ANALYSIS OF TELECOMMUNICATIONS OUTAGES DUE TO POWER LOSS

A thesis presented to
the faculty of
the College of Communication of Ohio University

In partial fulfillment
of the requirements for the degree
Masters in Communications Technology and Policy

Kavitha Chayanam

June 2005

This thesis entitled

ANALYSIS OF TELECOMMUNICATIONS OUTAGES DUE TO POWER LOSS

BY

KAVITHA CHAYANAM

has been approved for

the J. Warren McClure School of Communication Systems Management

and the College of Communication by

Andrew Snow

Associate Professor of Communication Systems Management

Gregory J. Shepherd

Interim Dean, College of Communication

CHAYANAM, KAVITHA. M.C.T.P. June 2005. Communication Systems Management

Analysis of Telecommunications Power Outages Due to Power Loss (120pp.)

Director of Thesis: Andrew P. Snow

ABSTRACT

This work presents an analysis of telecommunications outages in the US due to power loss, based on carrier reports submitted to the Federal Communications Commission. This analysis covers the outages due to power loss over an eight year period (1996 through 2003). Data collected from the reports included variables such as the date, time and duration of the outage and customers affected. A major conclusion is that the number of telecommunication power outages after the Sep 11/01 attack decreased. In addition, analysis strongly suggests that this reliability growth can be attributed to the telecommunication industry, rather than the power industry. The outage causes were categorized based on the trigger and root causes, in addition to identifying the component that is most closely associated with the root cause. The analysis indicates that many of the outages were caused by operations failures, or human errors. Outages also occurred due to either alarm system failure or insufficient response to the generated alarms. The analysis also indicates that many outages are due to violation of Network Reliability and Interoperability Council (NRIC) best practices, suggesting that the power outages can be further reduced if those best practices are implemented.

Approved:

Andrew Snow

Associate Professor of Communication Systems Management

Acknowledgements

With out the help and support of so many people it would have been very difficult for me to achieve my goal. I would like to take this opportunity to thank every one of them for their valuable support during my journey.

First and foremost I would like to thank Dr. Andrew Snow, Director of my thesis for his invaluable guidance and support through out the research. He has been very patient and provided me with valuable suggestions and motivated me all the time. I had many enjoyable discussions with Dr. Snow, and this helped me in analyzing and presenting my results more clearly. Working with him was a great pleasure and I will remain indebted to him for the time that he spent in explaining various things to me and helping me understand the scenario of an actual telecommunication complex.

I would like to thank my committee members Dr. Phil Campbell and Dr. Gary Weckman for their questions and suggestions during my presentations which helped me understand the importance of my research topic.

I specially would like to thank my parents and my brother for giving me words of encouragement during the time when I was down. I would also like to thank my colleague Shweta Agarwal, for her suggestions during the process of my research.

I have no words to thank for the help and support extended by Rajesh, a close friend of mine, during the times when I needed some words of care and encouragement.

Table of contents

List of Tables

List of Figures

Chapter 1: Literature Review

In the early 1990’s the Public Switched Telephone Network (PSTN) experienced many telecommunications outages and hence since 1991, the Federal Communications Commission (FCC) has required wireline telecommunications carriers to report large service disruptions. Since then, wireline telecommunications carriers have had to report service disruptions to the Federal Communications Commission that meet certain threshold requirements, such as those of at least 30 minute in duration and 30,000 customers affected [1] . These outage reports are known as FCC-Reportable outages. Outage reports include such information as the reporting carrier, location, date and duration of the outage, and the number of customers affected and the blocked calls.

The Network Reliability Steering Committee (NRSC) was established under the support of an industry association, the Alliance for Industry Telecommunications Solutions (ATIS). The NRSC was formed to analyze network reliability using FCC-Reportable outages. The NRSC provides an analysis of the reliability performance of the telecommunications network and releases quarterly summary reports and annual reports every year regarding this performance. The main objective of the NRSC in analyzing the outage reports is to observe any outage trends and distribute the results of its analysis to the industry and FCC. In addition, some matters are also referred to industry forums for further discussion [1]. The NRSC analyzes the reports in terms of the Facility outages, Local Switch outages, Common Channel Signaling outages, Tandem Switch outages, Digital Cross-connect System (DCS) outages, Central Office (CO) power outages. In addition, outages are analyzed in terms of the duration of the outages, customers affected, blocked calls and the frequency of outages [2] [3] [4] [5] [6].

Although the industry outage analysis by the NRSC gives significant information in the form of statistical data and the graphs which give a comparison of the outages for that particular year and that of the previous years [2], the analysis performed by the NRSC is somewhat superficial, in that it focuses on the summary statistics and trends more so than on the actual causality of the outages. Although the reports identify root causes, these classifications provide little insights into how to decrease the frequency of outages, one of the major responsibilities of the NRSC. Though the data is presented clearly, the analysis does not contain a detailed discussion of the root causes that are leading to the outages, other than the broad categories mentioned.

The Network Reliability and Interoperability Council (NRIC) is an advisory council to the FCC. The NRIC makes reliability and interoperability recommendations to the FCC and public telecommunications networks industry. The NRIC is actually the successor of Network Reliability Council (NRC) that was formed by FCC in 1992 after a major series of outages. The FCC established the council to study and analyze the causes of the telecommunications outages and to suggest recommendations that would reduce the outage number and their impact on customers [7].

In 1993, NRC published a compendium of technical papers in “Network Reliability: A Report to the Nation”, which made a wide range of recommendations to the carrier industry relating to reliability. These recommendations came to be known as the “Best Practices”. The NRC suggested that the industry should study and understand the proposed best practices and suggested that the proposed recommendations should be implemented in their companies in order to reduce outage frequency [7]. For wireline carriers, in the power category there are 99 best practices [8].

Some of the telecommunications outages were reported to the FCC during electric power grid blackouts. Blackouts affect many customers and result in power loss over wide geographic areas [9]. The Power grid in the United States is susceptible to small and very large blackouts. For instance, the blackout occurring in August 2003 started in the in the northeastern part of the Cleveland, and was the biggest in the history of United States [10] [11]. Blackouts are difficult to prevent and more and more blackouts are expected to occur. Since such blackouts cannot be completely eliminated, communication complexes must be able to operate on alternate power sources in such an environment. During the past, more blackouts occurred than predicted by statisticians [12].

A literature review of telecommunications power outages indicates very little research and analysis has been completed on power losses to telecommunications complexes and facilities. In order to reduce the frequency of telecommunications service disruptions due to power loss, research is required that will enhance understanding into this process.

Chapter 2: Introduction

2.1 Overview

Telecommunications outages occur due to many different reasons, one of which is loss of power to communications equipment. This study analyzes this special class of telecommunications outages from the year 1996 through 2003. This study is based on the information gathered from the FCC-reportable outages made by the wireline service providers. The analysis is made based on the frequency of power outages, date and time of the occurrence of power outages, customers affected, blocked calls, trigger causes, and root causes. As the outages involve the failure of a number of redundant power systems, the sequential events leading to the complete power failure are also investigated.

2.2 FCC Reportable Outages

Telecommunication service disruptions that meet certain thresholds are reported to the FCC by the respective service providers. Any outage that has affected more than 30,000 people for greater than 30 minutes must be reported to the FCC. Additionally, certain outages that do not meet this threshold considered to be 'Special Outages' must also be reported to the FCC. Special outages are those affecting major airports, 911 service, nuclear power plants, major military installations and government facilities [1]. The outages reported to the FCC must include certain information about the outage, including the date, time, duration of the outage, customers affected and the blocked calls due to the outage, the carrier's assessment of root cause and an assessment of best practices. The reports also contain the steps taken to restore customer service and also the precautions that have been taken to avoid any such outage in the future.

During the period from 1996-2003, there were 1,557 FCC-reportable outages. These outages can be attributed to a failure in switching, transmission, signaling capability, or loss of power to communications equipment. In about 10% of the cases, the outage resulted because of loss of power. This study considers all the telecommunications outages from 1996-2003 in which the service disruption was caused because of the loss of power to communications equipment, and are referred to as 'Power outages'.[1]

2.3 Power Outages

Power outages form a special class of the telecommunications outages. There are often several factors to be considered in analyzing these power outages. Power outages might occur because of the loss of the commercial alternating current (AC) power and the subsequent malfunction of backup power systems, or the failure of the other power related equipment such as the rectifiers, circuit breakers or the fuses that are connected between the power input and the communications equipment.

A communications complex has switching, transmission, and signaling equipment which require power. If the power to the equipment is lost then the equipment stops processing, transmitting, or signaling calls or data. Hence it is important that there are sources of backup power for the equipment. Without these backup sources, loss of commercial AC to the communication complex results in service disruption. In order to avoid such outages telecommunication complexes are provided with two backup power supplies, so as to supply the required power to the equipment in the event of commercial AC failure.

The typical communication complex is triply redundant in terms of power. The primary power source is commercial AC while there are two alternate power supplies

---

[1] This is different from the utility industry perspective where 'power outage' means loss of AC service to customers. Although the loss of power to communications equipment often begins with the loss of commercial AC, telecommunication facilities have a number of backup power sources.

– AC generator and batteries. In communication complexes, if commercial AC is lost, the generator is supposed to automatically start and provide AC to the complex. If the generator successfully starts and subsequently fails, (for reasons such as piston seizure, over heating of the engine, fuel depletion etc.), the load is then transferred to batteries. Also, there are cases where the generator fails to start due to the poor maintenance or due to fuel contamination. Battery capacity typically can supply power to the communication complex for 8 hours. Whenever there is a loss of AC power to the complex (commercial AC and/or generator failure), alarms are generated. If the complex is not staffed, the carrier Network Operations Center (NOC) must recognize the alarm and dispatch maintenance personnel to the site in order to fix the problem. In the mean time the batteries provide the power to the complex's telecommunications equipment. If AC is not restored before the batteries are depleted, the complex suffers a telecommunications outage. In some cases the batteries could not maintain the minimum required voltage levels, and protective mechanisms shut the equipment down. Problems such as these were first reported in [13].

In spite of most communication complexes being provided with redundant power supply systems (backup generator and the direct current, or DC, batteries), many telecommunication outages still occur due to power loss. The NRIC proposed best practices for the wireline network service operators and providers as a way to avoid or decrease telecommunication outages. In many instances, outages are seemingly due to industry not implementing best practices.

Power outages sometimes occurred because of maintenance and operations errors. There were some instances where either the telecommunications complex's alarm system failed to indicate the loss of power, or the failure of alarms to display at the NOC resulted in telecommunication outages. In these instances, the NOC was unaware of the critical situation and do not realize the problem until there is a complete loss of switching, transmission and signaling capability at the complex due to power loss. All critical equipment in the complex like batteries, generator, rectifiers and circuit breakers are connected such that their failure generates an alarm at the NOC. Then, the concerned personnel are dispatched to the site to rectify the problem before the generator ceases to function and batteries are depleted. Unless alarm systems are periodically tested, there can be no assurance that alarms will be generated at the NOC in the event of a failure.

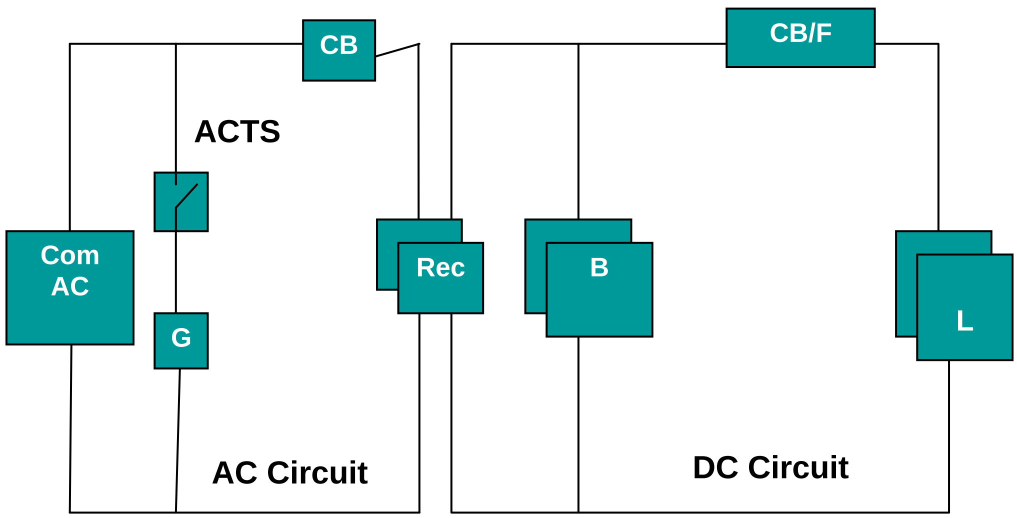
In other cases power outages were triggered by heavy rain, lightening and snow storms. In these instances voltage variations lead to power surges and resulted in the failure of the rectifiers or caused circuit breakers to open. A telecommunications outage can occur because AC loss results in the complex switching to battery power. If the circuit breakers are not manually reset before the batteries deplete, a telecommunication outage occurs.

Some other reasons for outage occurrences are human errors during maintenance activities. In some instances outages occurred when the maintenance personnel working in the communication complexes inadvertently dropped a tool on equipment in the complex, causing a short circuit in the power system.

Since this work involves the study of telecommunications outages that occurred because of power loss to equipment, all 1,557 outages reported to the FCC during the study period (1996-2003) are not considered. All these outages were reviewed and 150 of these outages were selected as telecommunications equipment power loss outages for further study.

2.4 Equipment Involvement

The power system in a communications complex is quite involved as the equipment typically runs on DC. The equipment in these complexes is interconnected in such a way so that when the commercial AC is lost, backup power supplies can provide power to all the telecommunications equipment in the complex. The typical power wiring diagram is shown in Figure 2.1. The power equipment consists of generators supplying AC power, batteries providing DC power, rectifiers providing DC power, circuit breakers, AC transfer switch and DC distribution Panel. The functionality of the power equipment in this diagram is explained below in detail.



Com AC:	Commercial AC	**Rec**:	Rectifiers
ACTS:	AC Transfer Switch	**B**:	Batteries
CB:	Circuit Breakers	**F**:	Fuse
G:	AC Generator	**L**:	DC Load

Figure 2.1: Power Wiring Diagram.

The power enters the complex in the form of AC. Almost all communication complexes are provided with AC generators as a backup to commercial AC. In case of failure of commercial AC, the AC transfers switch switches to the generator circuit after it senses the generator is producing nominal AC voltage levels. Most telecommunications equipment in a communication complex requires a DC voltage supply, so the AC power is converted to DC power by rectifiers. The rectifiers also trickle charge the batteries. These batteries provide the required DC power to the equipment in case of failure of both the commercial AC and the AC generator.

Although Figure 2.1 shows the typical power equipment connections generally found in a communication complex, there can be deviations. However these deviations are not always apparent from the outage reports. Throughout this study, the analysis is made based on the configuration shown in Figure 2.1. The functionality of each of the components involved is explained in more detail below.

a. ***AC Transfer Switch***

If commercial AC is lost, the generators are designed to start automatically and provide the AC power to the communication complex. Upon sensing loss of commercial AC, about 3-4 seconds is required for the generator to start and for the AC voltage to stabilize. Once this is accomplished, a switch brings the generator online. This switch is called the AC Transfer Switch. Some outages occurred because of the failure of the AC transfer switch to perform this critical function.

b. ***Generator***

The generator provides AC power to the communications complex in the event commercial AC power is lost. When this happens, the generator starts automatically and supplies power to the rectifiers. If the generator fails to start for some reason, then an alarm is generated and transmitted to the appropriate NOC and maintenance personnel come to check the cause of failure. The generator operates continuously until the commercial AC comes back online or until fuel is depleted or until it fails.

c. ***Circuit Breakers***

Circuit breakers (CB) are on-off safety devices whose job is to protect the complex whenever the current jumps above a safe level. These devices cut the AC power off to the complex if the current/voltage is too high. Fuses are infrequently used instead of circuit breakers, as they can only be used once. After a CB is tripped or fuse is blown, if the complex is not staffed, maintenance personnel must visit the complex to restore commercial AC power by resetting the CB or replacing a fuse.

d. __Rectifiers__

Rectifier circuits, sometimes referred to as inverters, are used to convert the AC power to DC for the communications equipment and to charge the batteries continuously so that they can supply the power to the communications equipment in case of AC power loss. Commercial AC enters the communication complex and is converted to -48V. Rectifiers also provide the functionality of smoothing any power surges such as those induced by lightning or thunderstorm. Thus they also protect the equipment from sudden changes in voltage or current.

e. __Batteries__

Batteries provide the -48V DC power to the equipment if the rectifiers fail to do so. In general, enough batteries are provided to sustain the complex for 8 hours. In many instances telecommunication outages have occurred because the batteries were completely exhausted before AC is restored. In other cases, outages occurred because the batteries could not maintain the minimum DC voltage level required for the equipment to operate. Batteries also perform one additional function. As mentioned before, when a loss of commercial AC occurs, it takes 3-4 seconds for the AC transfer switch to transfer the power source from the commercial AC to the generator. During these 3-4 seconds the batteries have to supply the power to the complex.

f. __DC Distribution Panel__

A DC distribution panel is used to distribute DC power safely from the rectifiers/battery bank to the communications equipment. Individual DC circuits are routed to individual equipment. Each DC circuit is protected by either a fuse or a CB.

Fuses/circuit breakers are chosen depending upon the amount of current drawn by the equipment. These fuses and breakers blow/open if excess DC power conditions occur. The main purpose of these devices is to insure communications equipment is not damaged.

Alarms are installed such that when power or communications equipment fails, the failure is detected and an alarm is generated locally, and at the appropriate NOC. If the facility is not staffed, maintenance personnel are dispatched to the location to fix the problem. Alarms should be in place to monitor the generators, batteries, AC transfer switch, rectifiers and the CB. There are instances in which the alarm system at the complex is not operative, and as the power loss is undetected, a telecommunications outage results.

Chapter 3: Research Questions

The purpose of this research is to analyze the power problems that resulted in reportable telecommunication outages. Outages reported from 1996-2003 are considered in order to understand this aspect of critical infrastructure vulnerability. One goal is to infer if there is any reliability growth or deterioration in power related outages over the study period. Another goal is to investigate the causality of power outages reported during the 1996-2003 timeframe. Each power outage report has been examined and data such as the number of lines affected, the number of blocked calls, the total customers affected, and the duration of the outage is collected. Research questions considered for this analysis of the power outage reports are as follows:

Research Question 1

Can distributions be fitted to duration, customers affected, blocked calls, and total number of customers affected?

Fitting distributions to these variables provides their mean and variance. Knowing the distribution for each variable provides insights into the chance that the variable will exceed a certain size, given the occurrence of an outage. The total customers affected is a function of customers affected and blocked calls, which will be discussed later.

Research Question 2

Are there any seasonal effects in the reported outages?

The trigger causes for power outages vary substantially. Some of the power outages started due to lightning, thunderstorms, torrential rains, tornados, hurricanes, snow storms and flooding incidents. As such, the data should be examined for seasonality and periodicity. This analysis would be helpful in understanding power outages and whether seasonal precautionary measures would be fruitful.

Research Question 3

How strong an inference can be made regarding observed reliability growth, and is this reliability growth related to Sep 9-11?

The data obtained from the outage reports indicates that the number of power outages decreased over the study period. A visual examination of a cumulative outage count over time indicates a deceleration of outage events near 9-11. This indicates there may statistically significant reliability growth, and if so, it would be logical to investigate whether this reliability growth is a statistically linked to the September 11/01 attack.

Research Question 4

Can power outages be categorized in a way to provide helpful insights?

The power related outages occurred for a variety of reasons and circumstances. However, there are undoubtedly some power outages that occurred because of similar reasons. Some outages may have followed a similar or the same sequence of events leading up to the outage. Outages might be grouped together and analyzed by group. In addition, the number of outages in each group could point to the relative importance of these groupings, and where additional effort might be expended to improve.

Research Question 5

What are the different root causes and their frequencies (Root Cause Failure Analysis)?

It would be advantageous to know the root causes of various outages and the type of equipment failures involved in the outages. This can help us understand the circumstances that led to the power outage. Understanding and analyzing root causes provides an idea as of why the outage has occurred, so that preventive steps can be taken to decrease the frequency of outages.

Research Question 6

Are the causes of the high impact outages same as the low impact outages?

The customers affected in the reported telecommunication outages ranged form the hundreds to millions. In addition, outage duration ranged from fractions of hours to days. The outages that affected larger number of customers or those that lasted very long can be termed as the high impact outages. On the other hand, outages that affected few customers and those that lasted for few minutes can be termed as the low impact outages. The study of the causes for both the high impact and low impact outages would help to understand any differences associated with why the outages occurred.

Research Question 7

To what extent are deviations from the 'Best Practices' involved in power outages?

Under the power category, NRIC proposed 99 best practices for wireline telecommunications service providers and network operators. Industry should follow these best practices in order to avoid outages. By analyzing the root cause of the incident that has resulted in the power outage, a conclusion could be drawn if the industry is following the best practices as proposed by NRIC. This research question would help in investigating if deviations from the 'best practices' by the industry are contributing to the number of power related outages. Also, this analysis might indicate which best practices were violated more frequently.

Chapter 4: Methodology

4.1 Overview

This chapter presents the methodology used to reduce and analyze the data so that the research questions could be addressed. From the year 1996-2003, there were 1,557 FCC reportable outages. These outages were reviewed to identify which were primarily caused by power loss. Of the 1,557, 150 were identified as being power loss related. Each of these power outages reports were analyzed in detail, and the data reduced and coded. This data was captured in excel spreadsheets. Most reports provided information very clearly but some outage reports were very unclear with minimal information. The analysis is made based on assumptions which are detailed in section 6.2 of chapter 6.

4.2 Preliminary Data Analysis

Both the total number of outages and those attributed to power appear to have decreased over time. The table below shows a listing of the total number of outages reported from 1996 – 2003 and the number of Power outages in each year.

Table 4.1: Total Outage count and the Power outage count (1996-2003).

Year	**Total number of outages**	**Power Outages**
1996	**219**	19
1997	**222**	24
1998	**218**	22
1999	**230**	20
2000	**224**	27
2001	**200**	18

Table 4.1 Continued

2002	**137**	8
2003	**107**	12

A plot of the cumulative number of power outages over the study period is shown in Figure 4.1. This curve provides a visual indication of reliability growth, wherein the frequency of outages decreased over time. Near the end of the study period, a cluster of 6 power outages can be seen that occurred at the same time. These outages occurred during the August 2003 blackout in the North Eastern part of United States.

As mentioned earlier, data was collected from the reports made over the 8 year study period. This data included the number of customers affected per outage, number of blocked calls per outage, the date and time of the outage, and its duration. A variety of cumulative and time series plots for these data are shown in Appendix 1, 2 and 3.

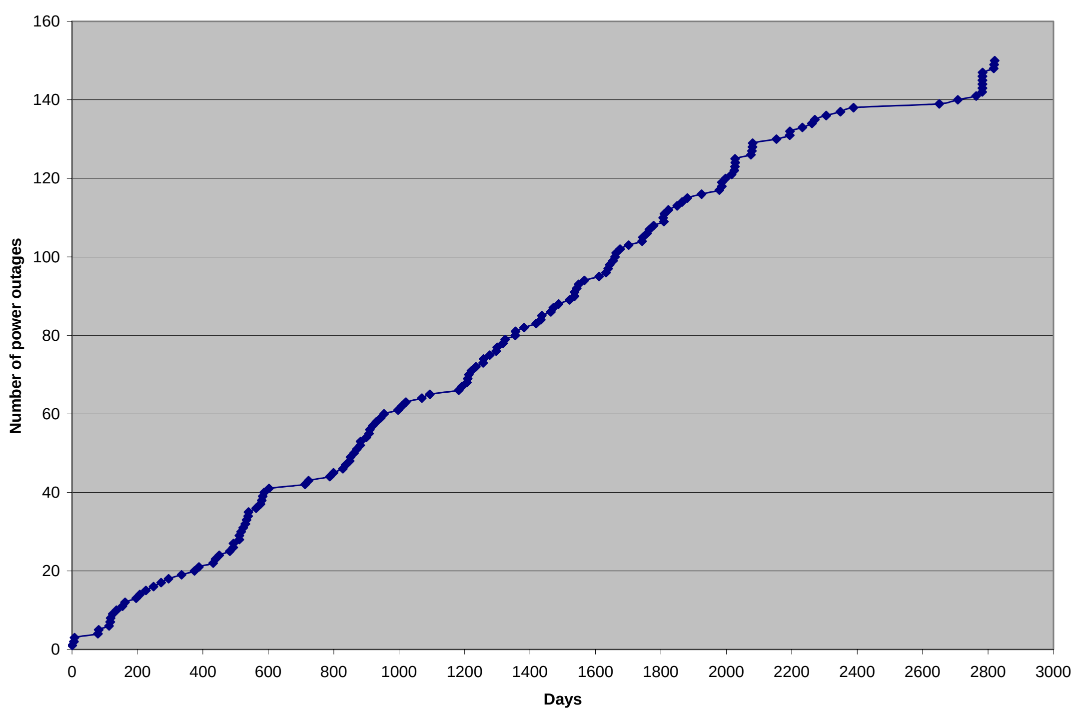


Figure 4.1: Cumulative power outage count Vs time period from 1996-2003

4.3 Fitting Distributions to Variables

A commercially available software application called 'Best Fit' Version 4.5.3 was used for frequency distribution analysis.

4.3.1 Best Fit

Best Fit checks the data to be fitted against 28 different distribution functions and determines maximum likelihood estimators (MLE) for each distribution under test. Best Fit then uses four different statistics to measure goodness of fit: chi-squared, Kolmogorov-Smirnov, Anderson-Darling and Root-Mean Squared Error [14]. For a data set, Best Fit ranks all the fitted distributions using one or more fit statistics. The statistics indicate how good the distribution fits the input data set. The data sets for the previously mentioned variables are analyzed using Best Fit.

4.3.2 Empirical Frequency Distribution

Frequency Distribution is a very powerful tool for organizing data in a way that provides insights into the variation of data. The frequency distribution data are plotted for the duration in minutes, total number of customers affected[2] and the number of blocked calls[3].

The total number of customers is obtained from the variables: customers affected and blocked calls. This value can be obtained using the formula:

Total customers affected = Access lines (Customers affected) + Blocked calls/3. (1)

---

[2] Total customers affected give the actual number of customers potentially affected during the power outage.

[3] Blocked calls that were generated during a power outage indicate all the attempted calls that could not connected due to loss of communication capability.

Access lines can be defined as the actual number of lines that run from a central office to the customer's home. The term blocked calls/3 comes into the picture since it's a general human tendency to try a call for a maximum of three times in case they get a busy signal. This is a common industry method of estimating the number of customers affected.

In the outage reports made to the FCC, there is specific mention of the customers affected or the customer access lines affected. They both mean the same. There is also a mention of the blocked calls that were generated during the outage. All these variables can be substituted in the above formula to obtain the total number of customers that were affected during the power outage.

4.4 Laplace trend test

The Laplace trend test is performed to statistically infer if any trend is present in a set of time series data [15]. This test is given by [16]:

$$U = \frac{(\Sigma t_i - 0.5 * n * t_0)}{t_0 * \sqrt{n/12}} \tag{2}$$

i= 1, 2, 3, …..n;

Where, n is the number of events, t_0 is the total time of the observation period and t_i is the time each outage event started. The test statistic U is a Z-score and is normally distributed with mean equal to zero and standard deviation equal to 1. The null hypothesis is that there is no trend. Based on the value obtained for U the hypothesis is tested as follows.

- U = +1.96 means reject no trend, infer reliability deterioration alpha=0.05.
- U = -1.96 means reject no trend, infer reliability growth alpha=0.05.

Large positive values of U means that the cumulative of the power outage times tend to occur towards the end of the time interval and this shows reliability deterioration of the process. Large negative values of U indicate that there is a reliability improvement. Smaller positive and negative values mean that the hypothesis of no trend cannot be rejected.

In this study the values of n, t_0 are 150 and 8 years respectively. Since there are n events there are 150 different values of t_i corresponding to each event.

4.5 Fourier analysis

Fourier analysis can be used to investigate periodicity in time series event data. When a Fourier analysis is performed on that data, a series of mathematical terms called harmonics are obtained. Each of the harmonic terms has a sine or cosine component as a part of the value of that term. Each harmonic term has amplitude that gives an idea of how large the effect is of that term. Harmonics plotted by time are called a power spectrum.

Considering the power outages from 1996-2003, 150 data points were used for plotting the power spectrum. A plot of the power spectrum from the Fourier analysis is shown in Figure 4.2. From the graph shown below it can be clearly seen that there are no major spikes that could be observed and hence it is inferred that there is very little or no periodicity/seasonality in the power outage data. A very small spike is observed around 100 days, but the amplitude is not strong enough to conclude any periodicity.

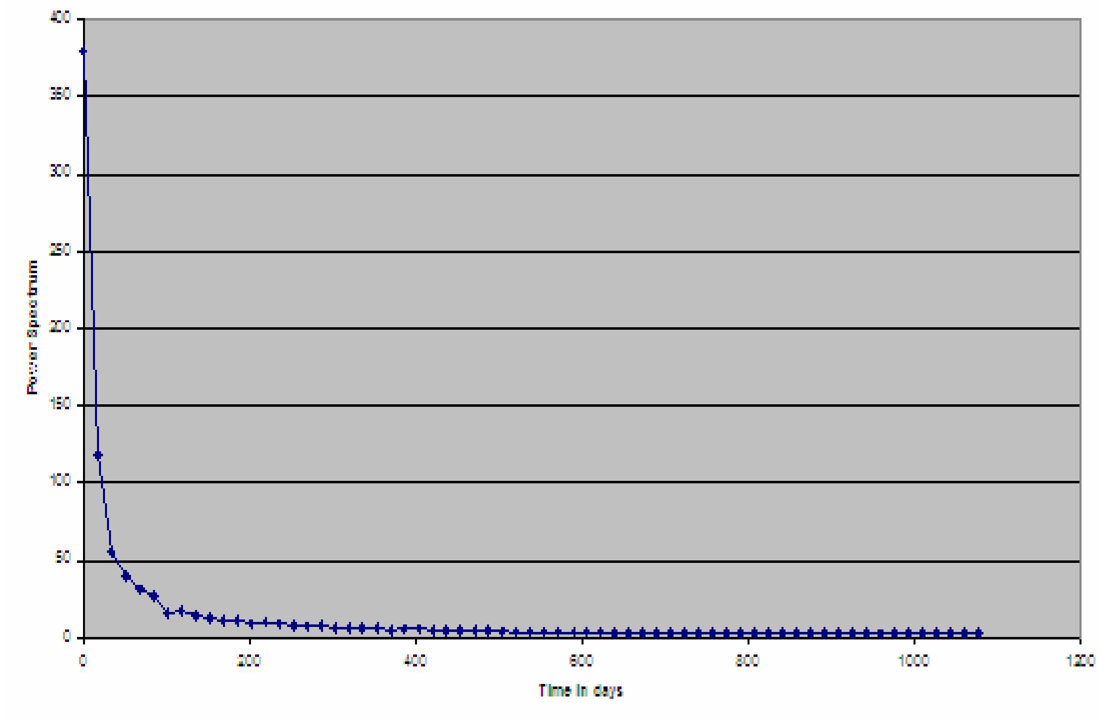


Figure 4.2: Power Spectrum vs. time in days using Fourier analysis.

4.6 Poisson Model

Outage data can also be sorted into count data, or events per time period (e.g. month or quarter, or year) which can be analyzed for reliability relationships. The power outage count can depend on one or more explanatory variables. To find out if the explanatory variables have an impact on the power outage count, the Poisson model can be used to find out how the outage rate varies with time. Potential explanatory variables in counts can be analyzed using Poisson regression [17], given by:

$$\log(\mu_i) = b_0 + b_1 \log(X_1) + b_2 \log(X_2) + b_i \log(X_i) \qquad (3)$$

Where μ_i is the expected count, b_0, b_1, …b_i are the constants associated with the explanatory variables X_1, X_2… X_i , respectively.

The software used for Poisson Regression is Mac ANOVA (Macintosh Analysis Of Variance), which was originally developed by the University of Minnesota, for an Apple environment [18]. This software is also available for PC environments. It has a command line interface and the functions used for the Poisson regression are explained in Appendix 5.

The empirical count data for the Poisson regression given above was shown in Figure 4.1. That figure shows a plot for the cumulative number of power outages vs. the time period in days. From the figure it is clear that it would be possible to investigate a piece wise linear model with a break point, as discussed in section 4.7.

4.7 Piecewise Linear Model

A break point indicates a particular point of time when the frequency of the power outages abruptly changes. This reliability growth phenomenon can thus be analyzed using the piece wise linear model. The Piecewise linear model, seen from Figure 4.3, can be investigated with Poisson regression. The Poisson model looks for a break in outage arrival rate, $\lambda(t)$.

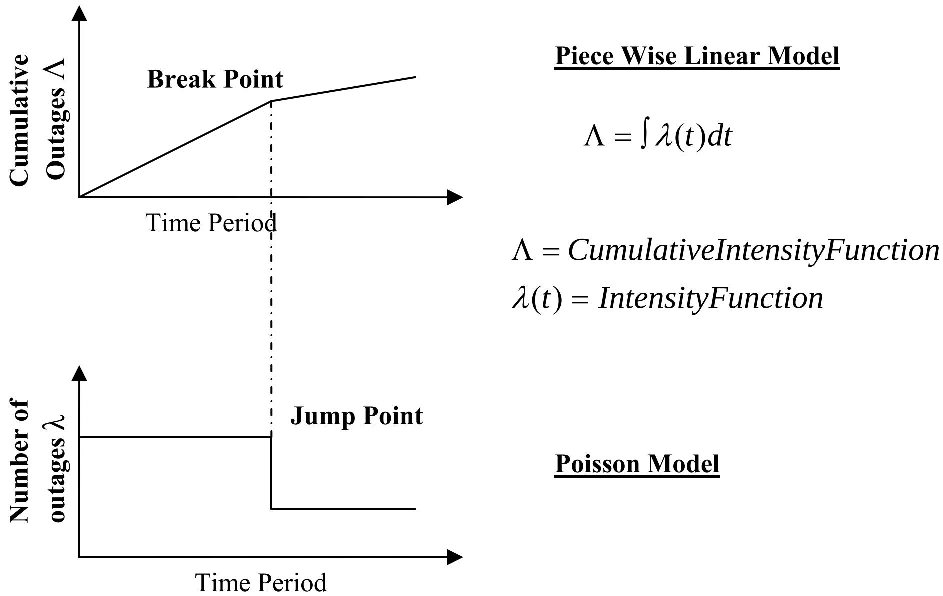


Figure 4.3: Piecewise Linear Model and the Poisson Model.

The Piecewise Linear Model [19] segments the data into intervals based on a suspected statistically significant break point found using the Poisson Regression. The model can segment the data into any number of intervals to determine the most likely breakpoint. Our hypothesis is that the breakpoint occurs right after the September 11/01 attack. The break point can thus be investigated using Poisson regression by considering the explanatory variables of the Poisson Model to be:

X_1 = Power Outage count per time period.
X_2 = Binary variable

{ = 0; For all the power outages before September 2001.

{ = 1; For all the power outages after September 2001.

The analysis consists of computing the count (total number of power outages per quarter) and then assigning a dummy variable with values 0 for outages up to, and including, the fourth quarter of the September 2001 and a value of 1 to all the outages after the September 2001 quarters. Poisson Regression will provide statistical evidence to accept or reject the piecewise linear model.

4.8 Power Law Model

The power law model is also called the Weibull reliability growth model [20]. This model may be appropriate as it is a commonly used infinite failure model [21]. This process is a Non Homogenous Poisson Process (NHPP), as is the Piecewise linear model, and has the intensity function given by the equation shown below.

$$\lambda(t) = \frac{\beta}{\theta}\left(\frac{t}{\theta}\right)^{\beta-1} \qquad (4)$$

The parameter β affects how the system deteriorates or improves over time and is depicted clearly in Table 4.2. Consider two cases when β is greater than one and a case when β is less than one. When β is greater than one the intensity function increases which indicates that the failures tend to occur more frequently. When β is less than one the intensity function decreases indicating that the system is improving. When β is equal to one, the intensity function reduces to a homogenous Poisson process that has a constant arrival rate with value equal to 1/ θ, where θ is a scale parameter. For the time series data the MLE's for β and θ are given by the following equations.

$$\hat{\beta} = \frac{n}{\sum_{i=1}^{n} \log(t_n / t_i)} \quad \text{and} \quad \hat{\theta} = \frac{t_n}{n^{1/\hat{\beta}}} \qquad (5)$$

Table 4.2: Relation Between β and the intensity function.

β	Intensity Function	Inference
>1	**Increases**	System is deteriorating.
<1	**Decreases**	System is improving

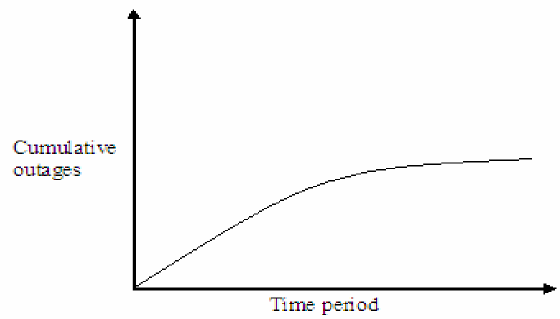


Figure 4.4: Power Law Model.

4.9 Outage Causes

The reasons for the power loss outages are manifold. There is no one particular reason why an outage occurs; rather the outages trigger a sequence of events that leads to service disruption, thus defeating triply redundant power (commercial AC, AC generator, and batteries). These reasons can be human errors, power surges, natural disasters or equipment failure. These trigger causes however provide little insight as to why the outage has occurred. To understand the reason why outages occur requires root cause analysis.

Hence, for understanding an outage in detail, the outages had to be analyzed further based on the trigger cause, direct cause and the root cause. The trigger cause of an outage is defined as the cause that initiates the sequence of events that finally resulted in an outage. The direct cause of the outage can be defined as the final event in the sequence of events that lead to the outage. The root cause of the incident gives an insight of why the outage occurred, and provides insights into how to avoid such outages in the future. An outage's root cause can be determined through a technique called Route Cause Analysis (RCA) [22], which is explained below.

The RCA technique is used to find out the real cause of the problem and to indicate how to minimize the chance of such problems reoccurring [23]. This technique is useful where outages result from the same type of problems [24].

A root cause analysis of all the individual power outages can provide insights into what actually happened and when it has happened [25]. RCA involves analyzing the events logically by asking a series of why and what questions until all the factors that have contributed to an outage are better understood. This analysis helps in recognizing changes that should be made in order to improve the system performance [26] [27] [28]. This analysis also is useful in identifying all the associated factors of an outage and in considering design changes that could reduce the frequency of power outages. Examples of RCA analysis are given in the following cases.

Case 1:

A lightning strike resulted in a commercial AC power surge, causing the main circuit breakers to trip open, terminating the flow of AC to the facility. This means that AC from either the primary or backup source cannot be converted to DC. As a consequence, the batteries must supply power until the rectifiers are manually switched back on line. The alarm system does not work properly, and the NOC is not notified of the problem. After some time the batteries are exhausted and the communications equipment looses power, and an outage occurs.

- Trigger Cause: Lightning strike.
- Direct Cause: Battery Depletion.
- Root Cause: Failure of alarm system.

Case 2:

Torrential rains and flooding due to a tropical storm in Houston causes commercial AC power failure. The generators in the communication complexes are supplied with fuel from the supply pumps that are located in the basement of the building. Due to the flooding, water entered the basement causing the failure of supply pumps. Hence, the generators did not have any fuel supply and they stooped functioning. Hence, the communication complex was on the power supplied by the batteries. To conserve battery power the equipment was placed in a simplex mode. Placing the equipment in the simplex mode means that that the cooling system for the equipment is switched off. After some time, the batteries stopped supplying power to the equipment thus resulting in an outage.

- Trigger Cause: Storms (Flooding).
- Direct Cause: Battery depletion (failure).
- Root Cause: Human Error due to engineering failure (The pump system which was supposed to supply fuel to the standby turbine engines was placed in the basement).

Case 3:

Some outages occurred due to the failure of the AC generator. Outages have occurred when power was lost to the complex and the generator started supplying power to the load. However, after some time, the generator stopped functioning due to reasons such as over heating, piston seizure etc. After generator failure, batteries could hold the required voltage levels only for a few minutes. This was due to the improper connection of the battery strings. So, the batteries, instead of supplying the power for 8 hours as per their design, supplied the required power levels for a much shorter time. When the batteries failed to provide the required power levels to the equipment, an outage resulted. In this case, the alarms did not notify the NOC about the failure of the

AC generator and hence the no maintenance personnel were sent to the site to fix the problem.

- Trigger Cause: Failure of commercial AC power.
- Direct Cause: Failure of batteries.
- Root Cause: Failure of the alarm system.

Case 4:

Outages also occurred because of installation errors. In some instances blown fuses in the DC distribution system resulted in loss of DC power to communications equipment. In this case, equipment was added to individual DC circuits without increasing the necessary fuse capacity.

- Trigger Cause: Improper fuse specification.
- Direct Cause: Blown fuses.
- Root Cause: Human error due to installation failure

Case 5:

The power outages also occurred because of improper training. In one instance, a wrench dropped by a maintenance worker landed on an exposed DC power bus which shorted out. Maintenance personnel error can be reduced by providing sufficient training to personnel. Exposed power buses should be covered before maintenance activity starts.

- Trigger Cause: Dropping a tool.
- Direct Cause: DC short circuit.
- Root Cause: Human error due to maintenance failure

Case 6:

Outages also occurred during, or in preparation for, scheduled commercial AC power outages. To make sure that the generator is functioning properly, a routine check should be made on a periodic basis. During this routine the commercial power supply is intentionally removed. This should result in the generator coming online and taking the entire AC load. In one outage report, during such a test, the AC transfer switch malfunctioned and the generators could not supply the power, placing the site on battery backup power. After some time the plant was in a low voltage condition. The low voltage alarm was not received at the NOC and so, after the batteries were depleted, an outage resulted.

- Trigger cause: Failure of AC transfer switch.
- Direct Cause: Battery depletion.
- Root Cause: Failure of Alarm system.

As seen from these cases, outage summaries must be studied to identify trigger, direct, and root causes. This analysis should provide better understanding of why the outage has occurred and what can be done to prevent like occurrences.

4.10 Sequencing Power Outage Events

A reportable power outage is the result of a sequence of events. Event sequencing gives a clear idea of the chain of events leading to the outage. Event sequencing can be displayed on reliability diagrams, as shown in the incidents depicted in Figures 4.5 and 4.6.

Failure of commercial AC power itself is not a valid reason for the occurrence of an outage, as communication complexes are provided with backup power. One of the reasons for outage occurrence is the case where the back up power supply fails to provide the required power upon the loss of commercial AC. Other reasons occur in spite of the proper functioning of the generator and the batteries, rectifiers fail or circuit breakers trip.

Two representative examples of event sequencing are shown in Figures 4.5 and 4.6. What must be kept in mind is that power loss to equipment must last at least 30 minutes before the outage is reportable.

<u>Sequencing Case 1:</u>

The diagram shown below has the sequencing which indicates that the commercial AC power first failed. Although the generator operated properly, the rectifiers were damaged by the commercial AC failure. Since the rectifiers failed, even though the generator was working properly, no DC power could be generated. The batteries supplied the required DC voltage levels until they were depleted. The information provided in the outage report did not indicate how the rectifiers were eventually restored.

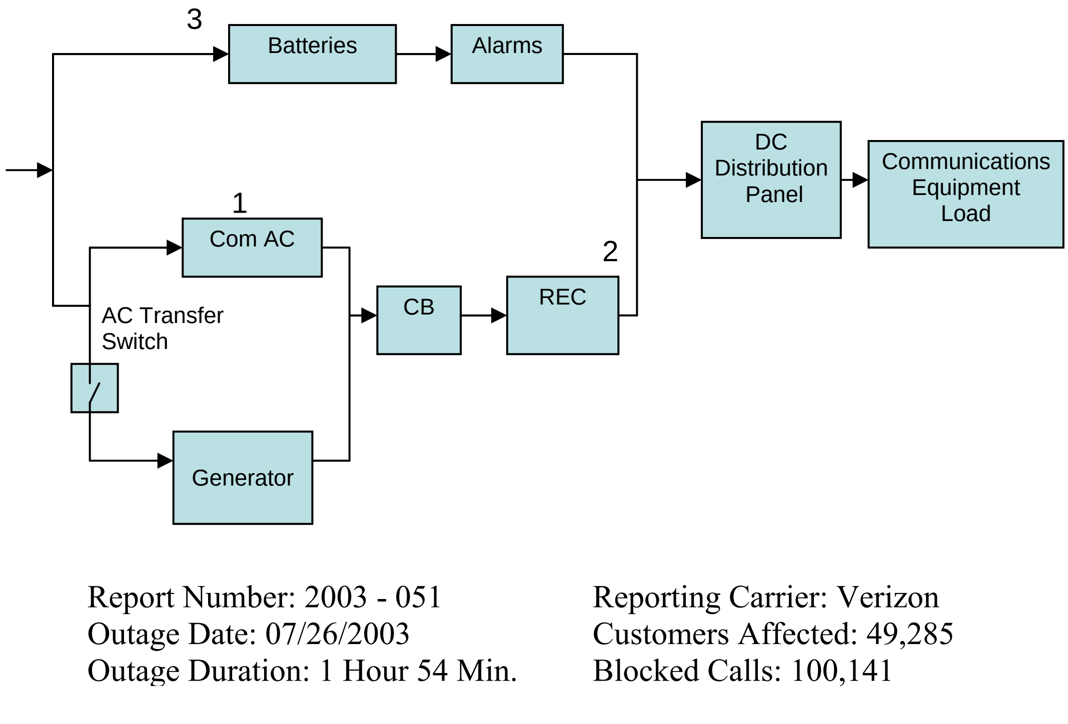
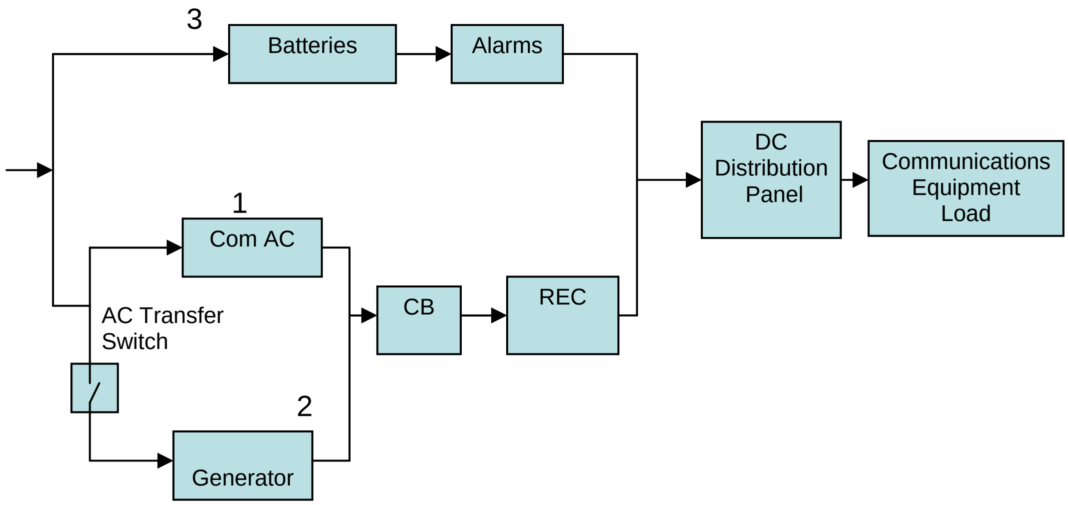


Figure 4.5: Sequencing of events: Example 1.

Sequencing Case 2:

The figure shown below has the sequence wherein the commercial AC is first lost, followed by the AC generators and finally the batteries. The commercial AC was lost due to a heavy thunderstorm and the backup emergency generator started supplying the power to the site. After some time the back up generator was shutdown because of a piston seizure. The site was now on the DC power supply from the batteries and after some time the communications equipment shut down when the DC voltage dropped below the minimum equipment rating.



Report Number: 1998-136
Outage Date: 08/11/1998
Outage Duration: 46 Minutes

Reporting Carrier: SBC
Customers Affected: 38,185
Blocked Calls: 225,476

Figure 4.6: Sequencing of events: Example 2.

4.11 Outage Categorization

As mentioned in section 4.9, an outage can be best described by its trigger cause, direct cause and the root cause. Some of the outages can have similar causes. It would be useful to gain additional insights by outage grouping based on the similar trigger, direct, and direct causes. However, direct cause of a power outage does not seem to provide much insight into why the outage has occurred. It only provides the information of the final event in the sequence of events that resulted in the power outage. For almost all power outages, the direct cause is the failure of batteries or the failure of the circuit breaker/fuse bay. This does not help much in analyzing the power outages. Hence, power outages are categorized and grouped together based on their root causes and trigger causes.

From the study of the power outage reports, the four trigger cause categories are identified:

1) Natural Disasters
    - Hurricanes
    - Tornado
    - Flooding
2) Power Surges
    - Improper AC electrical distribution.
    - Improper DC electrical distribution.
3) Loss of commercial AC
    - Scheduled
    - Unscheduled
4) Human Errors

All outages had trigger causes in one of these four major categories. There are also subcategories identified. Outages due to natural disasters include the cases in which the outages are triggered by hurricanes, flooding and tornados. Loss of commercial AC can either be scheduled or unscheduled. In some cases the commercial AC power is removed intentionally in order to conduct routine tests to make sure that the backup power supplies are functioning properly. Outages occurring in such situations are classified in the subcategory of scheduled outages. Some of the power outages occurred due to power surges, such as those induced during lightning strikes. Power arrestors or surge suppressors should be in place to suppress any sudden changes in the current or voltage, thus preventing damage to the power or telecommunications equipment in the complex.

Some of the power outages were triggered due to human errors. In one instance, the technician working on the fuse bay removed the wrong fuse. This power outage has the trigger cause as human error and hence comes under the human errors category.

Root causes can be classified as being related to human error or unforeseen circumstances:

- Engineering Errors
- Installation Errors
- Maintenance Errors
- Operations Errors
- Unforeseen Circumstances

An example of engineering error is the case where the central office power equipment was designed to be located in the basement of a building that is prone to flooding. Installation error includes the cases such as where the alarm system is improperly installed (e.g., improper wiring). An example of maintenance error includes the cases when water leaks into the building because of poor roof maintenance. Failure to recognize and respond to the alarms generated is an operations failure. An example of unforeseen circumstances includes the case of September 11/01 terrorist attack on twin towers in New York. The commercial AC was lost due to the collapse of the building. The generator failed to start thus triggering the battery backup to supply power. The batteries eventually exhausted after some time. Since the area was completely sealed off, no personnel were allowed to enter that area thus restricting any restoration activities.

Analyzing all the power outages and categorizing them based on the root causes, and the component most associated with the root cause, helps in understanding the preventive actions necessary to ensure similar mistakes are not repeated.

The components that are most closely related to the root causes are listed below.

- Rectifiers
- Batteries
- Generators
- Circuit Breakers
- Communications equipment
- Fuses/Fuse panel
- Commercial AC
- AC Transfer switch
- Alarm System
- Environmental Systems

Environmental Systems include the air conditioning system. Almost all the equipment is kept in a place that is not affected by any outside environmental changes. In case of failure of the environmental systems, generators (if inside) or rectifiers might get over heated and could stop functioning. Hence, environmental systems can also be associated with the root cause of an outage. The details about the other above mentioned equipment was discussed in detail in chapter 2, section 2.4. Thus, these components play an important role in RCA.

4.12 Alarm Analysis

From the FCC outage reports it is quite clear that some power outages relate to the alarm systems. The alarm system was not placed in all branches of the reliability diagram because if the alarm system fails, and all other components operate properly, no outage occurs. However, as the alarm system plays a role in a number of power outages, it receives special treatment here. Alarm system problems can be an engineering, operations, and installation or maintenance failure.

Alarms are wired to all the major power equipment in the communications complex. They are wired such that if any component fails to perform its function, the alarm system senses the non operation of the equipment. Then an alarm is generated locally and transmitted to the NOC. Alarm systems operate on separate battery backup power in the event of DC power loss to the complex. The following diagram shows how the alarms are wired to all the major power equipment in the complex.

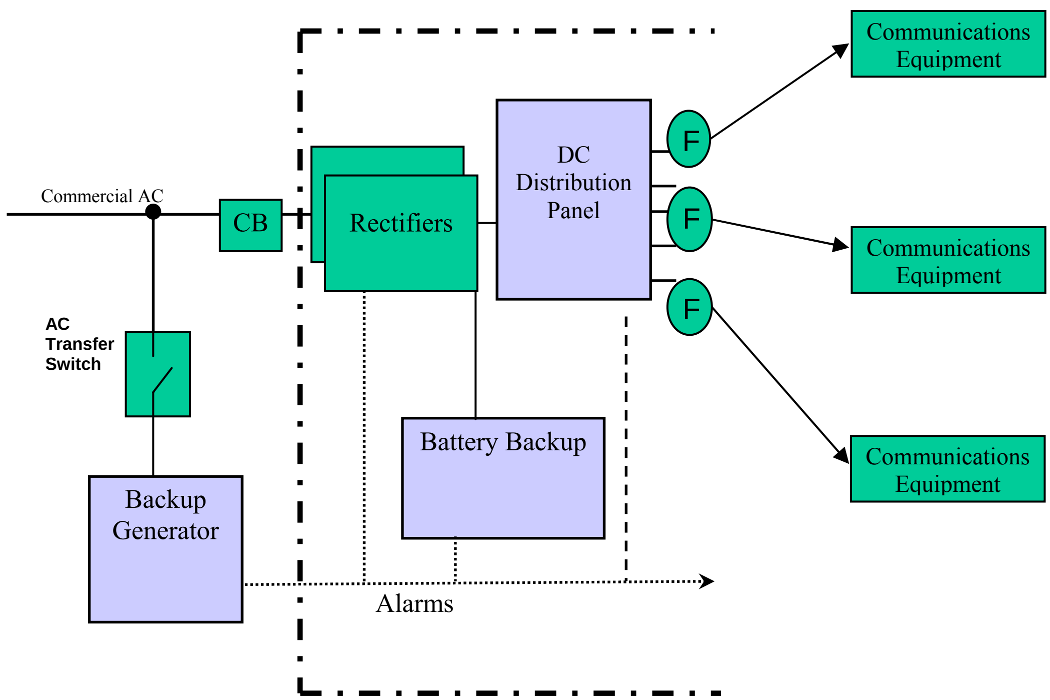


Figure 4.7: Alarm System Connections.

Engineering problems include the cases where the alarms are not provided at a complex, or where incremental designs/additions to the site are not connected to existing alarm equipment. In these cases, no indications of any failures are made, and the NOC hears about outages from customers. This is especially problematic at un-staffed sites. This naturally increases the duration for which the outage otherwise would have lasted. In fact, if the repairs could be made in within 30 minutes, the outage would not be reportable.

Operations problems include the situations in which the alarms work properly and generate an indication that power or power equipment has failed. However, the personnel at the NOC either ignore the alarm, or do not recognize the gravity of the situation. This is a serious problem because consider the example where the NOC receives an indication for the failure of the generator. The personnel at the NOC simply ignore or misinterpret the alarm. Since the generator failed and commercial AC is down, the site is on battery backup. If commercial AC or the generator is not restored within 8 hours, an outage occurs which must be reported if maintenance personnel do not arrive to correct the problem within 30 minutes of battery depletion. The staff at the NOC should be provided sufficient training to recognize alarms.

Installation problems include the instances when alarm connections are not properly made and tested. All the connections should be verified to make sure that when equipment fails the corresponding alarm is generated at the NOC. Maintenance problems include cases where the alarm systems at the sites are not tested at regular intervals of time to make sure that they are functioning properly.

Hence, the outages that occurred due to the failure of an alarm system or to insufficient response to alarms can be categorized as:

- Engineering problems.
- Operations problems.
- Installation problems.
- Maintenance problems.

This categorization would thus be helpful in understanding what role the alarm system played in the root cause of the outage.

4.13 NRIC Best Practices

NRIC proposed a variety of best practices for service providers and network operators [8]. By following these best practices, the severity and frequency of outages could be decreased. From the information in the FCC reported outages, an analysis might provide insights into the degree to which best practice violations are involved in power outages. There are 99 best practices suggested by the NRIC that are associated with power for wire line carriers. It would be quite interesting to note that the outages occurred even after equipping the communications complex with a triply redundant power supply.

For example, one of the best practices as proposed by the NRIC is that the service providers should maintain the power alarms by testing them regularly on a scheduled basis. However, many outage reports indicate that the root cause is the failure of the alarm systems. This shows that some service providers are not following best practices proposed by the NRIC. Such outages might be avoided by regularly testing alarm systems. The degrees to which best practice violations are associated with power outages have been analyzed.

Chapter 5: Findings

This chapter presents the results of the analysis performed on the power outage data, using the methodology explained in Chapter 4.

5.1 Fitting Distributions to Variables

Distributions are fitted to the outage variables (blocked calls, customers affected, total customers affected, and outage duration in minutes). Best Fit software and the frequency distribution technique are used for this analysis. The results are shown in sections 5.1.1 and 5.1.2.

5.1.1 Best Fit

As mentioned in section 4.3.1 chapter 4, distributions are fitted using the Best Fit. The results of the fit are shown in Table 5.1.

Table 5.1: Results of Best Fit: Probability Distribution Functions.

Variable	Distribution	Associated Parameters	Parameter Values
Blocked calls	Inverse Gaussian	μ= Continuous parameter λ= Continuous parameter	μ= 707,910 λ= 1,861
Customers Affected	Pearson5	α= Continuous shape parameter β= Continuous scale parameter	α= 1.44 β= 73,948
Total Customers Affected	Pearson5	α= Continuous shape parameter β= Continuous scale parameter	α= 1.23 β= 89,437
Duration in minutes	Pearson5	α= Continuous shape parameter β= Continuous scale parameter	α= 1.37 β= 167.3

The Inverse Gaussian distribution [29] was the best fitted distribution for blocked calls. The density function and cumulative functions are given by the following equations [30]:

Inverse Gaussian Functions:

Density function:

$$f(x) = \left[\sqrt{\frac{\lambda}{2\pi x^3}}\right] e^{-\left[\frac{\lambda(x-\mu)^2}{2\mu^2 x}\right]} \tag{6}$$

Cumulative function:

$$F(x) = \phi\left[\sqrt{\frac{\lambda}{x}}\left(\frac{x}{\mu}-1\right)\right] + e^{2\lambda/\mu}\phi\left[-\sqrt{\frac{\lambda}{x}}\left(\frac{x}{\mu}+1\right)\right] \tag{7}$$

From the Table 5.1 it can be noted that for all the other variables, customers affected, total customers affected and the duration in minutes, the Pearson5 distribution is best fitted distribution function.

Pearson5 Functions [18]**:**

Density function:

$$f(x) = \frac{1}{\beta\,\Gamma(\alpha)} * \frac{e^{-\beta/x}}{\left(x/\beta\right)^{\alpha+1}} \tag{8}$$

The Cumulative function F(x) has no closed form.

Figure 5.1 shows the Inverse Gaussian distribution cumulative plot, compared to blocked calls data from Best Fit. Cumulative plots seemed to be more informative and hence are shown here. Similar cumulative plots and the probability distribution frequency plots for the other variables can be seen in Appendix 4.

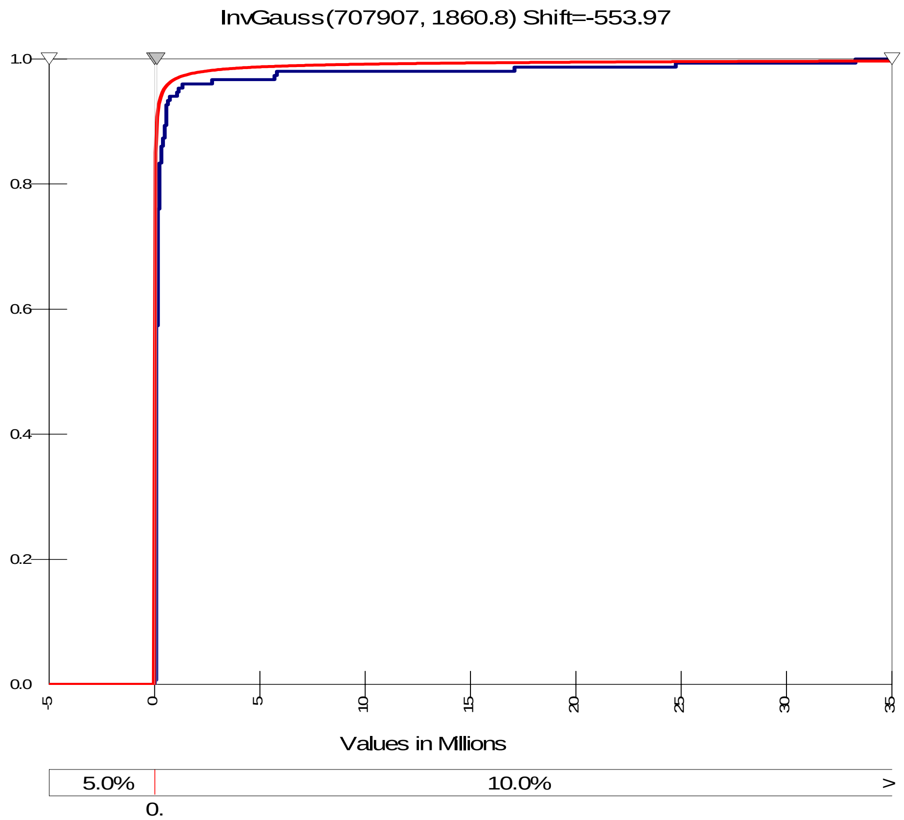


Figure 5.1: Blocked calls: Inverse Gaussian distribution.

5.1.2 Frequency Distribution

From a frequency distribution perspective, explained in section 4.3.2 Chapter 4, some statistics observed for the 150 power loss outages are:

- Customers affected: 72 power outages in the range [30,000, 60,000].
- Total customers affected: 48 power outages in the range [30,000, 60,000].

- Blocked calls: 69 power outages in the range [0, 30,000].
- Outage duration: 26 power outages in the minutes range [31, 60] and 22 outages in the range [61, 90].

For example, the outage duration frequency distribution is plotted in Figure 5.2. More frequency distribution plots are shown in Appendix 4.

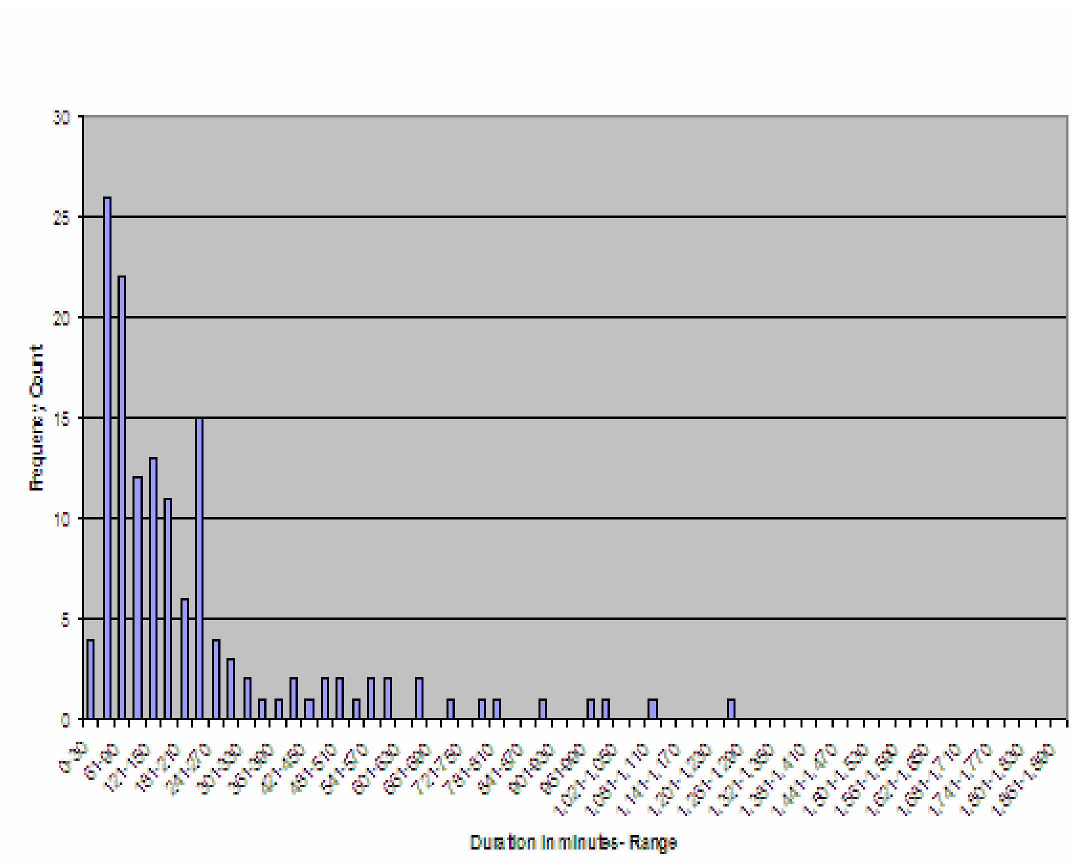


Figure 5.2: Frequency distribution plot for Duration in Minutes.

5.2 Laplace Trend Test

The methodology for analyzing the data with the Laplace trend test is explained in Section 4.4. This test was first performed on the first 5.7 years data (the point at which a visual assessment of the cumulative power outages (Figure 4.1) indicated a possible change in constant power outage rate. The Z score obtained is 0.996 and the alpha is 0.319. This value implies that the null hypothesis (no trend) cannot be rejected. So, the Laplace trend test indicates no trend for the first 5.7 years of the study period.

The Laplace trend test was also performed on the entire 8 year dataset. The Z score obtained is equal to -2.332 with an alpha of 0.020. Since the value of alpha is very small it implies that the probability that there is no trend can be rejected. In addition, since the Z score is negative, a strong reliability growth can be inferred over an 8 year period. The trend test results are summarized in Table 5.2.

Table 5.2: Results of the Laplace trend test.

Number of years	U- Z Score	Alpha	Null Hypothesis: No Trend
5.7	0.996	0.319	**No trend accepted.**
8	-2.332	0.020	**Strong negative trend accepted**

The implication of these tests is that a break point might be present indicating a higher outage rate before the breakpoint, and a lower rate after the break point. To investigate the break point hypothesis, Poisson regression was performed using the Mac ANOVA.

5.3 Reliability growth after Sep 11/01 Incident

A visual examination and Laplace trend test is highly suggestive that a breakpoint in the vicinity of 9-11 may be present. In this section, to investigate a possible breakpoint, a piecewise linear model is analyzed using Poisson regression. A very common infinite failure model, called the Power Law model, is also investigated as a competing model.

5.3.1 Piecewise Linear Model or Breakpoint Model

A Piecewise Linear model was investigated using the methodology presented in Section 4.7. The explanatory variables that were considered in this analysis were as following:

Y= Power outages count per time period (quarter.)

X_1 = Quarter (where the quarters are numbered 1 through 32).

X_2 = Dummy variable.

{ = 0; For all the power outage counts before quarter of interest.

{ = 1; For all the power outage counts beginning with the quarter of interest.

As for the breakpoint analysis, different Poisson models are analyzed by changing the break point to quarters in the vicinity of the 4th quarter 2001. Using this methodology, the Piecewise linear model with a breakpoint at the quarter that includes 9-11 (July, August, and September 2001), is shown in Figure 5.3. The 9-11 quarter is quarter number 23. This model shows a different outage rate, starting the quarter after 9-11, or quarter 24 (January, February, and March 2002). Although an excellent model seems apparent, there is a question of whether there are other quarters that are better break points. This question is investigated in the next Section.

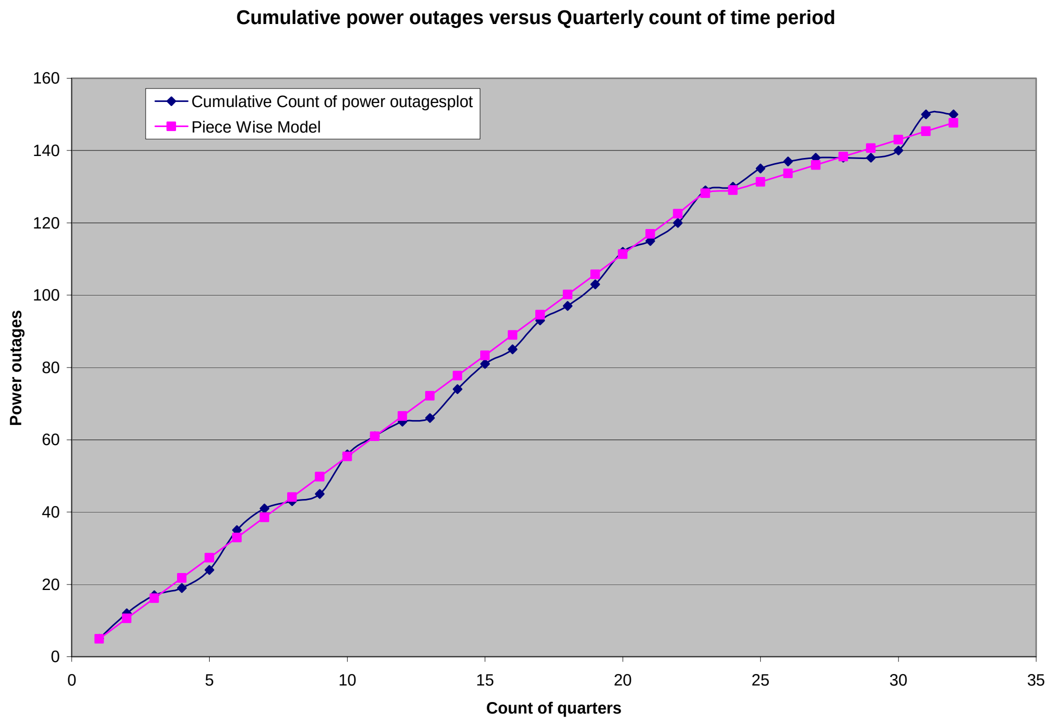


Figure 5.3: Piece Wise Linear Model.

5.3.2 Finding the Best Breakpoint Model

Poisson regression was first used for the quarter after 9-11 as the breakpoint. The results are shown in a deviance table, Table 5.3. A deviance table allows the investigator to consider whether variables should be removed form the overall model.

Table 5.3: Deviance Table: Likelihood Ratio statistic for models with different explanatory variables.

Model	-2 Log L	Λ (Likelihood Ratio Statistic)
μ	81.511	N/A
X_1	75.399	6.112
X_2	64.52	16.911
(X_1, X_2)	63.901	0.619

The model μ is the null model which means that all the other explanatory variables are ignored and the count mean is constant. The model labeled X_1 is the model that is fitted using the explanatory variable X_1 and the mean. This model would say that the rate is a constant plus the influence of a rate change as time progresses. The model fitted for X_2 says that the rate does not change as time progresses; rather it is due to two different regions in time. For the model labeled (X_1, X_2), the model is fitted using the mean and the explanatory variables X_1 and X_2 and says that the mean is influenced not only by changing time, but also by two time regions.

Poisson regression model hypotheses are tested using the likelihood ratio statistic. The value of the likelihood ratio statistic indicates the goodness of fit of one model over the other. Likelihood ratio statistics are obtained using the formula *-2logL* where *L* is the ratio of the maximized likelihood functions. From the Poisson Regression using Mac ANOVA, the values are obtained directly for the *-2LogL*. In order to compare a model with a particular explanatory variable, to the model without that explanatory variable, the likelihood ratio statistic is used to draw conclusions about the effect of adding the explanatory variable to the model. Hence, we need to have a small value in the column for *-2Log L* for a model to be considered good.

The likelihood ratio statistic is indicated by Λ, and has a χ^2 (Chi-Square) distribution with d_1-d_0 degrees of freedom where, d_1 indicates the number of parameters that are estimated in the model with the added variables and d_0 indicates the number of parameters that are estimated in the same model without those added variables [17]. In this case, d_1 is equal to 1 since, as there is only one explanatory variable in the model considered and d_0 is equal to 0. Hence the degree of freedom is equal to 1.

Since the likelihood ratio statistic follows a χ^2 distribution, the significance level or the probability can be obtained from the χ^2 distribution tables with 1 degree of freedom. The significance level can also be obtained using an inbuilt function in excel. The function is CHIDIST(X, degrees of freedom), where, X is the likelihood ratio statistic and degrees of freedom is 1 in this case.

The likelihood ratio statistic is 16.911 for the model with explanatory variable X_2, with a significance level of 3.76E-05; this variable should be included in our analysis. Now, when considering the two variable model with X_1 and X_2 as the explanatory variables, the likelihood ratio is 0.619 compared to the model X_2 with significance level of 0.43142. This significance level means that the probability of obtaining a difference this large when X_1 is not associated with the failure count is 0.43142. So, the model that is chosen has only the explanatory variable X_2. This means that there is no trend, but there are two different regions of constant counts.

The regression coefficients for the above models were obtained from Mac ANOVA using the command line tools specified in Appendix 5. From the regression coefficients, the model equation would be given as shown below:

$$\text{Log}(\mu_i) = 5.6087 - 3.2754\, X_2, \qquad (9)$$

where X_2 is the dummy variable. This means that when $X_2 = 0$, the model is $\text{Log}(\mu_i) = 5.6087$ and when $X_2 = 1$ the model is $\text{Log}(\mu_i) = 2.333$.

From the cumulative power outages plot shown in Figure 4.1, the breakpoint could not be clearly verified by eye so different breakpoints were considered in the vicinity of the 9-11 quarter. From the values observed for the Likelihood ratio statistic, the inference is that the reliability growth started after the 9-11 quarter. The table below shows the Likelihood ratio statistics for the models that were considered for the analysis with different break points.

Table 5.4: Likelihood Ratio statistics for different Breakpoint models

Break Point	Likelihood Ratio Statistic	p – value
3Q2001	8.646	3.28E-03
4Q2001	9.595	2.00E-03
1Q2002	**16.991**	**3.76E-05**
2Q2002	12.447	4.18E-04
3Q2002	14.722	1.24E-04

The first column indicates the quarter from which the explanatory variable X_2 is equal to 1. The second column shows the Likelihood ratio statistic that was obtained for the models. The Likelihood ratio statistic for the models shown in the table above indicates that the model with the first quarter of 2002 is the best breakpoint model. So, the result observed from the Poisson regression indicates that the reliability growth in telecommunication power outages can be inferred to have started after the September 11/01 attack.

The Poisson model plotted as a time series is as shown in the Figure 5-4. This is also called as a jump point model. This is an alternate presentation of the same model shown in the cumulative plot, Figure 5.3. In both instances, an excellent fit is indicated visually and statistically.

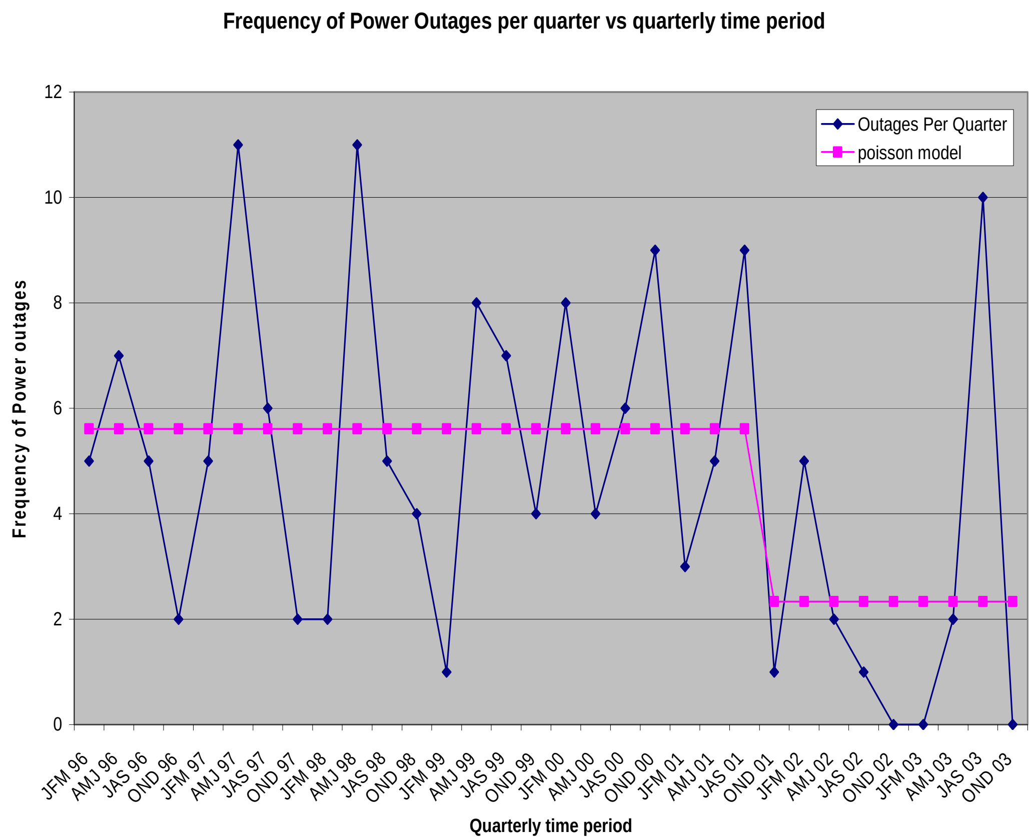


Figure 5.4: Jump point model.

5.3.3 Power Law Model

To insure that the breakpoint is the best model, the Power Law model is also investigated. The power law model or the Weibull reliability growth model is alternately given by the following equation [19]:

$$\frac{\Lambda(t)}{t} = \beta \cdot t^{\beta-1} or \rightarrow \Lambda(t) = \alpha . t^{\beta} \tag{10}$$

Where, $\Lambda(t)$ is the cumulative power outages by time t, and β and α are parameters. If β is positive reliability growth, is indicated and if negative reliability deterioration is indicated. If beta is zero, reliability is constant over time t. Estimators for α and β can be made by first taking the logarithm of the cumulative intensity function:

$$\log [\Lambda(t)] = \beta \log(t) + \log(\alpha) \tag{11}$$

Next, linear regression is performed to assess the fit for the power law model and find the estimators α and β. The data used for the linear regression is the time period in years for t_i and the cumulative power outage count. After performing the regression on this data the value of the R^2 for the model is observed to be equal to 0.93. The estimators for α and β are found to be 27.47 (p-value 2E-150) and 0.77 (p-value 3.57 E-85), respectively. The power law model equation becomes:

$$\Lambda(t) = 27.28t^{0.77} \tag{12}$$

This model is compared to the actual cumulative number of power outages in Figure 5.5. From the plot it can be clearly observed that there is a large positive residual error. Based on the visual assessment, the power law model is not an appropriate fit for the power outage data. This further strengthens the piecewise linear model as more representative of the power outage arrival process. Earlier, maximum likelihood estimators (MLE) were presented for the power law model. However, the fit to this linear regression model is so poor; there is no need for precision.

Figure 5.5: Power Law Model.

5.4 Outage causes

This section provides the findings of the regarding outage causes and their impact. A new impact variable defined as "lost customer hours" is used in the analysis. Outages are categorized as low, medium and high impact. In addition, further analysis is presented on trigger cause, root cause and the component most associated with the root cause.

5.4.1 Outage Impact

A natural question is whether low, medium, and high impact outages have different causes. To assess this question, outages first must be sorted by impact category. Power outage impact based solely on either the total number of customers affected or the duration for which the outage lasted does not provide sufficient insight as an outage affecting a large number of customers might have lasted only for a short time. Likewise, an outage of long duration might have affected very few customers. Hence, to assess the impact of an outage, the product of those two variables, or "lost customers hours" is used [31]. Based upon this metric, the 150 power outages were sorted into low, medium, and high impact outages are shown in the Table 5.5.

Table 5.5: Outage Impact Categories

Impact Category	Lost Customer Hours (LCH) In Thousands	Number of Outages
Low	LCH < 250	89
Medium	250 ≤ LCH < 1,000	30
High	≥ 1,000	31

The table above shows that about two-thirds of the power outages had Lost Customer Hours less than 250 thousand. Each of the low, medium and high impact power outages were analyzed based on their trigger cause, root cause, and the component associated most with the root cause.

Distributions were fitted to the entire Lost Customers Hours dataset using the Best Fit software mentioned in section 5.1.1. The Inverse Gaussian probability distribution seemed to be the ‘best Fit’ for this variable. The associated parameter values for the Inverse Gaussian distribution fit are μ= 17,000,000 and λ= 1861.

Figure 5.6 shows the Inverse Gaussian distribution for the Lost Customer Hours variable. After running the best fit with a data set, plots are displayed both as time series and cumulative. Cumulative plot seemed to be more informative and hence is shown here below.

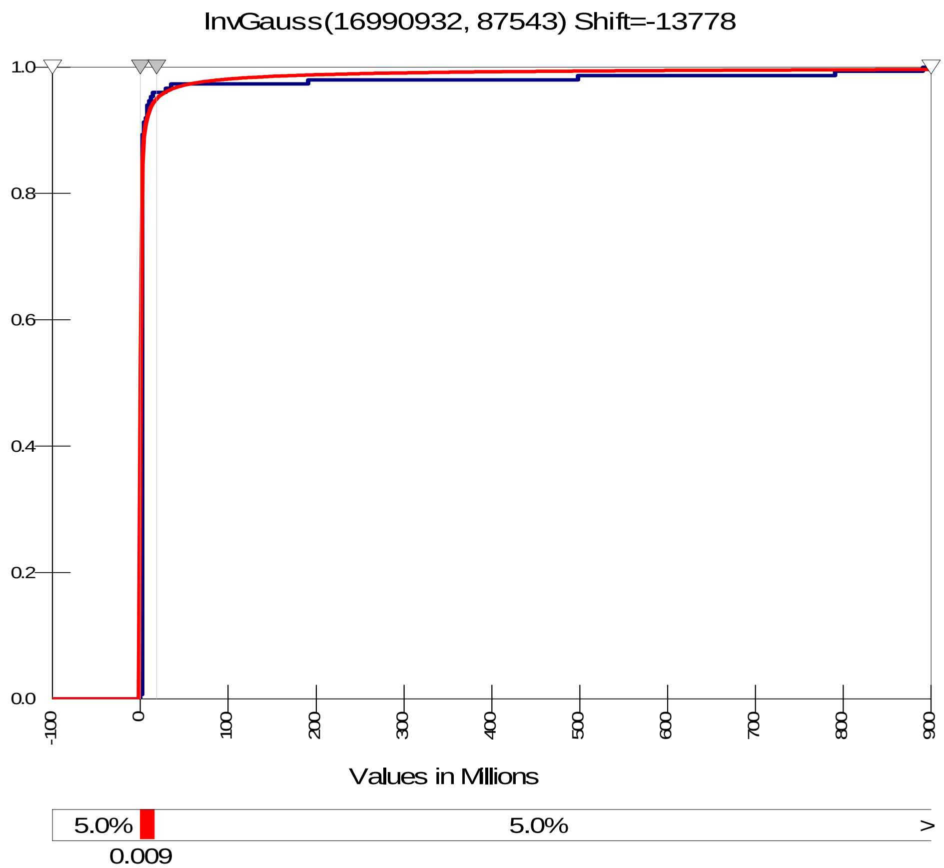


Figure 5.6: Lost Customer Hours: Inverse Gaussian distribution.

5.4.2 Trigger Cause Analysis

First, each power outage was analyzed for trigger cause, using the methodology presented in section 4.9. Next, the outages were placed into one of the three impact categories, as seen in Table 5.6. The same data represented as percentages rounded to differences in trigger causes for the impact categories.

Table 5.6: Categorization of low, medium and high impact outages based on their Trigger causes.

Trigger Cause	Total Outages	Low Impact	Medium Impact	High Impact
Natural Disasters	21	7	5	9
Power Surges	27	20	3	4
Commercial AC Loss	57	35	11	11
Human errors	45	27	11	7
Total	**150**	**89**	**30**	**31**

Outages categorized under Commercial AC loss can be attributed to the power industry, whereas outages categorized under natural disasters are due to the environmental conditions such as hurricanes, storms etc.,

Table 5.7: Trigger causes and the % of power outages under each category.

Trigger Cause	Total Outages	Low Impact	Medium Impact	High Impact
Natural disasters	14 %	8 %	16 %	29 %
Power Surges	18 %	23 %	10 %	13 %
Loss of Commercial AC	38 %	39 %	37 %	35 %
Human errors	30 %	30 %	37 %	23 %
Total	**100 %**	**100 %**	**100 %**	**100 %**

From the table 5.7, it can be observed that loss of commercial AC was uniform in each outage impact category. However, natural disasters trigger more outages in the high impact category while commercial AC loss triggered a large number of outages in the low impact category.

Many of these high impact outages include those triggered by flooding. These outages involved cases in which the communication complexes had power equipment in the basement which flooded. Also from the table, it is obvious that 38% of all telecommunications power outages were triggered by the loss of commercial AC. This indicates that the power industry also plays a major role in triggering outages.

5.4.3 Root Cause Analysis

The low, medium and high impact outages are also analyzed based on their root causes. The root cause analysis results are shown in Table 5.8. The same data is presented on a percentage basis rounded to the nearest percent in Table 5.9, indicating some interesting differences in root causes for the outage impact categories.

Table 5.8: Categorization of low, medium and high impact outages based on their root causes.

Root cause	Total Outages	Low Impact	Medium Impact	High Impact
Engineering Error	16	4	1	11
Installation Error	35	24	8	3
Operations Error	50	33	10	7
Maintenance Error	41	23	11	7
Unforeseen Circumstances	8	5	0	3
Total	**150**	**89**	**30**	**31**

Table 5.9: Root causes and the % of outages under each category.

Root cause	Total Outages	Low Impact	Medium Impact	High Impact
Engineering Error	2 %	4 %	3 %	35 %
Installation Error	23 %	27 %	27 %	10 %
Operations Error	33 %	37 %	33 %	23 %
Maintenance Error	27 %	26 %	37 %	23 %
Unforeseen Circumstances	5 %	6 %	0.0 %	10 %
Total	100%	100%	100%	100%

Here, it is seen that engineering error accounts for over one-third of high impact outages. These outages are mainly due to the flooding and the hurricanes that damaged the equipment below grade. One of the best practices proposed by NRIC specifies that the power equipment in communications complexes should not be located in basements to avoid damage from water. Power outages during flooding and hurricanes also last for a long time since it takes time to remove water from the basement and repair/replace the damaged power equipment. This offers an excellent example of the difference between NRIC reporting, which would report the root cause as natural disaster. In this analysis the natural disaster is the trigger, but the root cause is an engineering error.

Operations and installation errors show up more in small and medium outage impact categories, and account for about two-thirds of all outage impact in these categories. Operations errors include situations where there is insufficient response to power alarms, errors encountered during the upgrading power equipment, and errors made during the routine tests, such as testing sufficiency of backup power.

5.4.4 Power Equipment Most Associated with Root Cause

Through the Root Cause Analysis technique, components most closely associated with the outage can be identified. Trigger component failures typically are not the root cause of an outage. For example, loss of commercial AC can be a trigger cause for an outage. But, since the communication complexes are provided with the backup power supplies, batteries and generators should provide the power in case of loss of commercial AC. In some cases, after running for some time, the generator runs out of fuel. Next, batteries supply power until they fail. In this case by using the RCA technique, generator becomes the component that is most associated with the root cause of this power outage even though the root cause is a maintenance error.

Root cause component failures offer understanding into which major components in the power circuitry is associated with the most outages. A summary of components associated with power outage root cause is shown in Table 5.10 and the percentages are shown in Table 5.11. Included in the scope of this study were power problems in communications equipment, often caused by damage to power circuits by the DC distribution system. It is evident from the table that most number of power outages had involved failure of circuit breakers or the AC generators.

Table 5.10: Component Causing Outage.

Component	Total Outages	Low Impact	Medium Impact	High Impact
Rectifiers	21	8	6	7
Batteries	20	8	7	5
Generators	27	14	4	9
Circuit Breakers	30	20	5	5
Communications Equipment	18	13	3	2
DC Fuses/Fuse Panel	16	12	2	2
Commercial AC	3	3	0	0
AC Transfer Switch	4	3	1	0
Alarm System	10	8	1	1
Environmental systems	1	0	1	0
Total	**150**	**89**	**30**	**31**

Table 5.11: Component Causing Outage (percentages).

Component	Total Outages	Low Impact	Medium Impact	High Impact
Rectifiers	14%	9%	20%	23%
Batteries	13%	9%	23%	16%
Generators	18%	16%	13%	29%
Circuit Breakers	20%	23%	17%	16%

Table 5.11 Continued

Communications Equipment	12%	15%	10%	7%
Fuses/Fuse Bay	11%	14%	7%	7%
Commercial AC	2%	3%	0%	0%
AC Transfer switch	3%	3%	3%	0%
Alarm system	7%	9%	3%	3%
Environmental systems	**1%**	**0%**	**3%**	**0%**

From the table above its clear that one third of all outage impact could have been prevented if circuit breakers and fuses were manually switched or replaced within thirty minutes. Also note that almost 30% of high impact outages were related to generator failure, some where the fuel pump system is in the basement of the building.

Table 5.12 gives a brief explanation of the power outages for all the components mentioned in Table 5.10. These examples indicate how the component is typically associated one with the root cause.

Table 5.12: Examples of Components Associated with Outage Root Cause.

Component	Example
Rectifiers	1. Power surge, say due to lightning strike. 2. Rectifiers damaged thus batteries not charged. 3. Batteries eventually exhausted.
Batteries	1. Loss of commercial AC. 2. Batteries failed because of loose battery cell strings.
Environmental Systems	1. Loss of commercial AC. 2. Generator started running. 3. Failure of Air Conditioning system. 4. Generator over heated and stopped functioning.
Circuit Breakers	1. Loss of commercial AC.

Table 5.12 Continued

	2. Main Circuit breaker opens due to an AC power surge. 3. Site is supplied power from batteries. 4. Batteries eventually exhausted.
Generators	1. Loss of commercial AC. 2. Generator started but stopped after some time due to piston seizure, contaminated fuel, or runs out of fuel. 3. Batteries supply power until finally exhausted.
Alarm system	1. Loss of commercial AC. 2. Generator started to run but stopped due to overheating. 3. Alarm system failed to generate an alarm at NOC. 4. Site runs on batteries until exhausted.
AC Transfer Switch	1. Loss of commercial AC. 2. Failure of AC transfer switch to generator circuit. 3. Site is left on batteries until exhausted.
Communications Equipment	1. Technician working on the communications equipment drops tool shorting DC bus 2. Equipment shutdown.
Fuses/Fuse Panel	1. Fuses to telecommunications equipment blow since they were drawing more current than their rated specifications. 2. Equipment Shutdown.
Commercial AC	1. Some outages occurred due to the loss of Commercial AC. 2. No information given about the series of events in report.

5.5 Sequencing of Power Outages

Table 5.12 shows there is promise in attempting to detail the sequence of events leading to power outages. Grouping the power outages based on the sequence of events provides additional insight about the outage occurrences. For each of the 150 outages, the sequence of events was determined, as shown on the reliability diagram presented earlier in Section 4.10. A total of 18 different sequences were found. In this section, the top four sequences common among the 150 power outages are presented. The following table shows the power outage sequences that occurred most frequently, accounting for just over half the outages.

Table 5.13: Sequencing of power outage events.

Sequence Number	Com AC	G	CB	R	Batt	Fuse Panel	AC/TS	Other	No. of Power Outages
Sequence 1	1	2	0	0	3	0	0	0	23
Sequence 2	0	0	0	0	0	0	0	1	21
Sequence 3	0	0	0	0	0	1	0	0	20
Sequence 4	0	0	0	1	2	0	0	0	13

The short forms used for the notation in the table are explained below.

Com AC – Commercial AC G -- Generators CB -- Circuit Breakers

AC/TS -- AC Transfer Switch R -- Rectifiers Batt -- Batteries

From the entry for Sequence 1 in the table above it is clear that 23 power outages resulted from the loss of commercial AC triggered the outage followed by the failure of generators and battery depletion. Sequence 2 shows that reasons other than the power equipment resulted in outages. These other reasons included causes such as the human errors during operations and maintenance periods. An example for this case is the outage that occurred due to the maintenance person dropping the wrench that resulted in a power surge, thus shutting down the all communications equipment.

5.6 Outages caused by Alarm System Errors

As already mentioned in section 4.12 of Chapter 4, efficient functioning of alarms play a major role in decreasing the time for which an outage can last. Failure of alarm systems can be due to many reasons such as an installation or maintenance failure. Cases involve situations when the alarms were generated but the operations personnel at the NOC, who hold the responsibility to take necessary action for clearing the alarms, did not respond properly. Failure of alarm systems or insufficient response to an alarm is often the root cause of power outages. There are 10 cases in which the alarm systems failed and 12 cases where insufficient response to the alarms resulted in power outages. These power outages could have been avoided by proper installation of alarm systems and by responding properly to the alerts generated by alarm systems. This section explains some of the scenarios associated with alarm systems.

The alarms are connected such that upon the failure of any one of the components, an alarm is generated at the NOC indicating the failure of that particular component at that site. Consider a scenario where commercial AC has failed and the load then transferred to the AC generator. After some time the AC Generator fails and now the site is on battery power. The battery voltage after some time dropped and telecommunications equipment received lower voltage levels than that required for normal functioning, and shuts down. The NOC should receive an alarm indicating that the site lost commercial AC. Next, a generator alarm should occur once the generator failed. Lastly, a low voltage alarm should be received. There were situations when the generator failure alarm was generated at the NOC, but alarms were not received due to low voltage. Since the NOC did not receive the low voltage alarm, operators are under the assumption that they have time to start the dispatch process. In fact the communications complex is down and once it is down for more than 30 minutes, it is reportable.

The case specified above comes under the category of maintenance failure because of not testing alarms. There were also the cases where there was insufficient recognition or response to alarms on the part of NOC operators. This situation can be categorized as an operations failure. In the instances where there are no alarms at the site, then this comes under the category of engineering failure. Other situations involve cases when the alarms were not properly terminated to the required components. This can be categorized as an installation failure. Most of the outages under the failure of alarms category were found to be due to Maintenance failure and the operations failure.

5.6.1 Alarm System Failure

In the analysis conducted for the power outages from 1996-2003, there were 10 cases out of 150 in which the alarms did not function properly and so, the NOC did not know that one of the components at the CO went down and this eventually resulted in service disruption. Outages caused by failure of the alarm accounts for about 7% of the total power loss outages.

5.6.2 Operational Errors

Some outages occurred even though the alarms functioned properly. This is due to the human errors and included cases where there was insufficient response to the alarms generated at the NOC. This may indicate need for training or additional staffing. Out of the 150 power outages there were 12 such cases in which service disruptions were due to insufficient response, even though the alarms were functioning, or about 8%.

5.7 Deviations from NRIC proposed Best Practices

As mentioned in Chapter 4, Section 4.14, the NRIC proposed 99 power related best practices for wireline telecommunications services providers. The NRIC suggested that these recommendations be implemented to decrease the chances of service disruptions. For the power outages occurring the study period an analysis was conducted to see how often NRIC best practices were not followed, and which best practice violations were involved in outage incidents. As the reports are narrative, some had insufficient data to conclude if that service provider violated any best practices. So, it was decided to put the power outages under two categories. If the service providers did not follow the Best practices, they come under the category ‘Yes’ which means that they violated the best practices and ‘Unsure’ if the data is not sufficient to come to a conclusion. From the study of all the 150 power outages there were 38 power outage reports from which no conclusion could be drawn if the service provider followed the best practices. There were 112 power outage reports from which it could be specified that the service providers did not follow the best practices, or about 75%. Also, while studying the outage reports it was observed that the there were instances where more than one best practice was violated. Figure 5.7 shows the list of best practices that were violated and the number of instances each was violated.

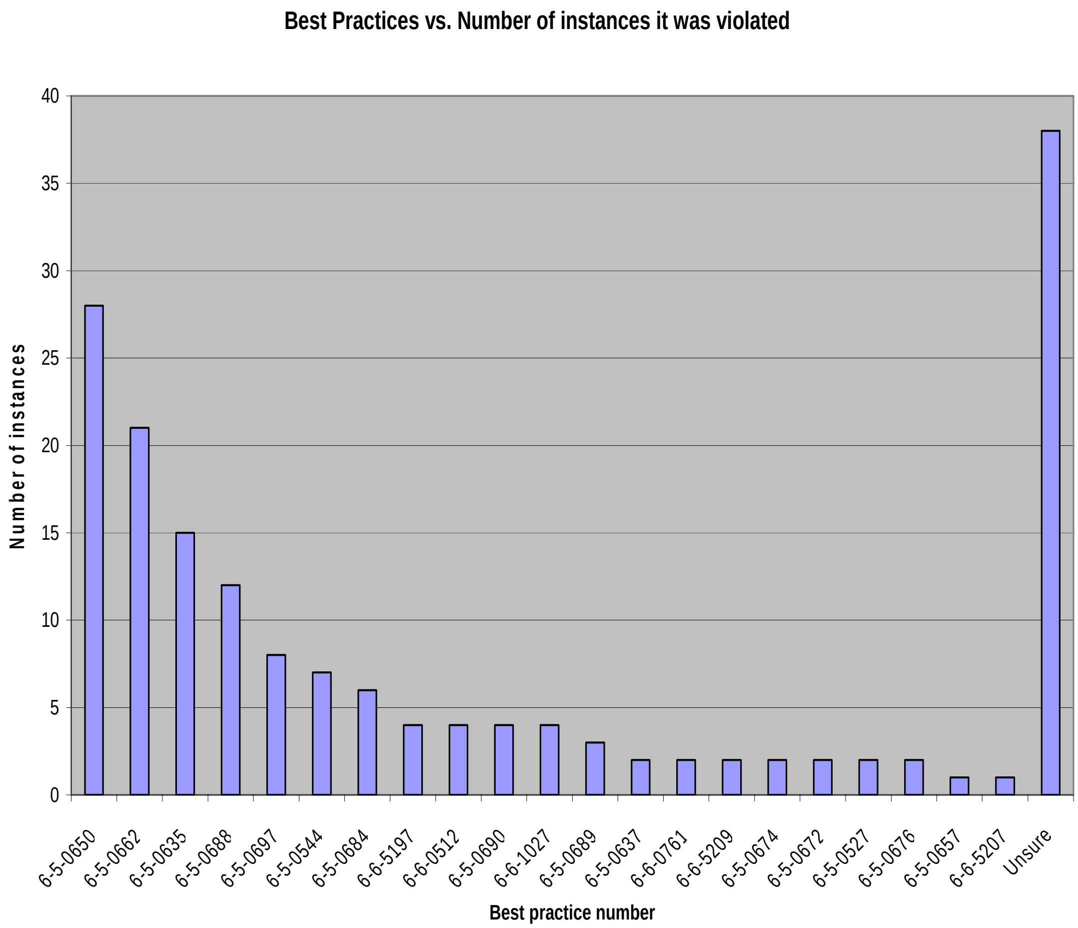


Figure 5.7: Best practices and the number of instances the best practice was violated.

There are 21 best practices that are violated most frequently by the service providers. Table 5.18 provides the list of best practices numbers and a brief summary of the recommendation proposed in that best practice [8], listed by frequency of occurrence shown in Figure 5.7. A detailed explanation of the recommendations under each best practice is given in Appendix 8.

Table 5.19: Best practices and the number of instances each was violated.

Best Practice	Summary of Best Practice
6-5-0650	Provide training for operation and maintenance of power equipment, alarm system operation and response procedures.
6-5-0662	, Test generators every month, running them for at least one hour. Test generator alarms.
6-5-0635	AC surge protection provided at the service entrance to minimize the effects due to lightning or voltage fluctuations.
6-5-0688	Each company to have an alarm strategy.
6-5-0697	Implement an 'Ask Yourself' program to supplement conventional training.
6-5-0544	In order to avoid damage from floods, power equipment not to be kept in the basement.
6-5-0684	Fusing levels be verified to avoid over-fusing or under fusing.
6-6-5197	Periodically test and inspect grounding systems.
6-6-0512	Periodic inspection of cable-ways. Use of sealing compounds, floor and passage ways, water stoppage etc.,
6-6-0690	Redundancy must be provided so that failure of alarm system at a single point will not result in an outage.
6-6-1027	Availability of onsite battery strings and emergency power sources and periodic maintenance of batteries.
6-5-0689	Alarm system be programmed to repeat every 15 minutes and a separate battery discharge alarm should be provided.
6-5-0637	Insure alarm testing programs exist.
6-6-0761	Periodic verification of the synchronization plan, timing links, power feeds and alarms.
6-6-5209	Maintenance of transfer switch and spare parts available for

Table 5.19 Continued

	the switch.
6-5-0674	To ensure that outdated equipment is phased out of plant.
6-5-0672	Minimum of 3 hours battery reserve for CO's with automatic standby systems.
6-5-0527	Equipment areas should be maintained within the temperatures as per the manufacturer's ratings.
6-5-0676	Not to use low voltage disconnects at the battery plant.
6-5-0657	To design standby generators for automatic operation and also with the ease of manual operation in case of emergency.
6-6-5207	In case of major disruptions (e.g. hurricanes) precautions must be taken for fuel supplies.

From Figure 5.7, it can be observed that the number of instances the best practice numbered 6-5-0650 has been violated is 28. This best practice recommends that strong emphasis should be given on human activities that involve the operation with power systems which include the maintenance procedures, alarm system operation and maintenance procedures and training for operations personnel. From the reports it was clear that some of the outages occurred due to human errors when working on the equipment. The NRIC suggests that training should be given to the technicians and the personnel at the site so that they are well aware of what they are doing. The NRIC recommends that service providers should employ an 'Ask Yourself' program which intends to make sure that the employee ensures flawless network service. This is recommended in the best practice numbered 6-5-0697.

There are 38 instances where it was difficult to analyze because of the insufficient data in some cases. Other cases had the situations where the outage occurrence was due to flooding. In these outages, the duration for which the outage lasted was large and due to transportation problems and flooding condition no restoration activities could be started immediately. Batteries in such cases would not last for more than 4-8 hours and the generators could not be running continuously all the time due to fuel exhaustion. From the outage reports, for these instances it was not clear if the carrier implemented the best practice or not. So, these cases were put under the ‘Unsure’ category.

5.8 Power Industry vs. Telecommunications Industry

Some of the power outages occurred due to the loss of commercial AC and this is attributed to the power industry. Outages also occurred due to the errors/failures at the communications complex and these are attributed to the telecommunications industry. As is seen from the data the frequency of power outages decreased after the 9-11. Hence, it would be interesting and also informative to know if the credit goes to the power industry or the telecommunications industry. This section presents some results of the Laplace trend test that was done in order to see if the reliability growth credit goes to the power industry or the telecommunications industry.

A telecommunications power outage, due to loss of power to equipment, has a sequence of events that finally result in a service disruption. For the purpose of the analysis mentioned in the above paragraph, power outages which had the first event as the loss of commercial AC are separated from the 150 power outages. There were 57 such power outages. These power outages indicate that the power outage trigger is due to the failure of power industry rather than the telecommunications industry. However, in order to see if the data for the power outages due to the loss of commercial AC followed any trend, the Laplace trend test was performed on the 57 commercial AC loss events. The results of the Laplace trend test are explained below in detail.

From the data used for the Laplace trend test, the value of U is -1.17 and the value of alpha is 0.243. This value of alpha is large enough to indicate that the hypothesis of no trend cannot be rejected. From this an inference of constancy can be made.

From the Laplace trend test for the total power outages data, it was observed that there is a negative trend indicating reliability growth. But, the results of the Laplace trend test conducted for the power outages data triggered by the loss of commercial AC indicate that there is no trend. This implies that the credit goes to the telecommunications industry for the reliability growth since 9-11.

The plot below shows the power outages that were triggered due to the loss of commercial AC. Visually no trend could be observed from the graph, and this is consistent with the Laplace trend test results.

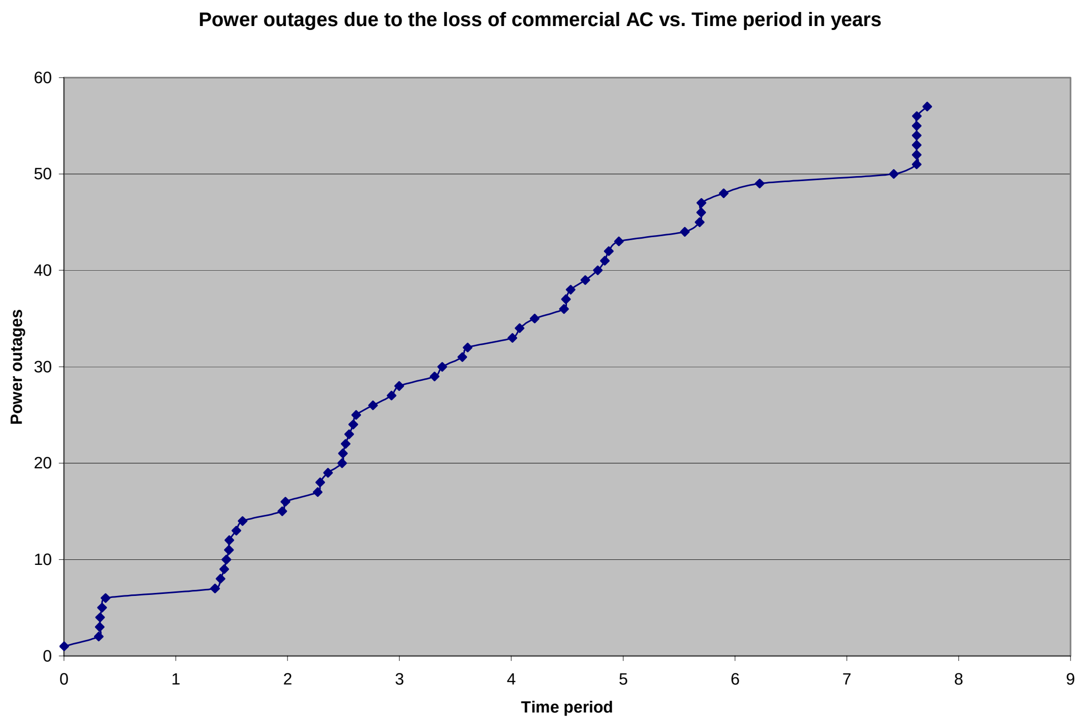


Figure 5.8: Power Outages with trigger cause as the loss of commercial AC.

5.9 Conclusions

The conclusions of this research are summarized below.

- ***No seasonality in frequency of occurrence of power outages could be observed.***

From the result of the Fourier analysis of the data, no seasonality or periodicity could be observed. This shows that the power outages can not be grouped and analyzed based on the months or quarters.

- ***Strong negative trend observed using Laplace trend test indicates strong reliability growth.***

The results of the Laplace trend test indicate a strong statistical evidence of trend. There is a negative trend indicating reliability growth, or a decrease in frequency over the study period.

- ***Reliability growth after the Sep 11/01.***

The break point model is the best model found to represent the observed reliability growth. Two separate processes were indicated – a higher arrival rate process before 9-11 and a lower arrival rate process after.

- ***Human errors are the main cause of power outages.***

Human error is most often the trigger or the root cause of power outages during the study period. Human error triggered 45 of the 150 power outages, or 30% of the total power outages. Root causes of the power outages most of the times were due to the human errors. If the technicians and the personnel at the site are provided with sufficient training and/or proper staffing levels, the number of power outages could be reduced. Un-staffed facilities appear to play a major role in telecommunication power outages.

- ***Deviations from NRIC proposed Best Practices were involved in most outages.***

From the information available form the reports about the outage causes, there were 112 instances when the best practices were not implemented, or 75% of the total. There were 38 power outage reports from which it could not be said if they implemented the best practices or not. They were placed under the 'Unsure' category.

- ***Alarm system failure or failure to respond to alarms account for a small amount of outages.***

There were 12 instances in which outages occurred due to the insufficient response to the power alarms, and 10 instances in which the power alarms didn't function properly. So alarms were involved in about 15% of all power outages. This clearly indicates that the number of power outages and the power outage duration can be reduced by responding quickly to the alarms generated, or testing alarms periodically

- ***Flooding accounts for most of the high impact power outages, mostly because of power equipment below grade.***

Most of the high impact outages occurred in areas prone to flooding where the central office equipment, and/or power equipment was kept in the basement of the building. In these areas the restoration activities often could not be immediately started due to severe weather. In addition, it takes additional time to repair water damage and cleanup before trying to fix power equipment. Such high impact outages can surely be reduced if care is taken not to place equipment in basements.

- ***Frequency of power outages can be reduced by implementing maintenance programs.***

About 27% (41 of the total 150) power outages were caused due to the maintenance errors at the communications complex. Maintenance activities assure that the equipment is functioning properly. Any malfunctioning equipment or improper wiring mistakes can be recognized during the maintenance tests, thus avoiding power outages.

- ***About 20% of the power outages affected over one million customers.***

About 60% of power outage incidents were low impact, affecting less than 250,000 customers. About 20% of power outage incidents were high impact, affecting over 1 million customers.

- ***The reliability growth over the 1996-2003 can be attributed to improvements by the telecommunications carriers.***

The reliability growth after 9-11 can be inferred to be mainly attributable to telecommunications carriers. The results of the Laplace trend test indicated that there is no trend in the case of power outages that occurred triggered by loss of commercial AC power.

5.10 Implications

- This work suggests the FCC may want to consider a rule requiring that all the carriers implement the NRIC best practices, in order to reduce the frequency of power outages. Considerations may include whether there is sufficient competition to forgo regulation.

- Service providers should seriously examine best practice adoption.

- The reporting rules in place during the study period resulted in poor data reporting, hampering study and assessment of the industry performance.

Chapter 6: Research Limitations

6.1 Some reports with insufficient data.

The analysis of the data in this study is done based on the number of the outage reports that were reported to the FCC. Some reports were reported to the FCC which had very little information. These reports did not have the details necessary for analyzing the data. This surely is a limitation that has to be considered while reviewing the results of the data analysis. Some reports included no information about required reporting - customers affected, date and time, and blocked calls. Often, details of the outage occurrence were also not clearly specified in the outage reports, thus leaving the reader to guess reasons of why the outage occurred.

6.2 Assumptions

- **All the events were reported to the FCC.**

The assumption that all the events were reported to the FCC was important in all the types of analysis performed, such as reliability growth.

- **All sites have both the backups.**

Some of the power outage reports did not specify all the information about the causes of the outage clearly. Some reports did not discuss backups during an outage. For example, some reports contained information indicating that the outage occurred because of the non operation of the generator due to the reasons like the piston seizure, over speed etc. However, nothing was mentioned about the batteries. The assumption was made that all the sites have both generator and battery backups.

Chapter 7: Further Research

- This research is based on the power outages that occurred during the time period 1996-2003. Research can be further extended to include the time series through 2004 to check if the reliability growth is still continuing or not. New FCC rules starting January 2005 prohibit the public dissemination of outrage reports. It will not be possible to study the data after 2004.

- This research does not analyze which carrier most violated the best practices. Research can be done in that area analyzing which carrier had violated the NRIC proposed best practices the most, and which best practice was violated the most by that carrier.

- Further research could be performed separately by segmenting the data into subpopulations. Trends and cause analysis used for the entire population could be applied to different subpopulations:
  - Time of the day..
  - Carrier.
  - “Before 9-11” and “After 9-11”.

Bibliography

[1] *About the NRSC,* Retrieved from World Wide Web on 15th November 2004, from http://www.atis.org/nrsc/nrscinfo.asp.

[2] *Network Reliability Steering Committee Annual Report 2003*, Network Reliability Steering Committee, Retrieved from World Wide Web on 15th November 2004 from http://www.atis.org/NRSC/Docs/2003%20Annual%20Report%20-Final%20%20_2_.pdf.

[3] *Network Reliability Steering Committee Annual Report 2002*, Network Reliability Steering Committee, Retrieved from World Wide Web on 15th November 2004 from http://www.atis.org/NRSC/Docs/2002rpt.pdf.

[4] *Network Reliability Steering Committee Annual Report 2001*, Network Reliability Steering Committee, Retrieved from World Wide Web on 15th November 2004 from http://www.atis.org/NRSC/Docs/2001rpt.pdf.

[5] *Network Reliability Steering Committee Annual Report 2000*, Network Reliability Steering Committee, Retrieved from World Wide Web on 15th November 2004 from http://www.atis.org/NRSC/Docs/2000rpt.pdf.

[6] *Network Reliability Steering Committee Annual Report 1999,* Network Reliability Steering Committee, Retrieved from World Wide Web on 15th November 2004 from http://www.atis.org/NRSC/Docs/1999rpt.pdf.

[7] *NRIC Publications,* Retrieved from World Wide Web on 20th February from http://www.nric.org/pubs/index.html.

[8] *NRIC Best Practice,* Retrieved from World Wide Web on 16th August 2004 from http://www.bell-labs.com/cgi-user/krauscher/bestp.pl?textsearch=&networktype=wireline&operator=AND&kw_1=power&kw_2=&kw_3=&fieldList=.

[9] *2003 North America blackout,* Retrieved from World Wide Web on December 15th 2005 from http://www.answers.com/topic/2003-north-america-blackout.

[10] *Is our Power grid more reliable one year after the blackout?* Retrieved from World Wide Web on December 28th, 2004, from http://www.eere.energy.gov/state_energy_program/feature_detail_info.cfm/fid=32.

[11] Report to the U.S-Canada Power System Outage Task Force, Retrieved from World Wide Web on November 22nd 2004 from http://www.electricity.doe.gov/documents/blackout_oneyearlater.pdf.

[12] Fairley, P. (2004) "*The Unruly Power Grid,*" IEEE Spectrum, pp. 22-27. August 2004.

[13] Snow, Andrew P., "Network Reliability: The Concurrent Challenges of Innovation, Competition and Complexity", IEEE Transactions on Reliability, Vol. 50, No. 1, March 2001.

[14] *Best Fit,* Retrieved from World Wide Web on 1st December 2004 from http://www.comsol-online.com/content.php?si=222.

[15] *Trend tests,* Retrieved from World Wide Web on 21st June 2004 from http://www.itl.nist.gov/div898/handbook/apr/section2/apr234.htm.

[16] Steven, E and Asit, P. (2000) "Testing for the Homogenous Poisson Process," in *Statistical Methods for the Reliability of Repairable Systems,* pp.110-112.

[17] *"The Analysis and use of Software Reliability and Quality Data,"* Bellcore, Special Report SR-TSY-001547, Issue 1, January 1990.

[18] Bingham, C and Oehlert, G.W. (2001) *"An Introduction to MacAnova"* Technical Report Number 600.

[19] Snow, A.P and Weiss M.B.H (1997) *"Empirical Evidence of Reliability Growth In Large-Scale Networks,"* Journal of Network and Systems Management, Vol. 5, No. 2, pp. 197-213.

[20] Steven, E and Asit, P. (2000) "Inference for the power law process: Failure truncated case," in *Statistical Methods for the Reliability of Repairable Systems,* pp.116-118.

[21] *Power Law (Duane) Model,* Retrieved from World Wide Web on 10th August 2004 from http://www.itl.nist.gov/div898/handbook/apr/section4/apr452.htm.

[22] *Definition of Root Cause Analysis, Retrieved from World Wide Web on January 20th 2005 from* http://www.maintenanceworld.com/Articles/downtimecentral/Root-Cause-Analysis.htm.

[23] *Root Cause Analysis,* Retrieved from World Wide Web on 10th August 2004 from http://www.systems-thinking.org/rca/rootca.htm.

[24] *Root Cause Analysis: Will it find the weak link?,* Robert J. Latino, Retrieved from World Wide Web on January 20th 2005 from http://www.maintenanceworld.com/Articles/latinor/rootcause.html.

[25] *Root Cause Analysis (RCA)*, Retrieved from World Wide Web on 10th August 2004 from http://www.patientsafety.gov/rca.html.

[26] *Root Cause Analysis for Beginners James J. Rooney and Lee N. Vanden Heuvel* Retrieved from World Wide Web on 6th October 2004 from World Wide Web on http://www.asq.org/pub/qualityprogress/past/0704/qp0704rooney.pdf.

[27] *Getting Root Cause Analysis to Work for You,* Alexander (Sandy) Dunn, Retrieved from World Wide Web on December 26th 2004 from http://www.maintenanceworld.com/Articles/plantmaintenance/root-cause-analysis.pdf.

[28] *Root Cause Analysis,* Retrieved from World Wide Web on January 20th from http://www.maintenanceworld.com/Articles/systems-thinking/root-cause-analysis.htm.

[29] Govind S. Mudholkar, Rajeshwari Natarajan and Yogendra P. Chaubey (2001) *"A Goodness-of-Fit Test for the Inverse Gaussian distribution using its independence characterization"*, Sankhya Indian Journal of statistics 2001, Volume 63, Series B, pt.3, pp 362-374.

[30] *A Concise Summary of @RISK Probability Distribution Functions,* Retrieved from World Wide Web on 2nd December 2004 from http://61.222.167.226/html/Download_File/Document/015056_005152_DistFunc.pdf.

[31] Snow, A. P (2004) *"Assessing pain below a regulatory outage reporting threshold",* Telecommunications Policy, Vol. 28/7-8 pp 523-536.

APPENDIX 1: Variable Time Event Plots

Time series of events plots are presented in this appendix for customers affected, blocked calls, total customers affected, duration of outages and the frequency count of the outages.

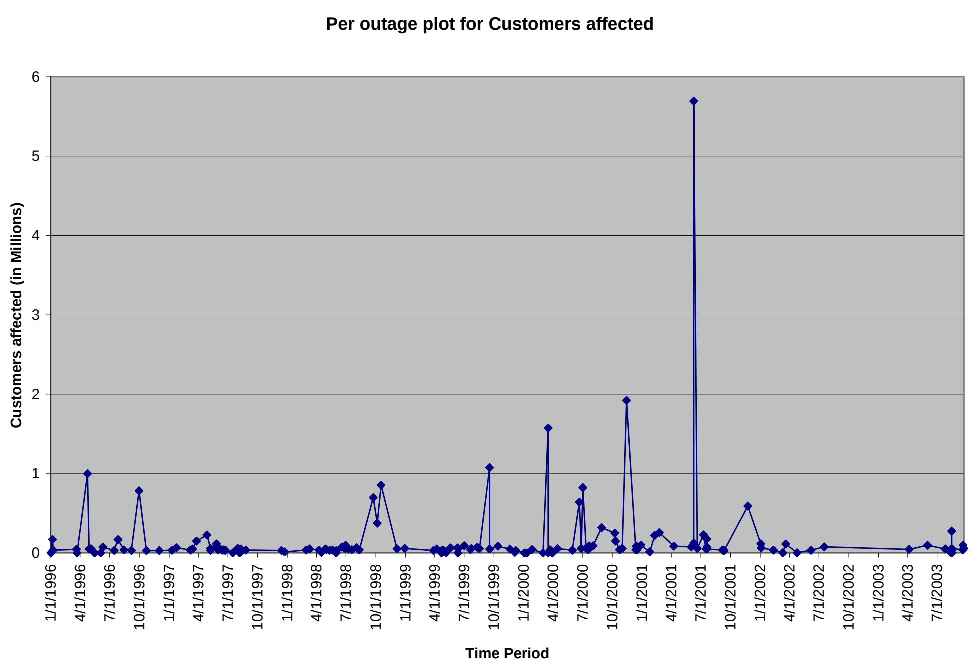
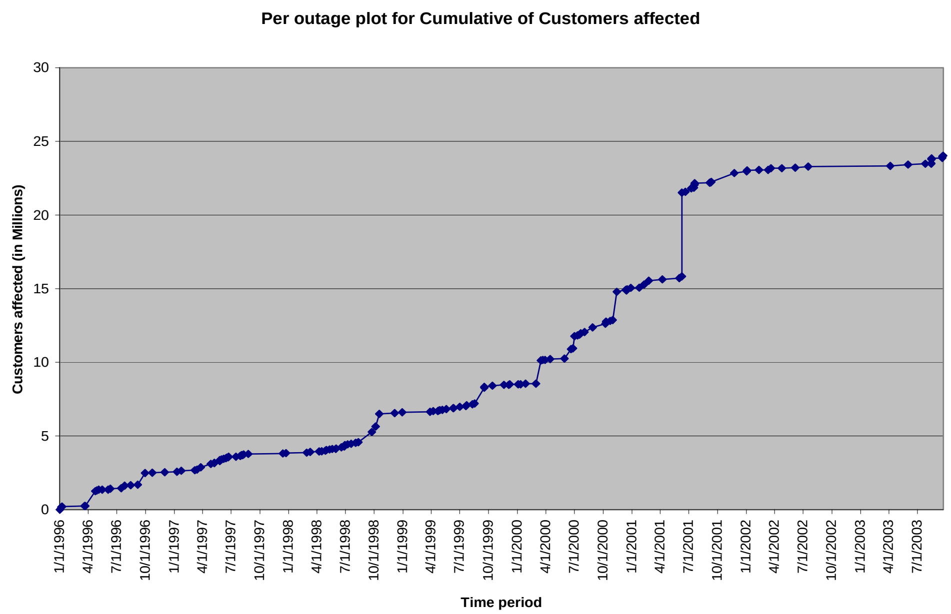


Figure A1.1: Customers affected vs. Time period.



FigureA1.2: Cumulative plot of customers affected vs. time period.

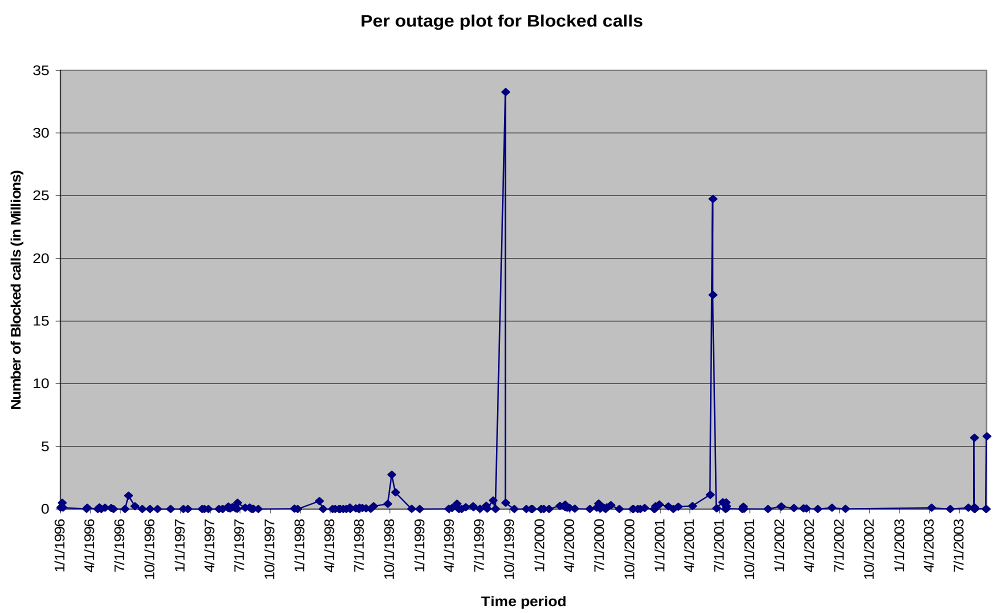


Figure A1.3: Blocked calls vs. Time period.

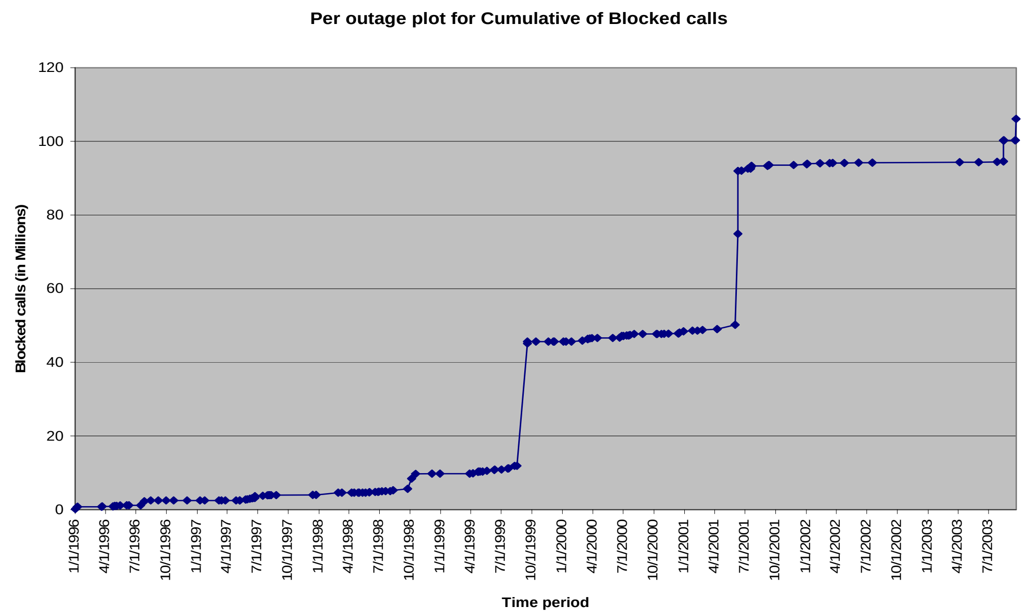


Figure A1.4: Cumulative plot of Blocked calls vs. time period.

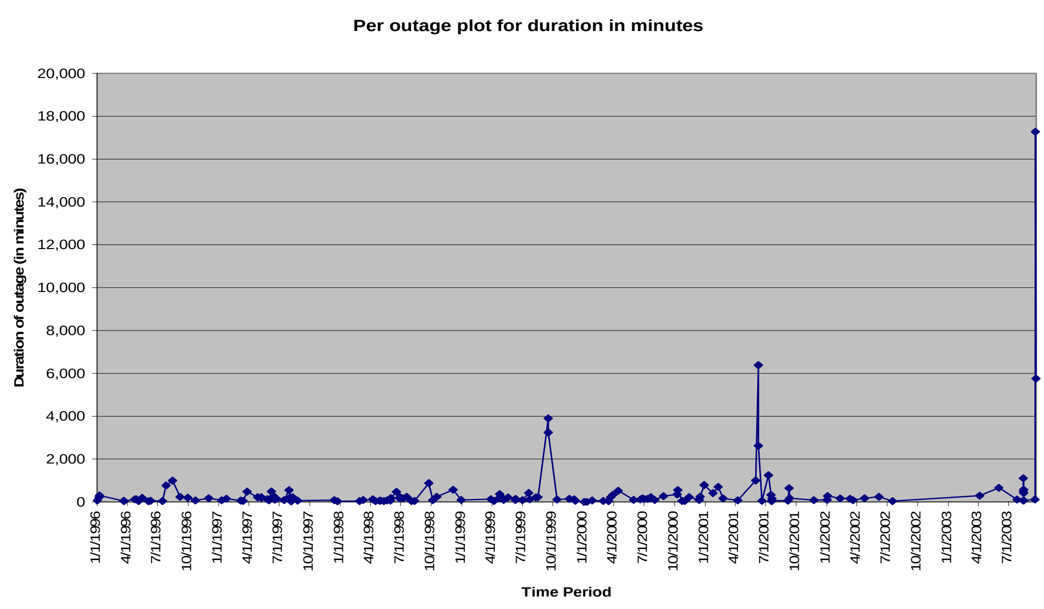


Figure A1.5: Duration in minutes vs. Time period.

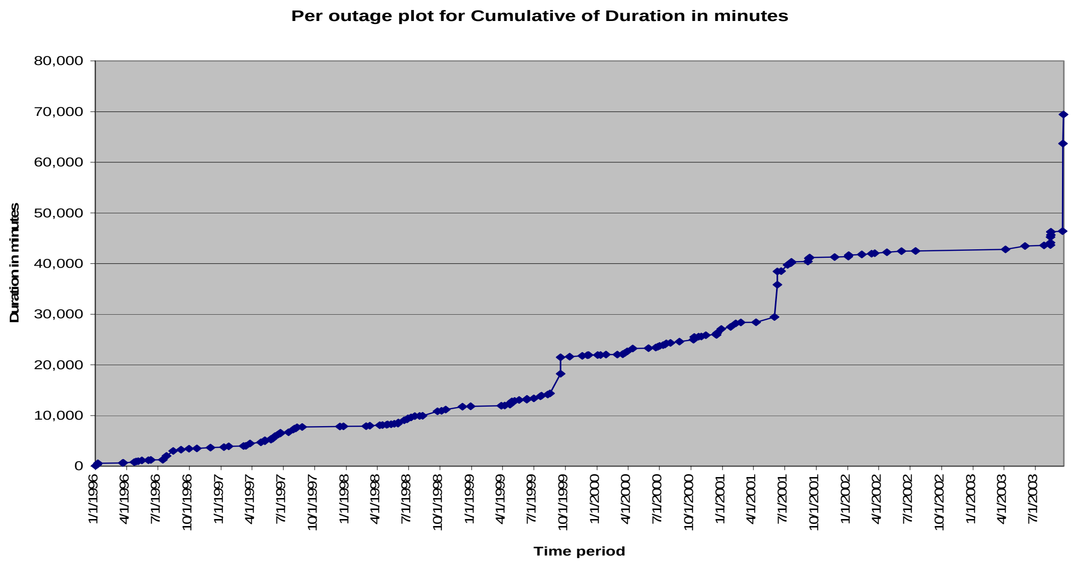


Figure A1.6: Cumulative of duration in minutes vs. Time period.

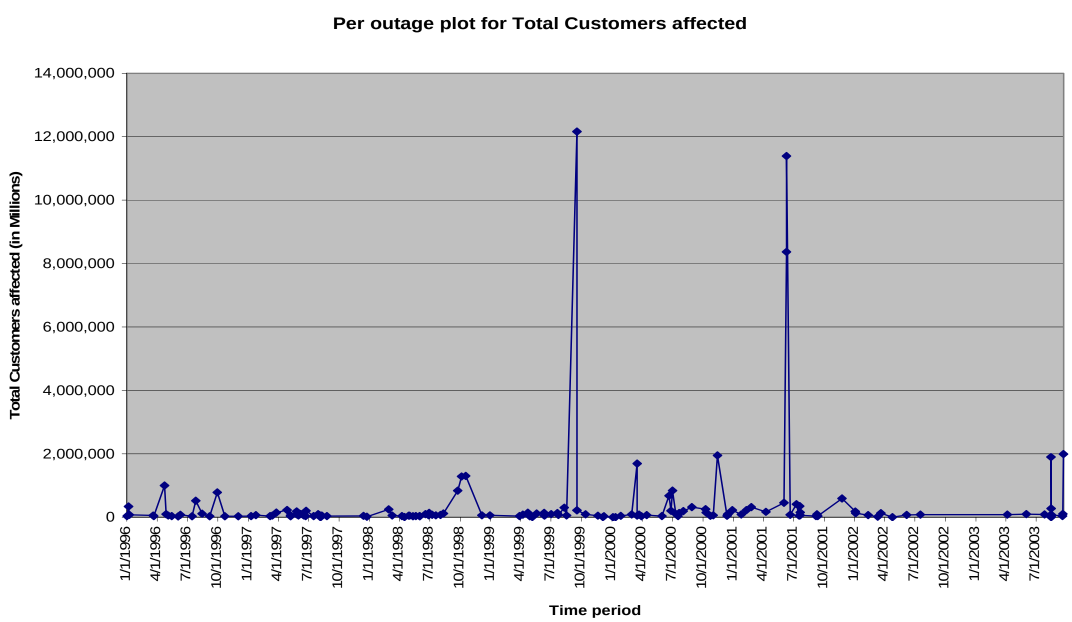


Figure A1.7: Total customers affected vs. Time period.

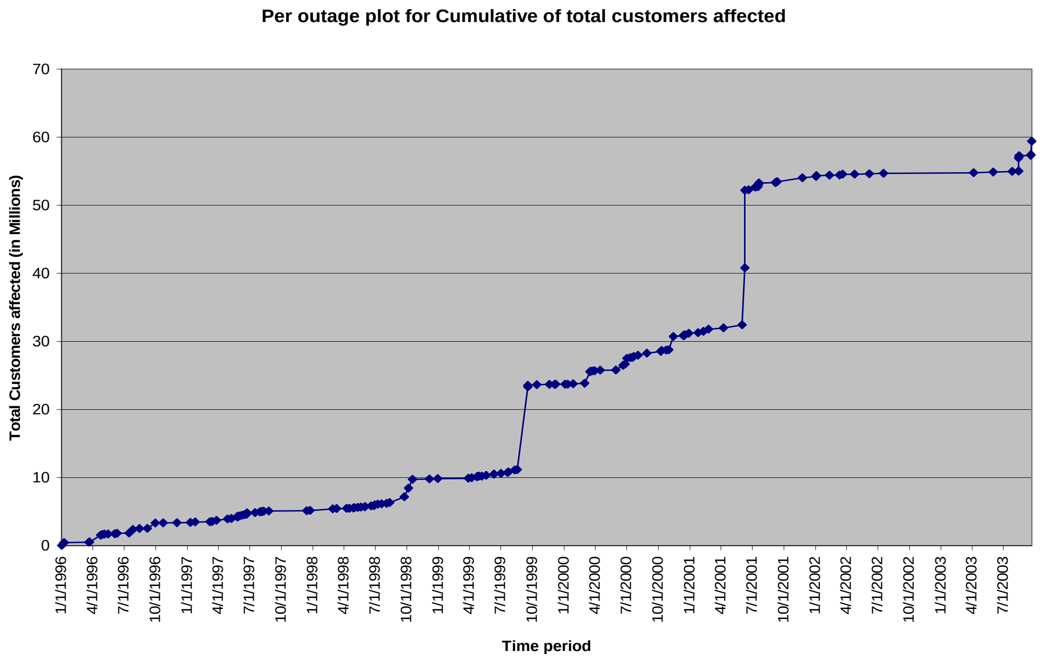


Figure A1.8: Cumulative of Total customers vs. Time period.

APPENDIX 2: Monthly Analysis of the Power Outages data

This appendix presents monthly plots for customers affected, blocked calls, total customers affected, duration of outages and the frequency count of the outages.

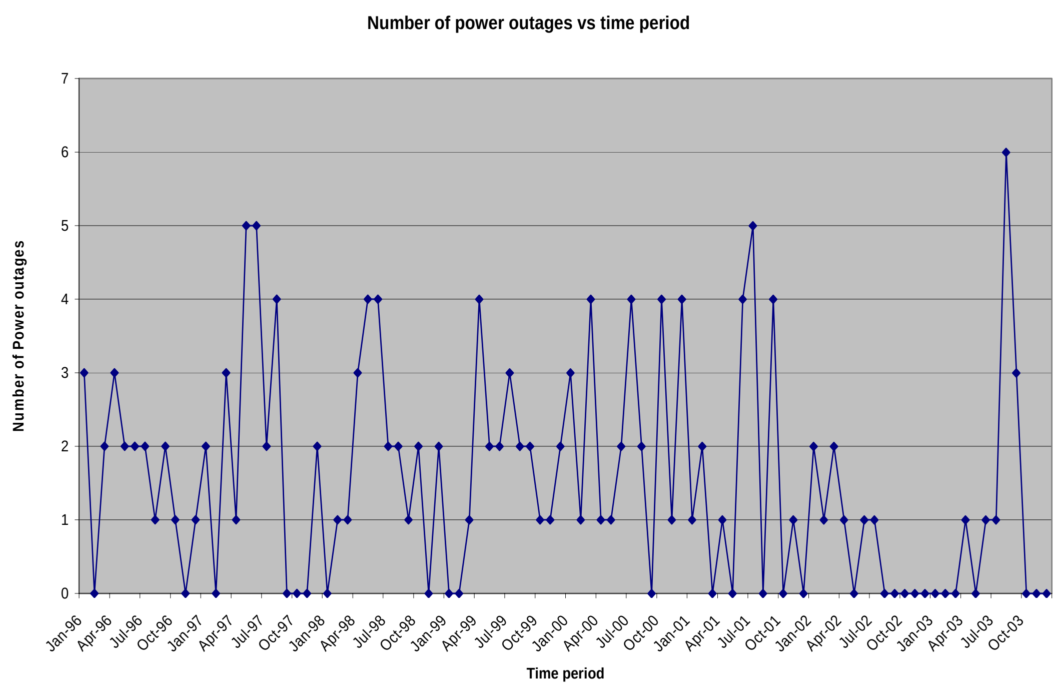


Figure A2.1: Power outages per month vs. Time period.

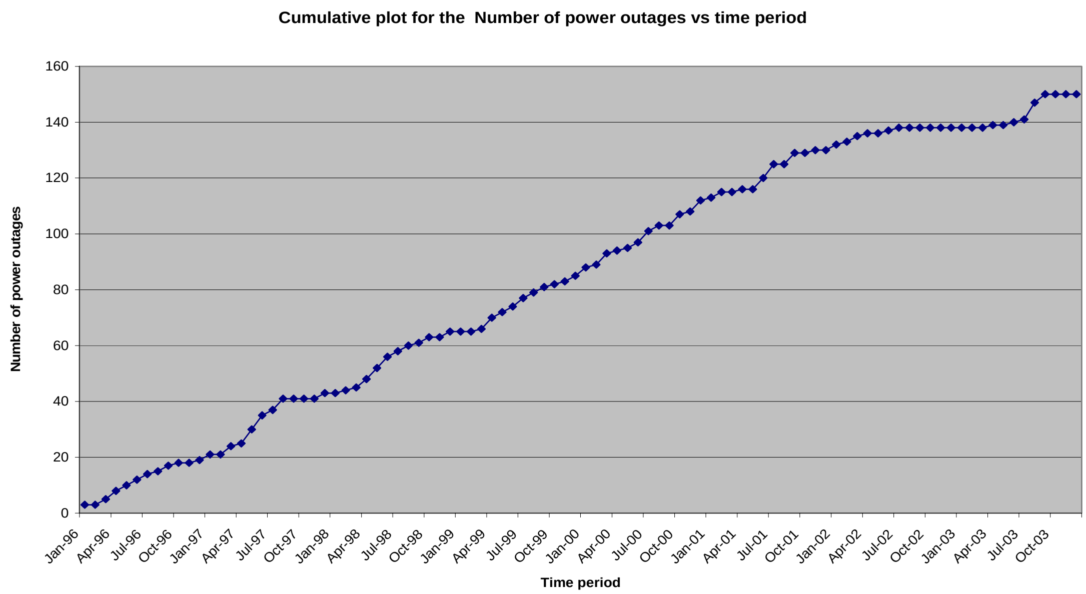


Figure A2.2: Cumulative power outages count vs. Time period.

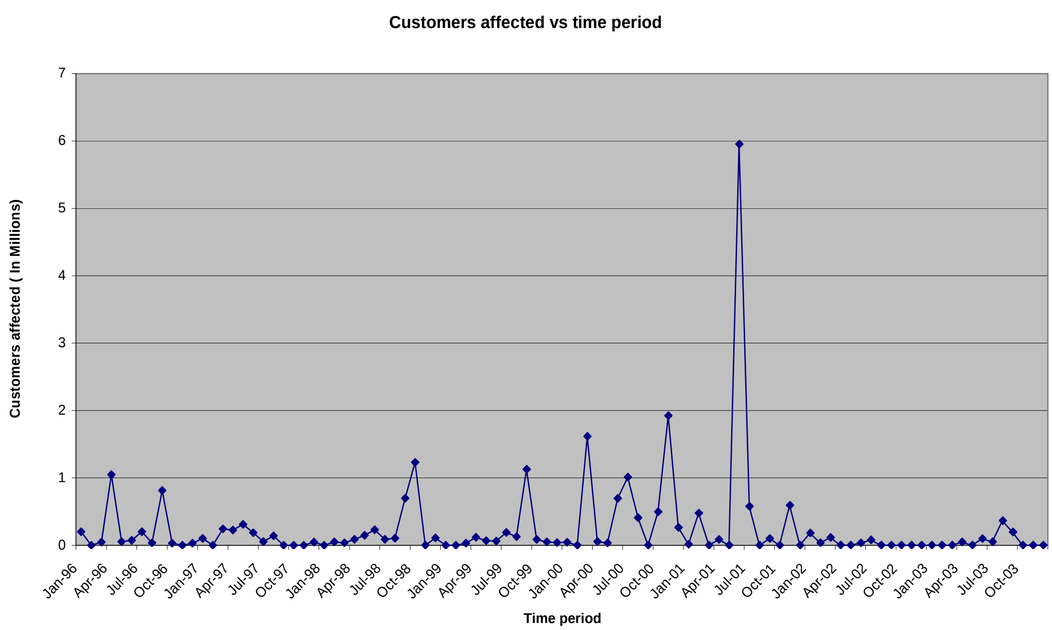


Figure A2.3 Customers affected vs. Time period.

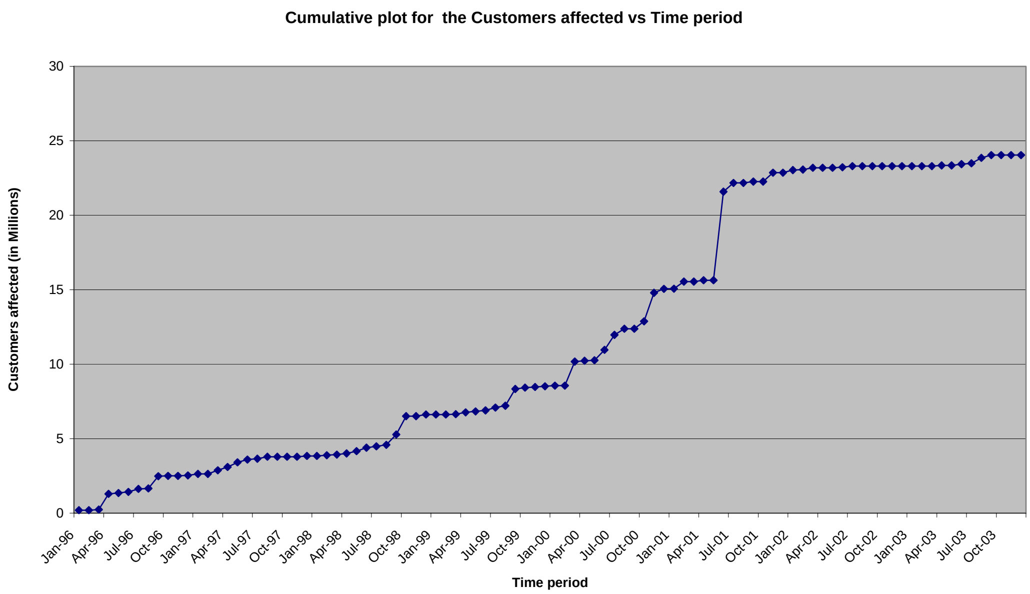


Figure A2.4: Cumulative of Customers affected vs. Time period.

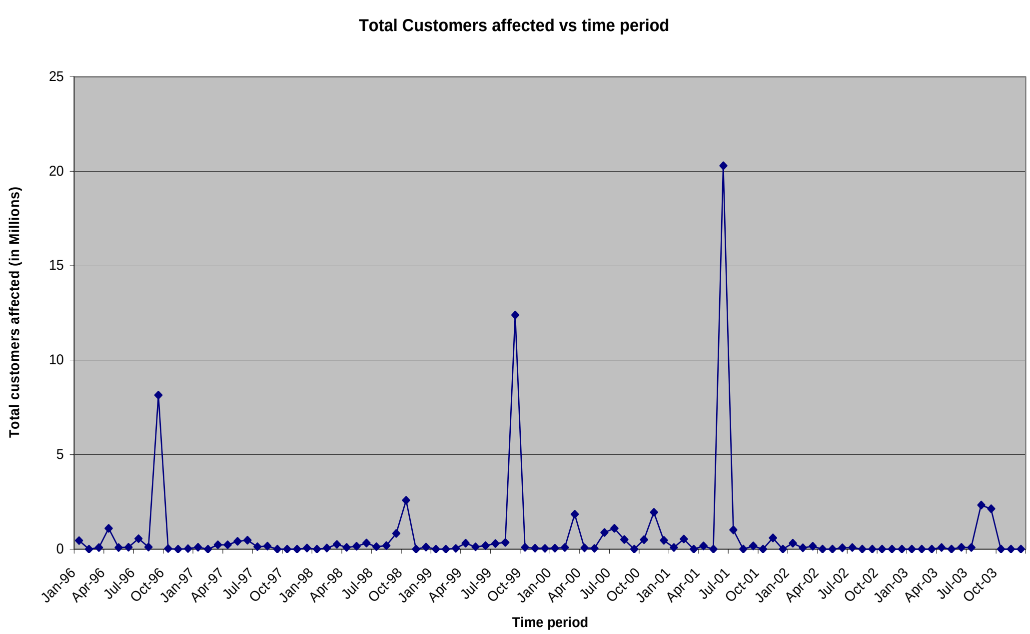


Figure A2.5: Total customers affected vs. Time period.

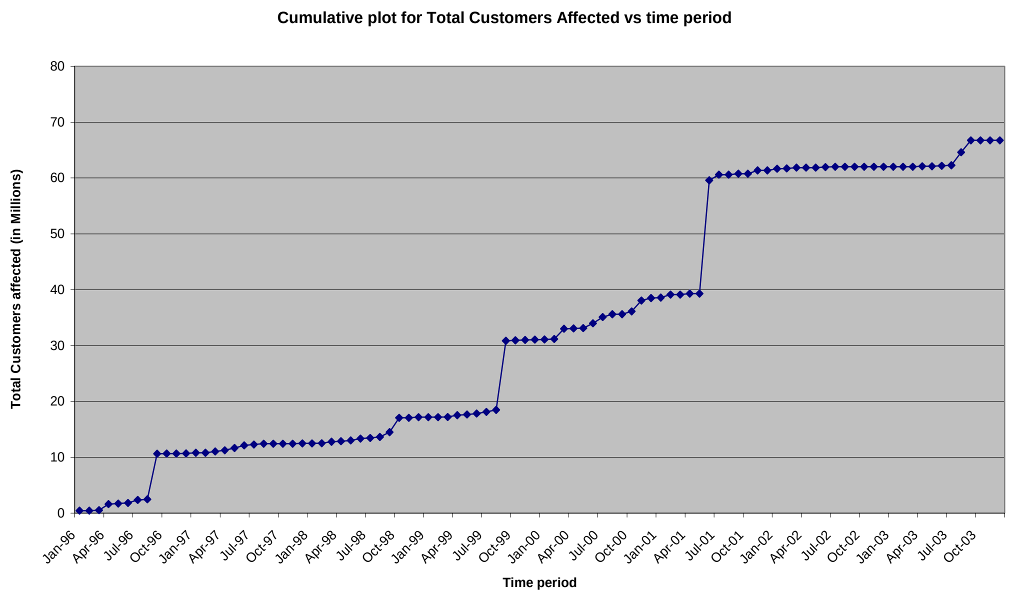


Figure A2.6: Cumulative of Total Customers affected vs. Time period.

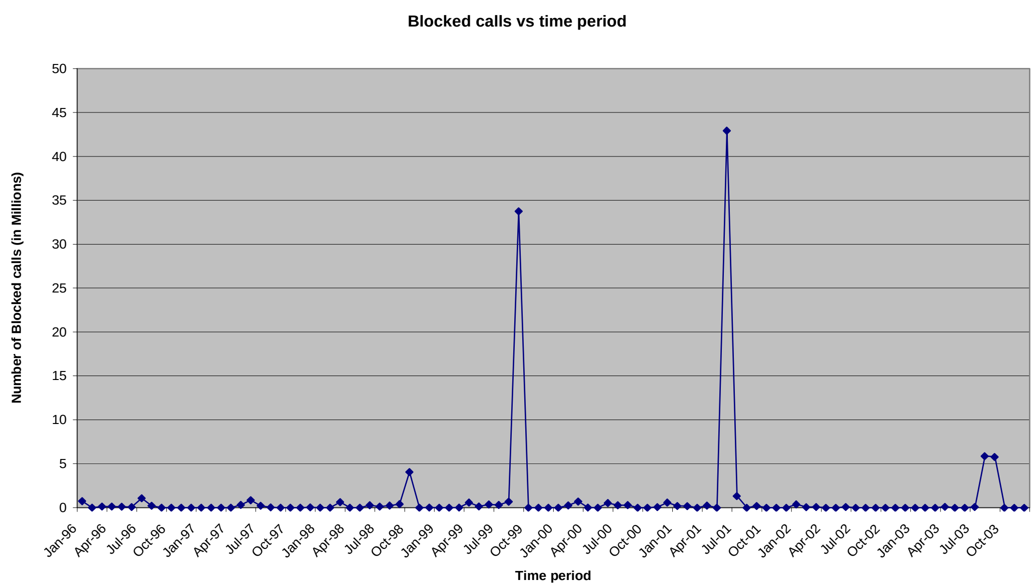


Figure A2.7: Blocked calls vs. Time period.

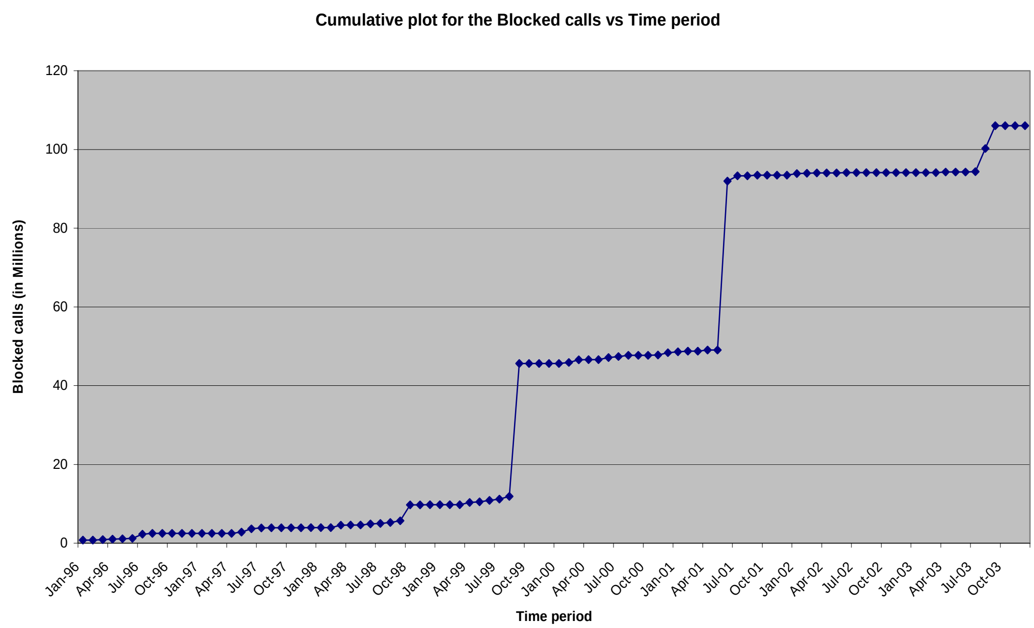


Figure A2.8: Cumulative of Blocked calls vs. Time period.

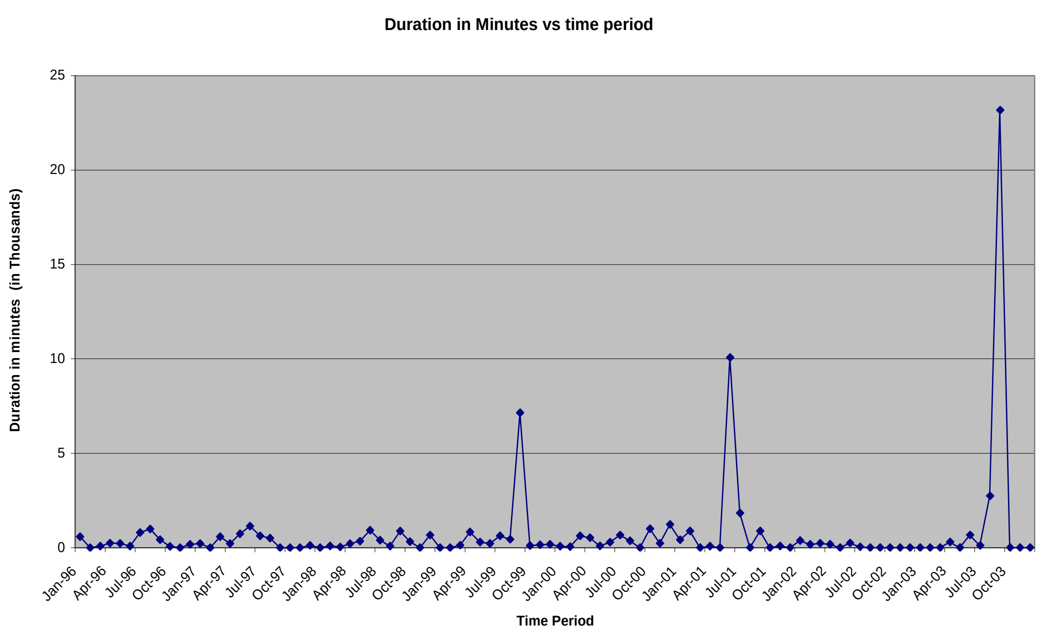


Figure A2.9: Duration in Minutes vs. Time period.

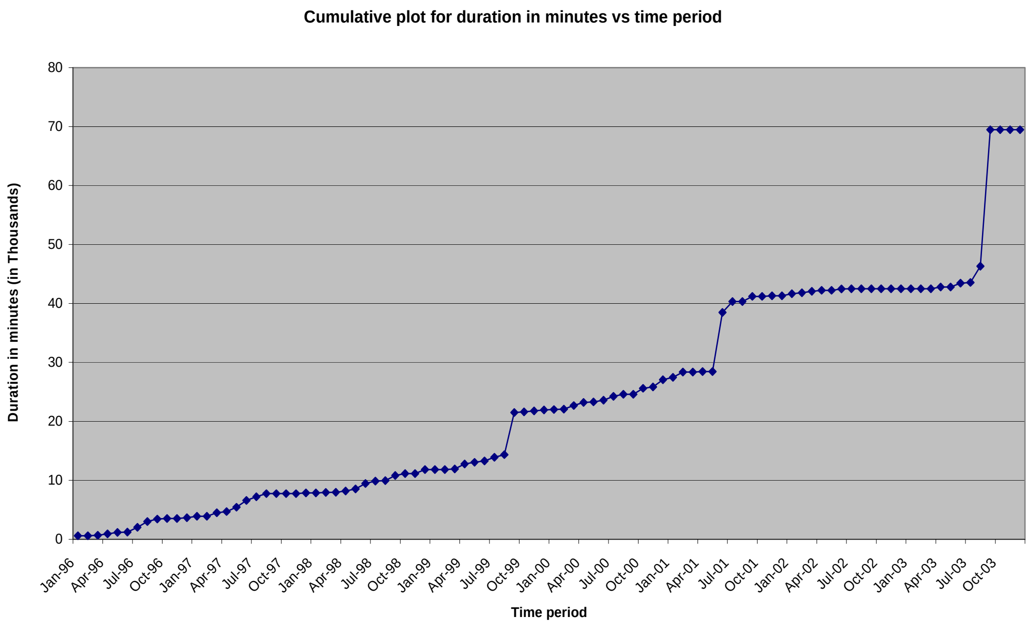


Figure A2.10: Cumulative Duration in Minutes vs. Time period.

APPENDIX 3: Quarterly Analysis of the Power Outages data

This appendix presents quarterly plots for customers affected, blocked calls, total customers affected, duration of outages and the frequency count of the outages.

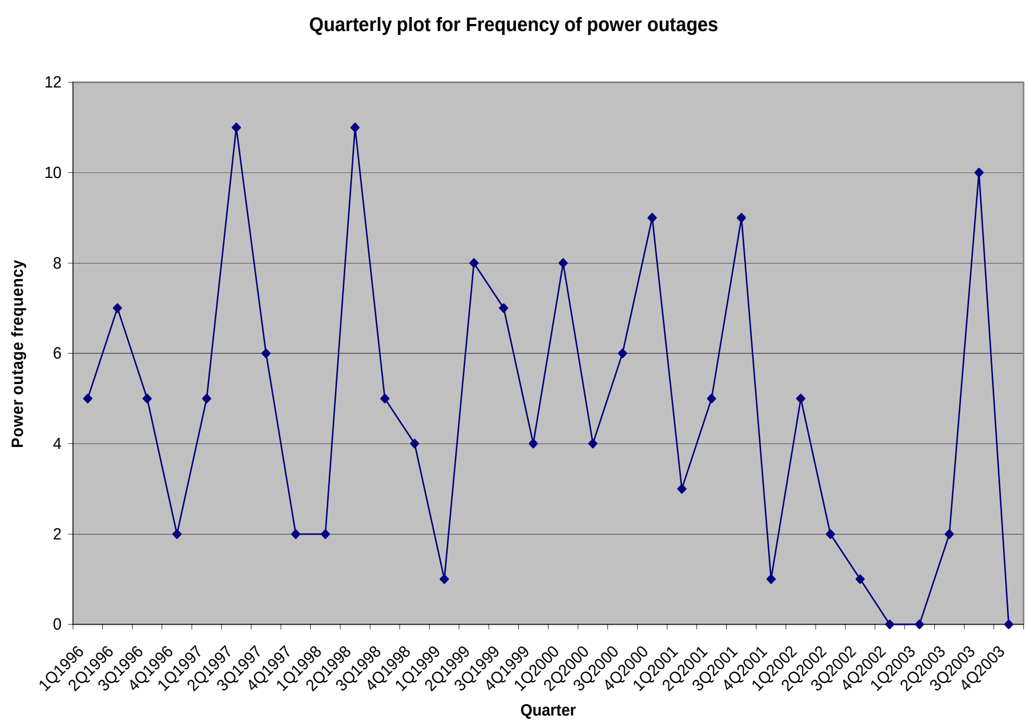


Figure A3.1: Power outage frequency vs. Time period.

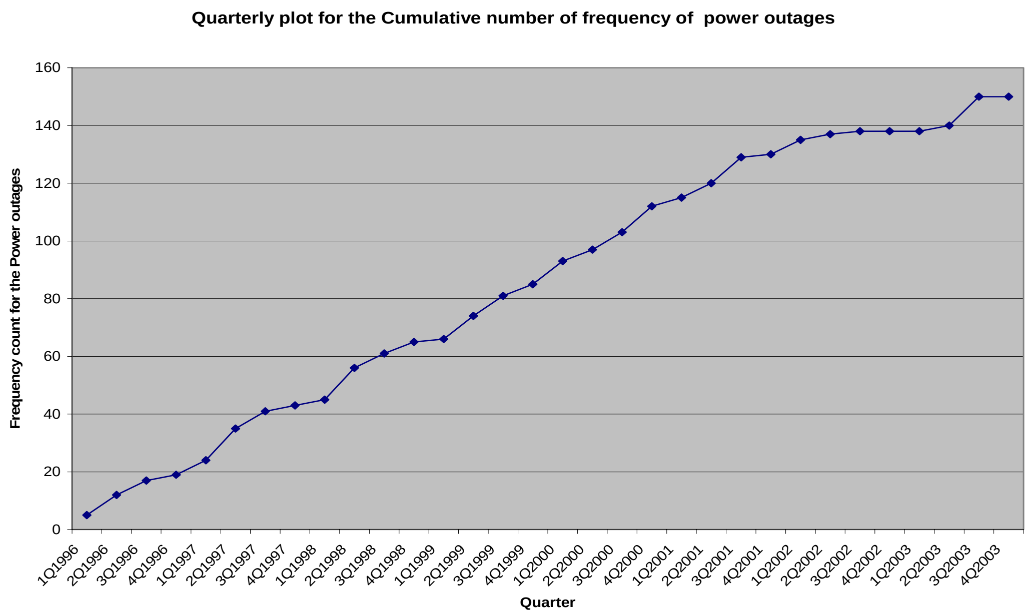


Figure A3.2: Cumulative of Power outages count vs. Time period.

Figure A3.3: Customers affected vs. Time period.

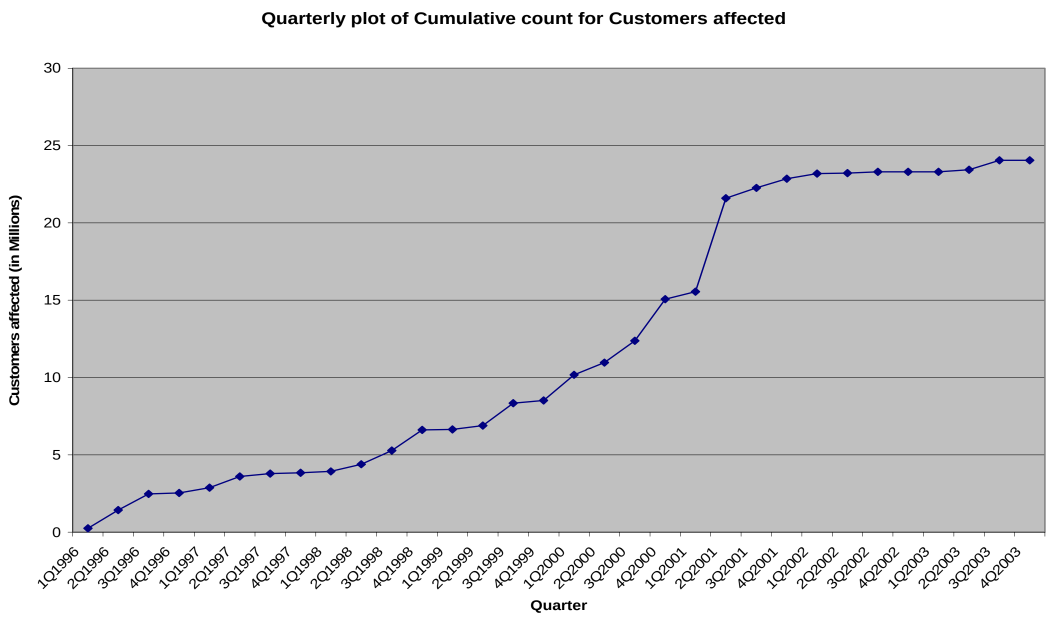


Figure A3.4: Cumulative of Customers affected vs. Time period.

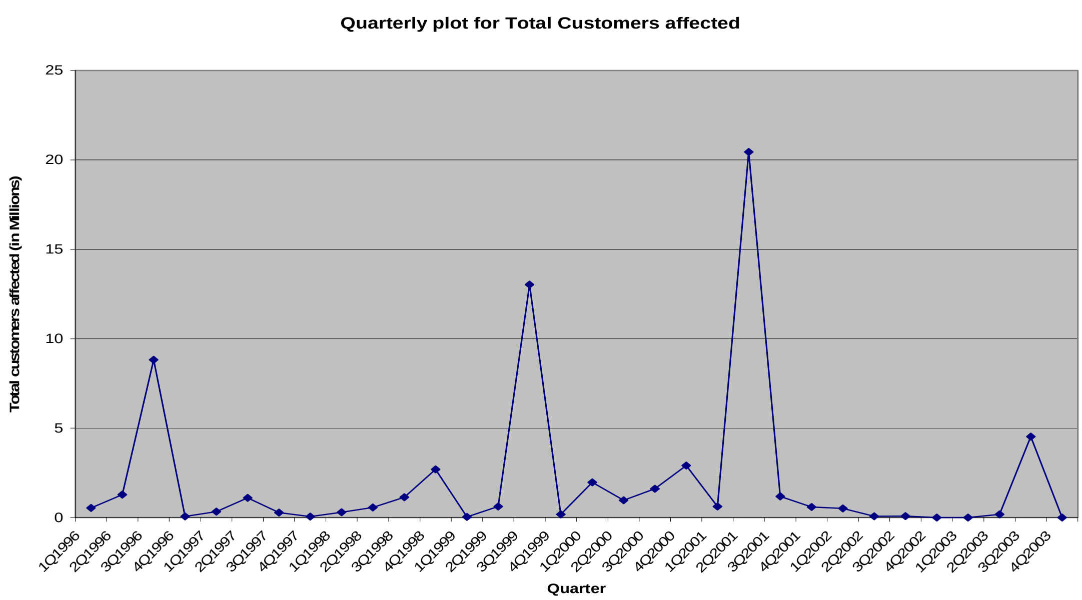


Figure A3.5: Total Customers affected vs. Time period.

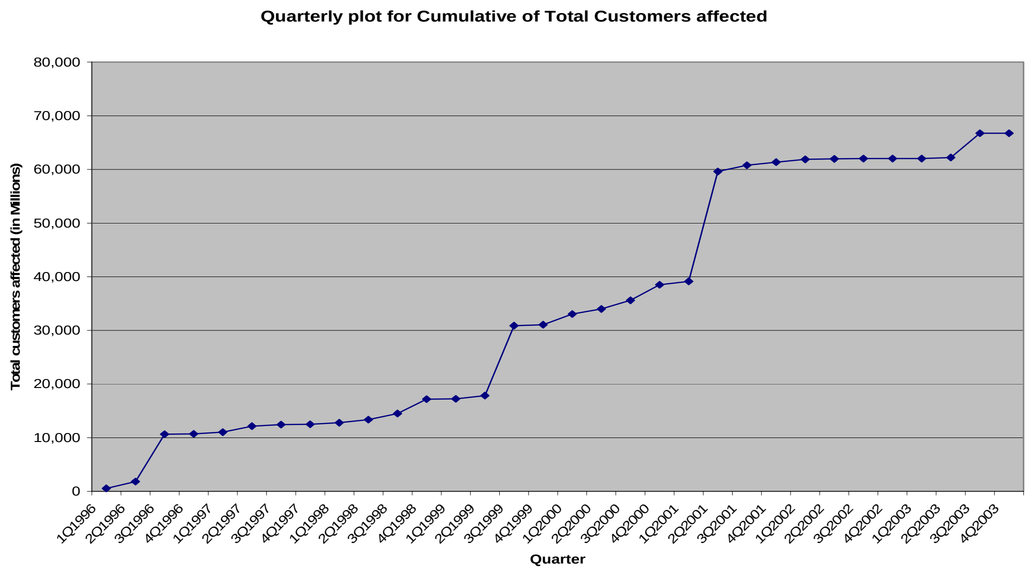


Figure A3.6: Cumulative of Total Customers affected vs. Time period.

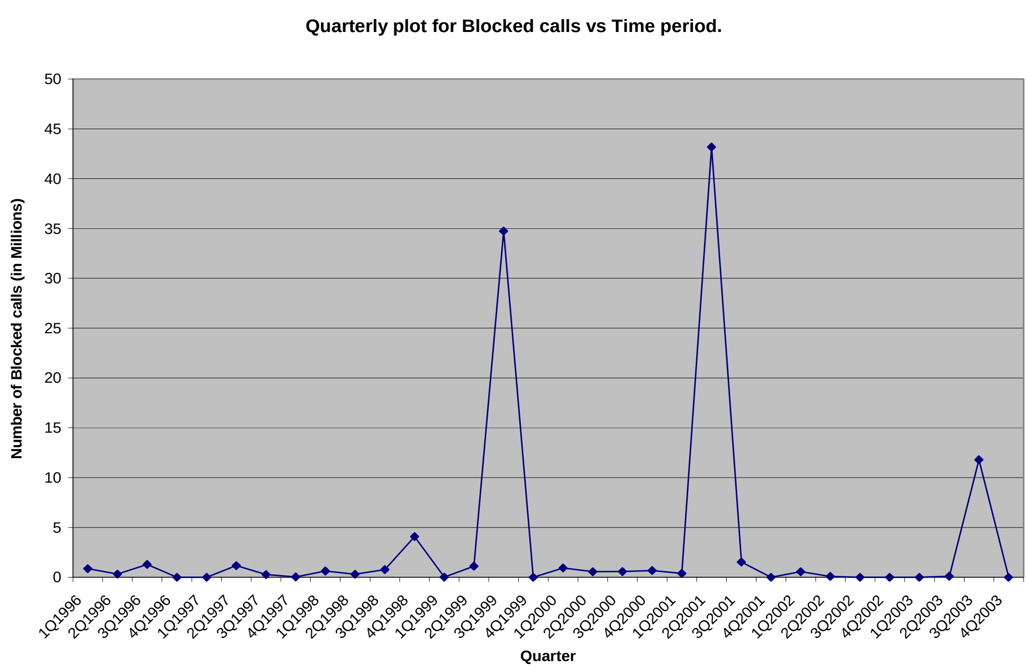


Figure A3.7: Blocked calls vs. Time period.

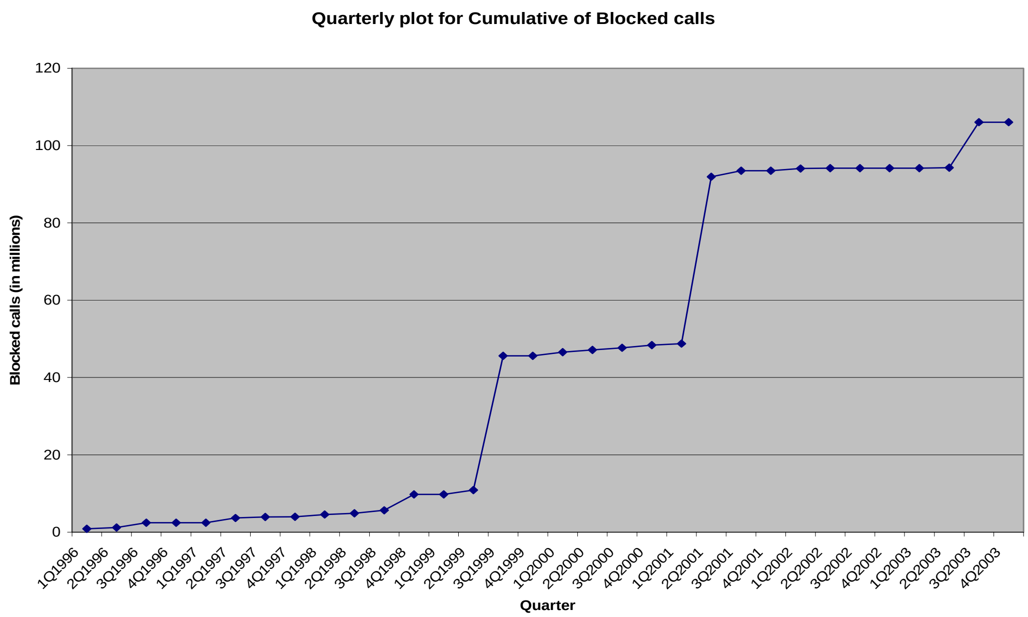


Figure A3.8: Cumulative of Blocked calls vs. Time period.

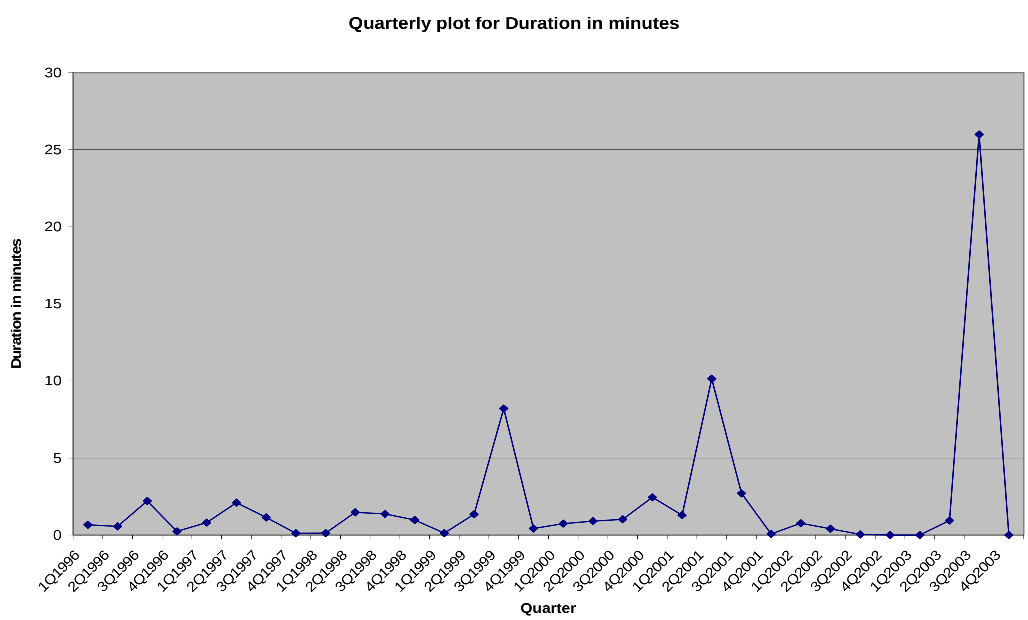


Figure A3.9: Duration in minutes vs. Time period.

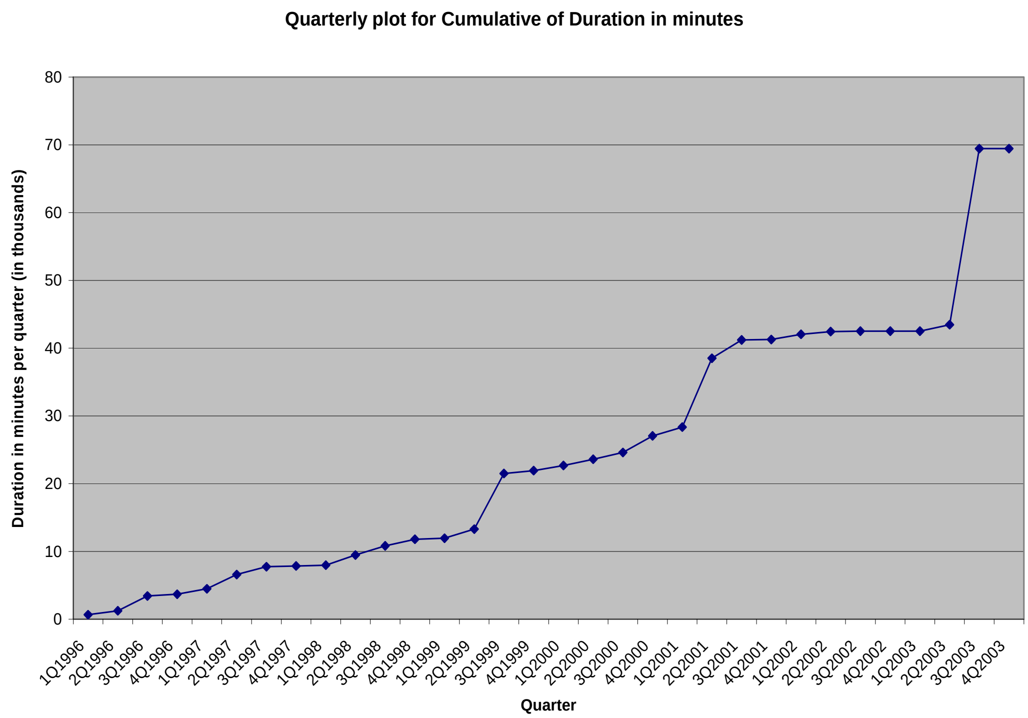


Figure A3.10: Cumulative of Duration in Minutes vs. Time period.

APPENDIX 4: Probability distribution plots for variables

This appendix presents fitted probability distributions and empirical distributions. Fitted functions include probability distribution functions (PDF) and cumulative distribution functions (CDF) for customers affected, blocked calls, total customers affected, duration of outages and the frequency count of the outages.

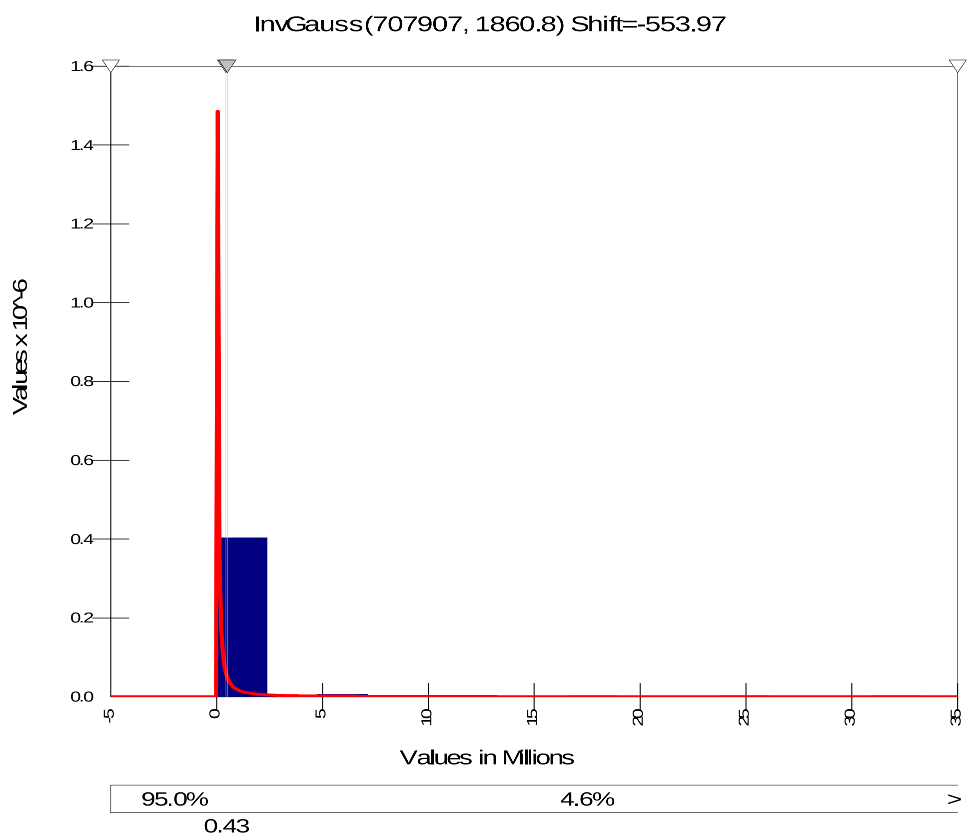


Figure A4.1 Blocked calls: Inverse Gaussian distribution (Density-Area plot).

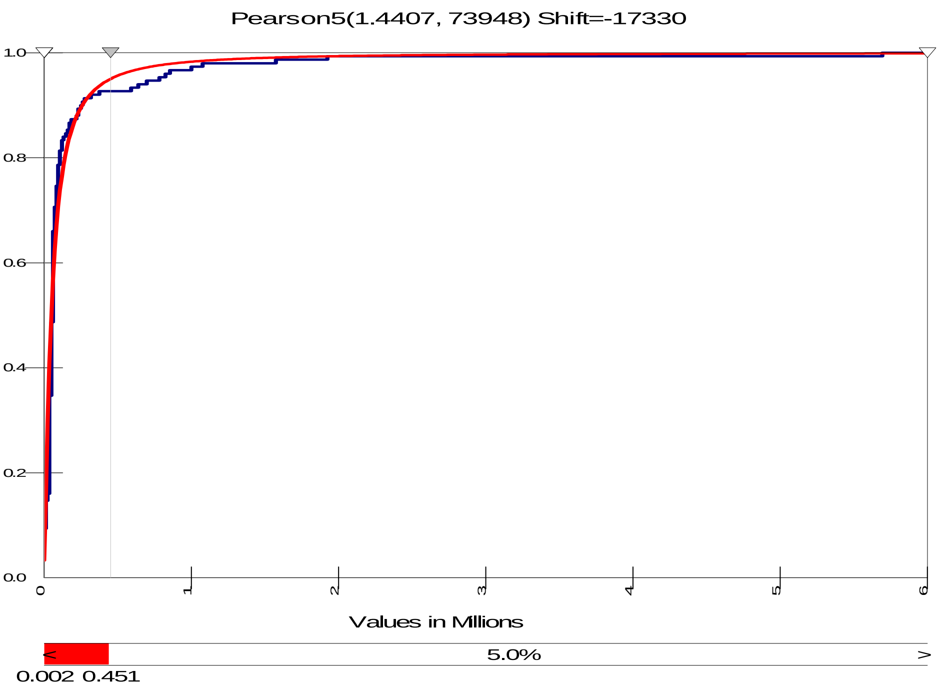


Figure A4.2: Customers affected: Pearson5 distribution.

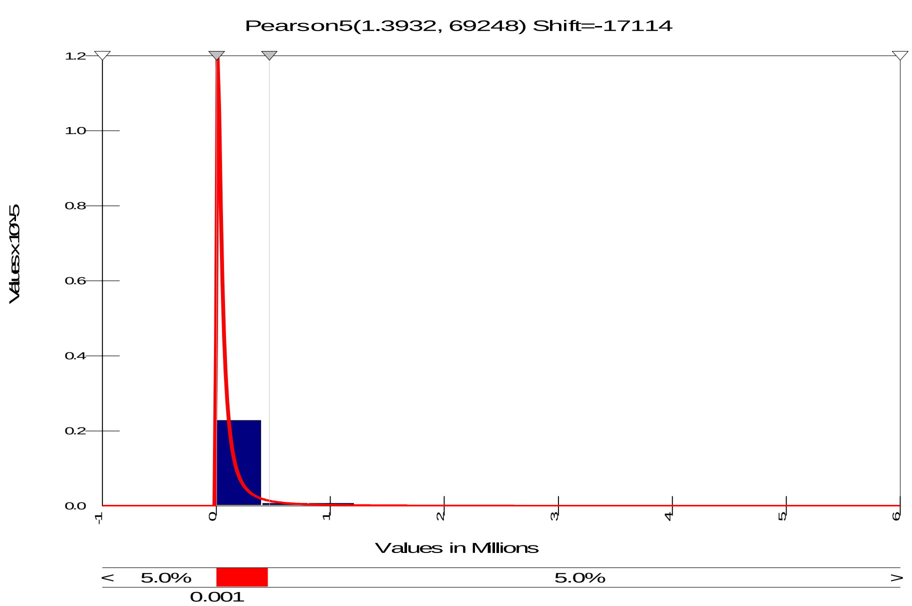


Figure A4.3 Customers affected: Pearson5 distribution (Density-Area plot).

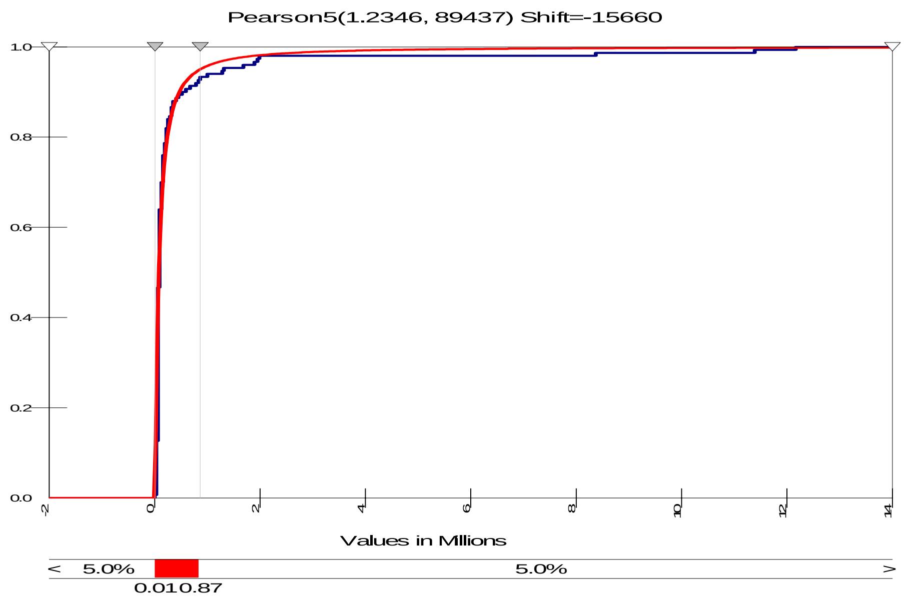


Figure A4.4: Total Customers affected: Pearson5 distribution.

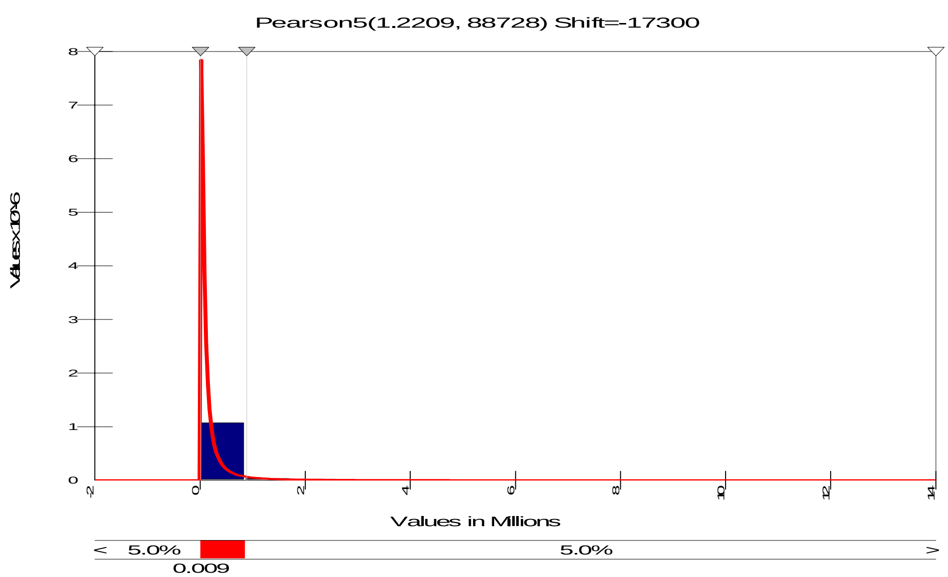


Figure: A4.5 Total Customers affected: Pearson5 distribution (Density- Area plot).

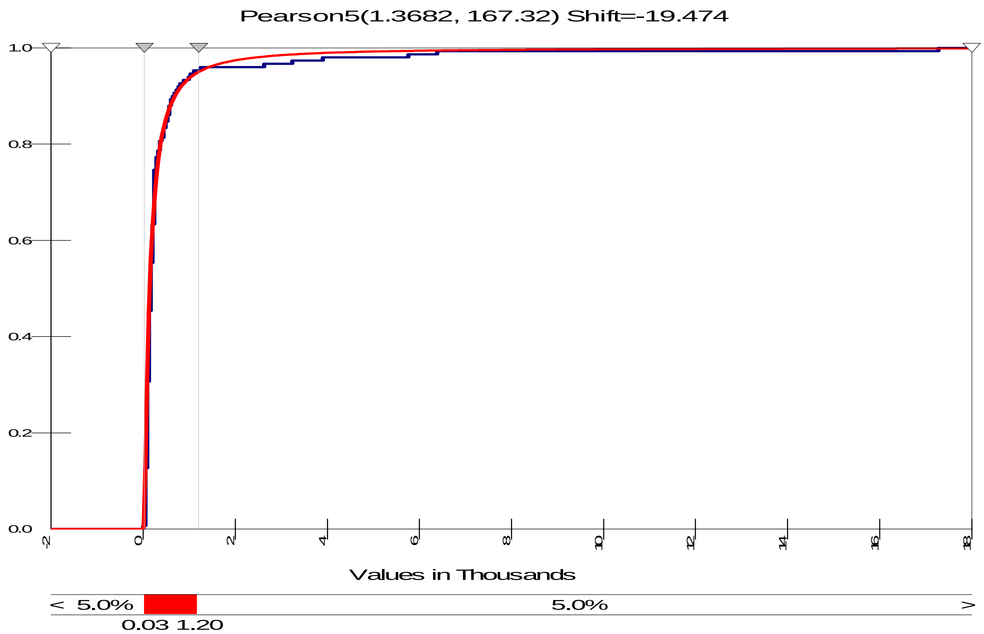


Figure A4.6: Duration in minutes: Pearson5 distribution.

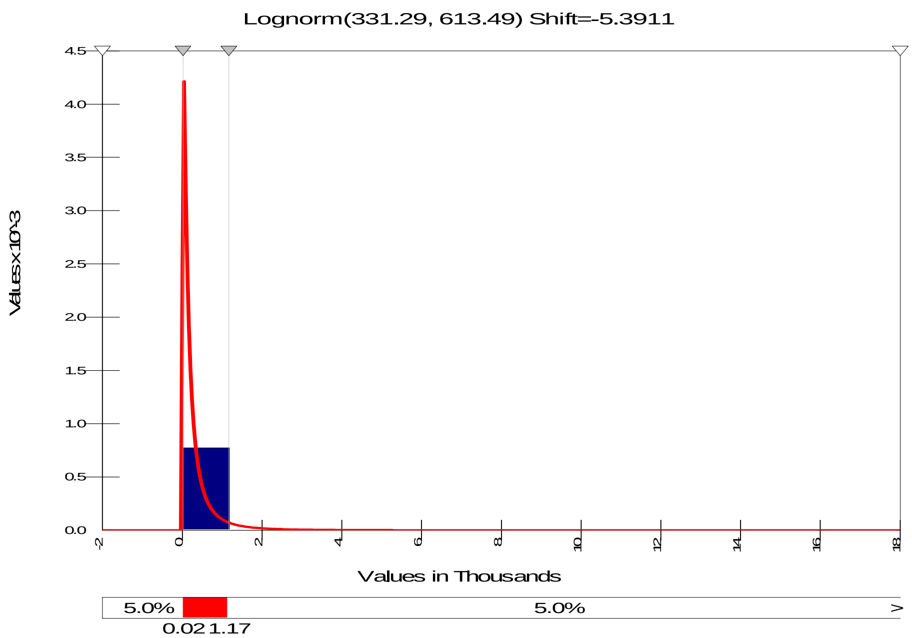


Figure: A4.7: Duration in Minutes: Pearson5 distribution (Density-Area plot).

Figures A4.8, A4.9 and A4.10 show the frequency distribution plots for the variables-Blocked calls, customers affected and the total customers affected respectively.

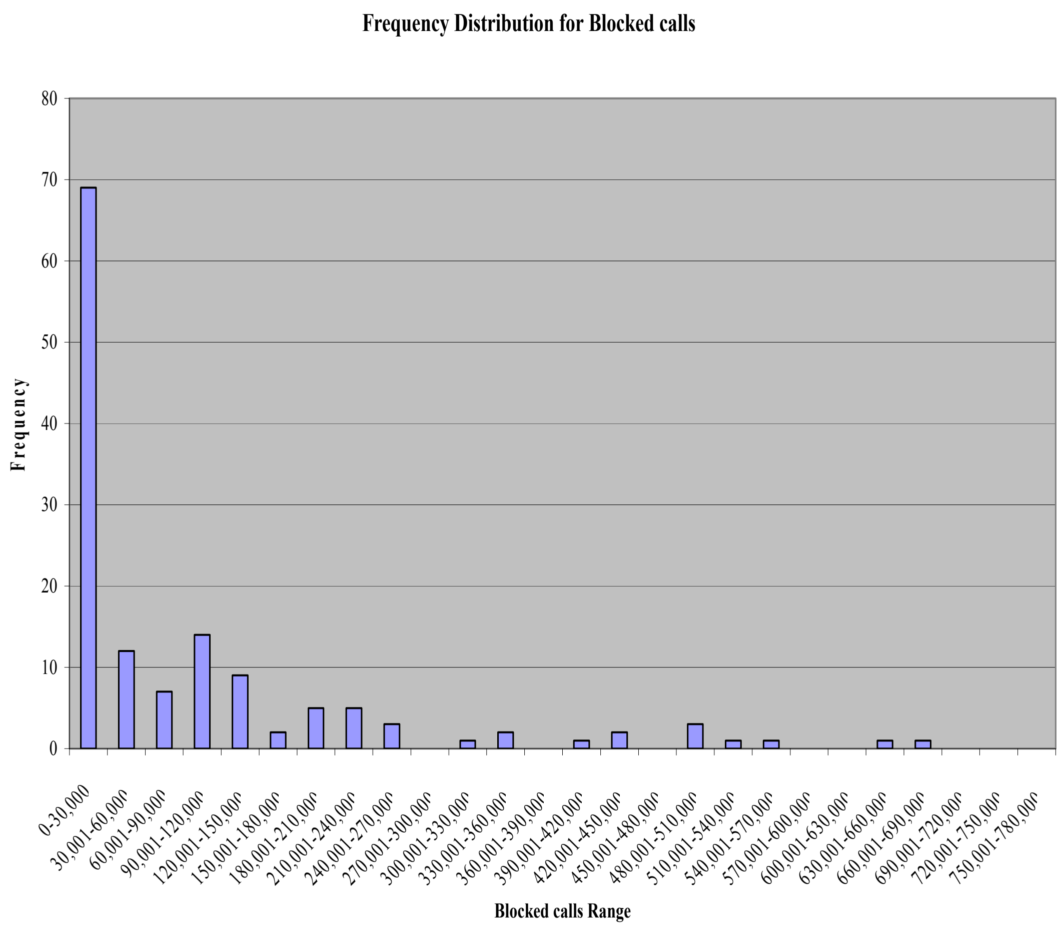


Figure A4.8: Frequency Distribution for Blocked calls.

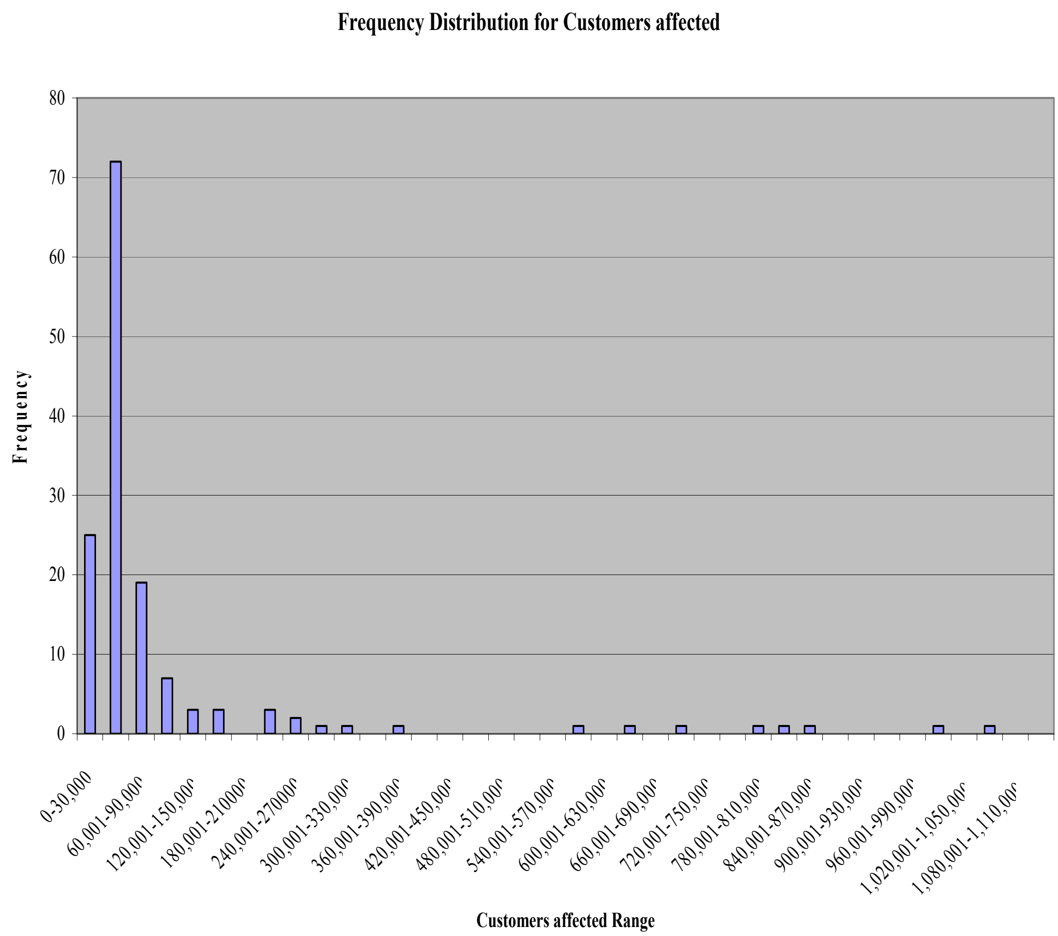


Figure A4.9: Frequency Distribution plot for Customers affected.

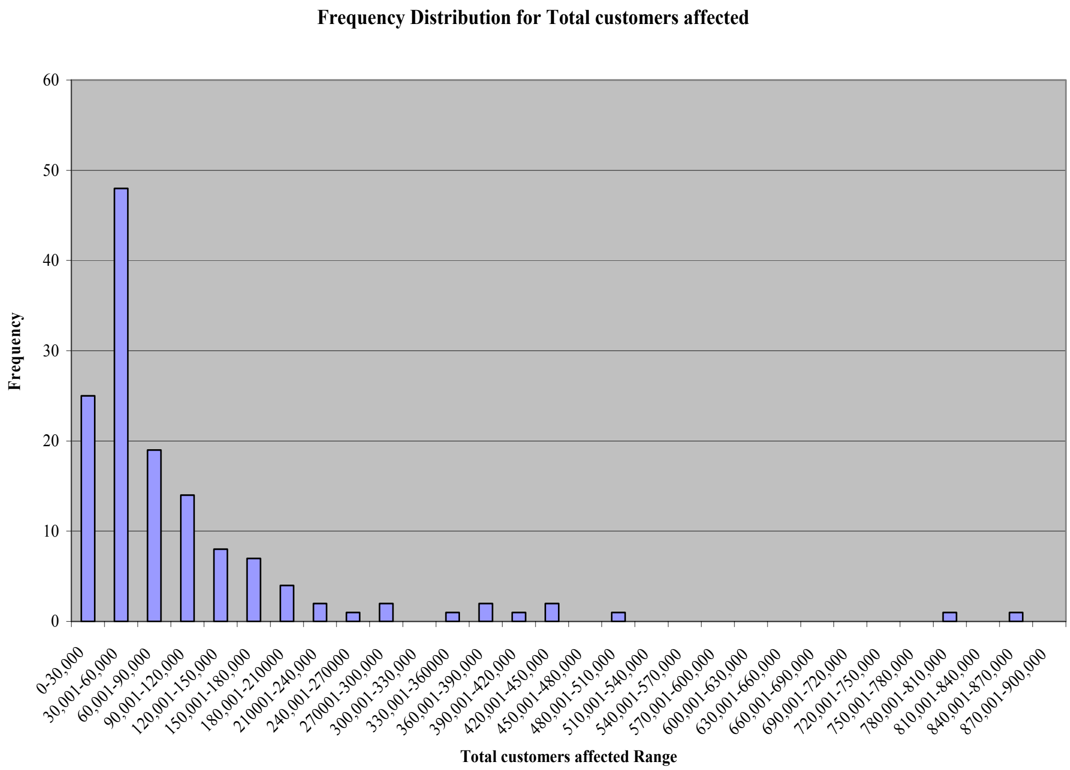


Figure A4.10: Frequency Distribution plot for Total Customers affected.

APPENDIX 5: Commands in Mac ANOVA for Poisson Regression

The following table shows some of the commands used for the Poisson regression in Mac ANOVA.

Table A5.1 Commands used for Poisson Regression in Mac ANOVA.

Function	**Operation**
Vecread (string: CLIPBOARD)	Reads the content from the clipboard sequentially row by row.
Poisson (Model Equation)	Used to perform Poisson regression for the model equation given in the parenthesis.
Regcoefs (Model equation)	Used to obtain the regression coefficients for the model equation given in the parenthesis.

APPENDIX 6: Low, Medium and High impact outages

The plot below shows the total number of power outages that come under the different categories for the trigger cause.

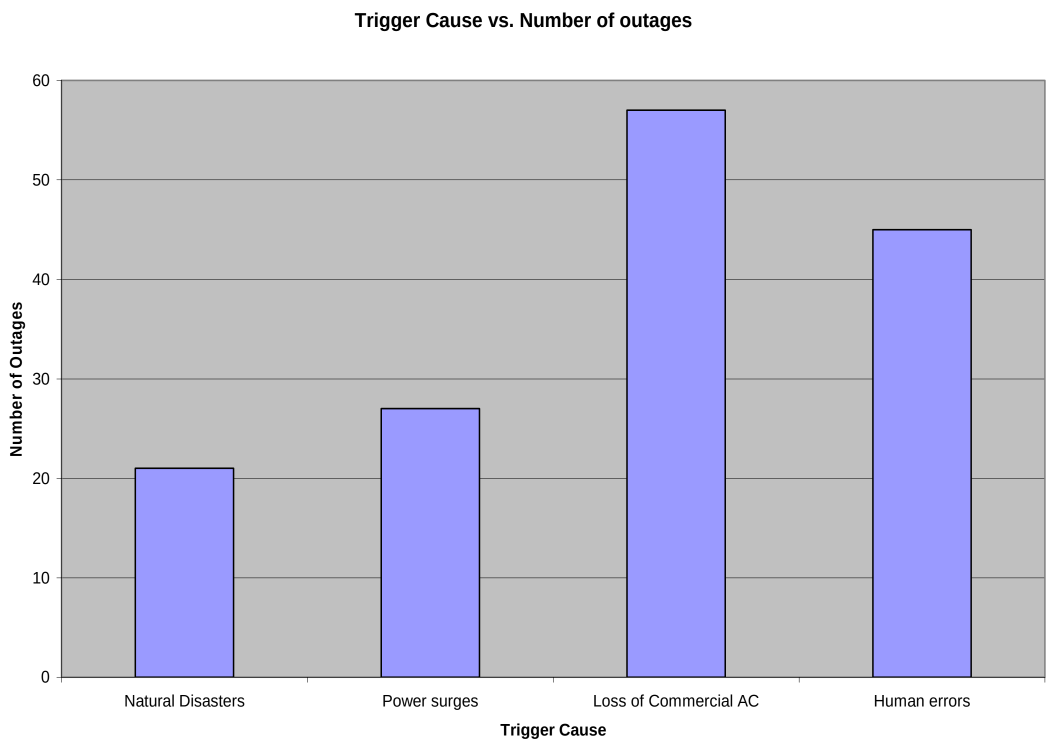


Figure A6.1: Trigger causes vs. number of power outages under each cause.

The plot below shows the total number of power outages that come under each category of the different root causes.

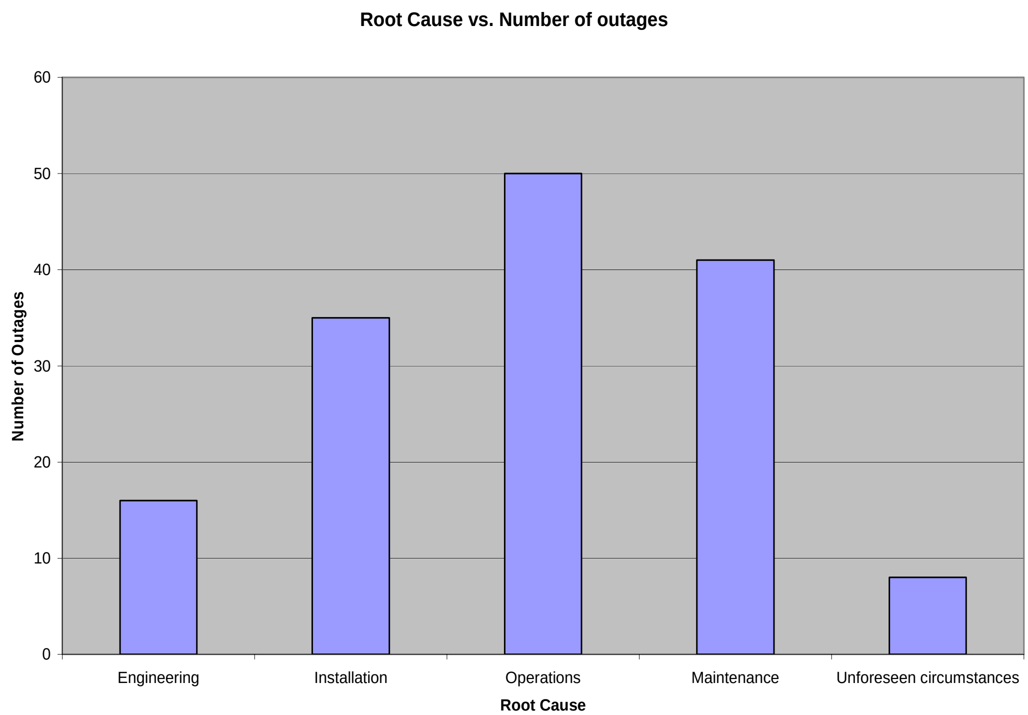


Figure A6.2: Root causes vs. number of power outages under each cause.

The plot below shows the component that is most closely associated with the root causes of the power outages and the total number of power outages that come under each category.

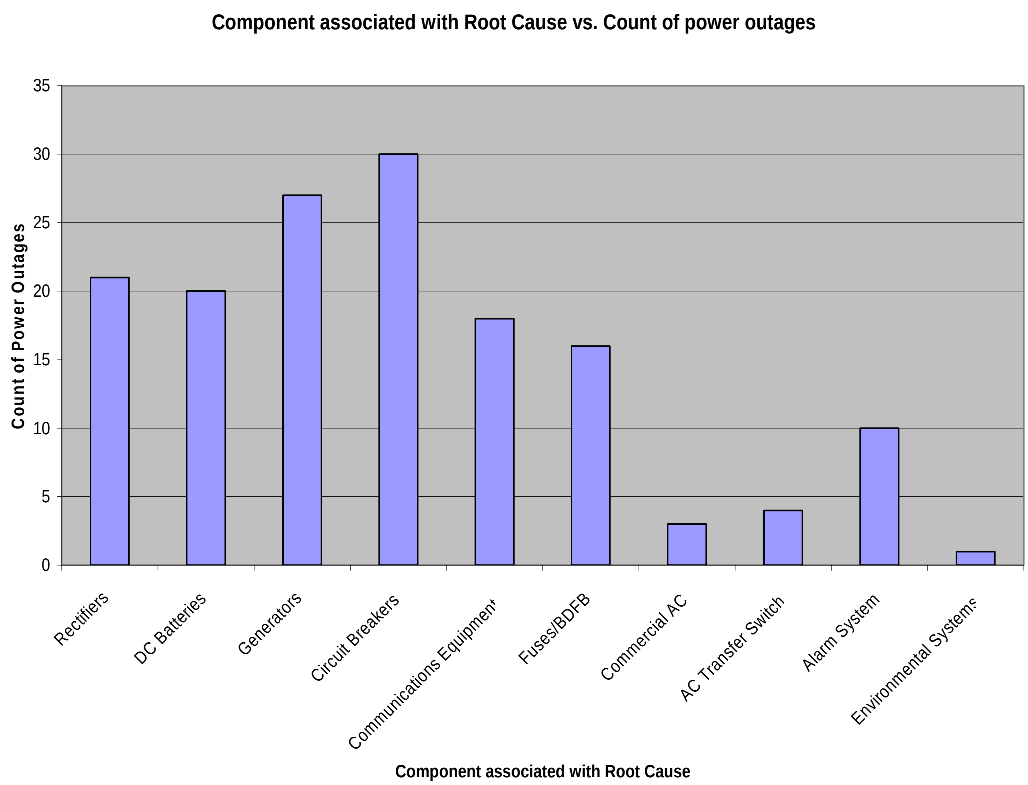


Figure A6.3: Component most associated with the root cause vs. Number of power outages associated with each component.

APPENDIX 7: NRIC proposed Best Practices [4]

Table A7: Best Practices and the recommendations.

Best practice number	Recommendation
6-5-0688	Each company must have an alarm strategy.
6-5-0672	Provide a minimum of 3 hours battery reserve for central offices equipped with fully automatic standby systems.
6-5-0690	Redundancy must be provided, so that no single point alarm system failure will lead to a battery plant outage.
6-5-0689	Provide a separate "battery discharge" alarm for all battery plants. Program the alarm to repeat (e.g., at least every 15 minutes).
6-5-0697	Employ an "Ask Yourself" program to supplement conventional training. This initiative is intended to reinforce the responsibility every employee has to ensure flawless network service. Employees should stop and resolve problems when they can't answer yes to any of the following questions: • Do I know why I'm doing this work? • Have I identified and notified everybody who will be directly affected by this work? • Can I prevent or control a service interruption? • Is this the right time to do this work? • Am I trained and qualified to do this work? • Are work orders, MOPs, and supporting documentation current and error-free?

[4] These Best Practices are taken from the NRIC website as it is and reproduced here for the convenience of the reader.

	• Do I have everything I need to quickly restore service if something goes wrong? • Have I walked through the procedure?
6-5-0650	Place strong emphasis on human activities related to the operation of power systems (e.g., maintenance procedures, alarm system operation and response procedures, and training for operations personnel (craft)). Provide hands-on training for operation and maintenance of power equipment, including regularly scheduled refresher training. Train local workforces on AC switchgear to understand procedures and stage occasional rehearsals.
6-5-0635	In concert with other tenants in the location, ensure that AC surge protection is provided at the service entrance to minimize the effects caused by lightning or extreme voltage fluctuations.
6-5-0662	Service Providers should run engines for a period of at least 1 hour on a monthly basis and, at least 5 hours, with all available loads annually. Perform annual evaluation/maintenance of all power equipment. Maintain the power alarms by testing the alarms on a scheduled basis.
6-5-0527	Equipment areas should be controlled and alarmed within manufacturer's specifications (e.g., temperature, humidity).
6-6-1027	Central Offices should be equipped with on-site battery

	strings and emergency power sources to provide an immediate and continuous source of power in the event that commercial power is interrupted in order to ensure continuity of services. Periodic maintenance routines of the batteries and power sources including, but not limited to engine runs should be performed to assure stand-by power reliability.
6-5-0657	Design standby generator systems for fully automatic operation and for ease of manual operation, when required.
6-5-0676	Low voltage disconnects should not be used at the battery plant.
6-6-5207	Service Providers, Network Operators and Property Managers should take appropriate precautions at critical installations to ensure that fuel supplies and alternate sources are available in the event of major disruptions in a geographic area (e.g., hurricane, earthquake, pipeline disruption). Consider contingency contracts in advance with clear terms and conditions (i.e. Delivery time commitments, T&Cs).
6-5-0684	Verify DC fusing levels throughout the power supply and distribution system, especially at the main primary distribution board, to avoid over fusing or under fusing. All new power equipment, including batteries should conform to NEBS.
6-6-5197	Service Providers should periodically inspect, or test as appropriate, the grounding systems in critical network facilities.
6-6-0512	Service Providers and Network Operators should

	perform periodic inspection of cable ways (e.g., through floor and through wall passage ways, sealing compounds, fire and water stopping, etc.). Public Safety Service and Support providers should also perform these inspections at their communication centers.
6-5-0637	Assure programs exist for alarm testing.
6-6-0761	Network Operators and Service Providers should conduct periodic verification of the office synchronization plan and the diversity of timing links, power feeds and alarms.
6-6-5209	Service Providers, Network Operators and Property Managers should tightly control access to the AC transfer switch housing area, and ensure that scheduled maintenance of the transfer switch is performed and spare parts are available.
6-5-0674	A modernization program should be initiated or continued to ensure that outdated power equipment is phased out of plant. Service Providers should consider and include the capabilities of smart controllers, local and remote monitoring, and alarm systems when updating their power equipment. Power monitors and smart controllers should be integrated into engineering and operational strategies.
6-5-0544	To avoid water damage from floods, it is recommended that power equipment and other critical network elements should not be located in basements, if possible.