb – PaPb

The sum of Pa and Pb is less than PaPb, (which is included twice) this becomes:

P(a OR b) = 1 – (1 – Pa)(1 – Pb)

Hence, the probability of one or more of n events occurring is:

1 – (1 – Pa)(1 – Pb),......................(1 – Pn)

A8.3 The Binomial Theorem

The above two rules are combined in Binomial theorem. Consider a pack of 52 playing cards. A card is removed at random. A second card is then removed. The possible outcomes are:

Two hearts
One heart and one another card
Two other cards.

If P is the probability of drawing a heart then, from the multiplication rule, the outcomes of the experiment can be calculated as:

Probability of two hearts	P^2	
Probability of one heart	2pq	
Probability of 0 heart	q^2	where q = (1 – P)

Similar reasoning for an experiment involving three cards yield:

Probability of 3 hears	P^3
Probability of 2 heart	$3p^2q$
Probability of 1 heart	$3Pq^2$
Probability of 0 heart	q^3

The above probabilities are the terms of the expressions $(P + q)^2$ and $(P + q)^3$. this leads to a general statement that if P is the probability of some random event, and if q = 1 – P, then the probabilities of 0, 1, 2, 3, ...outcomes of that event in n trials are given by the terms of the expression:

$(P + q)^n$ which equals

$$Pn,\ np^{(n-1)}q,\ \frac{n(n-1)P^{(n-2)}q^2}{2!}\ ....q^n$$

This is known as Binomial expansion.

A8.4 The Bayes Theorem:

The marginal probability is its simple probability. Consider a box of seven cubes and three spheres in which case the marginal probability of drawing a cube is 0.7. To introduce the concept of conditional probability assume that four of the cubes are black and three white, and that of the spheres, two are black and one is white as shown in Figure A8.2.

The probability of drawing a black cube among the cubes is 4/7. this is a conditional probability. The conditional probability of drawing a black sphere from the three spheres is 2/3. on the other hand the probability of drawing a black sphere from the whole box is 2/10 and this is called a joint probability.

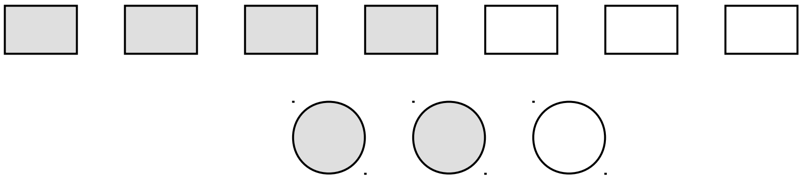


Figure A8.2 Bayes Theorem

Comparing joint and conditional probabilities, the conditional probability of drawing a black sphere among the spheres only (2/3), is equal to the joint probability of drawing a black sphere (2/10) divided by the probability of drawing any sphere from :the box (3/10). The result is hence 2/3. therefore

$$P_{b/s} = P_{bs}/P_s$$

$P_{b/s}$ is the probability of drawing a black sphere from the spheres only.
Pbs is the joint probability of drawing a black sphere from the box, and
Ps is the probability of drawing any sphere from the box. This is known as Bayes :theorem. If the probability of drawing a white sphere is Pws then

$$P_s = P_{bs} + P_{ws} = 2/10 + 1/10 = 3/10$$

Appendix 9

Human Error Rates

In general Reliability work, system MTBF calculations often take account of the probabilities of human errors. A number of studies have been carried out in the UK and the USA, which attempt to quantify human error rates. The following is an .overview of the range of error rates, which apply

These failure rates strongly affect the MTTR.

Possible task	**Read reason**	**Physical operation**	**Everyday task**
Fail to isolate supply		0.0001	
Read single alphanumeric wrongly	0.0002		
Read 5 letters word with good resolution wrongly	0.0003		
Read a checklist wrongly	0.001		
Set multi-position switch		0.001	

wrongly			
Wrongly carry out visual inspection	0.003		
Fail to correctly replace PCB		0.004	
Select wrong switch among similar		0.005	
Read analog indicator wrongly	0.005		
Read 10 digits number wrongly	0.006		
Leave light on			0.003
Read graph wrongly	0.01		
Do simple arithmetic wrongly	0.01 – 0.03		
Wrongly replace a part		0.02	
Put 10 digits into calculator wrongly	0.05		
Dial 10 digits wrongly		0.06	
Fail to recognize incorrect status during inspection		0.1	
New work-shift – Fail to check hardware first			0.1
Fail to act correctly after 1 minute in emergency situation		0.9	