BNL-72166-2004
Formal Report

Electrical Substation Reliability Evaluation with Emphasis on Evolving Interdependence On Communication Infrastructure

(Non-Proprietary Version)

M. A. Azarm and R. A. Bari

Brookhaven National Laboratory
Upton, NY 11973-5000

and

Z. Musicki
Consultant to Brookhaven National Laboratory

January 15, 2004

Brookhaven National Laboratory
Upton, New York 11973-5000

Electrical Substation Reliability Evaluation with Emphasis on Evolving Interdependence On Communication Infrastructure

(Non-Proprietary Version)

M. A. Azarm and R. A. Bari

Brookhaven National Laboratory
Upton, NY 11973-5000

and

Z. Musicki
Consultant to Brookhaven National Laboratory

January 15, 2004

Energy Sciences and Technology Department

Brookhaven National Laboratory
P.O. Box 5000
Upton, NY 11973-5000
www.bnl.gov

Managed by
Brookhaven Science Associates, LLC
for the United States Department of Energy under
Contract No. DE-AC02-98CH10886

*This work was performed under the auspices of the U.S. Department of Energy.

*This work was performed under the auspices of the U.S. Department of Energy.

ABSTRACT

The objective of this study is to develop a methodology for a probabilistic assessment of the reliability and security of electrical energy distribution networks. This includes consideration of the future grid system, which will rely heavily on the existing digitally based communication infrastructure for monitoring and protection. Another important objective of this study is to provide information and insights from this research to Consolidated Edison Company (Con Edison) that could be useful in the design of the new network segment to be installed in the area of the World Trade Center in lower Manhattan. Our method is microscopic in nature and relies heavily on the specific design of the portion of the grid being analyzed. It extensively models the types of faults that a grid could potentially experience, the response of the grid, and the specific design of the protection schemes. We demonstrate that the existing technology can be extended and applied to the electrical grid and to the supporting communication network. A small subsection of a hypothetical grid based on the existing New York City electrical grid system of Con Edison is used to demonstrate the methods. Sensitivity studies show that in the current design the frequency for the loss of the main station is sensitive to the communication network reliability. The reliability of the communication network could become a more important contributor to the electrical grid reliability as the utilization of the communication network significantly increases in the near future to support "smart" transmission and/or distributed generation. The identification of potential failure modes and their likelihood can support decisions on potential modifications to the network including hardware, monitoring instrumentation, and protection systems.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

EXECUTIVE SUMMARY

The objective of this study is to develop a methodology for a probabilistic assessment of the reliability and security of electrical energy distribution networks including the future grid system, which will rely much more heavily on the still developing digitally based communication infrastructure for monitoring and protection. The identification of potential failure modes and their likelihood will support decisions on potential modifications to the network including hardware, monitoring instrumentation, and protection systems. In particular, the U. S. Department of Energy noted that an important objective of this study is to provide information and insights from this research to Con Edison that could be useful in the design of the new network segment to be installed in the area of the World Trade Center in lower Manhattan.

The traditional approach to electrical grid reliability is based on deterministic analyses for congestion and transient response under normal conditions or a condition that satisfies "a single failure criterion." Such methods have been shown to be effective and have resulted in sound designs, which are robust to major single failures. Con Edison's network and supporting transmission and substation design is unique and exceeds this "single failure" criterion in many respects. Nevertheless, past events have shown that multiple cascading failures under unfavorable conditions have been the major contributor to losses of electrical distribution systems, in general, and even in the case of Con Edison's unique design. Another factor in the evolution of the electrical grid systems is their recently increasing reliance on the newer digital communication infrastructures for protection and monitoring which are not easily amenable to traditional deterministic analysis. This reliance is expected to greatly increase to provide anticipated communication architectures that would be required to deal with coordination and control of remote "smart" transmission (self-healing grid) and/or a future larger population of smaller distributed generators and/or micro-grids.

Powerful reliability methods have been developed over the past three decades, which could be tailored for use in evaluating the reliability of the existing and the future electrical grid system. These methods have the capability of systematically, and in an efficient manner, incorporating the deterministic models for congestion and transient response analyses.

Our method is microscopic in nature and relies heavily on the specific design of the portion of the grid being analyzed. It extensively models the types of faults that a grid could potentially experience, the response of the grid, and the specific design of the protection schemes. The importance of fault detection and protection schemes is heavily emphasized and the role of future reliance on the communication infrastructure is addressed. Finally, the methods proposed here are quantitative in nature, thereby allowing prioritization, reliability allocation to different modules, and verification that the design meets the allocated reliability parameters.

This report demonstrates that the proposed methodology can be extended and applied to the electrical grid and to the supporting communication network. A small sub-section of a hypothetical grid based on the existing New York City electrical grid system of Con Edison is used to demonstrate the methods. Our effort included: familiarization with the Con Edison design criteria and their electrical grid distribution system and configuration, customizing the methodology to be used for reliability evaluation of the coupled electrical and communication networks, and demonstrating that methodology for prototypic situations in the real world.

The system considered here is comprised of a main station, which feeds to substations. We considered two types of abnormal events for our example grid: a fault in a substation or a fault on the connecting power lines between the main and the substations. The metric or the "undesirable end-state" with which

we measured the electric grid reliability was the loss or potential loss of the main station, which would result in a widespread loss of electric power to consumers. We also calculated the frequency of other end states, which would have lesser impacts.

The results for the two abnormal events analyzed in this report showed that an upper bound frequency of the loss of the main station was on the order of 1E-3/yr (i.e., 1 x 10^{-3} times/year). If all the combinations of similar challenges connected to the main station were added up (i.e., combinations of the main station with all other substations fed by the main station), the overall frequency of the loss of the main station would rise by about a factor of 20, or approximately to2E-2/yr (or about once every 50 years). This is the approximate frequency of widespread power loss due to loss of a main station. The frequency of the loss of both substations (when the main station is not lost) is an order of magnitude lower (about 1.6 E-3) (however, the number of affected customers would be much smaller than in the case of loss of a main station). The loss of single substation did not appear to be likely since Con Edison utilizes "N-2" contingency measure. Per Con Edison design, there are only 10 hours per year that three out of five transformers operation per substation is required. Thus during this short period, a loss of three transformers is necessary to cause a loss of the substations. This probability by far was smaller than the probability of other faults simulated.

The two cases (abnormal events) analyzed here also showed about equal contributions to the loss of the main station frequency, i.e., in both cases, the conditional probability of this end state occurring (given the occurrence of the abnormal event) is about 1E-3. Furthermore, the examinations of various design features and potential configurations analyzed in this study did not show any obvious vulnerability in any of the two scenarios.

Sensitivity studies show that the frequency for the loss of the main station is sensitive to the Verizon communication network reliability, and it is also sensitive to common cause failure within the electrical network. There is a fair degree of redundancy and diversity in responding to challenges, but this can still be obviated by some common cause failures. The reliability of the communication network is expected to become a major contributor to the electrical grid reliability as its utilization significantly increases in the near future. It was shown that the reliability and independence of the common portion of communication infrastructure, i.e., the central offices, would become the most important issue in maintaining the grid reliability. Therefore, common cause failures and external events capable of affecting a number of central offices would require formal analyses. Preliminary examination of the experiential data and of the modeling techniques determined that accidents (not routine unavailabilities) with the capability of affecting more than one central office would become the major issue in maintaining the communication network reliability. A preliminary reliability guideline is proposed in Section 5.5.2 to ensure a high reliability for the communication network, given the adverse impact of potential accident conditions.

Upon continuation of this project, we will work collaboratively with Con Edison to apply the methods in a systematic way to a larger portion of the actual New York City grid. We also envision the emergence of a procedure guide for standardize reliability evaluation of the grid system to be used by all analysts for further applications and for development of methods, associated tools, and databases.

ACKNOWLEDGMENTS

The authors are grateful for the helpful collaboration and guidance of the Consolidated Edison Company of New York in performing this research. In particular, we thank Howard Chu for many helpful discussions and for providing instructive comments and essential information on relay protection features. We are also thankful to many others at Con Edison, especially Arthur Kressner, Frank Doherty, John Miksad, Pat Duggan, and Jay Wilamowski for their cooperation and interest. Con Edison arranged for a tour of a representative substation in Manhattan, which proved to be an essential aspect of this work.

We had several valuable discussions with Eugene McAuliffe of Verizon on the reliability of the existing and potential communication interfaces with the Con Edison electrical network.

At the U. S. Department of Energy, we thank Patricia Hoffman for sponsoring this research and for helping to provide a focus for the formulation of the problem addressed. Our project monitor was Joseph Galdo (now retired from DOE) and he provided encouragement and support during the course of this work. We are indebted to Tina Kaarsberg (now on the Science Staff of the U. S. House of Representatives) for providing thoughtful guidance and suggestions during the early stages of this program. Finally, we are grateful that Philip Overholt has continually shown interest in this research and has willingly provided perspective and context within the DOE mission and the electrical energy needs of the nation.

A Laboratory Directed Research and Development Program award has supported the basic development aspects of this work by Brookhaven National Laboratory.

1. INTRODUCTION AND OBJECTIVES

The traditional approach to electrical grid reliability [1-1, 1-2] is based on deterministic analyses for congestion and transient response under normal conditions or a condition that satisfies "a single failure criterion." Such methods have been shown to be effective and have resulted in sound designs, which are robust to major single failures. Past events [1-3 - 1-5] have shown that multiple cascading failures under unfavorable conditions have been the major contributor to losses of electrical distribution systems. Another factor in the evolution of electrical grid systems is their ever-increasing reliance on communication infrastructures for protection and monitoring, which are not easily amenable to traditional deterministic analysis.

Others have developed methods for identification of the potential vulnerability of a large grid system using the grid topology (e.g., application of small world techniques), and use of empirical fault propagation using epidemiological models [1-9 – 1-11]. These methods are macroscopic in nature and do not address the detailed design issues of a grid system. At best, they can identify portions of the grid that are suspected of potential vulnerabilities.

To examine multiple cascading failures and to develop an integrated model to account for communication interface, reliability methods have been utilized by this study. Powerful reliability methods have been developed in the past three decades in the nuclear industry [1-6 – 1-8], which could be tailored for use in evaluating the reliability of the existing and the future electrical grid system. These methods have the capability of systematically, and in an efficient manner, incorporating the deterministic models for congestion and transient response analyses.

In contrast to the traditional models, our model, as demonstrated in this report, is microscopic in nature and relies heavily on the specific design of the portion of the grid being analyzed. It extensively accounts for the types of faults that a grid could potentially experience, the response of the grid, and the specific design of the protection schemes. The importance of fault detection and protection schemes is heavily emphasized and the role of future reliance on the communication infrastructure is addressed [1-12]. Finally, the methods proposed here are quantitative in nature, thereby allowing prioritization, reliability allocation to different modules, and the verification that the design meets the allocated reliability goals.

The objective of this study is to develop a methodology for a probabilistic assessment of the reliability and security of electrical energy distribution networks including the future grid system. The latter will rely heavily on the existing digitally based communication infrastructure for monitoring and protection. The identification of potential failure modes and their likelihoods will support decisions on potential modifications to the network including hardware, monitoring instrumentation, and protection systems. In particular, the U. S. Department of Energy noted that an important objective of this study is to provide information and insights from this research to Con Edison that could be useful in the design of the new network segment to be installed in the area of the World Trade Center in lower Manhattan.

The purpose of this report is to demonstrate that the existing technology can be extended and applied to the electrical grid and to the supporting communication network. A small subsection of a hypothetical grid based on the existing New York City electrical grid system of Con Edison is used to demonstrate the methods. Upon continuation of this project, we will work collaboratively with Con Edison to apply the methods in a systematic way to a larger portion of the actual New York City grid. We also envision the emergence of a procedure guide for standardizing reliability evaluation of the grid system to be used by all analysts for further applications and for development of these methods, associated tools, and databases.

Implications for the Transmission Grid

While the present study focuses on a distribution network, the methods developed and demonstrated here can be applied to the analysis of a transmission grid. This could support some of the objectives identified in the National Electric Delivery Technologies Roadmap Workshop [1-12]. The approach presented here could more specifically support the short- and long-term objectives for reliability and security areas as summarized below:

- Metrics for quality reliability and availability at grid level
- Improved reliability via probabilistic methods
- Reduce outages to one per year for entire national grid
- Design N-3/N-4 contingency grid including risk analysis.

It is noteworthy to excerpt the following from Appendix F on of Reference 1-13 on advanced transmission technologies.

"Requisite technologies include:

- Improved real-time tools to examine power system signals for warnings of dangerous behavior. The more rapidly that operator intervention is initiated, the more likely that a blackout can be averted.
- Improved visualization, giving operators a bird's-eye view of the power system.
- Mathematical criteria, tools, and procedures for reducing and/or characterizing errors in power system models.
- Characterizations and probabilistic models for uncertainties in power-system resources and operating conditions.
- Probabilistic models, tools, and methodologies for collective examination of contingencies that are now considered individually.
- Cost models for quantifying the overall impact of contingencies and ranking them accordingly. It is essential that these models be realistic and suitable for use as standards for planning and operation of the overall transmission grid.
- Risk management tools, based on the above probabilistic models of contingencies and their costs, that "optimize" use of the electricity system while maintaining requisite levels of reliability.

Development of the technology noted above can likely be expedited through technology transfers from outside the power industry. Even so, there are special and difficult problems. The knowledge base for actual power system behavior, required both to define the subject technologies and obtain best value from their use, is not well evolved. The knowledge base and the technologies should develop together, in or close to a practical utility environment.

Furthermore, probabilistic planning is not just a smooth extrapolation of current practices. It requires new skills and practices."

We believe that our study is in tune with several of these recommendations. In particular, our introduction of probabilistic tools and methods can be readily extended to the transmission grid. Further, we are aligned squarely with the recommendation that the "knowledge base and the technologies should develop together, in or close to a practical utility environment," as is evidenced by the collaboration with Con Edison throughout this project.

Implication for Critical Infrastructure Protection

This study addresses reliability and security in the context of the ability of an electrical system to function under degraded conditions. The methods developed and demonstrated here can also be applied to address the question of the vulnerability of the infrastructure to various external disturbances, both by naturally caused phenomena (e.g., storms) and by human-induced events. Human error is already incorporated in the analysis. However, the likelihood of acts of commission is more difficult to model probabilistically because they may involve an understanding of motivation of such acts. Nevertheless, a system designed and/or improved through the use of risk-informed insights can provide a margin of protection that would enhance the robustness of the system against external disturbances.

References

1-1 Wood, A.J., and Wollenberg, B.F., "Power Generation, Operation, and Control Book," Published by Wiley, New York, 1996.

1-2 Morison, G.K., Kao, B., and Kundur, P., "Voltage Stability Analysis Using Static and Dynamic Approaches," IEEE Transaction on Power System, pp. 1159-1171, August 1993.

1-3 "Review of Selected Electrical System Disturbances in North America," North America Electric Reliability Council, Princeton, New Jersey, March 2001.

1-4 "The Washington Heights Network Shutdown - July 6, 1999," Report by the Corporate Review Committee, Consolidated Edison Company of New York. New York, NY, December 10, 1999.

1-5 Report of the U. S. Department of Energy's Power Outage Study Team, March 2000, http://certs.lbl.gov/pdf/POST_Final.pdf.

1-6 "Severe Accident Risks for VVER Reactors: Vol. 3: Procedure Guides," NUREG/CR-6572, BNL-NUREG-52534, Brookhaven National Laboratory, September 1999.

1-7 "Procedure for Conducting Probabilistic Safety Assessment of Nuclear Power Plants (Level 1)," Safety Series No. 50-P-4, International Atomic Energy Agency (IAEA), 1992.

1-8 "PRA Procedure Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," NUREG/CR-2300, U.S. Nuclear Regulatory Commission, January 1983.

1-9 Adamic, L., " The Small World Web," Proceeding of the European Conference on Digital Libraries, 1999.

1-10 Cassandras, C.G., and Pepyne, D.L., "Optimal Control of a Class of Hybrid Systems," IEEE Transactions on Automatic Control, November 1999.

1-11 Wolpert, D.H., and Macready, W.G., "No Free Lunch Theorems for Optimization," IEEE Transaction on Evolutionary Programming, Vol. 1, No. 1, pp. 67-82,1997.

1-12 Draft Proceedings of National Electric Delivery Technologies Roadmap Workshop, July 8-9, 2003, Washington, DC.

1-13 In the "National Transmission Grid Study," U. S. Department of Energy, May 2002, http://tis.eh.doe.gov/ntgs/reports.html, the importance of information management and control for future transmission grids was highlighted.

2. CON EDISON ELECTRICAL NETWORK

Con Edison is a member of the New York Power Pool (NYPP) and the Northeast Power Coordinating Council. Con Edison serves the most dense electrical load pocket in the world with more than 3.1 million customers in a 604 square-mile area. The company uses a unique concept, called a distributed network, in which each network operates independently from its neighboring networks and is fed from multiple distribution feeder cables. In this manner, the networks are designed so that they can remain energized and continue to carry load even if two or more feeder cables are out of service. This arrangement allows the other feeders to serve the network if two feeders are out of service (second contingency) and distributes the resulting increased load more equitably among the remaining feeder cables. This is done to enhance the overall reliability of the network system.

Con Edison relies heavily on fault zone protection and requires two independent and diverse fault protection schemes for each fault zone, i.e., primary and backup (sometimes referred to as direct and protracted). On some key feeders, Con Edison may have primary, secondary, and backup protection with primary and secondary high-speed trip, and backup trips with some time delay. Fast and reliable isolation of a fault is assured through this design. Con Edison also relies on a communication network for fault isolation as will be discussed next. Con Edison currently is utilizing two types of communication infrastructures. Con Edison is currently using and planning to significantly increase the use and reliance on the leased Verizon network. The communication network system is an integral part of Con Edison electrical network system and is, therefore, an important element in Con Edison's reliability and security system.

2.1 Reliance on Communication Technology

The actuation trip signals from electrical protection logics are transformed to analog audio-tone signals for transmission from one substation to another. The audio-tone signal then should be transmitted from one substation to another for the purpose of isolation of the faulted zone. Another mechanism to provide protection is through the use of pilot wire protection. This uses dc transfer trip, which sends tripping to the remote by applying dc onto the pilot wire, which can be over Verizon leased lines, copper wire, or Con Edison owned telephone lines. The signal transmission could be done by analog means, such as modulated wireless connection (e.g., microwave), or digitally through an existing network, such as Verizon. The latter is currently considered to be more practical and cost effective due to varying distances and geographic conditions between the two options.

Successful implementation of digitally connected could bring about an evolutionary transformation of the current grid system to a future grid system, which would be totally digitally based for the purpose of protection, control, and monitoring. This would, however, increase the reliance of the electrical grid infrastructure on that of the communication infrastructure. Reliability, security, and vulnerability evaluation of both the electrical and communication networks in an integral fashion would be a challenging task worthy of standardization. Con Edison has a strong interest in the development of this new grid paradigm and clearly wants to understand how it would evolve most effectively and reliably.

2.2 Con Edison Reliability Guide

Con Edison has established the following guidelines in order to meet the single failure criteria in retrofitting the existing areas [2-1]. Reference 2-1 describes transmission lines with tapped transformer loads and describes primarily the clearing of faults involving these transformers vs. transmission lines with no tapped transformer loads. Two of these guidelines relating to fault protections are provided below:

1. Provide two independent methods for physically isolating the transmission feeder during station faults,

2. Provide two independent lines of backup protracted fault protection.

The two acceptable independent methods for isolating the transmission feeder during station faults are shown in Table 1.

Table 1 Acceptable Methods for Isolating the Transmission Feeders

Options	Circuit Switcher (CS)	Circuit Interrupter (CI)	Audi-tone transfer trip (ATTT) or Auto-Ground Switch (AGS)
1	PRIMARY	BACKUP	Not Applicable
2	PRIMARY	Not Applicable	BACKUP
3	Not Applicable	PRIMARY and BACKUP	Not Applicable
4	Not Applicable	PRIMARY	BACKUP
5	Not Applicable	Not Applicable	PRIMARY (NEW) and BACKUP (EXISTING)
6	Not Applicable	Not Applicable	PRIMARY (ATTT) and BACKUP (AGS)

A protracted fault relay system consisting of voltage controlled over-current phase relays and a neutral over-current ground relay exist in each switchgear. A backup fault relay trip output should be coordinated with the switchgear protracted fault relay trip such that it would be the last protective system to operate. The trip output should be wired to both primary and backup trip devices.

Additional guidelines are included in Con Edison's electrical design criteria, which specifically deal with segregation, separation, and protection against fire.

References

2-1 Consolidated Edison Guidance on "Electrical Design Criteria: Area Reliability Retrofit Program," Internal Report, Rev No. 0, Jan 21, 1993.

3. EXAMPLE ELECTRICAL NETWORK

For the purpose of the following discussion, it is important to select an example of a semi-hypothetical area design. For this purpose, a portion of the Con Edison substation area connections was used as a guide. However, the example presented below is a simplification of the actual network to facilitate the discussion and the analysis. In this sense, it can be considered as a realistic hypothetical network.

The example is derived from a specific configuration in Manhattan. Con Edison provided relevant information to model the essential features of their network for the purposes of this demonstration study. A plant walk down was done during the summer of 2002 at a specific location in Manhattan. Valuable information was obtained about the operation of the Con Edison network as a result of this familiarization process. A top-level summary of the electrical network rather than a detail discussion is provided in the next section. This is mainly done to comply with the proprietary nature of the Con Edison systems and to abide with the agreement signed between BNL and Con Edison.

3.1 Area Connections

Figure 1 presents a simplified block diagram of this hypothetical network. A ring bus configuration of a 345 kilovolt (KV) substation is feeding several smaller areas through 138 KV lines. Two specific substations–namely, Substations 1 and 2–are considered as a part of this study. The main focus would be on Substation 1. Substation 1 consists of five transformer banks feeding two main sync buses in a typical sync bus connection. Operation of two out of these five transformers would be sufficient for carrying the loads. There is approximately 10 hours during a year that three out of five transformers would be required.

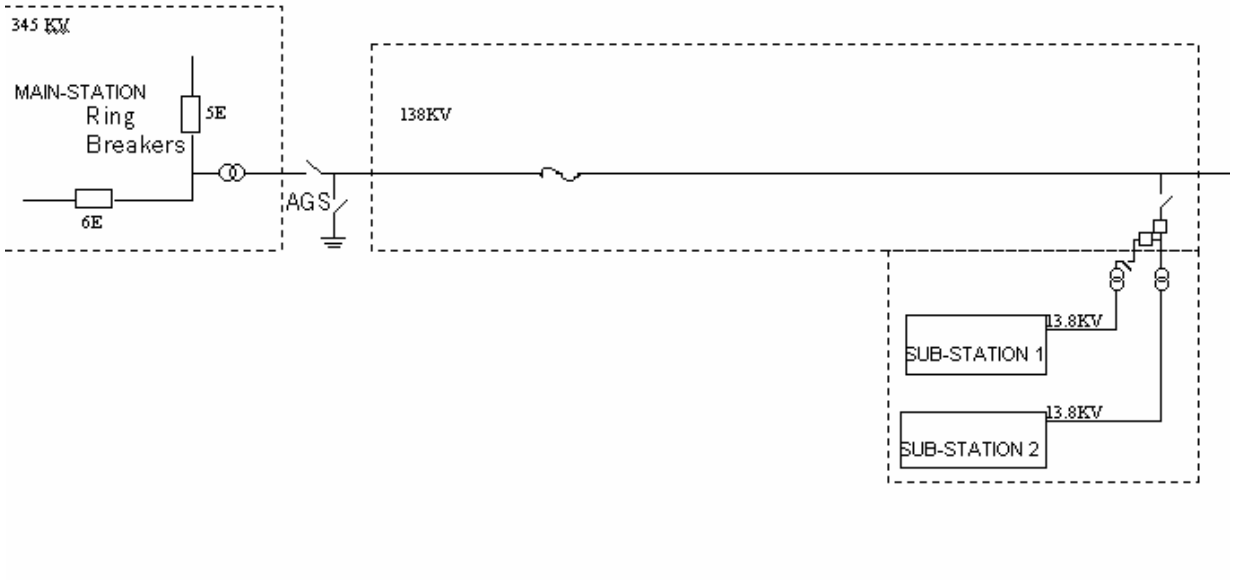

Figure 1 To Level Diagram of the Example Connections

3.2 Primary and Backup Fault Protection Scheme

Five 138 KV feeder lines feed the five banks of transformers in Substation 2 through the associated circuit switchers. The 138 KV circuit switcher will be the primary supply feeder protection, and the Audio Tone Transfer Trip (ATTT) is the second independent means of clearing the source for a fault at Substation 2. The ATTT system will consist of two ATTT chassis per 138 KV feeder. The operation of two chassis together forms a second line of diverse actuation in the main station (it also trips the transformer at Substation 2). The 138/13 KV transformers in a delta-Y arrangement are used for feeding to standard double synch area station. Each 138/13 KV transformer is protected for transformer differential, zero-sequence over voltage protection, reverse current, and the transformer neutral ground differential protection. Each 13 KV feeder is protected for over-current, and they are equipped with two independent (diverse) relay protections with their communication ports connected to the LAN.

For the purpose of this discussion, a fault is simulated in two zones, and the fault protection response of the network is discussed. The two zones considered are a fault in a substation or a fault on the connecting power lines between the main and the substations.

A fault in line between the main station and substations would be cleared depending on the location of the fault. A fault on this line close to the main station would actuate the opening of the associated main station ring breakers and temporary closure of the AGS switch. Closure of AGS will be sensed as a ground fault at the substation and will be subsequently cleared. The ATTT is not needed for clearing of this type of faults. Opening of other ring breakers of the main station that are upstream of the failed ones will compensate failure of either ring breakers. Failure of AGS will only affect protection of the substation, while ring breakers protect the main station.

A fault in the connecting lines between the main station and substations that is first sensed by the substations (closer to substation) will initially be cleared by the fast acting protection. An ATTT signal will also be sent to the main station to clear the fault by opening the appropriate ring breakers.

In the current design, the ATTT receiver is at the main station with the transmitter at the substation. In an alternate design, sometimes used by Con Edison, the AGS is replaced by an equivalent ATTT circuitry. In this case, both the main station and the substations are equipped with ATTT receivers and transmitters.

It should be noted that in this study we assume that there are two separate ATTT circuits and the actuation of both is necessary for the trip signal. Failure of an ATTT channel automatically causes the trip actuation logic to revert to single channel tripping.

A fault in one substation will be sensed through differential or other primary protective relays, causing the high-speed trip actuation, and actuation of the backup protective relays to trip with a time delay. In summary, there is two-actuation circuitry for opening main circuit switcher and two-actuation circuitry for transmitting an ATTT signal (both are time-delayed).

3.3 Audio Tone Transfer Trip (ATTT)

The actuation trip signals from electrical protection logics are transformed to analog audio tone signals for transmission from one substation to another. The audio tone signal then should be transmitted from one substation to another substation for the purpose of isolation of the faulted zone. The signal transmission could be done by analog means, such as modulated wireless connection (e.g., microwave), or digitally through the existing digital communication network infrastructure. The latter is currently considered to be more practical and cost effective due to varying distances and geographic conditions between the two substations.

Con Edison utilizes the Verizon communication infrastructure for transmission of ATTT. In a simplest connection, Verizon provides copper wires for each audio tone channel through which the signal would be carried to an A/D converter and a multiplexer nearby. The digital signal from the multiplexer then is transmitted to the closest Verizon Central Office (C/O) through a T1 line and connects to the Verizon network. In the receiving end at a remote location, the digital signal is received from the nearby C/O and transformed to the appropriate channel-based audio tone signals for the purpose of protection and tripping the isolation devices.

An alternative to ATTT is through the use of digitally based pilot wire scheme. In this design, a digital signal representing the DC Transfer Trip (DCTT) is used for remote transmission to others for the purpose of differential tripping or monitoring. To regenerate the DC on the pilot wire from the digital signal and to simulate the traditional copper wires (i.e., a 1200 ohm copper pair resistance regardless of length), an electronic board is typically utilized. This approach is utilized because Verizon can no longer provide copper wire telephony in many cases. Ultimately, the use of transmitters and receivers using ATTT or DCTT will be supplanted by direct transfer trip between Relay at Substation 1 communicating with Relay at Substation 2 directly over a digital communication channel or dark fiber.

The Verizon central offices are connected through an Enterprise network in a ring topology. Therefore, a failure of a central office would only impact one path of communication; that is, the ring topology assures robustness to a single failure as long as there would be no common link between the central offices (not susceptible to a common cause or hazard). However, the connection between the substation and the C/O may be a weak point in the system. This arises from the use of copper wire for connection between the substations to the multiplexer. Higher reliability could be achieved by devising redundancy, i.e., by utilizing two channels of audio tones, leasing two pairs of copper wires which access the substation in two different locations, feeding two different multiplexers, and finally entering two different central offices. Use of redundancy for each channel could also help with minimizing the spurious trip signal by utilizing some kind of "voting" logic.

Figure 2 shows a simplified diagram of an ATTT connection used for the example network being analyzed in this study. It should be noted that two channels of audio tone signals is shown in this figure for simplicity, even though the actual example circuit is composed of five channels for the five banks of transformers feeding the two synch buses. Furthermore, the detail of Verizon communication network is currently not available and it is not shown to reflect the lack of information in this regard.

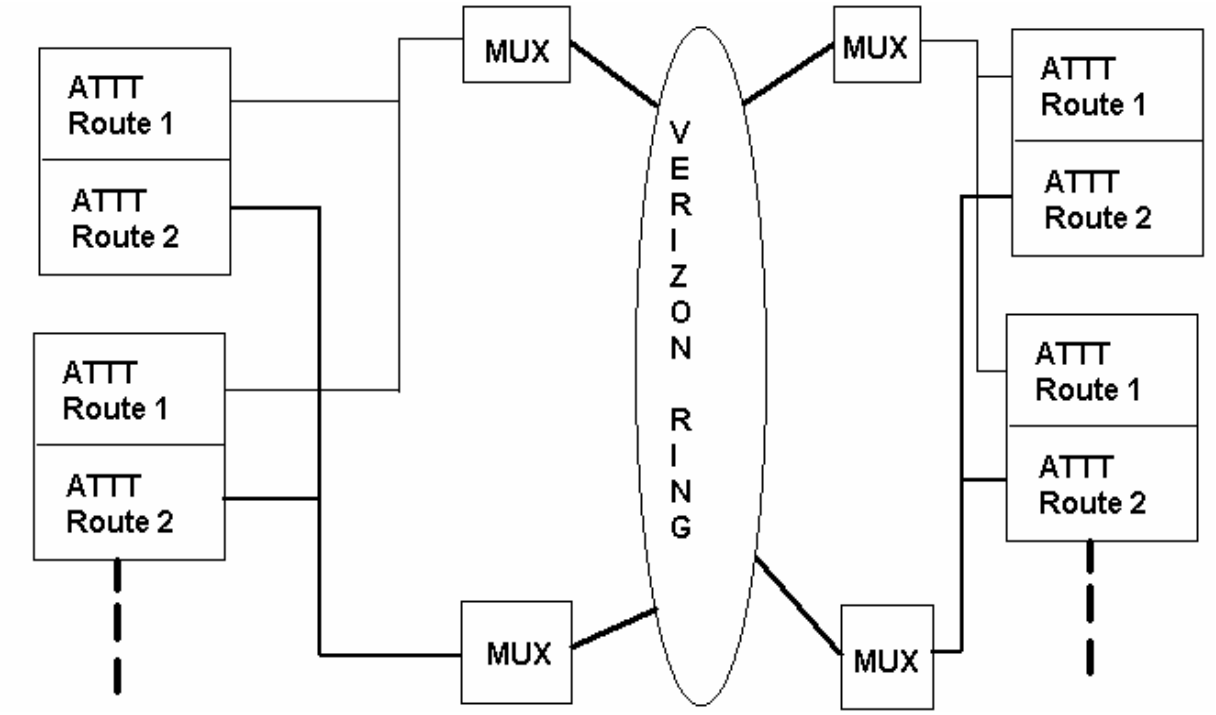

Figure 2 A simplified diagram of ATTT transmission through Verizon's Network

4. APPROACH AND METHODS FOR RELIABILITY PREDICTION

This section describes the proposed methodology to be used for electric network reliability prediction. A synopsis is presented here, with a more detailed discussion can be found in the various references provided. Generally, the methods employed for this study are those that have been developed in the past three decades in the nuclear industry, which have been tailored, for use in evaluating the reliability of the existing and the future electrical grid system. These methods have the capability of incorporating the deterministic models for congestion and transient response analyses to the probabilistic evaluation of the network failures systematically and in an efficient manner.

The electrical grid system has to respond to occasional upset events (also called "initiating events"). Such events could be due to an internal fault (e.g., a transformer short circuit) or an external occurrence, such as a fire, a flood, a storm, etc. In this approach, we look at "upset" or abnormal events and examine how the grid will respond to them. Upset events or "initiating events" are identified here based on experimental data, and/or based on analysis of system failures, which will necessitate actuation of protective features. The initiating events are classified based on their impact on the distribution network. This classification is done based on the response of the protective features to the initiator and the impact of the initiator on both the protective features and the network elements. A representative model, albeit conservative, would be developed for each class of the initiators. This model would include the responses of the network, protective devices, consequential isolation or failure of network elements, and potential manual reconfiguration by the operator actions. The model for each class of initiator is then transformed to a tree-type representation known as event trees. The event trees are the frameworks, which identify all of the pathways (combinations of protective features failures and successes) in response to each initiating event. The result of each such pathway can be a successful recovery of the system, or partial or complete failure. In our case, such result might be the electrical fault has been isolated without substantial loss of distribution capacity. In this approach, we track progression of an accident from its initiating event, through the response of the protective features of the system, to its appropriate end state. The various progression paths identified by the event tree are based on the success or the failures of the various functions. Comprehensive decomposition of these functional level progression paths to the constituent basic elements, component, and human actions, such as relays and breakers, are done through the development of the fault trees and utilization of the fault trees analysis codes. Integrated fault tree codes are also capable of estimating the probabilities associated with various combinations of events. In such manner, the probabilities associated with each progression path can be estimated.

The fault trees are constructed using mostly AND and OR gates, or constructing a Boolean expression of individual failures leading to a higher-level failure. The eventual inputs are component data in the form of probability of failure. All pertinent failure modes are included, e.g., failure to run, failure to start, failure to open, failure to close, spurious actuation, calibration errors, test and maintenance errors, etc. In our model, we mostly deal with failure to open (of the breakers), failure to close (as in the case of AGS7 above), failure to function between test and maintenance (in the case of relays, logic boards, batteries, etc.), and any calibration errors, which may cause actuation logic to operate improperly.

An important failure mode, which must be included, because it defeats redundancy, is common cause failures. These are failures, which may occur at more than one component at once, for example, due to improper maintenance, environmental factors, etc. There are several ways of including such failures in the fault trees.

Using the fault tree analysis codes, the end result is presented in terms of frequencies (in units of /yr) of occurrence of various end states. The probabilities of protective features' successes and failures in response to a particular event are calculated using this framework which logically relate probabilities of

component failures to probabilities of failure of protective features containing such components. Component failure probabilities should be derived from the appropriate reliability data sources [4-1,4-2,4-3]. Thus, the availability and maintenance of such reliability data sources is an integral activity within this approach.

The methodology then consists of the following parts: identification and classification of initiating events; analysis and understanding of the grid response, identification of protective features which will respond to the initiating event; construction of event trees depicting system responses to the initiating events; construction of fault trees depicting failures of protective features broken down into basic component failure data; gathering of component failure data and initiating event frequency data; consolidation of all the previous step in a computer model [4-4]; running and quantification of the model and deriving insights from the results.

References

4-1 "Survey of Ranges of Component Reliability Data for Use in Probabilistic Safety Assessment," IAEA-TECDOC-508, International Atomic Energy Agency, Vienna, 1989.

4-2 Fletcher, P.L., and Degen, W., on behalf of CIGRE Working Group 13.06, "A Summary of the Final Results and Conclusions of the Second International Enquiry on the Reliability of High Voltage Circuit Breakers," Proceedings of "The Reliability of Transmission Equipment" Conference, 29-31 March 1995, Conference Publication No. 406, ©IEEE, 1995.

4-3 Billinton, R., Ghajar, R., Filippelli, F., and Del Bianco, R., "Transmission Equipment Reliability Using the Canadian Electrical Association Information System," Proceedings of "The Reliability of Transmission Equipment" Conference, 29-31 March 1995, Conference Publication No. 406, ©IEEE, 1995.

4-4 Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 7.0, Idaho National Engineering & Environmental Laboratory, Idaho Falls, ID 83415.

5. DEMONSTRATION OF APPROACH

5.1 Electrical Network Reliability (An Overview)

In order to demonstrate the approach, a sample Con Edison configuration of a main "feeder" distribution and connected load distribution s is considered. Two abnormal events are analyzed: (1) a zone fault between the main and the load substation and (2) a transformer fault in the primary winding of the load substation. The demonstration then proceeded along the lines discussed in Section 4, i.e., identification of initiating events and their effects, construction of event trees and fault trees, gathering of data and quantification of the computer model. The computer model uses the code "SAPHIRE," a well-known code for probabilistic risk assessment, as the vehicle for constructing and evaluating the model.

In order to demonstrate the approach explained in Section 4, we have considered and modeled a main station and two substations, which are part of the Con Edison network in New York City. The main station is a major "feeder" substation – 345 kV lines come into the main station, the voltage is stepped down to 138 kV, and 138 kV lines come out of the main station and feed smaller substations, which supply the actual consumer loads. The main station topology is that of two ring buses, side by side. This imposes some conditions on substation protection–namely, opening of at least two ring breakers, one on each side of the outgoing line feeding the fault.

The main station feeds a number of "distribution" substations. This arrangement provides diversity of power sources to the sync buses, such that a problem in one of the transformers or feeder lines will not necessarily lead to a loss of power on the sync bus.

The two substations are fed from the main station. It is somewhat unique in both substations are similar, and in such a topology, that Substation 2 is connected to Substation 1 (via a circuit switcher for each 138 kV/ 13.8 kV transformer, as explained above), and Substation 1 gets its 138 kV power from Substation 2. Thus, a typical Substation 1 transformer can be disconnected from the 138 kV feeder line, either by opening its own switcher (connecting it to relevant bank of Substation 2), or by opening the relevant switcher at Substation 2, connecting that substation to the main station. For this case study, there would be 10 hours/year that three out of five transformers per substation are needed to carry the loads. Therefore, the loss or failure of one transformer if successfully isolated would be non-consequential.

In this demonstration, we are simulating two events: (1) a zone fault between the main and the load substation and (2) a transformer fault in the primary winding of the load. The object of our calculation is to obtain the frequency at which these two faults translate into a potential loss of the main station, and thus, a major, region-wide loss of power event. An event of lesser consequences outcome is also calculated, e.g., frequency of loss of one substation.

As can be inferred from the above discussion, such frequencies would depend on the topologies of the network in question, those of their interconnections, and of the reliability of various protective devices within and between the substations. One of the protective features is the ATTT signal, with its associated relays and logic boards, and the telecommunications network carrying the signal (Verizon network in this case).

In addition to the frequencies of the undesirable end states (loss of the main station, etc.), we can also parametrically explore major assumptions and uncertainties in our understanding of the system, in our model and in our data. One of the parameters that were subjected to sensitivity analysis is the unavailability of the Verizon network, carrying the ATTT signal. Sensitivity evaluation of this parameter could provide insights regarding future use of network technology in the electrical infrastructure. In the

case that this network is a substantial contributor to the risk of an undesired end state, we can calculate acceptable availability parameters for this network, in order that acceptable frequencies for loss of the main station are met. The model can also calculate uncertainty distribution if so desired, but this is not shown in the results, as we wanted to present a demonstration of the capabilities. Our approach can point out potential vulnerabilities, and component failures, which are particularly important, either as contributors to risk, or as "weak links."

Protection Strategies for Each Accident

Accident 1: Primary fault in No. 4 transformer at Substation 1. Various current transformers in the primary line will sense this fault, and transferred, via relays, to logic boards, which will, in turn, cause actuation of certain protective features.

Accident 2: A zone fault in one of the five 138 kV lines between the main station and Substation 2. The fault sensing and actuation of protective features will be done in a similar manner to the above, with fault sensing at the main station and Substation 2. At the main station, sensing is done on the current on the secondary side of the particular 345 kV/138 kV transformer feeding the particular line to Substation 2.

5.2 Simplified Event Tree

To illustrate the concept a simplified event tree is presented in Figure 3. This event tree is for purpose of discussion only and it is not used in the model. The event trees used in the actual model are by far more detailed than the one shown here.

Starting from the most left-hand side of the event tree, the first top event, usually known as the initiating event, is T4/SB1. T4/SB1 can be thought of as a transformer fault in Substation 1 (Transformer T4 for example). Such transformer fault could occur randomly with an average frequency estimated from the empirical data. This transformer fault normally is detected and isolated by opening of a Circuit Switcher CS4 (top event CS4/SB1) in one side and the sync breakers (top event TSYB) in the other side. The failure probability for each of these top events is estimated using a method known as fault tree analyses. Fault tree analyses typically are detailed enough to identify the combination of failures in instrumentation, relay logic, support systems (HVAC, and DC power), and the breakers that can lead to the failure of the top event. The probabilities associated with these failure combinations are evaluated using reliability models and the statistical failure data estimation.

The second break point in the event tree at the top of the graph questions the potential failure of the synch breakers. If any of the associated synch breakers fails, then the fault remains in the system and can be back fed by other transformers. Electrical transient analysis tools are usually used to estimate the fault current as seen by other transformers, and the time it would take before the fault protection on other transformers to actuate. This approach, i.e., performing electrical transient analyses, was not generally utilized in this report. The event trees were typically developed based on conservative engineering judgments. The top heading SYOB reflects the opening of all other synch breakers to clear the fault. The success of SYOB, of course, clears the fault, but it would also result in loss of power to the customers fed from the substation. In an unlikely event that SYOB is also failed, the main station feeder to the substation could be isolated through the ATTT signal (top heading MSATTT). If MSATTT fails, a prolonged (non-cleared) fault on the transformer will eventually result in opening of the ring breakers on the main station. It is not intuitive that such isolation would occur in a timely manner and that it is safe. Electrical transient analysis is required to evaluate the possible outcome of such a scenario. A common practice, which is also used here, is to initially assume that the outcome of such a scenario is not safe and

evaluate the likelihood of its occurrence. This likelihood or probability then is used for screening purpose to decide if further refinement or detail analyses are warranted.

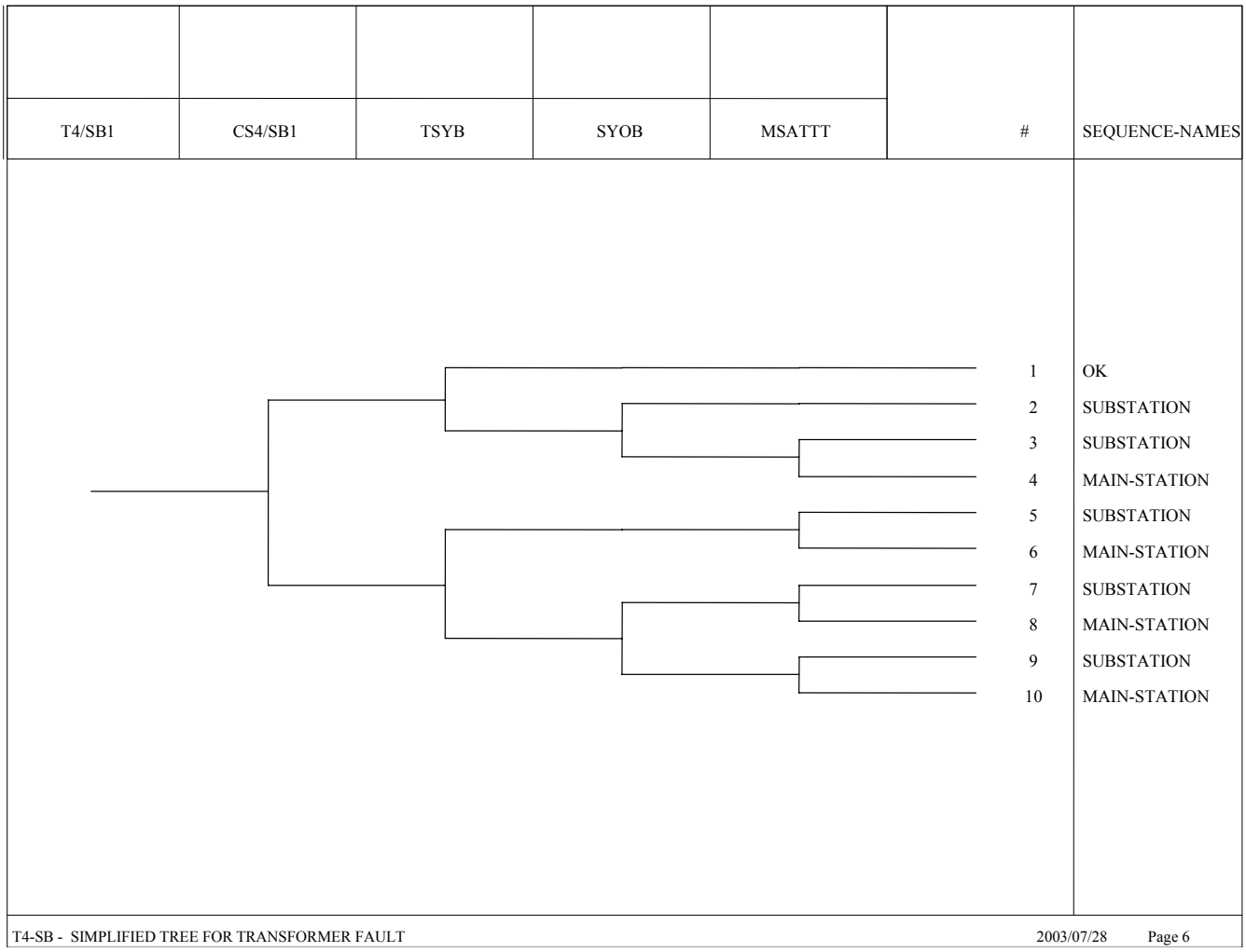

Figure 3 Simplified Tree for Transformer Fault

5.3 System Modeling and Quantification

Each one of the top headings in the event trees is modeled by fault trees whose logic describes how combinations of basic event (component) failures may lead to the top event failure. An example fault tree is shown for event TATBSYASYB (isolating the sync buses via sync breakers) in Figure 4. To isolate a fault, both the A and the B sides must be opened (indicated by an OR gate such that failure of isolating of either side will fail event TATBSYASYB). However, since each side has two breakers (TA and SYA on the A side), either of which can isolate the sync bus (i.e., AND gate represents that both TA and SYA must fail in order to fail TATBSYASYB). Common cause failures between the TA and SYA breakers are also shown. Also shown are the logic elements that need to operate in order to actuate opening of these breakers.

Modeled in the fault trees are two trains of 125 V DC power (backed up by batteries and chargers), which are used to support logic elements for actuation of protective features. There are also two trains of 48 V DC power which power ATTT transmitters (and receivers at the main station). It is assumed that there are two trains of HVAC in the cabinet area and two separate trains in the transformer vault.

Basic events in the fault trees use failure rates and unavailability data from various sources were collected and combined into a database. Initiating event frequencies for the transformer fault and the zone fault are taken from the data shown in the Canadian high voltage transmission line study [5-1].

Utilizing the above event trees, fault trees and failure/unavailability data, the computer code SAPHIRE[5-2] automatically calculates end-state frequencies, uncertainties, importance measures, and facilitates running of sensitivity analyses.

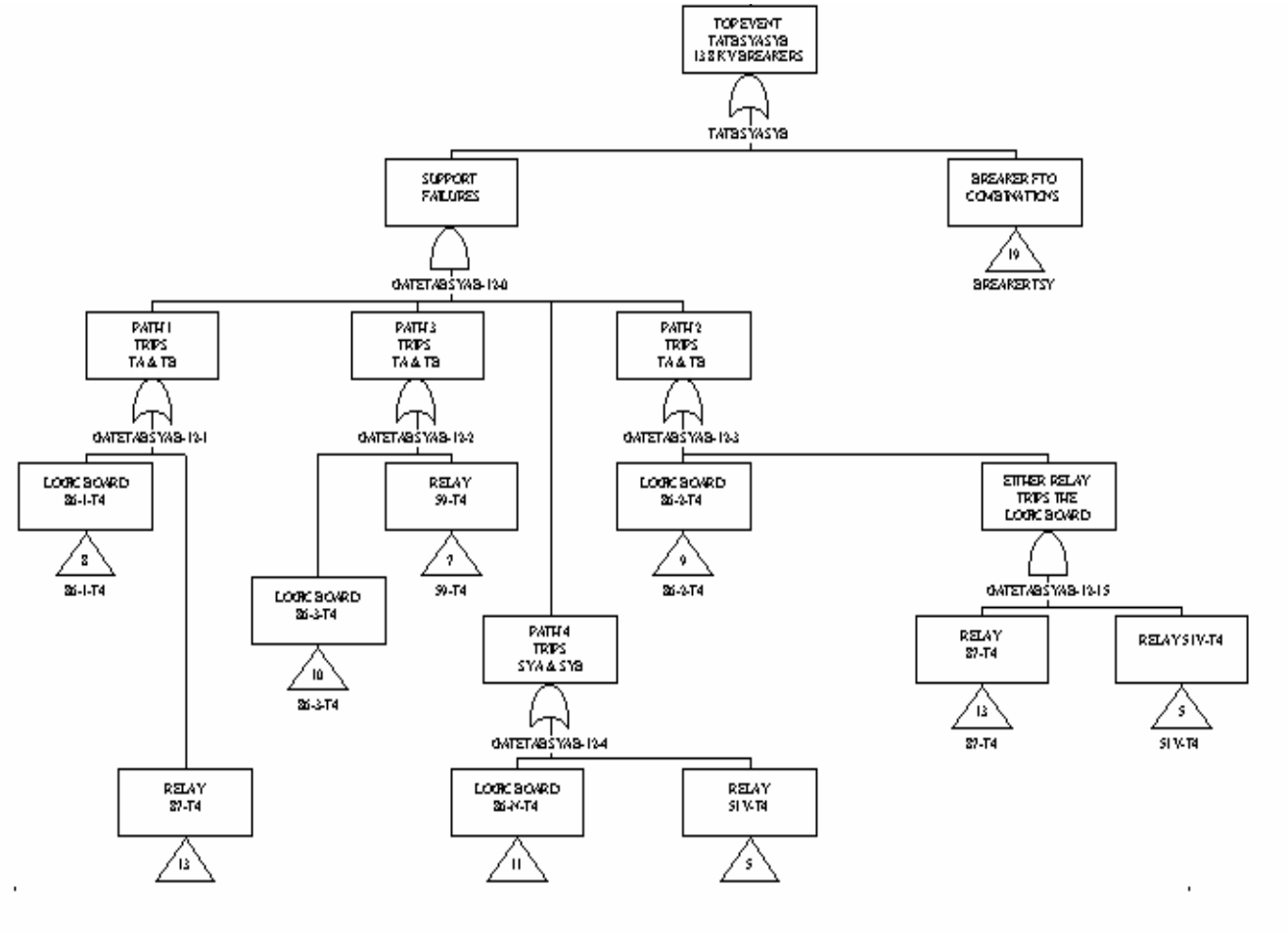

Figure 4 The Example Fault Tree for The Sync Bus Protective Breaker

5.4 Major Assumptions and Uncertainties

Assumptions had to be made consistent with the spirit of the pilot study. Some assumptions had to be made in order to avoid performing time-consuming and detail electrical transient analyses. As an example, assumptions were made not to credit the protection outside a fault zone since its actuation may not be timely for safe fault clearance. Other assumptions were made regarding certain system configuration and operation. For example, a battery charger with sufficient capacity could carry the DC loads if the battery is not available. However, some battery chargers may not be capable of carrying the DC loads and their sole purpose is to charge the battery. Without a detail system diagram and system description, a conservative assumption was not to credit the battery charger as a load carrying supply (even though it was found later that this is not the case for Con Edison system). In our modeling, there was lack of knowledge in many areas, and assumptions usually were made in a conservative manner. Some of these assumptions could be verified and modified when detailed information becomes available from Con Edison and Verizon.

One of the areas of uncertainty was failure and unavailability data for certain components. With the exception of some unavailability data on Verizon telephone lines collected by Con Edison, all other failure data were obtained from generic data. Considerations, such as specific type of equipment, maintenance practices, test intervals, will impact such data. For example, there is uncertainty about the types of relays used for various functions. There is uncertainty about applicability of certain generic data for certain types of components, about component boundaries and about component makeup of certain equipment, such as ATTT interface equipment.

Another area of uncertainty is degree of common cause coupling between similar equipment. This will depend on similarity between components, their respective locations, maintenance practices, etc. For example, will relays used for different functions have appreciable common cause coupling? In any case, specific data from experience is preferred to modify generic data used.

There are also uncertainties about equipment configurations. For example, the relationship between batteries and chargers (as discussed before) that power up the protective logic via the 125 V and the 48 V DC buses. We are unsure about the HVAC needs and configuration in the substation (we have assumed two train redundancy and a separate train in the transformer vault; however, due to assumed slow room heat up rates and presumed awareness of HVAC status, our base case assumes that HVAC will not contribute to equipment failures during a challenge event).

Another area of uncertainty is the design and the unavailability of the Verizon network carrying the ATTT signal. In this regard, we received some data from Con Edison regarding the line unavailability. The exact number of lines and the number of hours that this data were collected for were not known. A rough estimate of line unavailability is more than 0.01. Sensitivity analyses have been performed to better understand the impact of communication reliability on the electrical network reliability.

It was also assumed that the two ATTT channels are not redundant, but both need to work for ATTT signal transmission in order to minimize spurious actuation of protective features, which might lead to unnecessary interruption of service. Another situation-specific feature is the relatively short distance between the main station and the substation (only about one mile), which will impact the initiating event frequency for the zone fault.

However, overall, we believe that we have modeled accident progression in a relatively comprehensive manner, with sensitivity analyses covering the uncertainties and assumptions.

5.5 Communication Network Reliability

5.5.1 Communication Network Reliability - An Overview

Much effort has been expended in the past two decades to address reliable operation of communication networks given the growth trends and the explosion of demand in recent years. The problem of too little reliability information has not only disappeared but has been replaced by too much information in need of categorization and assessment. In this regard, an event reporting system has been established and accessible through www.fcc.gov/oet/outage. In addition, reliability data are provided through testing for various hardware and software from the manufacturers as a common practice. Self-healing structures have been utilized to allow the network to survive with minimum impact under certain degraded conditions until restoration takes place. Understanding of reliability data, root causes of operational events, and the important role of technicians/operators, the network software reliability, and dynamics of self healing and restoration are important in reliable operation of a communication network. Lessons learned in this regard has been documented by Network Reliability and Interoperability Council (NRIC) IV and V in 2002[5-4].

Sample review of the operational events in www.fcc.gov/oet/outage reveals that major losses/degradation of network are usually caused by fire, explosion, transportation accidents, losses of electrical power, improper software upgrades, and errors by technicians and operators. Hardware failures, such as failure of BIT module (Building Integrated Timing Source) and synchronization, have occurred with a lesser frequency. The events highlight the importance of redundancy, diversify, utilization of digital crossover frames, and separation/segregation. Even though the events reported indicate that in most cases one central office is lost for a day or two, there are some events that reveal significant degradation of network system. Examples are the break down in AT&T's frame relay network in April of 1998 and Verizon's service disruption resulting from the World Trade Center disaster on September 11, 2001.

The embedded network reliability excluding the types of accidents discussed above is expected to be from 0.99999 to 0.9995 (from 4.3 hrs to 5 minutes of downtime per year) as experienced by a customer. This indicates that the routine unavailability of a well-maintained network is a small contribution to overall reliability of a network when one includes the accidental outages as discussed above. Therefore, it is not surprising that the emphasis on good practices should focus on those mitigation capabilities and control mechanisms that minimize the impact and the duration of the accidental events on the network.

Identifying the critical network elements considering a wide variety of hazards and devising practices and design feature to minimize the impact of such hazards ensures network availability. A first step in such analysis, therefore, is to identify the failure paths, i.e., the elements that can fail to degrade the network. In reliability language, this is known as generating or enumerating the minimal cutsets. Generating the minimal cutsets is a fundamental step in many algorithms for evaluating the reliability of network and identification of its critical elements. Many methods have been proposed to generate the minimal cutsets of directed and undirected graphs [5-5, 5-6, 5-7]. All these methods rely on presenting the network topology in the form of matrices and utilizing the appropriate matrix operation to enumerate the minimal failure paths.

The second step in the network reliability is to devise appropriate algorithms to evaluate the occurrence likelihood of these minimal cutsets. Here, the analyst should account for hardware reliability, software reliability, and the impact of hazard, adjustment for dependent failures, self-healing capabilities, and restoration activities with associated durations. This step requires availability of reliability data, human performance parameters, hazard frequency, and software reliability. Some preliminary applications of these algorithms have been proposed [5-8]. More detailed reliability evaluation algorithms should be developed for the purpose of quantifying the minimal cutsets.

Finally, the generation and evaluation of minimal cutsets would not only allow a prediction of the network reliability for various degraded conditions but also would allow decomposition of the results to prioritize the major contributors and thereby identification of the critical network elements.

Formal reliability methodologies as discussed above was not applied to Verizon's network as a part of this study both due to lack of information on Verizon's network and also due to unavailability of appropriate integrated computer codes and reliability data to perform the analyses. Instead, the authors examined the good practices as delineated by the NRIC council and identified a minimal set to ensure some level of protection for various perceived hazards. This is contained in the next section.

5.5.2 Communication Network Reliability - Minimal Reliability Guidelines

Reliability Centered Operation, Maintenance, and Recovery:

Identification of Critical Network Elements (e.g., Domain Name Servers, Signaling Servers).

Application of Redundancy, Security and Diversity to Critical Network Elements.

Maintaining Spares, Repair and Emergency Restoration Procedure.

Criteria should be established by each Service Provider to ensure that all new hardware (e.g., routers, switches, call servers, signaling servers) meets a mutually agreed upon reliability threshold before it is brought into service on the network.

Periodic inspection and continuous surveillance, including alarms and monitoring.

All network element failures, regardless of impact, should be candidates for root cause analysis. Network Operators should conduct their own failure data collection and analysis procedures to perform root cause analysis. Network Operators and Equipment Suppliers should work together to jointly perform this analysis and implement corrective measures.

Initialization durations should be optimized to minimize service impact. Software and hardware upgrades should be non-service affecting. In particular, equipment suppliers should provide a mechanism for changes (e.g., provisioning, feature adding/activation) that allows for "soft" or "warm" activation rather than a full re-initialization.

To keep track of the numerous changes to both the product and the corresponding documentation, a change control and release planning process is recommended.

Protection Against Single Failure and Potential Common Cause Failures

Traffic monitoring and trending, forecasting, simulated failure analysis, and emergency procedures should be designed and implemented in networks. Routing controls should be implemented and managed to prevent routing conditions, such as infinite looping, and flooding of data across data networks.

No single point of failure should exist in paths linking network elements deemed critical to the operations of a network (with this design, two or more simultaneous failures or errors must occur at the same time to cause a service interruption).

Equipment areas should be controlled and alarmed within manufacturers' specifications (e.g., temperature, humidity).

The concept of self-healing should be implemented in the network design to the extent possible.

Critical network elements should store multiple software versions and be able to fallback to an earlier version.

Redundant support systems for critical network elements, such as electric power and HVAC (heat, ventilation, and air conditioning), should be provided. Diversity should be designed within this redundancy to the extent possible. Ensure diversity within power supply and distribution system so that single point failures are not catastrophic. For large battery plants in critical offices, provide dual AC feeds (odd/even power service cabinets for rectifiers). Transfer switches (UL standard 1008) should be used in lieu of paired breakers. The two transfer breakers (in power transfer systems) must be mechanically and electrically interlocked. Dual commercial AC power feeds with diverse routing from separate sources should be provided for the most critical network facilities and data centers.

Service Providers should establish a general requirement for some level of power conditioning, monitoring and protection for sensitive equipment.

Design standby generator systems for fully automatic operation and for ease of manual operation, when required. Maintain adequate fuel onsite and have a well-defined re-supply plan. Improve fuel systems reliability by providing redundant pumps for day tanks and a manual-priming pump. Wherever possible, use dual-source generators with direct line natural gas as the primary and liquid fuel (normally diesel) as a backup to provide a long-term fuel source in times of long power outages.

Power wire, cable, and signaling cables that meet NEBS (Network Equipment-Building System) should be provided in all telecommunications locations. Wherever possible, DC power cables, AC power cables and telecommunications cables should not be mixed. 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.

Link diversification validation should be performed at a minimum of twice a year; at least one of those validations shall include a physical validation of equipment compared to the recorded documentation of diversity. The validation of diversification is the responsibility of every network Service Provider that provides or utilizes any signaling paths. Limitations on diversification should be considered at the time of deployment, such limitations might consist of geography, facilities, circuit design or tariffs.

Protection Against Flooding Hazard

To avoid water damage from floods, it is recommended that power equipment and other critical network elements should not be located in basements or at susceptible elevations, if possible. Possibility of diverse geological locations at different elevation, use of flood barriers, flood alarms, confinement, water tight doors, and the utilization of drain pump should be considered to ensure a flooding condition could not impact several central offices.

Protection against internal flooding if critical network components are co-located near water pipes should be provided by rapid detection and isolation of the broken pipe in addition to the mitigation capabilities stated above.

Protection Against Fire Hazard

The concept of separation in different buildings should be implemented to the extent possible to ensure that the concept of redundancy and diversity is not defeated upon occurrence of a single fire. In cases that separation and segregation is needed within a building, the rated fire barriers or blankets should be utilized to the extent possible.

The occurrence frequency of a fire and its impact should be minimized by automatic detection and suppression systems and adherence to the various administrative control guidelines for transient fire sources and combustible materials.

Service Providers still using pre-1989 versions of Valve Regulated Lead Acid (VLRA) batteries should test them periodically using impedance instruments. The aging properties of these batteries can lead to thermal runaway that may cause a fire.

Some specific guidelines for network central offices:

Historic data indicates that rectifiers are a frequent cause of fires in equipment locations. Service Providers are encouraged to establish case history files by equipment category for rectifiers to facilitate decisions to replace such equipment with more efficient equipment based on failure trends.

Transportation accidents in the vicinity of the communication lines (near bridges or under over pass) have the capability of destroying a large number of lines. Coordination with fire department and police with pre-pan restoration activities should be considered.

Electric utility transformers should be placed external to the buildings.

Regularly inspect motors (air handling fans, air compressors, pumps, etc.).

Exercise & calibrate circuit breakers per manufacturers' recommendations.

Develop and/or adopt a defined procedure for removal of unused equipment and cable (e.g., cable mining) if this work can be economically justified without disrupting existing service.

Service Providers and Network Operators should perform periodic inspection of cable ways (e.g., through floor and through wall passageways, sealing compounds, fire and water stopping, etc.).

Avoid use of combustible landscape material.

Use over-current protection devices and fusing.

Inspect and maintain HVAC areas.

Ensure certified inspection of boilers and fuel storage units.

Provide and/or verify that all critical facilities have a modern smoke/heat detection system and appropriate ventilation systems including the motor room.

Wherever possible, DC power cables, AC power cables and telecommunications cables should not be mixed.

Protection Against Human Hazard

When excavation is to take place within the specified tolerance zone, the excavator exercises such reasonable care as may be necessary for the protection of any underground facility in or near the excavation area. Methods to consider based on certain climate and geographical conditions include: hand-digging when practical (potholing), soft digging, vacuum excavation methods, pneumatic hand tools, other mechanical methods with the approval of the facility owner/operator, or other technical methods that may be developed.

Service Providers and Network Operators should ensure physical building security in order to minimize intrusion attacks.

Protective devices for below ground facilities – use armored cable or type "C" conduit in rodent-infested areas.

Secure access points, such as manholes, cabinets, cable vaults, etc.

References

5-1 Billinton, R., Ghajar, R., Filippelli, F., and Del Bianco, R., "Transmission Equipment Reliability Using the Canadian Electrical Association Information System," Proceedings of "The Reliability of Transmission Equipment" Conference, 29-31 March 1995, Conference Publication No. 406, ©IEEE, 1995.

5-2 Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 7.0, Idaho National Engineering & Environmental Laboratory, Idaho Falls, ID 83415.

5-3 Malec, Henry A., " Communication Reliability: A historical perspective," IEEE Transactions on Reliability, Vol 47, SP 333-344, September 1998.

5-4 Beigel, J.E., " Determination of Tie Sets and Cutsets for a System Without Feedback," IEEE Trans. Reliability, Vol R-26, 1977, pp 39-42.

5-5 NRIC, Network Reliability and Interoperability Council V, Subcommittees 2.A, Focus Group 2, "Network Reliability Best Practices, Packet Switching and Circuit Switching, Final Report," January 2002.

5-6 Jasmon, G.B., and Kai, O.S., "A New Technique in Minimal Path and Cutset Evaluation," IEEE Trans. on Reliability, Vol R-34, 1985, pp 136-141.

5-7 Ahmad, Hasanuddin, "Simple Enumeration of Minimal Cutsets of Acyclic Directed Graph," IEEE Trans. on Reliability, Vol.37, December 1988, pp. 484-488.

5-8 Houeto, Fabien, Pierre, Samuel, et al., "Reliability and Cost Evaluation of Third-Generation Wireless Access Network Topologies: A Case Study," IEEE Trans. on Reliability, Vol.51, June 2002, pp. 229-239.

6. RESULTS AND CONCLUDING REMARKS

In this study, we utilized the methodologies from probabilistic risk assessment for the first time to microscopically evaluate the robustness of a power grid against system failures. The objective of the study was four-fold: (1) to introduce the reader to the proposed methodology for electrical grid reliability considerations; (2) to demonstrate that methodology in an actual relevant application; (3) using the methodology and the sample application, to provide an initial estimate of the order of magnitude contribution of the communications network to the electrical grid reliability, as well as contributions of other major components; and (4) provide information and insights from this research to Con Edison that could be useful in the design of the new network segment to be installed in the area of the World Trade Center in lower Manhattan.

We used a hypothetical electrical network designed based on a portion of the grid in New York City, owned and operated by Consolidated Edison Company of New York, as the example for demonstrating our approach. We have shown that our approach can yield appropriate results and satisfy the requirements for the four objectives mentioned above. Our effort included familiarization with the Con Edison design criteria and their electrical grid distribution system design and configuration, customizing the PRA methodology to be used for reliability evaluation of the electrical and communication network, and demonstrating that methodology on a prototypic sample situations from the real world.

In our demonstration, we considered two types of abnormal events for our example grid: (1) a zone fault between the main and the load substation and (2) a transformer fault in the primary winding of the load substation. The metrics with which we measured the electric grid reliability in this case or the "undesirable end state" was the loss, or potential loss, of the main station, which would result in a widespread loss of electric power to consumers. We also estimated the frequency of loss of the two substations; therefore, the loss of loads fed by the two sync buses. This end state, of course, has a lesser impact than the loss of the main station. Different end states were not combined in the current study, even though such aggregation to a single metric is possible by weighting the number and the importance of the customers who lose power in each scenario. Estimation of such an integrated metric would be important for developing a prioritized list of the potential cost-effective improvements.

The results for the two abnormal events (i.e., two cases) analyzed in this report showed that the frequency of the loss of the main station (due to connection to these two substations) was on the order of 1.E-3/yr. If we consider all other substations that are connected to this main station, and add up the frequencies of all the combinations of similar challenges, the overall frequency of the loss of the main station would rise by about a factor of 20, or approximately to 2.0E-2/yr. This frequency approximately indicates that loss of the main station and experiencing potential widespread power loss to all connected substations is expected, on average, once every 50 years. Similarly, the frequency of the loss of both s is an order of magnitude lower and it is about 1.E-3 (or once every 1000 years). Of course, this contribution does not include the fraction of losses of both substations as a result of the loss of the main station. The low likelihood for loss of both substations was expected since these substations were designed and upgraded recently with due considerations for double contingency and Con Edison's adherence to redundancy and diversity.

The study showed that the communication system under Verizon's responsibility could significantly contribute to loss of the main station, and, to a lesser degree, to the loss of the substations. Initial results shows that the Verizon network and the associated lines and the interface cards account for about 26 percent of loss of main station and 6 percent to loss of substations. These results were obtained when the overall reliability of the communication interface were assumed to be around 99 percent (or 1 percent unavailability). Sensitivity analysis of the overall unavailability of the communication system and its

impact on loss of main station is depicted in Figure 5. As shown in this graph, at 0.1, overall unavailability for the communication network, the probability of loss of the main station increases by a factor of 3.3 (approximately one loss per 15 years). About 80 percent of the total loss probability for main station is due to communication network. Therefore, it would be important to maintain the overall communication system reliability per station at above 99 percent to ensure reliable grid performance. It also should be noted that these analyses are currently conducted for use of communication system for Audio Tone Transfer Trip (ATTT). Future use of Verizon's network in a digital manner or advanced pilot wire applications would require more stringent operational and reliability requirements that have not yet been studied. Different overall unavailability values are expected when the reliability of the interface cards and the overall digital network are included. Furthermore, pilot wire and future digital applications for monitoring is expected to increase the importance of the overall communication reliability, thus suggesting the need for increased reliability of the communication network. Preliminary examination of the experiential data and the modeling techniques determined that accidents (not routine unavailabilities) with the capability of affecting more than one central office would become the major issue in maintaining the communication network reliability.

The study also indicates that the design of the two substations appear to be quite reliable. Therefore, adherence to the Con Edison design guideline ensures highly reliable substations. The reliability of the main station, however, could be improved by adding additional circuit switchers rather than relying on the ring breakers only. There is currently a fair degree of redundancy (no diversity) in responding to challenges, but this can be obviated by some common cause failures.

Finally, the study clearly showed and demonstrated that the PRA technology can be utilized for reliability assessment of the electrical grid system. It was shown that the PRA technologies used in this manner is microscopic in nature and relies heavily on the specific design of the portion of the grid being analyzed. It extensively models the types of faults that a grid could potentially experience, the response of the grid, and the specific design of the protection schemes. The importance of fault detection and protection schemes is heavily emphasized in this methodology. The methodology would systematically identify the cases where supporting electrical transient analyses are required. This would minimize the number of such analyses to the most critical ones. Finally, the methods utilized here are quantitative in nature, thereby allowing prioritization, reliability allocation to different modules, and verification of that the design meets the allocated reliability parameters.

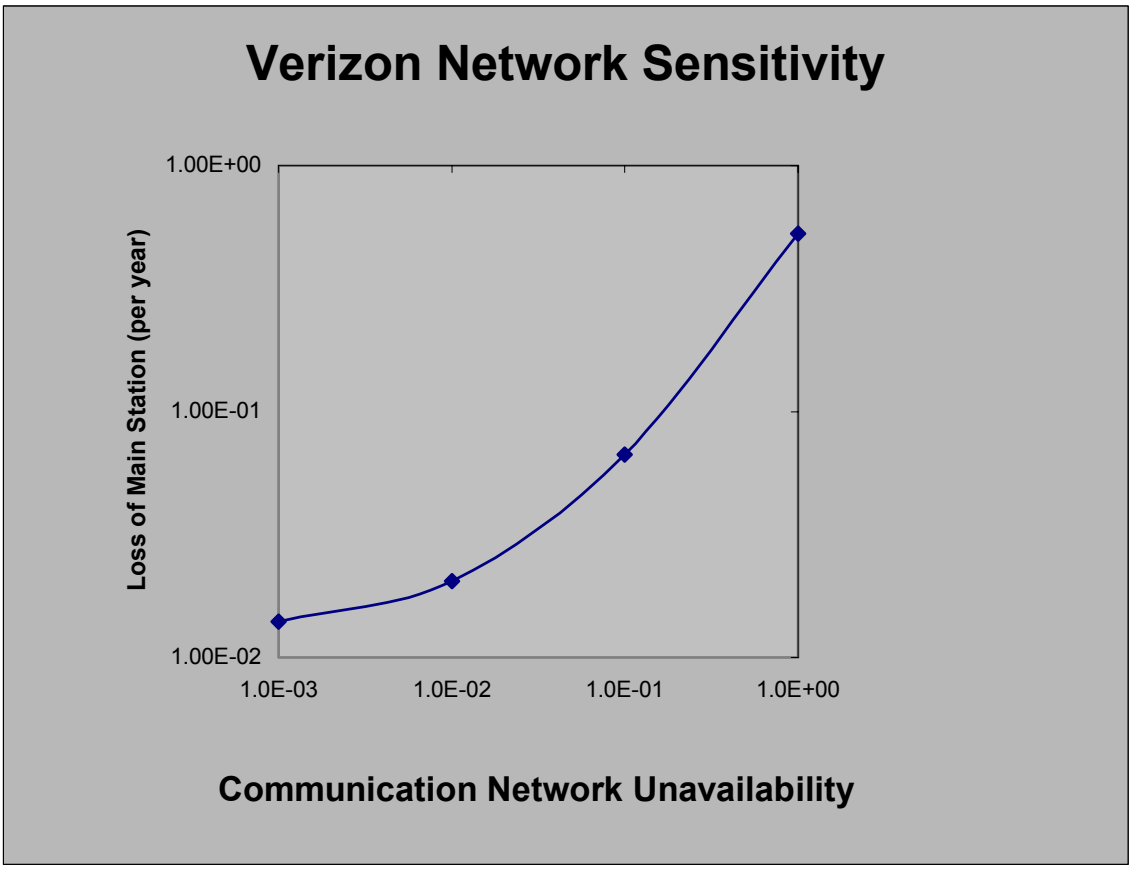

Figure 5 Sensitivity Analysis of Loss of as a Function of the Unavailability of Communication Network